Tivoli Netcool/OMNIbus
Version 8.1

Guide d'installation et de déploiement

SC43-0822-01

Tivoli Netcool/OMNIbus
Version 8.1

Guide d'installation et de déploiement

SC43-0822-01

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 713.

Deuxième édition - Novembre 2014

Réf. US : SC27-6264-01

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

La présente édition s'applique à la version 8, édition 1 d'IBM Tivoli Netcool/OMNIbus (numéro de produit 5724-S44) ainsi qu'à toutes les éditions et modifications suivantes, sauf indication contraire dans les nouvelles éditions.

Table des matières

Avis aux lecteurs canadiens ix

A propos de cette publication xi
Public visé xi
Publications xi
Accessibilité xiii
Formation technique Tivoli xiii
Informations de support xiii
Conventions utilisées dans cette publication . . . xiv

Chapitre 1. Introduction à Tivoli Netcool/OMNIbus 1
Le serveur ObjectServer 2
Sondes 3
Passerelles 3
Passerelles ObjectServer 3
Outils de bureau 4
Outils d'administration 5
Netcool MIB Manager 6
Interface graphique Web 6

Chapitre 2. Instructions de démarrage rapide 11

Chapitre 3. Instructions de mise à niveau rapide 15

Chapitre 4. Planification de l'installation ou de la mise à niveau . . 17
Dimensionnement de votre déploiement 17
Exemples de dimensionnement 20
Exigences d'espace disque 29
IBM Prerequisite Scanner 30
Obtention du module d'installation 31
IBM Installation Manager 32
Présentation d'IBM Installation Manager 32
Obtention de Installation Manager 34
Fichiers de réponses Installation Manager . . . 35
Installation de Installation Manager (interface graphique ou console) 36
Installation de Installation Manager (mode silencieux) 39
Installation d'Installation Manager pour l'interface graphique Web 41
Systèmes d'exploitation pris en charge 42
Exigences de l'environnement d'exécution Java (JRE) 49
Navigateurs de l'Interface graphique Web, environnements JRE et périphériques mobiles . . . 50
Exigences liées à l'interface utilisateur 51
Exigences relatives à l'aide en ligne 51
Prise en charge du protocole de réseau 52
Protocole de communication 53
Compatibilité avec des versions antérieures 54
Intégration à d'autres produits Tivoli 62
Découverte setuid des exécutables de Tivoli Netcool/OMNIbus 63

Chapitre 5. Installation et mise à jour de Tivoli Netcool/OMNIbus 65
Préparation à l'installation 65
Fonctions installables de Tivoli Netcool/OMNIbus 65
Structure du répertoire d'installation 67
Installation de Tivoli Netcool/OMNIbus 72
Installation de Tivoli Netcool/OMNIbus (interface graphique) 73
Installation de Tivoli Netcool/OMNIbus (console) 78
Installation de Tivoli Netcool/OMNIbus (mode silencieux) 82
Collecte des détails d'installation 85
Tâches de post-installation 86
Retrait de Tivoli Netcool/OMNIbus 109
Mise à jour de Tivoli Netcool/OMNIbus 111
Préparation à la mise à niveau 111
Mise à jour de Tivoli Netcool/OMNIbus (interface graphique) 112
Mise à jour de Tivoli Netcool/OMNIbus (console) 114
Mise à jour de Tivoli Netcool/OMNIbus (mode silencieux) 115
Collecte des détails d'installation 116
Rétrogradation de mises à jour 118
Mise à niveau à partir de V7.4 (et versions précédentes) 120
Migration de données 120
Fichiers migrés pendant une mise à niveau . . 122
Mise à jour du schéma de ObjectServer 125
Mise à niveau d'un ObjectServer connecté à une passerelle de base de données 128
Préparation des chiffrements de valeur de propriété pour la mise à niveau (en mode FIPS 140-2) 129
Instructions de mise à niveau vers le codage UTF-8 (Windows) 130
Mise à niveau d'une architecture à plusieurs niveaux 132
Installation de sondes et de passerelles dans un environnement Tivoli Netcool/OMNIbus mis à niveau 135
Remarques supplémentaires sur la mise à niveau et la migration 136

Chapitre 6. Installation et mise à niveau du composantInterface graphique Web 145
Préparation de l'installation ou de la mise à niveau de l'Interface graphique Web 147
Regroupement d'informations sur l'installation 147

Installation et mise à niveau de l'Interface graphique Web dans un environnement d'équilibrage de charge 149
Structure du répertoire d'installation Interface graphique Web 150
Installation de l'interface graphique Web 151
Installation de l'Interface graphique Web (interface graphique) 151
Installation de l'Interface graphique Web en mode console 154
Installation de l'Interface graphique Web en mode silencieux 156
Mise à niveau de l'Interface graphique Web et migration de données 158
Mise à niveau de la version 7.4.0 ou 7.3.1 sur Tivoli Integrated Portal version 2.2 ou 2.1 . . . 160
Mise à niveau à partir d'IBM Tivoli Netcool/Webtop version 2.2 ou de l'Interface graphique Web version 7.3.0 167
Migration à partir de IBM Tivoli Netcool/Webtop version 2.0 ou 2.1 167
Migration à partir de IBM Tivoli Netcool/Webtop version 1.3.1 172
Sauvegarde d'une installation V8.1 176
Restauration d'une installation V8.1 177
Exécution des tâches post-installation 178
Exécution des tâches postinstallation pour l'Interface graphique Web 178
Connexion 182
Protection du fichier de clés du coffre 183
Affectation de rôles d'Interface graphique Web à l'utilisateur administrateur 184
Changement des mots de passe des utilisateurs fournis 185
Configuration du client WAAPI 186
Activation du support multiculturel de l'Interface graphique Web 187
Identification et résolution des problèmes d'installation 189
La migration échoue avec des erreurs "Out of Memory" 189
Retrait de l'Interface graphique Web 190

Chapitre 7. Configuration du système Tivoli Netcool/OMNIbus 193
Assistant de configuration initiale 193
Création et exécution de serveurs ObjectServer . . 193
Présentation du serveur ObjectServer 194
Configuration de la reprise en ligne et de la reprise par restauration automatisées 196
Création d'un serveur ObjectServer 197
Démarrage d'un serveur ObjectServer 202
Arrêt d'un serveur ObjectServer 205
Configuration des détails de communication du serveur dans l'éditeur de serveur 207
Création et conservation des entrées serveur après l'installation 207
Configuration des informations de communication du serveur 209
Ajout d'un serveur ObjectServer de secours . . 213
Modification de la priorité des serveurs . . . 216
Masquage des serveurs ObjectServer de secours dans l'éditeur de serveurs (UNIX uniquement) . 216
Test d'un serveur 217
Edition manuelle du fichier de données de connexions 217
Configuration d'installations réparties 218
Etape 1 : Installation des composants Tivoli Netcool/OMNIbus 218
Etape 2 : Configuration des communications entre composants 219
Etape 3 : distribution des fichiers d'interfaces (UNIX uniquement) 221

Chapitre 8. Configuration et déploiement d'une architecture à plusieurs niveaux 223
Avant de commencer 223
Présentation d'une architecture standard à plusieurs niveaux 223
Conventions de dénomination pour l'architecture à plusieurs niveaux 226
Ressources des composants : identification du nombre de serveurs ObjectServer nécessaires . . 228
Gestion de la gravité 229
Emplacements des fichiers de configuration à plusieurs niveaux 232
Configuration de l'environnement à plusieurs niveaux standard 233
Configuration des informations de communication du serveur (architecture à plusieurs niveaux) 234
Installation du serveur d'agrégation ObjectServer principal 235
Installation du serveur d'agrégation ObjectServer de secours 236
Configuration de la passerelle d'agrégation ObjectServer bidirectionnelle 237
Installation du serveur de collecte ObjectServer principal 238
Configuration de la passerelle de collecte ObjectServer principale unidirectionnelle . . . 239
Installation du serveur de collecte ObjectServer de secours 239
Configuration de la passerelle de collecte ObjectServer de secours unidirectionnelle . . . 240
Installation du serveur d'affichage ObjectServer 1 241
Configuration de la passerelle d'affichage ObjectServer 1 unidirectionnelle 243
Installation du serveur d'affichage ObjectServer 2 243
Configuration de la passerelle d'affichage ObjectServer 2 unidirectionnelle 245
Installation de serveurs ObjectServer supplémentaires 245
Ajout d'une seconde paire de serveurs ObjectServer de collecte 246
Ajout d'un serveur ObjectServer d'affichage supplémentaire 251

Equilibrage automatique des charges des clients de liste d'événements 255
Création de déclencheurs personnalisés. 257
Déclencheurs de performances 258
Evénements synthétiques Resynchronisation terminée 260
Etapes finales 261
Modèles de fichier omni.dat 261
Déclencheurs utilisateur dans les environnements à plusieurs niveaux 263
Mise à niveau d'une architecture à plusieurs niveaux 264

Chapitre 9. Configuration de la haute disponibilité 267
Configuration de reprise en ligne. 267
Configuration de la reprise par restauration contrôlée des clients 269
Configuration des sondes pour la haute disponibilité. 271
Configuration des sondes pour une exécution en mode stocker-et-transmettre circulaire 272
Configuration du mode de reprise en ligne d'égal à égal. 273
Réduction de la perte d'événements suite à un échec du serveur ObjectServer lors de la resynchronisation 274
Réduction du délai de resynchronisation 275
Configuration de l'arrêt contrôlé d'un serveur ObjectServer. 275
Configuration des serveurs proxy pour la reprise en ligne 279

Chapitre 10. Configuration de la prise en charge de FIPS 140–2 pour les composants serveur 283
Création du fichier de configuration FIPS 283
Configuration des composants serveur pour le mode FIPS 140–2 284
Configuration des composants serveur pour le chiffrement étendu SP800-131 286
Configuration requise pour la connexion de clients version 7.2 ou inférieure aux serveurs version 7.2.1 ou supérieure en mode FIPS 140–2 288
Basculement de votre installation vers le mode FIPS 140-2 289

Chapitre 11. Importation et exportation de configurations du serveur ObjectServer. 293
Exportation et importation de configurations ObjectServer à l'aide de l'utilitaire nco_osreport . . 294
A propos de l'utilitaire nco_osreport. 294
Exportation de configurations ObjectServer et clonage de serveurs ObjectServer. 296
Options de ligne de commande pour la commande nco_osreport. 297
Exportation et importation de données de configuration à l'aide de l'utilitaire nco_confpack . 299
Terminologie de l'importation et de l'exportation 299
Objets importables et exportables. 299
Propriétés et options de ligne de commande pour nco_confpack 301
Création et édition des fichiers de liste de configuration 303
Exportation des configurations 309
Affichage du contenu du package de configuration 316
Importation des configurations 317

Chapitre 12. Configuration des serveurs ObjectServer de bureau. . . 325
Architecture du serveur ObjectServer de bureau 325
Remarques relatives à l'installation d'une architecture du serveur ObjectServer de bureau . . 327
Configuration d'une architecture ObjectServer de bureau 327
Création et configuration d'un serveur ObjectServer de bureau 328
Configuration de la passerelle ObjectServer unidirectionnelle 329
Affichage des résultats des actions d'outils à l'aide du mode écriture double 331
Affichage des entrées du journal opérateur à partir d'un bureau à deux serveurs (DSD) . . . 332
Authentification du serveur ObjectServer de bureau 332
Mode équilibrage de charges 333
Configuration du mode équilibrage de charges 333

Chapitre 13. Sécurité des accès utilisateur dans Tivoli Netcool/OMNIbus. 337
Mécanismes de sécurité des accès utilisateur . . . 337
Authentification 338
Autorisation. 338
Authentification en mode sécurisé 339
Mode sécurisé du serveur ObjectServer. . . . 340
Mode sécurisé du serveur proxy 340
Connexion sécurisée à partir de sondes et de passerelles 340
Sécurité du contrôle de processus 340
Protection par mot de passe de l'interface interactive SQL dans des scripts 341
Configuration du serveur ObjectServer pour l'authentification d'utilisateurs. 342
Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe . . 343
Propriétés LDAP 348
Exemples LDAP 352
Authentification PAM (sous UNIX et Linux) . . . 354
Configuration de Tivoli Netcool/OMNIbus pour utiliser PAM pour l'authentification externe . . 354
Configuration d'un serveur ObjectServer comme source d'authentification PAM. 356
Implémentation d'une autorisation à l'aide de groupes et de rôles 359
Droits système et objet 360
Rôles de Tivoli Netcool/OMNIbus par défaut 361

Groupes de Tivoli Netcool/OMNIbus par défaut 364
Utilisateurs de Tivoli Netcool/OMNIbus par défaut 365
Utilisation de filtres de restriction pour filtrer les informations de table 365
Définition et suivi d'une trace de contrôle 366
Chiffrement des valeurs de propriété 366
Génération d'une clé dans un fichier de clés . . 367
Spécification du fichier de clés comme propriété 368
Chiffrement d'une valeur de chaîne avec la clé 368
Ajout d'une valeur chiffrée à un fichier de propriétés 369
Options de ligne de commande nco_aes_crypt 370

Chapitre 14. Utilisation du protocole SSL pour les communications serveur et client 371
Instructions de configuration de SSL rapide . . . 372
Configuration des communications SSL 375
Utilisation de l'éditeur de serveur pour configurer SSL sous UNIX 375
Utilisation de l'éditeur de serveur pour configurer SSL sous Windows 376
UNIX : génération du fichier d'interfaces pour SSL. 376
Configuration de la SSL pour les installations distribuées 378
A propos des fichiers de la base de données de clés 379
Configuration d'un réseau protégé SSL 380
Création d'une base de données de clés . . . 381
Création d'un certificat autosigné. 385
Demande de certificat serveur auprès d'une autorité de certification 388
Signature d'un fichier de demande de certificat avec un certificat de signataire. 393
Réception de certificats de serveur d'autorités de certification 395
Distribution des certificats 397
Gestion des certificats numériques 401
Démarrage d'iKeyman 401
Spécification du certificat par défaut. 402
Affichage des détails du certificat. 403
Suppression de certificats 404
Modification du mot de passe de la base de données de clés 405
Options de ligne de commande nc_gskcmd . . . 406
Exemple de fichiers de clés. 410

Chapitre 15. Configuration IPv6 . . . 413
Configuration de la prise en charge d'IPv6 . . . 413

Chapitre 16. Support multiculturel . . 417
Configuration de votre environnement local . . . 418
Identification des environnements locaux pris en charge sur votre ordinateur. 422
Activation ou désactivation du tri localisé 423
Identification des environnements locaux pris en charge pour le bureau UNIX 423
Configuration de polices pour le bureau UNIX . . 423
Configuration du serveur ObjectServer pour utiliser le texte d'interface utilisateur traduit dans le bureau 426

Chapitre 17. Extension des fonctionnalités de Tivoli Netcool/OMNIbus. 429
Présentation du répertoire $NCHOME/omnibus/extensions 429
Activation des événements prévisibles et de l'analyse prévisionnelle 433
Installation et configuration des événements prévisibles 435
Installation et configuration de la tendance linéaire 439
Conditions préalables pour les événements prévisibles et les analyses prévisionnelles . . . 440
Ressources de configuration de Tivoli Netcool/OMNIbus pour les événements prévisibles 444
Configuration des événements prévisibles dans votre environnement intégré 448
Configuration des tendances linéaires 450
Configuration de la base de référence 454
Activation de la prise en charge des événements TADDM 456
Installation et configuration des événements TADDM 457
Fichiers de configuration Tivoli Netcool/OMNIbus pour les événements TADDM 458
Configuration du support pour les événements TADDM dans votre environnement intégré . . 459
Gestion d'environnements virtuels 465
Configuration de la gestion d'événements dans un environnement virtuelà l'aide d'une sonde pour SNMP et IBM Tivoli Netcool/OMNIbus Knowledge Library 465
Configuration de la gestion d'événements dans un environnement virtuel à l'aide de IBM Tivoli Monitoring 469
Application des déclencheurs de virtualisation à un environnement mis à niveau 476
Ressources de configuration Tivoli Netcool/OMNIbus pour la gestion de la virtualisation 477
Rechargement de plusieurs fichiers de règles de sonde 480
Importation des rapports récapitulatifs des événements dans Tivoli Common Reporting . . . 484
Activation des métriques de débit d'événements X en Y 487
Composants de la solution X en Y 488
Exemples de scénarios 493
Configuration des actions d'escalade personnalisées 495
Installation de la solution X dans Y 496
Désinstallation de la solution X en Y 499

Chapitre 18. Configuration de l'Interface graphique Web 501

Configuration de l'authentification des utilisateurs 501
Configuration de l'authentification d'utilisateurs sur un annuaire LDAP 503
Configuration de l'authentification d'utilisateurs sur un serveur ObjectServer 512
Identification et résolution des problèmes concernant les registres d'utilisateur 516
Suppression de référentiels d'utilisateurs . . . 517
Modification du registre d'utilisateurs dans lequel les droits d'utilisateur sont écrits. . . . 518
Sécurisation de l'environnement de l'Interface graphique Web 519
Configuration de l'accès HTTP et HTTPS . . . 520
Configuration d'une connexion SSL sur un serveur LDAP 522
Configuration d'une connexion SSL au serveur ObjectServer. 523
Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer . 525
Remplacement du certificat SSL par défaut pour les connexions aux clients d'interface graphique Web 527
Chiffrement des mots de passe de l'Interface graphique Web 532
Activation du mode FIPS 140-2 pour l'Interface graphique Web 534
Activation du chiffrement NIST SP800-131a . . 540
Configuration de l'interface graphique Web pour une utilisation en production 546
Configuration des sources de données 546
Configuration de variables d'environnement pour les graphiques 573
Configuration et gestion de l'authentification unique 573
Surveillance automatique 578
Extension de la fonctionnalité de l'Interface graphique Web 587
Configuration d'un environnement d'équilibrage de charge. 603
Définition de l'accès utilisateur au widget Cadre incorporé. 609
Activation des connexions multiples. 610
Installation et configuration de Tivoli Common Reporting 610
Fournisseur de données de l'Interface graphique Web 610
Visualisation de données d'événement dans le Concentrateur des services d'application du tableau de bord 613
Redémarrage du serveur 618

Chapitre 19. Exemples de scénarios d'installation de Tivoli Netcool/OMNIbus (architectures de base, de reprise en ligne et de bureau) 621

Exemple d'architecture de base de Tivoli Netcool/OMNIbus 621
Déploiement de l'architecture de base 621
Prérequis de l'architecture de base 622
Etape 1 : Installation du serveur ObjectServer et de l'agent de processus 622
Etape 2 : Installation de sondes 623
Etape 3 : Installation de la liste d'événements 623
Etape 4 : Configuration des communications 623
Etape 5 : Création du serveur ObjectServer . . 624
Etape 6 : Test du système 624
Etape 7 : Installation et configuration de la sonde Syslog et du démon Syslog 624
Etape 8 : Configuration du contrôle de processus. 626
Etape 9 : Ajout de colonnes au serveur ObjectServer. 628
Etapes suivantes 629
Exemple d'architecture de reprise en ligne de base Tivoli Netcool/OMNIbus 629
Déploiement de l'architecture de reprise en ligne de base 629
Prérequis de l'architecture de reprise en ligne de base 630
Etape 1 : Installation de l'architecture de base 631
Etape 2 : Installation du serveur ObjectServer de sauvegarde et de la passerelle du serveur ObjectServer. 631
Etape 3 : Configuration des communications 631
Etape 4 : Création et configuration du serveur ObjectServer de sauvegarde 632
Etape 5 : Configuration de la passerelle bidirectionnelle du serveur ObjectServer . . . 633
Etape 6 : Configuration de la sonde Syslog . . 633
Etape 7 : Configuration du contrôle de processus sur l'ordinateur de sauvegarde . . . 634
Etapes suivantes 635
Exemple d'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus 635
Déploiement de l'architecture du serveur ObjectServer de bureau 636
Prérequis pour l'architecture du serveur ObjectServer de bureau 637
Etape 1 : Installation des architectures de reprise en ligne de base 637
Etape 2 : Installation du serveur ObjectServer de bureau et de la passerelle unidirectionnelle . . 637
Etape 3 : Configuration des communications entre composants 638
Etape 4 : Création et configuration du serveur ObjectServer de bureau 639
Etape 5 : Configuration de la passerelle unidirectionnelle du serveur ObjectServer . . . 639
Etape 6 : Configuration du contrôle de processus sur l'ordinateur hébergeant le serveur ObjectServer de bureau 640
Etapes suivantes 641

Chapitre 20. Exemple de scénario d'installation pour les composants non Web et l'Interface graphique Web de Tivoli Netcool/OMNIbus (sous Windows) 643
Configuration d'un environnement de test 643
Installation de Tivoli Netcool/OMNIbus et configuration du serveur ObjectServer 645
Configuration et installation de la sonde . . . 648
Installation et configuration de l'Interface graphique Web 648
Etapes suivantes 651

Chapitre 21. Liste de contrôle de configuration pour le mode FIPS 140–2 653

Annexe A. Identification et résolution des problèmes 657
Identification et résolution des problèmes liés à la sécurité 657
Exigences d'accès root pour les processus Tivoli Netcool/OMNIbus 657
Echec de nco_pad lors de l'authentification du module PAM sous SUSE Linux 657
Echec d'authentification d'utilisateur avec les modules PAM 658
Test de la configuration LDAP. 659
Erreurs d'authentification LDAP communes . . 660
Calcul des temps de recherche LDAP 665
Connexion à l'Interface graphique Web après un échec du serveur LDAP 666
Identification et résolution des problèmes liés au support multiculturel. 666
Traitement des problèmes de connexion aux listes d'événements (Windows) 667
Traitement des problèmes liés aux erreurs de programme d'écoute ObjectServer (UNIX et Linux) . 668
Traitement des problèmes d'affichage (UNIX et Linux) 669
Collecte des détails d'installation 669
Identification et résolution des problèmes d'intégration. 671
Le changement de statut génère des valeurs d'événement Tivoli Monitoring incorrectes dans Netcool/OMNIbus 671
Informations de support. 673
IBM Support Assistant 673
Obtention de correctifs 682
Réception de mises à jour de support 683
Astuces de recherche 683

Annexe B. Numéros de port par défaut utilisés par Tivoli Netcool/OMNIbus. 685

Annexe C. Propriétés server.init . . . 687

Annexe D. Rapports Tivoli Common Reporting pour Tivoli Netcool/OMNIbus. 701
Distribution d'événement 701
Event_Selection. 703
Event_Severity 705
Event_Details 707
Acknowledgement_Summary 707
Acknowledgement_Details 710

Remarques 713
Marques 716

Index 717

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de cette publication

Tivoli Netcool/OMNIbus est un système de gestion du niveau de service (SLM) qui offre une surveillance centralisée et en temps réel des réseaux complexes et des domaines informatiques.

Le *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus* décrit comment installer, mettre à niveau, configurer et utiliser Tivoli Netcool/OMNIbus.

Public visé

La présente publication s'adresse aux administrateurs qui doivent installer et déployer Tivoli Netcool/OMNIbus.

Publications

Cette section dresse la liste des publications de la bibliothèque Tivoli Netcool/OMNIbus ainsi que des documents associés. Elle indique également comment accéder aux publications Tivoli en ligne et comment organiser les publications Tivoli.

Votre bibliothèque Tivoli Netcool/OMNIbus

Les documents suivants sont disponibles dans la bibliothèque Tivoli Netcool/OMNIbus :

- *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*,

  Comprend des procédures d'installation et de mise à niveau de Tivoli Netcool/OMNIbus et décrit la manière de configurer la sécurité et les communications des composants. La publication contient également des exemples d'architectures Tivoli Netcool/OMNIbus et explique comme les mettre en oeuvre.
- *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*,

  Explique comment effectuer les tâches d'administration à l'aide de l'interface graphique d'administration de Tivoli Netcool/OMNIbus, des outils de ligne de commande et des commandes de processus. La publication contient également des descriptions et des exemples de syntaxe SQL du serveur ObjectServer et des automatisations.
- *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* ,

  Décrit comment exécuter les tâches d'administration et de visualisation d'événements à l'aide de l'interface graphique Web de Tivoli Netcool/OMNIbus.
- *IBM Tivoli Netcool/OMNIbus User's Guide*,

  Présente les outils du bureau et décrit les tâches de l'utilisateur liées à la gestion d'événements à l'aide de ces outils.
- *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*,

  Contient des informations de présentation et de référence sur les sondes et les passerelles, notamment la syntaxe des fichiers de règles de sonde et des commandes de passerelle.
- *IBM Tivoli Monitoring for Tivoli Netcool/OMNIbus Agent User's Guide*,

Explique comment installer l'agent de moniteur d'état de Tivoli Netcool/OMNIbus et contient des informations de référence sur l'agent.

- *Guide de référence d'IBM Tivoli Netcool/OMNIbus Event Integration Facility* ,

  Décrit comment développer des adaptateurs d'événements adaptés à votre environnement réseau et aux besoins spécifiques de votre entreprise. Cette publication décrit également comment filtrer des événements à la source.
- *Guide des messages d'erreur d'IBM Tivoli Netcool/OMNIbus*,

  Décrit les messages système dans Tivoli Netcool/OMNIbus et les réponses à apporter à ces messages.
- *Guide d'utilisation de l'API d'administration de l'interface graphique Web (WAAPI) d'IBM Tivoli Netcool/OMNIbus*,

  Montre comment administrer l'interface graphique Web Tivoli Netcool/OMNIbus à l'aide de l'interface de programmation d'application XML nommée WAAPI
- *Guide de référence de l'interface HTTP ObjectServer d'IBM Tivoli Netcool/OMNIbus*, Décrit les URI et les comportements communs de l'interface de programme d'application (API) appelée interface HTTP ObjectServer. Décrit comment activer cette API et fournit des exemples de charges de message JSON et de demandes et réponses HTTP.
- *Guide de référence de l'interface OSLC ObjectServer d'IBM Tivoli Netcool/OMNIbus*, Décrit les services, les ressources et les comportements communs de l'interface de programme d'application (API) OSLC (Open Services for Lifecycle Collaboration), appelée interface OSLC ObjectServer. Décrit comment activer cette API et fournit des exemples de définitions de fournisseur de services, de charges de message RDF/XML et des demandes et réponses HTTP.

  Si vous utilisez d'autres produits IBM pour étendre les fonctionnalités de Tivoli Netcool/OMNIbus, tels que DB2, IBM Tivoli Monitoring ou Tivoli Common Reporting, consultez le centre de documentation du produit concerné, afin d'obtenir les publications appropriées.

Accès à la terminologie en ligne

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de logiciels IBM en un seul emplacement, pour des raisons pratiques. Vous pouvez accéder au site Web de terminologie à l'adresse Web suivante :

http://www.ibm.com/software/globalization/terminology

Accès à la documentation en ligne

IBM met en ligne les publications pour tous les produits Tivoli, dès leur parution ou leur mise à jour, sur le site des téléchargements Tivoli à l'adresse :

ftp://public.dhe.ibm.com/software/tivoli/Netcool/NetcoolOmnibus/library/

Remarque : Si vous imprimez des documents PDF dans un autre format que le format A4, définissez dans la fenêtre **Fichier** > **Imprimer** l'option qui permet à Adobe Reader d'imprimer des pages A4 sur votre format de papier.

Accessibilité

Les fonctions d'accessibilité aident les utilisateurs atteints d'un handicap physique, tel qu'une mobilité réduite ou une déficience visuelle, à utiliser correctement les applications logicielles.

Avec ce produit, vous pouvez utiliser des technologies d'assistance pour faciliter la navigation dans l'interface par des moyens audio-visuels. Vous pouvez également utiliser le clavier à la place de la souris pour exploiter certaines fonctions de l'interface graphique.

Formation technique Tivoli

Pour obtenir des informations sur les formations techniques Tivoli, reportez-vous au site Web de formation IBM Tivoli à l'adresse suivante :

http://www.ibm.com/software/tivoli/education

Informations de support

Si vous rencontrez un problème avec le logiciel IBM, vous pouvez le résoudre rapidement. IBM vous propose les solutions suivantes pour obtenir le support dont vous avez besoin :

En ligne
Accédez au site service de support logiciel IBM à l'adresse http://www.ibm.com/software/support/probsub.html, puis suivez les instructions.

IBM Support Assistant
IBM Support Assistant (ISA) est un plan de travail de maintenabilité logicielle gratuit qui vous aide à résoudre les problèmes liés aux applications logicielles IBM. ISA permet d'accéder rapidement aux informations de support et aux outils de maintenabilité pour identifier les problèmes. Pour installer le logiciel ISA, rendez-vous à l'adresse http://www.ibm.com/software/support/isa.

Documentation
Si vous avez une suggestion pour améliorer le contenu ou l'organisation de ce guide, envoyez-la à l'équipe de Tivoli Netcool/OMNIbus Information Development, à l'adresse :

mailto://L3MMDOCS@uk.ibm.com

Référence associée:

«IBM Support Assistant», à la page 673
IBM Support Assistant (ISA) est un outil de maintenabilité logicielle local gratuit qui vous aide à résoudre les problèmes liés aux applications logicielles IBM. ISA permet d'accéder rapidement aux informations de support et aux outils de maintenabilité pour identifier les problèmes.

Conventions utilisées dans cette publication

Cette publication utilise plusieurs conventions pour les actions et les termes spéciaux, ainsi que pour les commandes et les chemins d'accès liés au système d'exploitation.

Variables et chemins d'accès liés au système d'exploitation

Cette publication utilise la convention UNIX pour la définition des variables d'environnement et la notation des répertoires.

Lorsque vous utilisez la ligne de commande Windows, remplacez **$***variable* par **%***variable***%** pour les variables d'environnement. De la même façon, remplacez chaque barre oblique (**/**) par une barre oblique inversée (\) dans les chemins de répertoire. Par exemple, sur les systèmes UNIX, la variable d'environnement $NCHOME désigne le chemin du répertoire de base de Netcool. Sur les systèmes Windows, la variable d'environnement %NCHOME% désigne le chemin d'accès au répertoire de base de Netcool. Les noms de variables d'environnement ne sont pas toujours identiques dans les environnements Windows et UNIX. Par exemple, dans les environnements Windows, %TEMP% est l'équivalent de $TMPDIR dans les environnements UNIX.

Si vous utilisez l'interpréteur de commandes shell sur un système Windows, vous pouvez utiliser les conventions UNIX.

Emplacement d'origine de Netcool

L'emplacement d'origine de Netcool est le répertoire de base dans lequel Tivoli Netcool/OMNIbus est installé. L'emplacement d'origine de Netcool est défini par la variable d'environnement NCHOME. dont la valeur est la suivante :

- UNIX Linux `$NCHOME` a pour valeur par défaut `/opt/IBM/tivoli/netcool`
- Windows `%NCHOME%` a pour valeur par défaut `C:\IBM\Tivoli\Netcool`

Lorsqu'un répertoire ou un chemin de commande commence par la variable *NCHOME*, l'information s'applique à tous les systèmes d'exploitation pris en charge.

Les autres produits qui utilisent la variable d'environnement NCHOME, tels que IBM Tivoli Network Manager IP Edition, peuvent être installés dans l'emplacement d'origine de Netcool. Chaque produit installe ses composants et fichiers spécifiques dans un sous-répertoire de produits dédié dans l'emplacement d'origine de Netcool. Les fichiers qui sont communs à tous les produits sont installés dans des sous-répertoires partagés dans l'emplacement d'origine de Netcool.

Noms de répertoire spécifiques au système d'exploitation

Lorsque les fichiers Tivoli Netcool/OMNIbus sont identifiés comme se trouvant dans un répertoire *arch* sous NCHOME, *arch* est une variable qui représente le répertoire de votre système d'exploitation, comme indiqué dans le tableau suivant.

Tableau 1. Noms de répertoire pour la variable arch

Nom de répertoire représenté par *arch*	**Système d'exploitation**
`aix5`	Systèmes AIX
`hpux11hpia`	Systèmes HP-UX Itanium

Tableau 1. Noms de répertoire pour la variable arch (suite)

Nom de répertoire représenté par *arch*	**Système d'exploitation**
`linux2x86`	Systèmes Red Hat Linux et SUSE
`linux2s390`	Linux for System z
`solaris2`	Systèmes Solaris
`win32`	Systèmes Windows

Emplacement OMNIHOME

Les sondes et les passerelles, ainsi que les anciennes versions de Tivoli Netcool/OMNIbus, utilisent la variable d'environnement OMNIHOME dans de nombreux fichiers de configuration. Définissez la valeur d'OMNIHOME de la manière suivante :

- UNIX Linux Définissez `$OMNIHOME` avec la valeur `$NCHOME/omnibus`
- Windows Définissez `%OMNIHOME%` avec la valeur `%NCHOME%\omnibus`

Répertoire de base de Interface graphique Web

REP_INSTALL_WEBGUI

Fait référence au répertoire où l'Interface graphique Web est installée. Ce répertoire est connu comme le répertoire de base de l'Interface graphique Web. Les valeurs par défaut sont les suivantes :

UNIX Linux `/opt/IBM/tivoli/netcool/omnibus_webgui`

Windows `C:\IBM\tivoli\netcool\omnibus_webgui`

Le répertoire de base de l'Interface graphique Web est distinct des répertoires de base de Jazz for Service Management.

Répertoire de base de Jazz for Service Management

REP_INSTALL_WAS

Fait référence à l'emplacement où WebSphere Application Server est installé. Cet emplacement peut être spécifié lors de l'installation. Les valeurs par défaut sont les suivantes :

UNIX Linux `/opt/IBM/WebSphere/AppServer`

Windows `C:\Program Files\IBM\WebSphere\AppServer`

REP_INSTALL_JazzSM

Fait référence à l'emplacement où Jazz for Service Management est installé. Cet emplacement peut être spécifié lors de l'installation. Les valeurs par défaut sont les suivantes :

UNIX Linux `/opt/IBM/JazzSM`

Windows `C:\Program Files\IBM\JazzSM`

REP_INSTALL_JazzSM

Fait référence à l'emplacement du profil de serveur d'applications utilisé pour Jazz for Service Management. Cet emplacement se trouve dans le sous-répertoire `/profile` du répertoire de base de Jazz for Service Management.

UNIX Linux *REP_INSTALL_JazzSM*`/profile`

Windows *REP_INSTALL_JazzSM*`\profile`

REP_INSTALL_DASH

Fait référence à l'emplacement où Concentrateur des services d'application du tableau de bord est installé. Cet emplacement peut être spécifié lors de l'installation. Les valeurs par défaut sont les suivantes :

UNIX Linux `/opt/IBM/JazzSM/ui`

Windows `C:\Program Files\IBM\JazzSM\ui`

Pour les autres répertoires d'installation de Jazz for Service Management, consultez le centre de documentation de Jazz for Service Management à http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

Conventions relatives aux graphiques de repérage

La documentation de Tivoli Netcool/OMNIbus contient des graphiques de repérage qui indiquent les parties d'une rubrique ou d'une instruction qui ne s'appliquent que dans certaines conditions. Le tableau suivant décrit la signification de chacun de ces graphiques :

Tableau 2. Graphiques de repérage pour Tivoli Netcool/OMNIbus.

Graphique	Description
Web GUI	Le texte ou l'instruction ne s'applique qu'au composant de l'Interface graphique Web.
UNIX	Le texte ou l'instruction ne s'applique qu'aux systèmes d'exploitation UNIX, ce qui inclut AIX et Solaris. Les graphiques de repérage suivants sont utilisés pour AIX et Solaris lorsque cela est nécessaire : AIX Solaris
Linux	Le texte ou l'instruction ne s'applique qu'aux systèmes d'exploitation Linux.
Windows	Le texte ou l'instruction ne s'applique qu'aux systèmes d'exploitation Windows.
32-bit	Le texte ou l'instruction ne s'applique qu'aux systèmes d'exploitation 32 bits.
64-bit	Le texte ou l'instruction ne s'applique qu'aux systèmes d'exploitation 64 bits.
FIPS 140-2	Le texte ou l'instruction ne s'applique qu'à l'utilisation ou à la configuration du chiffrement FIPS 140-2.
Default	Le texte ou l'instruction décrit le comportement par défaut ou ne s'applique qu'aux configurations par défaut.
Fix Pack 1	Le texte ou l'instruction ne s'applique qu'au numéro de groupe de correctifs indiqué par le graphique. Les fonctionnalités ou les améliorations décrites dans le texte ne sont disponibles qu'après l'installation de ce groupe de correctifs. **Remarque :** Les groupes de correctifs pour le composant serveur et le composant de l'Interface graphique Web sont publiés séparément. Les groupes de correctifs de l'Interface graphique Web sont indiqués comme suit : Web GUI Fix Pack 1
Administrator	Le texte ou l'instruction ne s'applique qu'aux administrateurs de l'interface graphique Web. C'est-à-dire aux utilisateurs qui disposent des rôles ncw_user et ncw_admin.
C	Le texte ou l'instruction ne s'applique qu'au langage de programmation C.

Tableau 2. Graphiques de repérage pour Tivoli Netcool/OMNIbus. (suite)

Graphique	Description
Java	Le texte ou l'instruction ne s'applique qu'au langage de programmation Java™.

Conventions typographiques

Cette publication utilise les conventions typographiques suivantes :

Gras

- Commandes en minuscules et commandes à casse mixte pour mieux les distinguer dans le texte
- Contrôles d'interface (cases à cocher, boutons de commande, boutons radio, flèches d'incrément, zones, dossiers, icônes, zones de liste, éléments de zone de liste, listes à plusieurs colonnes, conteneurs, options de menu, noms de menu, onglets, feuilles de propriétés), libellés (tels que **Conseil :** et **Remarques relatives au système d'exploitation :**)
- Mots clés et paramètres dans le texte

Italique

- Citations (exemples : titres de publications, disquettes et CD)
- Mots définis dans le texte (exemple : une ligne spécialisée est appelée ligne *point-à-point*)
- Mise en évidence de mots et de lettres (exemples : "Utilisez le mot *que* pour introduire une clause restrictive." ; "L'adresse LUN doit commencer par la lettre *L*.")
- Nouveaux termes rencontrés dans un texte (sauf dans une liste de définitions) : une *vue* est un cadre situé dans un espace de travail qui contient des données
- Variables et valeurs que vous devez fournir : ... où *nom* représente....

`Espacement fixe`

- Exemples et extraits de code
- Noms de fichiers, mots clés de programmation et autres éléments qu'il est difficile de distinguer dans du texte
- Texte de message et invites adressées à l'utilisateur
- Texte que l'utilisateur doit entrer
- Valeurs d'arguments ou d'options de commande

Chapitre 1. Introduction à Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus est un système de gestion du niveau de service (SLM) qui offre une surveillance centralisée et en temps réel des réseaux complexes et des domaines informatiques.

Ces informations présentées par Tivoli Netcool/OMNIbus peuvent être traitées selon les besoins de votre entreprise. Par exemple, elles peuvent être transmises à des systèmes de service d'assistance, enregistrées dans des bases de données, répliquées sur des systèmes distants, et utilisées pour déclencher des réponses automatiques à certains événements.

Tivoli Netcool/OMNIbus peut également consolider des informations issues de différentes plateformes de gestion de réseau à domaine limité à des emplacements distants. En travaillant avec des applications et des systèmes de gestion existants, Tivoli Netcool/OMNIbus minimise le temps de déploiement et permet aux salariés d'utiliser les capacités de gestion de réseau existantes.

Tivoli Netcool/OMNIbus suit les informations d'alerte dans une base de données à hautes performances en mémoire, et présente les informations pertinentes aux utilisateurs spécifiques via des filtres et des vues qui peuvent être configurés individuellement. Tivoli Netcool/OMNIbus a des fonctions d'automatisation pouvant effectuer un traitement intelligent sur les alertes gérées.

Composants de Tivoli Netcool/OMNIbus

Les composants de Tivoli Netcool/OMNIbus travaillent ensemble pour collecter et gérer des informations d'événements réseau. Les noms des composants sont les suivants :

- ObjectServers
- Sondes
- Passerelles
- Outils de bureau
- Outils d'administration
- Interface graphique Web

La figure suivante présente l'architecture des composants Tivoli Netcool/OMNIbus. Les sondes envoient des alertes au serveur ObjectServer local, et une passerelle réplique ces alertes dans un autre serveur ObjectServer dans une configuration de reprise en ligne. Les alertes envoyées au serveur ObjectServer peuvent être affichées dans la liste des événements de l'Interface graphique Web ou dans la liste des événements de bureau. Des passerelles supplémentaires son également configurées pour transmettre des alertes aux autres applications, comme le centre d'assistance ou le système CRM (Customer Relationship Management), et un système de gestion de base de données relationnelle (RDBMS). Netcool/OMNIbus Administrator et les autres outils d'administration peuvent être utilisés pour configurer et gérer le système.

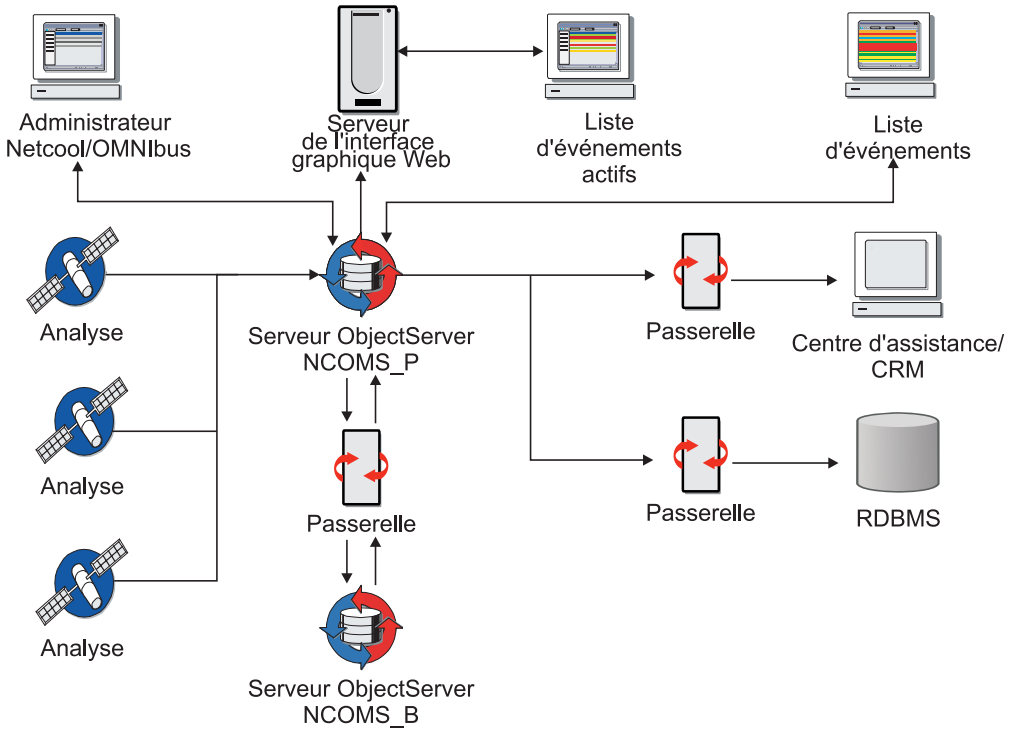

Figure 1. Architecture du composant Tivoli Netcool/OMNIbus

Le serveur ObjectServer

Le serveur ObjectServer est le serveur de base de données en mémoire situé au coeur de Tivoli Netcool/OMNIbus.

Les informations d'événement sont transmises au serveur ObjectServer depuis des programmes externes tels que les sondes et les passerelles. Ces informations sont stockées et gérées dans les tables de base de données, et affichées dans la liste des événements de l'Interface graphique Web ou dans la liste des événements de bureau.

Dédoublonnage et automatisation dans le serveur ObjectServer

Il se peut qu'une seule unité génère la même erreur de façon répétitive jusqu'à ce que le problème soit résolu. Le serveur ObjectServer utilise le *dédoublonnage* pour s'assurer que les informations d'événement générées par la même source ne soient pas dupliquées dans la liste d'événements. Les événements répétitifs sont identifiés et stockés en tant qu'événement unique afin de réduire la quantité de données figurant sur le serveur ObjectServer. Le serveur ObjectServer gère le total (ou la somme) des occurrences totales de cet événement.

Vous pouvez utiliser l'*automatisation* pour détecter les modifications dans le serveur ObjectServer et générer des réponses automatiques suite à ces changements. Vous permettez ainsi au serveur ObjectServer de traiter des alertes sans qu'un opérateur n'aie besoin d'intervenir.

Tâches associées:

«Création et exécution de serveurs ObjectServer», à la page 193
Chaque installation Tivoli Netcool/OMNIbus peut avoir au moins un serveur ObjectServer pour stocker et gérer les informations d'alerte. Vous pouvez également configurer plusieurs serveurs ObjectServer sur un ou plusieurs

ordinateurs hôtes.

Sondes

Les sondes se connectent à une source d'événement, détectent et récupèrent des données d'événement et les transmettent au serveur ObjectServer en tant qu'événements.

Les sondes utilisent la logique spécifiée dans un fichier de règles pour manipuler les éléments d'événement avant de les convertir en zones d'événement dans la table alerts.status du serveur ObjectServer.

Chaque sonde est conçue pour récupérer les données d'événement sur une source spécifique. Les sondes peuvent récupérer des données sur toute source de données stable, notamment les unités, les bases de données et les fichiers journaux. Les sondes peuvent également être configurées pour modifier et ajouter des données d'événement.

Passerelles

Les passerelles Tivoli Netcool/OMNIbus permettent l'échange des événements entre les serveurs ObjectServer et les applications tierces complémentaires, telles que les bases de données et les systèmes de centre d'assistance ou CRM (Customer Relationship Management).

Les passerelles permettent de répliquer des événements ou de gérer un serveur ObjectServer de secours. Les passerelles d'application vous permettent d'intégrer plusieurs fonctions d'entreprise. Par exemple, vous pouvez configurer une passerelle pour envoyer des informations d'événements vers un système de centre d'assistance. Vous pouvez également utiliser une passerelle pour archiver les événements dans une base de données.

Une fois la passerelle correctement installée et configurée, les opérateurs ont une vision transparente des transferts.

Passerelles ObjectServer

Utilisez les passerelles ObjectServer pour répliquer les alertes et d'autres données entre les serveurs ObjectServer. Les passerelles ObjectServer vous aident à améliorer la fiabilité et à augmenter l'évolutivité de votre système. Vous pouvez améliorer la fiabilité en gérant des serveurs ObjectServer de sauvegarde et améliorer l'évolutivité en établissant une configuration à plusieurs niveaux.

Les passerelles ObjectServer peuvent être unidirectionnelles ou bidirectionnelles. Elles consistent en plusieurs programmes de lecture et d'écriture. Les programmes de lecture extraient les alertes d'un serveur ObjectServer source. Les programmes d'écriture envoient les alertes à un serveur ObjectServer cible.

La passerelle ObjectServer est installée à l'aide du module d'installation de Tivoli Netcool/OMNIbus.

Les passerelles ObjectServer peuvent répliquer les données de n'importe quelle table entre les serveurs ObjectServer. Les détails des tables à répliquer sont stockés dans le fichier de définition de réplication de table et dans le fichier de définition de mappe.

Vous pouvez améliorer la fiabilité de votre système en définissant une paire de serveurs ObjectServer reliés par une passerelle bidirectionnelle. Tous les clients, à l'exception de la passerelle bidirectionnelle, se connectent au serveur ObjectServer principal. Le serveur ObjectServer de sauvegarde agit comme serveur de secours et est actualisé par la passerelle bidirectionnelle.

Dans une configuration à plusieurs niveaux, les passerelles ObjectServer fonctionnent de la manière suivante :

- Chaque ObjectServer de la couche de collecte possède sa propre passerelle unidirectionnelle ObjectServer dédiée qui relie le serveur ObjectServer à la couche d'agrégation.
- La couche d'agrégation inclut une paire de serveurs ObjectServer connectée par une passerelle bidirectionnelle ObjectServer pour que les serveurs restent synchronisés. La passerelle ObjectServer bidirectionnelle s'exécute sur l'hôte de secours.
- Chaque ObjectServer de la couche d'affichage possède sa propre passerelle unidirectionnelle ObjectServer dédiée qui relie le serveur ObjectServer à la couche d'agrégation. Chaque programme de lecture de passerelle d'affichage se connecte à la paire d'agrégation virtuelle alors que chaque programme d'écriture de passerelle se connecte, et est fixé, à son ObjectServer d'affichage dédié. Par conséquent, même si les programmes de lecture peuvent exécuter des opérations de reprise en ligne et de reprise par restauration entre les serveurs ObjectServer principal et de sauvegarde de la couche d'agrégation, le programme d'écriture reste connecté uniquement à son serveur ObjectServer d'affichage dédié. (Ces connexions de passerelle sont l'opposé des connexions de passerelle dans la couche de collecte.)

Pour plus d'informations sur la configuration de l'architecture à plusieurs niveaux, voir *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.

Outils de bureau

Le bureau est une suite intégrée d'outils graphiques utilisés pour afficher et gérer des événements, et pour configurer la présentation des données sur l'événement.

Les données sur l'événement sont livrées dans un format qui vous permet de déterminer rapidement la disponibilité des services sur le réseau. Lorsque la cause d'un événement a été identifiée, vous pouvez utiliser les outils de bureau pour résoudre rapidement les problèmes.

La plupart des fonctionnalités de bureau sont également disponibles dans le composant d'Interface graphique Web.

Restriction : Les outils de bureau ne sont pas pris en charge sur les systèmes Linux on System z ou HP-UX Integrity. Vous pouvez installer et configurer le composant d'Interface graphique Web puis utiliser les clients de l'Interface graphique Web pour afficher, gérer et configurer les événements d'une manière similaire aux outils de bureau.

Concepts associés:

«Interface graphique Web», à la page 6
L'Interface graphique Web est une application basée sur le Web qui présente les données d'événements provenant de sources de données multiples dans divers formats graphiques dans les navigateurs Web pris en charge et les appareils mobiles. L'Interface graphique Web contient la plupart des fonctionnalités des composants de bureau de Tivoli Netcool/OMNIbus.

Outils d'administration

Tivoli Netcool/OMNIbus inclut les outils que les administrateurs peuvent utiliser pour configurer ou gérer le système.

Les outils Tivoli Netcool/OMNIbus incluent Netcool/OMNIbus Administrator, une interface interactive SQL, un utilitaire d'importation et d'exportation et le contrôle de processus.

Netcool/OMNIbus Administrator

Netcool/OMNIbus Administrator est un outil graphique que vous pouvez utiliser pour configurer et gérer les serveurs ObjectServer.

Interface interactive SQL

Le serveur ObjectServer inclut une interface SQL (Structured Query Language) permettant de définir et de manipuler les objets de base de données relationnelle tels que des tables et des vues. Vous pouvez utiliser l'interface interactive SQL (nommée **nco_sql** sous UNIX et Linux, et **isql** sous Windows) pour vous connecter à un serveur ObjectServer, et utiliser les commandes SQL pour interagir et contrôler le serveur ObjectServer. L'interface interactive SQL vous permet d'effectuer des tâches telles que la création d'une base de données ou l'arrêt du serveur ObjectServer.

Utilitaire d'importation et d'exportation

Deux utilitaires, intitulés **nco_confpack** et **nco_osreport**, peuvent être utilisés pour importer et exporter des configurations de serveur ObjectServer.

Remarque : **nco_confpack** n'est pas approprié à la réplication ou au clonage de serveurs ObjectServer. Cet utilitaire est conçu pour exporter et importer des données de configuration entre les serveurs ObjectServer. Si vous avez accès à un système Tivoli Netcool/OMNIbus V7.3.1 (ou version ultérieure), vous pouvez faire appel à l'utilitaire **nco_osreport** pour répliquer ou cloner des serveurs ObjectServer.

Utilisez **nco_osreport** pour :

- Exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peuvent être entrés dans un nouvel ObjectServer créé à l'aide de la commande **nco_dbinit**.
- Exporter les contenus des tables du serveur ObjectServer vers un fichier HTML afin de capturer une image instantanée d'une configuration du serveur ObjectServer qui servirait, par exemple, à soumettre cette configuration à une équipe d'assistance technique.
- Exporter les contenus des tables du serveur ObjectServer vers un fichier XML qui pourrait être utilisé lors de la programmation, par exemple.

Utilisez **nco_confpack** pour :

- Extraire un sous-ensemble d'éléments de configuration des serveurs ObjectServer de Tivoli Netcool/OMNIbus (par exemple, les menus de liste d'événements et les automatisations) et les importer dans d'autres serveurs ObjectServer.
- Sauvegarder les données de configuration Tivoli Netcool/OMNIbus du serveur ObjectServer à des fins de sauvegarde.

Contrôle des processus

Le système de contrôle des processus effectue deux tâches principales :

- Il effectue des procédures externes spécifiées dans les automatisations. Les automatisations détectent les modifications dans le serveur ObjectServer et renvoient des réponses automatisées à ces modifications.
- Il gère les processus locaux et distants.

Le contrôle des processus permet de configurer les processus distants afin de simplifier la gestion des composants Tivoli Netcool/OMNIbus tels que les serveurs ObjectServer, les sondes et les passerelles. Le système de contrôle de processus est composé :

- des agents de processus, qui sont des programmes installés sur chaque hôte pour la gestion des processus
- d'un ensemble d'utilitaires de ligne de commande constituant une interface de gestion de processus

Concepts associés:

Chapitre 11, «Importation et exportation de configurations du serveur ObjectServer», à la page 293
Tivoli Netcool/OMNIbus fournit deux utilitaires, nommés **nco_confpack** et **nco_osreport** ; vous pouvez les utiliser pour importer et exporter les configurations d'un serveur ObjectServer.

Netcool MIB Manager

Netcool MIB Manager est une application IBM® basée sur Eclipse que vous pouvez utiliser pour analyser les fichiers MIB (base d'information de gestion) SNMP (Simple Network Management Protocol), à partir desquels vous pouvez générer des fichiers de règles Netcool.

Netcool MIB Manager est destiné à remplacer l'utilitaire **mib2rules**.

Interface graphique Web

L'Interface graphique Web est une application basée sur le Web qui présente les données d'événements provenant de sources de données multiples dans divers formats graphiques dans les navigateurs Web pris en charge et les appareils mobiles. L'Interface graphique Web contient la plupart des fonctionnalités des composants de bureau de Tivoli Netcool/OMNIbus.

Bien que l'Interface graphique Web reçoive généralement des données d'événement d'ObjectServers, elle peut se connecter à n'importe quelle source de données à partir de laquelle les informations d'événement peuvent être obtenues.

L'Interface graphique Web utilise une architecture client / serveur et elle est hébergée dans Concentrateur des services d'application du tableau de bord qui fait partie de Jazz for Service Management. Les clients se connectent à Concentrateur des services d'application du tableau de bord pour accéder à l'Interface graphique Web. Vous pouvez installer l'Interface graphique Web dans un système Jazz for Service Management existant. Sinon, installez un nouveau système Jazz for Service Management, soit avant l'installation de l'Interface graphique Web, soit pendant l'installation de l'Interface graphique Web. Plusieurs produits compatibles peuvent être hébergés dans un seul système Jazz for Service Management.

Concentrateur des services d'application du tableau de bord peut être déployée dans un environnement d'équilibrage de charge avec une base de données IBM DB2. Un droit de télécharger, installer et déployer DB2 dans un environnement d'équilibrage de charge est inclus dans la licence.

Pour plus d'informations sur Concentrateur des services d'application du tableau de bord, voir le centre de documentation Jazz for Service Management à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

- «Widgets d'affichage d'événement»
- «Applications mobiles», à la page 8
- «Outils d'administration», à la page 8
- «Flot de données», à la page 8

Widgets d'affichage d'événement

Les principales caractéristiques d'affichage d'événement de l'Interface graphique Web sont les suivantes. Ces données peuvent également être affichées dans des widgets Concentrateur des services d'application du tableau de bord tels que des tableaux, des graphiques et des jauges.

Dans les listes d'événements, des informations sur les alertes s'affichent dans la liste d'événements en fonction des filtres et des vues définis. Utilisez des filtres pour afficher un sous-ensemble d'événements qui sont fondées sur des critères spécifiques. Utilisez des vues pour choisir les zones d'événement à afficher. Des outils par défaut sont fournis pour exécuter des actions sur des événements. Vous pouvez également écrire vos propres outils.

Afficheur d'événements
: Liste d'événements de lecture/écriture mise en œuvre par JavaScript. Il est possible de regrouper des événements par attributs, tels que l'emplacement, et d'afficher les relations entre les événements. Les outils et les actions peuvent être exécutés sur les événements.

Liste d'événements actifs (AEL)
: Liste d'événements de lecture/écriture s'exécutant dans un applet Java. Pour les systèmes client, l'environnement d'exécution Java doit être installé. Les outils et les actions peuvent être exécutés sur les événements.

Tableau de bord des événements
: Présentation des informations d'alerte capturées par les filtres. Le tableau de bord des événements présente les informations d'alerte sous la forme d'un ensemble d'écrans de surveillance, à partir duquel vous voulez ouvrir les AEL.

Jauges
: Une synthèse des données d'événement est capturée par des métriques. Une métrique est un type de mesure utilisé pour déterminer une valeur quantifiable dans les tables ou propriétés d'ObjectServer. Les informations sont affichées dans une série de jauges et peuvent être consultées dans un navigateur ou publiées via une adresse URL sur une unité mobile prise en charge. Les destinataires peuvent ajouter des signets à l'adresse URL, de façon à pouvoir retourner aux jauges. Les actions qui ne demandent qu'un seul clic peuvent être associées aux jauges pour permettre aux utilisateurs d'explorer en aval les informations. Vous pouvez également utiliser les widgets de jauge qui sont inclus dans les widgets Concentrateur des services d'application du tableau de bord pour visualiser les données d'événement de l'Interface graphique Web.

Cartes Représentation visuelle d'un réseau contenant des vues graphiques interactives du réseau et de ses performances. Les cartes peuvent être conçues par les administrateurs. Les opérateurs peuvent utiliser des cartes pour surveiller les événements qui se produisent sur le réseau.

Composant de rendu du graphique
Les graphiques présentent des informations d'alerte réseau de haut niveau aux utilisateurs sous différents formats graphiques, notamment des diagrammes à barre et des diagrammes à secteurs.

Applications mobiles

Les événements peuvent être affichés sur les appareils mobiles pris en charge sur les applications suivantes :

Liste d'événements mobiles
Tableau de bord d'événements en lecture seule, liste d'événements et page de détails d'événement.

Jauges mobiles
Équivalent mobile de la page des jauges.

Outils d'administration

Des fonctions d'administration sont fournies pour la configuration de l'affichage des événements. Il s'agit par exemple d'interfaces utilisateur graphiques pour la création d'outils de gestion des événements. Pour l'administration à distance, le client d'API d'administration (WAAPI) de l'Interface graphique Web est fourni. Le client WAAPI est un utilitaire Java que vous pouvez utiliser pour gérer à distance le serveur de l'Interface graphique Web.

Flot de données

La figure suivante montre comment l'Interface graphique Web s'intègre dans le flux de données d'événement des ObjectServers. Les événements sont visualisés dans les affichages d'événements et affichés aux clients.

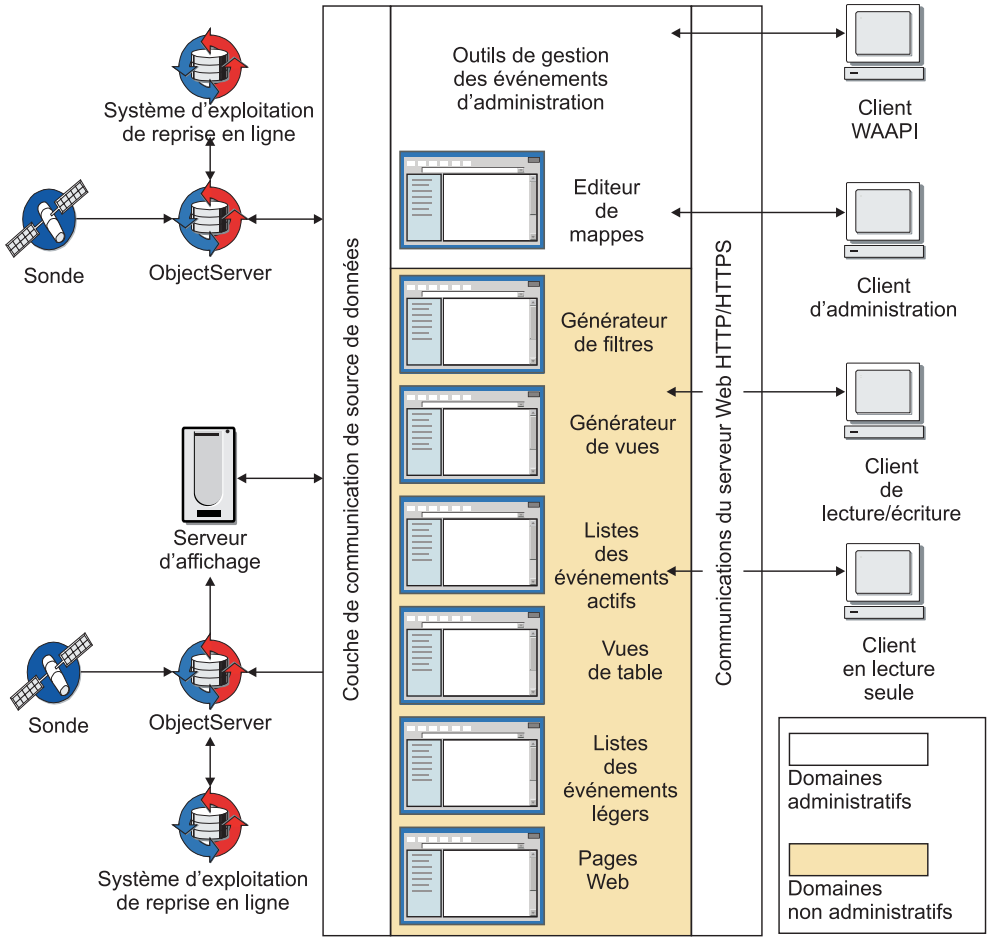

Figure 2. Communications de l'Interface graphique Web

Concepts associés:

«Outils de bureau», à la page 4
Le bureau est une suite intégrée d'outils graphiques utilisés pour afficher et gérer des événements, et pour configurer la présentation des données sur l'événement.

Chapitre 2. Instructions de démarrage rapide

Utilisez ces instructions si vous ne connaissez pas Tivoli Netcool/OMNIbus et que vous souhaitez effectuer une installation et une configuration rapides afin d'exécuter un serveur ObjectServer.

Les étapes sont les suivantes :

Tableau 3. Instructions de démarrage rapide

Action	Informations complémentaires
1. Préparez l'installation en vous assurant que vous disposez de la configuration requise et en obtenant le package d'installation. **Remarque :** Vous pouvez obtenir le module d'installation Interface graphique Web au cours de cette étape, mais vous ne pouvez pas installer Interface graphique Web.	«IBM Prerequisite Scanner», à la page 30 «Préparation à l'installation», à la page 65
2. Installez Tivoli Netcool/OMNIbus et acceptez toutes les fonctions d'installation par défaut.	«Installation de Tivoli Netcool/OMNIbus», à la page 72
UNIX Linux 3. Si nécessaire, définissez les variables d'environnement suivantes : • $NCHOME • $OMNIHOME • $PATH • $LD_LIBRARY_PATH (Solaris ou Linux uniquement) • $LIBPATH (AIX uniquement) • $SHLIB_PATH (HP-UX uniquement) Consultez les instructions pour définir ces variables d'environnement.	«Définition des variables d'environnement», à la page 87 «Vérification des chemins d'accès de la bibliothèque partagée», à la page 92
4. Créez un serveur ObjectServer en exécutant l'utilitaire d'initialisation de base de données, comme suit : UNIX Linux `$NCHOME/omnibus/bin/nco_dbinit -server` *`nom_serveur`* Windows `%NCHOME%\omnibus\bin\nco_dbinit -server` *`nom_serveur`* où *nom_serveur* est le nom du serveur ObjectServer, composé d'un maximum de 29 lettres en majuscules et qui ne peut pas commencer par un entier. Les tables de base de données, les données, les utilisateurs, les groupes, les rôles et le fichier de propriétés par défaut sont créés. (Pour vous connecter au serveur ObjectServer, vous pouvez utiliser l'utilisateur par défaut appelé `root (racine)`, qui est créé avec un mot de passe vide.)	«Création d'un serveur ObjectServer», à la page 197

Tableau 3. Instructions de démarrage rapide (suite)

Action	Informations complémentaires

5. Configurez les informations de communication avec le serveur ObjectServer sur l'ordinateur hôte.
 	
UNIX Linux
 	
1. Utilisez l'éditeur de serveurs pour ajouter les détails de communication en exécutant la commande suivante :
`$NCHOME/omnibus/bin/nco_xigen`
Ou :
2. Effectuez une mise à jour des informations sur la communication ObjectServer en éditant le fichier de données de connexion (`$NCHOME/etc/omni.dat`) et générez le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus à l'aide de la commande suivante :
`$NCHOME/bin/nco_igen`
Le fichier d'interfaces `$NCHOME/etc/interfaces.`*arch* est créé, *arch* représentant le nom du système d'exploitation.
Remarque : Les exemples d'entrées dans les détails de communication utilisent le nom d'hôte par défaut `omnihost`. Remplacez cette valeur par le nom de l'ordinateur sur lequel chaque serveur est exécuté.
 	
Windows
 	
Ajoutez les détails de communication à l'aide de l'éditeur de serveurs :
1. Cliquez sur **Démarrer** > **Programmes** > **NETCOOL Suite** > **Utilitaires système** > **Editeur de serveurs**.
2. Entrez et sauvegardez les informations de communication du serveur ObjectServer.
Le fichier de données de connexion (`%NCHOME%\ini\sql.ini`) est mis à jour avec ces détails.
	«Configuration des informations de communication du serveur», à la page 209

6. Démarrez le serveur ObjectServer en exécutant la commande suivante : UNIX Linux `$NCHOME/omnibus/bin/nco_objserv -name` *nom_serveur* Windows `%NCHOME%\omnibus\bin\nco_objserv -name` *nom_serveur* où *nom_serveur* est le nom du serveur ObjectServer.	«Démarrage manuel du serveur ObjectServer», à la page 204
7. Préparez l'installation de Interface graphique Web en contrôlant les conditions prérequises, en choisissant le type d'installation requis et en collectant les informations requises.	Chapitre 4, «Planification de l'installation ou de la mise à niveau» , à la page 17 Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145 «Regroupement d'informations sur l'installation», à la page 147
8. Installez Interface graphique Web en utilisant l'assistant, le mode console ou le mode silencieux. Utilisez les informations collectées au cour de l'étape 7 afin de spécifier les paramètres de l'installation.	«Installation de l'interface graphique Web», à la page 151

Tableau 3. Instructions de démarrage rapide (suite)

Action	Informations complémentaires
9. Connectez-vous à Interface graphique Web, affectez les rôles Interface graphique Web au changement d'utilisateur administratif et changez les mots de passe des utilisateurs fournis.	«Connexion», à la page 182 «Affectation de rôles d'Interface graphique Web à l'utilisateur administrateur», à la page 184 «Changement des mots de passe des utilisateurs fournis», à la page 185
10. Facultatif : exécutez la configuration du registre d'utilisateurs requis, par exemple LDAP, en fonction de l'installation Concentrateur des services d'application du tableau de bord.	«Configuration de l'authentification des utilisateurs», à la page 501

Informations complémentaires

Pour plus d'informations, lisez les scénarios d'installation suivants :

- Chapitre 19, «Exemples de scénarios d'installation de Tivoli Netcool/OMNIbus (architectures de base, de reprise en ligne et de bureau)», à la page 621
- Chapitre 20, «Exemple de scénario d'installation pour les composants non Web et l'Interface graphique Web de Tivoli Netcool/OMNIbus (sous Windows)», à la page 643

Chapitre 3. Instructions de mise à niveau rapide

Consultez ces informations pour procéder à une mise à niveau rapide des composants côté serveur de Tivoli Netcool/OMNIbus.

Les étapes sont les suivantes :

Tableau 4. Instructions sur la mise à niveau rapide des composants côté serveur

Action	Informations complémentaires
1. Etudiez les problèmes de compatibilité avec les versions précédentes du produit.	«Compatibilité avec des versions antérieures», à la page 54
2. Préparez la mise à niveau en vérifiant la configuration requise et en obtenant le package d'installation.	«IBM Prerequisite Scanner», à la page 30 «Préparation à l'installation», à la page 65
3. Si l'installation existante s'exécute en mode non-FIPS 140–2 et que vous souhaitez mettre à niveau le produit pour qu'il s'exécute en mode FIPS 140–2, utilisez la liste de contrôle de configuration de FIPS 140–2 pour savoir comment procéder. En fonction de votre configuration existante, certains étapes de configuration préalables peuvent être nécessaires. Des étapes de configuration sont également requises après la mise à niveau. Les étapes pré-mise à niveau sont généralement requises si les mots de passe utilisateur de votre système sont actuellement chiffrés avec un algorithme DES, ou si vous utilisez le chiffrement de valeur de propriété pour chiffrer les valeurs de chaîne dans les fichiers de propriétés.	Chapitre 21, «Liste de contrôle de configuration pour le mode FIPS 140–2», à la page 653
4. Sauvegardez votre système existant, puis utilisez IBM Installation Manager pour installer Tivoli Netcool/OMNIbus dans un nouveau répertoire. UNIX Linux Cela vous donne la possibilité de laisser Installation Manager migrer automatiquement vos données et la configuration existantes vers votre nouvelle installation.	«Préparation à la mise à niveau», à la page 111 «Mise à jour de Tivoli Netcool/OMNIbus», à la page 111
5. Consultez la liste des fichiers migrés et effectuez toute tâche de configuration manuelle requise.	«Fichiers migrés pendant une mise à niveau», à la page 122
6. Sur les systèmes d'exploitation UNIX, définissez les variables d'environnement suivantes si nécessaire : • $NCHOME • $OMNIHOME • $PATH • $LD_LIBRARY_PATH (Solaris ou Linux uniquement) • $LIBPATH (AIX uniquement) • $SHLIB_PATH (HP-UX uniquement) Consultez les instructions pour configurer ces variables d'environnement.	«Définition des variables d'environnement», à la page 87 «Vérification des chemins d'accès de la bibliothèque partagée», à la page 92
7. Mettez à niveau votre schéma ObjectServer vers le schéma version 8.1.	«Mise à jour du schéma de ObjectServer», à la page 125

Tableau 4. Instructions sur la mise à niveau rapide des composants côté serveur (suite)

Action	Informations complémentaires
8. Si vous avez effectué une mise à niveau à partir d'une version précédente utilisant le protocole SSL pour les communications client et serveur et que vous souhaitez continuer à utiliser vos anciens certificats, faites migrer vos fichiers de certificats et vos clés privées dans la base de données de clés utilisée pour la gestion de certificats. La migration de certificats est prise en charge en mode non-FIPS 140–2 uniquement. Si vous tentez d'opérer en mode FIPS 140–2, vous devez utiliser iKeyman pour recréer tous les anciens certificats que vous souhaitez réutiliser.	«Migration des certificats et des clés SSL», à la page 141 «Gestion des certificats numériques», à la page 401

Chapitre 4. Planification de l'installation ou de la mise à niveau

Avant l'installation ou la mise à jour du produit, lisez les exigences relatives à la configuration matérielle et logicielle requise, au système d'exploitation ainsi qu'à la communication pour Tivoli Netcool/OMNIbus. Vérifiez la compatibilité avec les versions précédentes et découvrez les modes d'installation et la structure usuelle du répertoire d'installation pour le portefeuille de produits Network Management.

Dimensionnement de votre déploiement

Concevez l'architecture système de votre déploiement de Tivoli Netcool/OMNIbus afin de répondre aux besoins de votre réseau. Assurez-vous que tous les hôtes qui sont utilisés dans votre déploiement peuvent prendre en charge les composants que vous installez.

Généralement, un serveur ObjectServer utilise un ou deux coeurs d'UC, mais cela dépend de votre environnement. Des coeurs d'UC supplémentaires sont utiles pour les serveurs ObjectServer qui établissent un grand nombre de connexions simultanées, par exemple au niveau de la couche d'agrégation ou de la couche d'affichage, ou dans des conditions de débordement ou de basculement. Du fait qu'ils prennent en charge simultanément plusieurs opérations de lecture et d'écriture, les serveurs ObjectServer peuvent évoluer sur plusieurs coeurs d'UC. Vous pouvez exécuter Tivoli Netcool/OMNIbus sur des architectures serveur multicoeur et vous pouvez dimensionner l'application en ajoutant des coeurs de processeur aux serveurs existants. La capacité d'un serveur ObjectServer dépend en grande partie de la charge de travail à laquelle vous souhaitez le soumettre.

Plusieurs demandes client peuvent être envoyées au serveur ObjectServer, ce qui signifie qu'un grand nombre d'utilisateurs peuvent être pris en charge, à la fois dans une architecture à un seul niveau et dans une architecture multiniveau.

L'Interface graphique Web peut obtenir des événements à partir de plusieurs sources de données et les afficher dans une Liste d'événements actifs (AEL) unique. Cette fonction vous offre une vue agrégée des événements issus de plusieurs serveurs ObjectServer, sans qu'il soit nécessaire d'ouvrir plusieurs Listes d'événements actifs (AEL).

Procédure

- UC : vérifiez que le serveur ObjectServer s'exécute sur des hôtes disposant des UC les plus rapides possible afin d'optimiser les performances du système. Utilisez les valeurs suivantes comme recommandations :
  - Vérifiez que les processeurs Intel ont une fréquence minimale de 2,4 GHz.
  - Vérifiez que les processeurs RISC ont une fréquence minimale de 1,5 GHz.
- Mémoire : allouez une grande quantité de mémoire. En tant qu'application 32 bits, Tivoli Netcool/OMNIbus peut prendre en charge jusqu'à 4 Go de mémoire RAM. En tant qu'application 64 bits, Tivoli Netcool/OMNIbus peut prendre en charge la mémoire maximale prise en charge par votre matériel. Généralement, un serveur ObjectServer ne consomme pas plus de 1 Go de RAM,

mais respectez une limite supérieure de 4 Go en cas de déferlements d'événements, de lourdes charges provenant des clients ou de conditions de reprise en ligne.

- Capacité du réseau : vérifiez que les composants de Tivoli Netcool/OMNIbus se trouvent dans un centre de données dont le réseau est fiable. En règle générale, les vitesses de connexion réseau de 100 mégabits par seconde, ou plus, sont suffisantes.
- Espace disque : vérifiez qu'un espace disque supérieur à 20 Go est alloué sur votre hôte pour une installation de Tivoli Netcool/OMNIbus, en plus de l'espace alloué à l'encombrement de l'installation. Cet espace supplémentaire permet les points de contrôle de stockage des fichiers journaux et des serveurs ObjectServer.

Exemple

Le tableau suivant contient des recommandations pour le dimensionnement de votre déploiement.

Important : Ces dimensionnements sont indiqués à titre d'exemples uniquement. Vous devez tester votre environnement afin de vous assurer qu'il peut prendre en charge les composants de Tivoli Netcool/OMNIbus.

Tableau 5. Recommandations liées aux exemples de dimensionnement

Composant	Recommandations de dimensionnement	Explication
Serveurs ObjectServer autonomes	Coeurs : 2 Mémoire RAM : 4 Go	Ces serveurs ObjectServer fonctionnent en mode autonome ou dans le cadre d'une paire de reprise en ligne. Ces recommandations de dimensionnement ne sont pas adaptées à un serveur ObjectServer qui prend en charge un grand nombre de sondes ou de connexions client.
Serveurs ObjectServer d'agrégation ou serveurs ObjectServer d'affichage	Coeurs : 4 Mémoire RAM : 4 Go	Ces serveurs ObjectServer font partie de l'architecture à 3 niveaux que vous devez utiliser pour les déploiements de grande taille.
Passerelles reliant une paire de serveurs ObjectServer	Coeurs : 1 Mémoire RAM : 2 Go	Les passerelles reliant une paire de serveurs ObjectServer sont soumises aux mêmes conditions requises en termes de mémoire et d'UC que les serveurs ObjectServer. Toutefois, ces passerelles ne sont pas soumises au même nombre de connexions que les serveurs ObjectServer.

Tableau 5. Recommandations liées aux exemples de dimensionnement (suite)

Composant	Recommandations de dimensionnement	Explication
Passerelles reliant un serveur ObjectServer à une base de données tierce	Coeurs : 2 Mémoire RAM : 4 Go	Les passerelles qui relient un serveur ObjectServer à une base de données tierce nécessitent davantage de mémoire et d'unité centrale que les passerelles qui relient une paire de serveurs ObjectServer, afin de prendre en charge les mécanismes de connexion à la base de données.
Sondes écoutant le réseau, par exemple la sonde pour SNMP ou la sonde Socket Reader Probe	Coeurs : 2 Mémoire RAM : 2 Go	Ces sondes peuvent généralement accepter et traiter des événements entrants sur des unités d'exécution séparées. Cette recommandation de dimensionnement est adaptée aux déferlements d'événements.
Sondes se connectant à une cible ou lisant à partir d'un fichier journal, par exemple la sonde SYSLOG ou la sonde CORBA	Coeurs : 1 Mémoire RAM : 2 Go	Ces sondes font une utilisation de l'unité centrale moins intensive que les sondes qui écoutent sur le réseau, mais elles requièrent la même quantité de mémoire.
Interface graphique Webserver	Pour jusqu'à 50 utilisateurs et jusqu'à 2 sources de données : Coeurs : 2 Mémoire RAM : 4 Go Pour jusqu'à 90 utilisateurs et 3 à 4 sources de données : Coeurs : 4 Mémoire RAM : 4 Go	Non disponible
Client Interface graphique Web	Espace disque : Minimum 1,5 Go Mémoire RAM : 1 Go minimum	Non disponible

Exemples de dimensionnement

Lorsque vous concevez l'architecture de votre déploiement Tivoli Netcool/OMNIbus, vos besoins en dimensionnement peuvent changer. Utilisez ces exemples qui affichent différents types de système Tivoli Netcool/OMNIbus pour vous guider. Ces exemples tiennent compte de l'allocation partagée de ressources pour les composants qui se trouvent sur le même hôte.

Ces exemples sont basés sur les recommandations de dimensionnement de la section «Dimensionnement de votre déploiement», à la page 17.

- «Petit système»
- «Système moyen», à la page 22
- «Grand système», à la page 25

Petit système

Ce système est conçu pour la capture d'événements simples, avec haute disponibilité et la visualisation des événements sur les navigateurs Web. Il se compose d'une paire de reprise en ligne de serveurs ObjectServer, connectés par une passerelle ObjectServer bidirectionnelle qui synchronise les données entre les serveurs ObjectServer, de plusieurs sondes TCP/IP sur un hôte distant qui écoutent sur le réseau les événements et transmettent les événements à la paire de serveurs ObjectServer, et d'un serveur Interface graphique Web qui est utilisé pour visualiser les événements dans la paire de serveurs ObjectServer.

Ce système est installé sur quatre hôtes, comme suit :

- Hôte A pour le serveur ObjectServer principal
- Hôte B pour le serveur ObjectServer de secours et la passerelle ObjectServer bidirectionnelle
- Hôte C pour les sondes
- Hôte D pour l'Interface graphique Web

Dans ce système, le serveur ObjectServer principal qui assume la plus grande charge système pendant les opérations normales, est soumis aux opérations suivantes :

- Opérations d'écriture simultanées à partir des sondes
- Opérations de lecture à partir de la passerelle ObjectServer bidirectionnelle
- Opérations de lecture et d'écriture à partir des connexions de l'Interface graphique Web

Si seuls quelques clients de l'Interface graphique Web sont connectés, la plus grande partie de la charge est émise à partir des opérations d'écriture simultanées par les sondes. Le tableau suivant répertorie les recommandations de dimensionnement pour ce système.

Tableau 6. Recommandations de dimensionnement pour un petit système Tivoli Netcool/OMNIbus

Hôte	**Recommandations de dimensionnement**	**Explication**
A	Coeurs : 2 Mémoire RAM : 4 Go	Si vous prévoyez uniquement quelques événements dans le serveur ObjectServer principal, par exemple moins de 50.000, vous pouvez envisager le plafonnement de l'allocation de mémoire. Sinon, permettez à la mémoire d'atteindre le maximum théorique de 4 Go.
B	Coeurs : 2 Mémoire RAM : 4 Go	Bien que les deux composants s'exécutent sur cet hôte, le serveur ObjectServer de secours n'est pas soumis à la même charge que le serveur ObjectServer principal, pendant les opérations normales. Lors d'une reprise en ligne, le serveur ObjectServer de secours prend le relais de toutes les opérations, mais la passerelle devient redondante, aucune synchronisation n'a lieu entre les serveurs ObjectServer. Pour cette raison, les directives de dimensionnement pour l'hôte A s'appliquent également à l'hôte B.
C	Coeurs : 2 pour chaque sonde Mémoire RAM : 2 Go pour chaque sonde	Allouez 2 coeurs à chaque sonde afin de réduire le risque de goulots d'étranglement. Si vos attentes de trafic réseau indiquent que les deux sondes sont peu susceptibles de récupérer des événements simultanément, réduisez le nombre de coeurs. Allouez une quantité importante de mémoire de sorte que les sondes peuvent être mises en mémoire tampon, si nécessaire.

Tableau 6. Recommandations de dimensionnement pour un petit système Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
D	Coeurs : 2 Mémoire RAM : 4 Go	Cette instruction est appropriée pour 30 à 40 utilisateurs simultanés. Si vous avez besoin d'un plus grand nombre d'utilisateurs de l'Interface graphique Web, augmentez le nombre de coeurs.

Ce système n'est pas approprié si vous prévoyez un débit élevé d'événements. Etant donné que le système utilise uniquement un serveur ObjectServer et un hôte unique pour les sondes, un goulot d'étranglement de processeur peut se produire sur ce système. Si le sondes sont soumises à un déferlement d'événements, l'hôte A et l'hôte C sont menacés. Un déferlement d'événements peut être une rafale d'événements extraits par une sonde après 30 secondes, à un débit supérieur à 400 par seconde. Un déferlement d'événements augmente la charge sur le processeur et le nombre d'événements résidant sur le serveur ObjectServer. Le risque augmente si plusieurs utilisateurs de l'Interface graphique Web affichent des pages contenant un nombre élevé d'événements, en raison de la charge supplémentaire placée sur le serveur ObjectServer.

Système moyen

Ce système est conçu pour des performances supérieures à celles d'un petit système, avec une haute disponibilité et des fonctions d'archivage pour les événements, et la visualisation des événements sur les navigateurs Web. Il se compose d'un serveur ObjectServer de collecte pour gérer les événements entrants provenant de sondes, de plusieurs sondes TCP/IP qui écoutent des événements sur le réseau, d'une passerelle ObjectServer unidirectionnelle qui transmet les événements du serveur ObjectServer de collecte vers la paire d'agrégation dans une connexion unique, d'une sonde SYSLOG qui envoie des événements sur le réseau, d'une paire de reprise en ligne de serveurs ObjectServer d'agrégation qui sont connectés par une passerelle ObjectServer bidirectionnelle pour synchroniser les données entre les serveurs ObjectServer, d'une base de données tierce distante, d'une passerelle ObjectServer unidirectionnelle qui archive les événements à partir de la paire de reprise en ligne de serveurs ObjectServer et transfère l'événement à la base de données, ainsi que d'un serveur d'Interface graphique Web qui est utilisé pour visualiser des événements dans la paire de serveurs ObjectServer.

Ce système est installé sur six hôtes, comme suit :

- Hôte A pour le serveur ObjectServer principal
- Hôte B pour le serveur ObjectServer de secours et la passerelle ObjectServer bidirectionnelle
- Hôte C pour les sondes de surveillance, la collecte ObjectServer et une passerelle ObjectServer unidirectionnelle
- Hôte D pour le serveur de l'Interface graphique Web
- Hôte E pour la sonde SYSLOG
- Hôte F pour la base de données tierce et la passerelle ObjectServer unidirectionnelle d'archivage

Dans ce système, le serveur ObjectServer de collecte réduit la charge sur le serveur ObjectServer principal en traitant les opérations d'écriture simultanées provenant des sondes. Les événements sont transmis en tant que connexion unique à partir de la collection ObjectServer vers le serveur ObjectServer principal via une passerelle unidirectionnelle. Par conséquent, les opérations d'écriture simultanées sur le serveur ObjectServer principal sont minimes, car la charge principale est constituée d'opérations de lecture à partir de la passerelle bidirectionnelle, de la passerelle unidirectionnelle d'archivage et de l'Interface graphique Web. L'Interface graphique Web génère des opérations d'écriture lorsque les utilisateurs modifient des événements.

Le tableau suivant répertorie les recommandations de dimensionnement pour ce système.

Tableau 7. Recommandations de dimensionnement pour un système moyen Tivoli Netcool/OMNIbus

Hôte	**Recommandations de dimensionnement**	**Explication**
A	Coeurs : 2 Mémoire RAM : 4 Go	Envisagez plus de 2 nœuds dans les cas suivants : • La capacité de l'hôte est faible. • Vous prévoyez un nombre élevé d'événements devant résider dans le serveur ObjectServer principal, par exemple, supérieur à 50 000. • Vous prévoyez un nombre élevé d'utilisateurs simultanés de l'Interface graphique Web, par exemple, supérieur à 40.
B	Coeurs : 2 Mémoire RAM : 4 Go	Bien que les deux composants s'exécutent sur cet hôte, le serveur ObjectServer de secours n'est pas soumis à la même charge que le serveur ObjectServer principal, pendant les opérations normales. Lors d'une reprise en ligne, le serveur ObjectServer de secours prend le relais de toutes les opérations, mais la passerelle devient redondante, aucune synchronisation n'a lieu entre les serveurs ObjectServer. Pour cette raison, les directives de dimensionnement pour l'hôte A s'appliquent également à l'hôte B.

Tableau 7. Recommandations de dimensionnement pour un système moyen Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
C	Coeurs : 6 Mémoire RAM : 8 Go	Les coeurs sont attribués comme suit : • 2 pour le serveur ObjectServer • 4 partagés entre la passerelle unidirectionnelle et 2 sondes La mémoire RAM est attribuée comme suit : • 4 Go pour le serveur ObjectServer • 4 Go partagés entre la passerelle unidirectionnelle et 2 sondes Bien que quatre composants soient installés sur cet hôte, il est peu probable que tous les composants auront une charge de traitement élevée simultanément. Alors que 6 coeurs sont suffisants, si vous prévoyez un débit faible d'événements, envisagez de revenir à quatre coeurs. Allouez une quantité importante de mémoire de sorte que les sondes peuvent être mises en mémoire tampon, si nécessaire.
D	Coeurs : 2 Mémoire RAM : 4 Go	Cette instruction est appropriée pour 30 à 40 utilisateurs simultanés. Si vous avez besoin d'un plus grand nombre d'utilisateurs de l'Interface graphique Web, augmentez le nombre de coeurs.
E	Coeurs : 1 pour chaque sonde Mémoire RAM : 2 Go pour chaque sonde	Les sondes qui se connectent à une cible ou lisent un fichier journal utilisent moins d'UC que les sondes d'écoute. Conservez de la capacité sur l'hôte pour l'application surveillée par la sonde.

Tableau 7. Recommandations de dimensionnement pour un système moyen Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
F	Coeurs : 2 Mémoire RAM : 4 Go	Les passerelles qui se connectent aux bases de données utilisent plus de mémoire que les passerelles ObjectServer, parce qu'elles ont de grandes quantités de données et parce que la méthode de connexion à la base de données cible peut être très consommatrice de mémoire.

Grand système

Ce système est conçu pour la capture d'événements hautes performances, la visualisation de sites multiples, c'est-à-dire des sources de données, des fonctions à haute disponibilité sur la couche collecte et la couche agrégation, des fonctions d'archivage des événements et la visualisation d'événements sur des navigateurs Web. Le système peut traiter un débit élevé d'événements et un grand nombre de clients d'affichage. Il inclut les composants suivants :

- Paire de reprise en ligne de serveurs ObjectServer de collecte qui gèrent les événements entrants provenant des sondes
- Sondes TCP/IP et sondes SYSLOG
- Paire de reprise en ligne de serveurs ObjectServer d'agrégation, qui sont connectés par une passerelle ObjectServer bidirectionnelle pour synchroniser les données entre les serveurs ObjectServer
- Passerelles ObjectServer unidirectionnelles pour transmettre des événements de la paire de collecte à la paire d'agrégation
- Serveur ObjectServer d'affichage qui gère les clients d'affichage, telles que l'Interface graphique Web
- Passerelle unidirectionnelle permettant de transmettre des événements de la paire d'agrégation au serveur d'affichage ObjectServer
- Base de données tierce distante et passerelle ObjectServer unidirectionnelle qui archive les événements à partir de la paire d'agrégation et transfère l'événement à la base de données
- Serveur de l'Interface graphique Web qui est utilisé pour visualiser les événements dans la paire d'agrégation et afficher les événements à partir d'un serveur ObjectServer distant ou d'une paire de serveurs ObjectServer.

Ce système est installé sur neuf hôtes, comme suit :

- Hôte A pour le serveur ObjectServer d'agrégation principal
- Hôte B pour le serveur ObjectServer d'agrégation de secours et la passerelle ObjectServer bidirectionnelle
- Hôte C pour le serveur ObjectServer de collecte principal et une passerelle ObjectServer unidirectionnelle
- Hôte D pour le serveur ObjectServer de collecte de secours et une passerelle ObjectServer unidirectionnelle

- Hôte E pour le serveur ObjectServer d'affichage et une passerelle ObjectServer unidirectionnelle
- Hôte F pour le serveur de l'Interface graphique Web
- Hôte G pour les sondes d'écoute
- Hôte H pour la sonde SYSLOG
- Hôte I pour la base de données tierce et la passerelle ObjectServer unidirectionnelle d'archivage

Dans ce système, le serveur ObjectServer de collecte principal gère les opérations d'écriture simultanées à partir des sondes afin de réduire la charge sur le serveur ObjectServer d'agrégation principal. Les sondes sont configurées pour effectuer une reprise en ligne sur le serveur ObjectServer de collecte de secours en cas de défaillance du serveur ObjectServer de collecte principal. La plus grande partie de la charge du serveur ObjectServer d'agrégation principal est constituée d'opérations de lecture à partir de la passerelle bidirectionnelle, de la passerelle unidirectionnelle d'archivage et de la passerelle unidirectionnelle vers le serveur ObjectServer d'affichage. Le serveur d'affichage ObjectServer gère les opérations de lecture et d'écriture à partir de clients d'affichage afin de réduire la charge sur le serveur d'agrégation ObjectServer principal. Dans cet exemple, les clients d'affichage sont des clients de l'Interface graphique Web et des clients de composant de bureau. Si le mode d'écriture double est configuré, les mises à jour d'événements à partir des clients de l'Interface graphique Web sont effectuées dans le serveur ObjectServer d'affichage et le serveur ObjectServer d'agrégation principal. L'Interface graphique Web est configurée pour gérer plusieurs sources de données, de sorte qu'elle peut gérer des événements à partir du serveur ObjectServer d'affichage et du serveur ObjectServer distant dans la même vue.

Tableau 8. Recommandations de dimensionnement pour un grand système Tivoli Netcool/OMNIbus

Hôte	**Recommandations de dimensionnement**	**Explication**
A	Coeurs : 4 Mémoire RAM : 4 Go	Etant donné que ce système est supérieur à celui de l'exemple précédent et qu'il prend en charge un plus grand nombre d'événements, davantage de coeurs sont nécessaires. Si vous utilisez moins de coeurs, le système risque d'être endommagé au cours des opérations de reprise en ligne et de reprise par restauration.

Tableau 8. Recommandations de dimensionnement pour un grand système Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
B	Coeurs : 4 Mémoire RAM : 4 Go	Bien que les deux composants s'exécutent sur cet hôte, le serveur ObjectServer de secours n'est pas soumis à la même charge que le serveur ObjectServer principal, pendant les opérations normales. Lors d'une reprise en ligne, le serveur ObjectServer de secours prend le relais de toutes les opérations, mais la passerelle devient redondante, aucune synchronisation n'a lieu entre les serveurs ObjectServer. Pour cette raison, les directives de dimensionnement pour l'hôte A s'appliquent également à l'hôte B.
C	Coeurs : 3 Mémoire RAM : 6 Go	Les coeurs sont attribués comme suit : • 2 pour le serveur ObjectServer de collecte principal • 1 pour la passerelle unidirectionnelle La mémoire RAM est attribuée comme suit : • 4 Go pour le serveur ObjectServer de collecte principal • 2 Go pour la passerelle unidirectionnelle Bien que deux composants soient installés sur cet hôte, il est peu probable que tous les composants auront une charge de traitement élevée simultanément.

Tableau 8. Recommandations de dimensionnement pour un grand système Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
D	Coeurs : 3 Mémoire RAM : 6 Go	Les coeurs sont attribués comme suit : • 2 pour le serveur ObjectServer de collecte de secours • 1 pour la passerelle unidirectionnelle La mémoire RAM est attribuée comme suit : • 4 Go pour le serveur ObjectServer de collecte principal • 2 Go pour la passerelle unidirectionnelle Les recommandations de dimensionnement pour cet hôte sont identiques à celles de l'hôte C.
E	Coeurs : 5 Mémoire RAM : 6 Go	Les coeurs sont attribués comme suit : • 4 pour le serveur d'affichage ObjectServer • 1 pour la passerelle unidirectionnelle La mémoire RAM est attribuée comme suit : • 4 Go pour le serveur ObjectServer de collecte principal • 2 Go pour la passerelle unidirectionnelle Etant donné que ce système est supérieur à celui des exemples précédents et qu'il prend en charge un plus grand nombre de clients d'affichage, davantage de coeurs sont nécessaires. Si seuls les clients de l'Interface graphique Web se connectent au serveur d'affichage ObjectServer, c'est-à-dire si aucun client de bureau ne s'y connecte, envisagez de réduire le nombre de coeurs. Allouez une grande quantité de mémoire.

Tableau 8. Recommandations de dimensionnement pour un grand système Tivoli Netcool/OMNIbus (suite)

Hôte	Recommandations de dimensionnement	Explication
F	Coeurs : 4 Mémoire RAM : 4 Go	Ces recommandations concernent un grand nombre de clients d'affichage, par exemple, plus de 40 utilisateurs de l'Interface graphique Web.
G	Coeurs : 2 pour chaque sonde Mémoire RAM : 2 Go pour chaque sonde	Allouez 2 coeurs à chaque sonde afin de réduire le risque de goulots d'étranglement. Si vos attentes de trafic réseau indiquent que les deux sondes sont peu susceptibles de récupérer des événements simultanément, vous pouvez réduire le nombre de coeurs. Allouez une quantité importante de mémoire de sorte que les sondes peuvent être mises en mémoire tampon, si nécessaire.
H	Coeurs : 1 pour chaque sonde Mémoire RAM : 2 Go pour chaque sonde	Les sondes qui se connectent à une cible ou lisent un fichier journal utilisent moins d'UC que les sondes d'écoute. Conservez de la capacité sur l'hôte pour l'application surveillée par la sonde.
I	Coeurs : 2 Mémoire RAM : 4 Go	Les passerelles qui se connectent aux bases de données utilisent plus de mémoire que les passerelles ObjectServer, parce qu'elles ont de grandes quantités de données et parce que la méthode de connexion à la base de données cible peut être très consommatrice de mémoire.

Exigences d'espace disque

Vérifiez que l'espace disque disponible est suffisant sur le volume pour le système d'exploitation sur lequel vous installez Tivoli Netcool/OMNIbus.

Composants non Web

Le tableau suivant présente l'espace disque d'installation obligatoire sur chaque système d'exploitation. Ces figures sont basées sur la supposition selon laquelle une installation complète des fonctions est exécutée, avec les spécifications suivantes :

- Quatre installations de sonde

- Des passerelles du serveur ObjectServer uniquement
- Des bases de données du serveur ObjectServer peu volumineuses, contenant de 50 à 100 événements

Tableau 9. Espace disque d'installation

Système d'exploitation	Installation Manager	Emplacement partagé de Installation Manager	Emplacement des données de Installation Manager	Tivoli Netcool/ OMNIbus (NCHOME)
AIX	215 Mo	340 Mo	10 Mo	765 Mo
HP-UX Integrity	315 Mo	215 Mo	5 Mo	530 Mo
Linux	200 Mo	330 Mo	5 Mo	620 Mo
Linux on System z	170 Mo	290 Mo	4 Mo	525 Mo
Solaris	250 Mo	310 Mo	5 Mo	780 Mo

UNIX Linux Lors de l'installation de Tivoli Netcool/OMNIbus, au moins 2 Mo d'espace libre sont nécessaires dans `/tmp`. Si d'autres produits sont installés dans le cadre de votre autorisation d'utilisation, davantage d'espace sera nécessaire. Vous pouvez modifier le répertoire utilisé avec la variable d'environnement `$TMPDIR`.

Interface graphique Web

Une installation complète de l'Interface graphique Web exige un espace disque minimum de 2 Go et une mémoire système minimale de 1 Go.

En fonction de votre installation, il se peut que vous deviez posséder au moins 2 Go d'espace disque supplémentaire et 2 Go de mémoire système.

Le répertoire d'installation de l'Interface graphique Web requiert 1 Go d'espace disque. Le répertoire temporaire dans `/tmp` ou `C:\temp` requiert 500 Mo d'espace disponible.

Si vous prévoyez d'effectuer une installation en tant qu'utilisateur non-root, le répertoire de base dans `/home/`*`nom d'utilisateur`* requiert 300 Mo d'espace disponible. En outre, vous devez vérifier que vous disposez d'un espace mémoire de permutation d'une taille adéquate disponible sur le serveur exécutant l'Interface graphique Web.

IBM Prerequisite Scanner

IBM Prerequisite Scanner est un outil de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit IBM.

Vous pouvez exécuter Prerequisite Scanner en tant qu'application autonome avant d'installer Tivoli Netcool/OMNIbus.

Vous pouvez télécharger Prerequisite Scanner du site Web IBM Fix Central. L'URL suivante mène directement à la page Select Fixes sur IBM Fix Central :

http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=ibm~Tivoli&product=ibm/Tivoli/Prerequisite+Scanner&release=All&platform=All&function=all

Reportez-vous à la note technique suivante pour plus d'informations sur l'utilisation de Prerequisite Scanner avec Tivoli Netcool/OMNIbus :

http://www.ibm.com/support/docview.wss?uid=swg21472859

Tâches associées:

«Installation de Tivoli Netcool/OMNIbus (interface graphique)», à la page 73
Installation de Tivoli Netcool/OMNIbus à partir de l'interface graphique Installation Manager.

«Installation de Tivoli Netcool/OMNIbus (console)», à la page 78
Installation de Tivoli Netcool/OMNIbus à partir de la console Installation Manager.

«Installation de Tivoli Netcool/OMNIbus (mode silencieux)», à la page 82
Vous pouvez installer Tivoli Netcool/OMNIbus en mode silencieux. Cette méthode d'installation est utile si vous souhaitez des configurations d'installation identiques sur plusieurs postes de travail. L'installation silencieuse nécessite un fichier de réponse qui définit la configuration de l'installation.

Obtention du module d'installation

Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

La distribution du fichier compressé contient IBM Installation Manager. Utilisez cette option lorsque vous souhaitez installer Tivoli Netcool/OMNIbus sur un petit nombre d'ordinateurs, ou si vous devez installer Tivoli Netcool/OMNIbus sans accès à Internet et que vous ne souhaitez pas gérer votre propre référentiel de logiciels IBM.

Alternativement, vous pouvez installer IBM Installation Manager séparément et l'utiliser pour télécharger et installer Tivoli Netcool/OMNIbus à partir d'un référentiel IBM ou à partir d'un référentiel local sur votre réseau. Utilisez cette option lorsque vous souhaitez installer ou mettre à jour à la dernière version du logiciel sans avoir à copier les fichiers compressés sur chaque ordinateur. À moins que chaque ordinateur ait un accès à Internet, vous aurez à conserver un ou plusieurs référentiels de logiciels. Voir la section suivante IBM Knowledge Center pour plus d'informations sur l'utilisation de IBM Installation Manager pour Enterprise Deployment et Installation Manager Packaging Utility :

http://www.ibm.com/support/knowledgecenter/SSDV2W_1.0.0/com.ibm.im.articles.doc/topics/entdeployment.htm

Procédure

1. Pour télécharger le produit, suivez les instructions du document à télécharger suivant :

   http://www.ibm.com/support/docview.wss?&uid=swg24037620
2. Extrayez le contenu du package d'installation vers un emplacement temporaire.

Que faire ensuite

Une fois ces tâches effectuées, vous pouvez exécuter le programme d'installation pour effectuer une nouvelle installation de Tivoli Netcool/OMNIbus ou pour mettre à niveau votre version existante.

Tâches associées:

«Mise à niveau à partir d'IBM Tivoli Netcool/Webtop version 2.2 ou de l'Interface graphique Web version 7.3.0», à la page 167
Pour mettre à niveau Netcool/Webtop version 2.2 ou l'Interface graphique Web version 7.3.0 vers l'Interface graphique Web version 8.1, mettez à niveau l'interface utilisateur Web vers la version 7.4, puis mettez à niveau vers l'Interface graphique Web version 8.1.

IBM Installation Manager

IBM Installation Manager est un outil permettant d'installer, de modifier, de mettre à jour et de désinstaller des produits IBM. Vous utiliserez IBM Installation Manager pour installer ou mettre à jour Tivoli Netcool/OMNIbus V8.1.

Remarque : La distribution de fichier compressé de Tivoli Netcool/OMNIbus qui est disponible sur IBM Passport Advantage et sur le DVD inclut IBM Installation Manager. Il vous suffit de télécharger Installation Manager séparément si vous installez Tivoli Netcool/OMNIbus directement à partir d'un référentiel IBM ou à partir d'un référentiel local.

Pour tout détail concernant le téléchargement et l'installation de Installation Manager, voir http://www.ibm.com/support/docview.wss?uid=swg24034941.

Pour tout détail concernant l'utilisation de Installation Manager, voir http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Présentation d'IBM Installation Manager

Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

Pour plus d'informations sur l'installation et l'utilisation d'Installation Manager, voir le centre de documentation IBM suivant :

http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Remarque : La distribution de fichier compressé de Tivoli Netcool/OMNIbus qui est disponible sur IBM Passport Advantage et sur le DVD inclut IBM Installation Manager. Il vous suffit de télécharger Installation Manager séparément si vous installez Tivoli Netcool/OMNIbus directement à partir d'un référentiel IBM ou à partir d'un référentiel local.

Modes utilisateur

Vous pouvez installer Installation Manager selon l'un des trois modes utilisateur : Mode administrateur, Mode non-administrateur ou Mode groupe. Les modes utilisateur déterminent qui peut exécuter Installation Manager, où les données sur les produits sont stockées et comment les différents produits sont gérés.

Si vous avez obtenu la distribution de fichier compressé de Tivoli Netcool/OMNIbus, vous pouvez installerInstallation Manager et Tivoli Netcool/OMNIbus en même temps avec l'un des scripts d'encapsuleur prévus : `install_gui.sh`, `install_console.sh`, ou `install_silent.sh`. Ces scripts sélectionnent automatiquement Mode administrateur quand ils sont exécutés par un utilisateur root ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root. Si vous souhaitez utiliser Mode groupe, ous devez installer manuellement Installation Manager avec la commande `groupinst` ou `groupinstc`.

Remarque : L'installation de Installation Manager dans Mode non-administrateur ou Mode groupe n'est pas prise en charge sur les systèmes d'exploitation Windows.

Le tableau suivant décrit la façon dont fonctionne chaque mode utilisateur.

Tableau 10. Modes utilisateur Installation Manager

Mode utilisateur	Description
Mode administrateur	Dans Mode administrateur, un administrateur ou utilisateur root peuvent installer une instance de Installation Manager. Les informations sur tous les produits gérés par cette instance sont stockées dans un répertoire de données unique. UNIX Linux Mode administrateur requiert des droits root. Les utilisateurs root peuvent installer plusieurs instances de Tivoli Netcool/OMNIbus. Windows Mode administrateur requiert des droits d'administrateur. Un administrateur par ordinateur peut installer une seule instance de Tivoli Netcool/OMNIbus par ordinateur.
Mode non-administrateur	Dans Mode non-administrateur, chaque compte d'utilisateur peut installer une seule instance de Installation Manager. Les informations sur tous les produits gérés par cette instance sont stockées dans un répertoire de données unique. Chaque compte utilisateur peut installer plusieurs instances de Tivoli Netcool/OMNIbus.
Mode groupe	Dans Mode groupe, vous pouvez installer un nombre illimité d'instances de Installation Manager. Chaque instance nécessite un répertoire de données différent. Tous les membres d'un groupe peuvent utiliser chaque instance. Installation Manager règle automatiquement les permissions de fichiers afin que tous les membres du groupe puissent mettre à jour l'installation.

Répertoires par défaut

L'installation, les données et les répertoires partagés par défaut sont différents selon le mode utilisateur que vous utilisez. Le répertoire de données est utilisé pour stocker les informations sur les produits qui sont installés avec Installation Manager. Le répertoire partagé est utilisé pour stocker les artefacts d'installation qui peuvent être utilisés ou réutilisés par un ou plusieurs produits.

Tableau 11. Répertoires par défaut : systèmes d'exploitation UNIX et Linux

Mode utilisateur	Répertoire d'installation par défaut	Répertoire de données par défaut	Répertoire partagé par défaut
Mode administrateur	`/opt/ibm/InstallationManager/eclipse`	`/var/ibm/InstallationManager`	`/opt/ibm/IBMIMShared`
Mode non-administrateur	`$HOME/IBM/InstallationManager/eclipse`	`$HOME/var/ibm/InstallationManager`	`$HOME/IBM/IBMIMShared`
Mode groupe	`$HOME/IBM/InstallationManager_Group/eclipse`	`$HOME/var/ibm/InstallationManager_Group`	`$HOME/IBM/IBMIMShared`

Tableau 12. Répertoires par défaut : systèmes d'exploitation Windows

Mode utilisateur	Répertoire d'installation par défaut	Répertoire de données par défaut	Répertoire partagé par défaut
Mode administrateur	32-bit `C:\Program Files\IBM\Installation Manager` 64-bit `C:\Program Files (x86)\IBM\Installation Manager`	`C:\ProgramData\IBM\Installation Manager`	32-bit `C:\Program Files\IBM\IBMIMShared` 64-bit `C:\Program Files (x86)\IBM\IBMIMShared`
Mode non-administrateur	`C:\Users\`*`utilisateur`*`\IBM\Installation Manager`	`C:\Users\`*`utilisateur`*`\AppData\Roaming\IBM\Installation Manager`	`C:\Users\`*`utilisateur`*`\IBM\IBMIMShared`

Tâches associées:

«Installation de Installation Manager (interface graphique ou console)», à la page 36
Vous pouvez installer IBM Installation Manager avec une interface graphique de type assistant ou une console interactive.

«Installation de Installation Manager (mode silencieux)», à la page 39
Vous pouvez installer IBM Installation Manager en mode silencieux. Ceci est utile si vous voulez des configurations d'installation identiques sur plusieurs postes de travail. Vous pouvez également utiliser un fichier de réponses pour définir la configuration de l'installation, si nécessaire.

Obtention de Installation Manager

IBM Installation Manager est disponible pour téléchargement à partir du site Web IBM Fix Central.

Remarque : La distribution de fichier compressé de Tivoli Netcool/OMNIbus qui est disponible sur IBM Passport Advantage et sur le DVD inclut IBM Installation Manager. Il vous suffit de télécharger Installation Manager séparément si vous installez Tivoli Netcool/OMNIbus directement à partir d'un référentiel IBM ou à partir d'un référentiel local.

Avant de commencer

Vous devez avoir un ID IBM pour télécharger le logiciel de IBM Fix Central. Vous pouvez vous inscrire pour un ID IBM à l'adresse http://www.ibm.com.

Consultez le document de téléchargement ci-dessous pour plus d'informations sur le téléchargement et l'installation d'IBM Installation Manager :

http://www.ibm.com/support/docview.wss?uid=swg24034941

Pourquoi et quand exécuter cette tâche

Le site Web IBM Fix Central propose deux approches pour trouver les fichiers de produit : **Select product** et **Find product**. Les instructions suivantes s'appliquent à l'option **Find product**.

Procédure

1. Ouvrez le site Web IBM Fix Central à l'adresse URL suivante :
   http://www.ibm.com/support/fixcentral/
2. Dans l'onglet **Find product** :
   a. Entrez IBM Installation Manager dans la zone **Product selector**.
   b. Sélectionnez 1.7.2.0 dans la liste **Installed Version**.
   c. Sélectionnez votre système d'exploitation hôte prévu dans la liste **Platform** et cliquez sur **Continue**.
3. Dans la page Identity Fixes, sélectionnez **Browse for fixes** et **Show fixes that apply to this version (1.X.X.X)**. Cliquez sur **Continue**.
4. Dans la page Select Fixes, sélectionnez le fichier d'installation correspondant à votre système d'exploitation hôte prévu et cliquez sur **Continue**.
5. Lorsque vous y êtes invité, saisissez votre nom d'utilisateur et votre mot de passe IBM.
6. Si votre navigateur est compatible Java, sélectionnez l'option Download Director. Sinon, sélectionnez l'option de téléchargement HTTP.
7. Lancer le téléchargement du fichier d'installation. Prenez note de l'emplacement de téléchargement.

Que faire ensuite

Installez Installation Manager.

Fichiers de réponses Installation Manager

Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Les fichiers de réponse Installation Manager sont des fichiers XML qui contiennent la configuration d'installation de votre scénario d'installation. Vous pouvez utiliser les méthodes suivantes pour créer un fichier de réponses :

- Créez manuellement un fichier de réponses.
- Utilisez l'option Installation Manager `-record` pour enregistrer un fichier de réponses. Cette option exécute une installation graphique et enregistre votre configuration choisie dans un fichier de réponses.
- Utilisez l'option Installation Manager `-skipInstall` avec l'option `-record` pour enregistrer un fichier de réponses sans réellement installer Tivoli

Netcool/OMNIbus. Cette option enregistre la configuration de votre installation prévue mais ne réalise pas l'installation du produit.

- Lorsque vous installez Tivoli Netcool/OMNIbus avec la console Installation Manager, choisissez de créer un fichier de réponses pour une réutilisation dans d'autres installations.

Pour plus d'informations sur la création et le déploiement de fichiers de réponses, consultez le centre de documentation IBM suivant :

http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

L'exemple suivant montre un fichier de réponses de base Tivoli Netcool/OMNIbus :

```
<?xml version="1.0" encoding="UTF-8"?>

<agent-input clean='true' temporary='false'>

 <profile id='IBM Tivoli Netcool OMNIbus' installLocation='/opt/ibm/tivoli/
netcool/omnibus'/>

 <server>
  <repository location='/home/repos/omnibus/repository/repository.config'/>
 </server>

 <install modify='false'>
  <offering id='com.ibm.tivoli.omnibus.core'/>
 </install>

</agent-input>
```

Installation de Installation Manager (interface graphique ou console)

Vous pouvez installer IBM Installation Manager avec une interface graphique de type assistant ou une console interactive.

Remarque : La distribution de fichier compressé de Tivoli Netcool/OMNIbus qui est disponible sur IBM Passport Advantage et sur le DVD inclut Installation Manager. Les scripts sont fournis qui installent Installation Manager et Tivoli Netcool/OMNIbus simultanément. La procédure décrite ici n'est nécessaire que si vous souhaitez installer Tivoli Netcool/OMNIbus directement d'un référentiel de logiciels IBM ou local, ou si vous voulez utiliser Installation Manager Mode groupe.

Avant de commencer

Effectuez les actions suivantes :

- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin.
- Extrayez le contenu du fichier d'installation Installation Manager dans un répertoire temporaire approprié.
- Veillez à ce que les autorisations utilisateur nécessaires soient en place pour les répertoires d'installation, de données et partagés.
- Le programme d'installation de la console ne signale pas l'espace disque requis. Assurez-vous que vous avez suffisamment d'espace libre avant de commencer l'installation à partir de la console.

Pourquoi et quand exécuter cette tâche

Les étapes d'installation initiales sont différentes selon le mode utilisateur que vous utilisez. Les étapes pour réaliser l'installation sont communes à tous les modes d'utilisateur et les systèmes d'exploitation.

Windows Vous devez installer Installation Manager en tant qu'utilisateur administrateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. Pour installer dans Mode administrateur :
   a. UNIX Linux Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
   b. UNIX Linux Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   c. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.
   d. Utilisez la commande suivante pour lancer l'installation :

      Installation par le biais de l'interface graphique

      - UNIX Linux `./install`
      - Windows `installation`

      Installation en mode console

      - UNIX Linux `./installc -c`
      - Windows `installc -c`

      Si nécessaire, utilisez l'option `-dL` pour spécifier un répertoire de données autre que le répertoire de données par défaut.
2. UNIX Linux Pour installer dans Mode non-administrateur :
   a. Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.
   c. Utilisez la commande suivante pour lancer l'installation :

      Installation par le biais de l'interface graphique

      ```
      ./userinst
      ```

      Installation en mode console

      ```
      ./userinstc -c
      ```

      Si nécessaire, utilisez l'option `-dL` pour spécifier un répertoire de données autre que le répertoire de données par défaut.
3. UNIX Linux Pour installer dans Mode groupe :

a. Utilisez l'utilitaire **id** pour vérifier que votre groupe utilisateur effectif est adapté à l'installation. Si nécessaire, utilisez la commande suivante pour lancer un nouveau shell avec le groupe effectif correct :

   ```
   newgrp nom_groupe
   ```

b. Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.

c. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.

d. Utilisez la commande suivante pour lancer l'installation :

   Installation par le biais de l'interface graphique

   ```
   ./groupinst -dL emplacement_données
   ```

   Installation en mode console

   ```
   ./groupinstc -c -dL emplacement_données
   ```

   Où *emplacement_données* spécifie le répertoire de données. Vous devez spécifier un répertoire de données auquel tous les membres du groupe peuvent accéder. Chaque instance de Installation Manager nécessite un répertoire de données différent.

4. Suivez les instructions du programme d'installation pour terminer l'installation. Le programme d'installation nécessite l'entrée suivante à différentes étapes de l'installation :

   Installation par le biais de l'interface graphique

   - Dans le premier volet, sélectionnez le package `Installation Manager`.
   - Lisez et acceptez le contrat de licence.
   - Lorsque vous y êtes invité(e), entrez un répertoire d'installation ou acceptez le répertoire par défaut.
   - Vérifiez que la taille totale de l'installation ne dépasse pas l'espace disque disponible.
   - A l'invite, redémarrez Installation Manager.

   Installation en mode console

   - Lisez et acceptez le contrat de licence.
   - Lorsque vous y êtes invité(e), entrez un répertoire d'installation ou acceptez le répertoire par défaut.
   - Si nécessaire, générez un fichier de réponses. Entrez le chemin du répertoire et un nom de fichier avec une extension `.xml`. Le fichier de réponses est généré avant que l'installation soit terminée.
   - A l'invite, redémarrez Installation Manager.

Résultats

Installation Manager est installé et peut maintenant être utilisé pour installer Tivoli Netcool/OMNIbus.

Que faire ensuite

Si nécessaire, ajoutez le chemin du répertoire d'installation Installation Manager à votre variable d'environnement `PATH`.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant

l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

Installation de Installation Manager (mode silencieux)

Vous pouvez installer IBM Installation Manager en mode silencieux. Ceci est utile si vous voulez des configurations d'installation identiques sur plusieurs postes de travail. Vous pouvez également utiliser un fichier de réponses pour définir la configuration de l'installation, si nécessaire.

Remarque : La distribution de fichier compressé de Tivoli Netcool/OMNIbus qui est disponible sur IBM Passport Advantage et sur le DVD inclut Installation Manager. Les scripts sont fournis qui installent Installation Manager et Tivoli Netcool/OMNIbus simultanément. La procédure décrite ici n'est nécessaire que si vous souhaitez installer Tivoli Netcool/OMNIbus directement d'un référentiel de logiciels IBM ou local, ou si vous voulez utiliser Installation Manager Mode groupe.

Avant de commencer

Effectuez les actions suivantes :

- Déterminez le mode utilisateur Installation Manager dont vous avez besoin.
- Extrayez le contenu du fichier d'installation Installation Manager dans un répertoire temporaire approprié.
- Lisez le contrat de licence. Le fichier du contrat de licence, `license.txt`, est stocké dans l'archive *répertoire_temp*`/native/license_version.zip`.
- Veillez à ce que les autorisations utilisateur nécessaires soient en place pour les répertoires d'installation, de données et partagés.

Pourquoi et quand exécuter cette tâche

Windows Vous devez installer Installation Manager en tant qu'utilisateur administrateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. Pour installer dans Mode administrateur :
   a. UNIX Linux Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
   b. UNIX Linux Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   c. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.
   d. Utilisez la commande suivante pour lancer l'installation :
      - UNIX Linux `./installc -acceptLicense`
      - Windows `installc -acceptLicense`

      Où l'option `-acceptLicense` indique que vous acceptez le contrat de licence.

Si nécessaire, utilisez l'option `-dL` pour spécifier un répertoire de données autre que le répertoire de données par défaut.

2. UNIX Linux Pour installer dans Mode non-administrateur :
   a. Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.
   c. Utilisez la commande suivante pour lancer l'installation :

      ```
      ./userinstc -acceptLicense
      ```

      Où l'option `-acceptLicense` indique que vous acceptez le contrat de licence.

      Si nécessaire, utilisez l'option `-dL` pour spécifier un répertoire de données autre que le répertoire de données par défaut.
3. UNIX Linux Pour installer dans Mode groupe :
   a. Utilisez l'utilitaire **id** pour vérifier que votre groupe utilisateur effectif est adapté à l'installation. Si nécessaire, utilisez la commande suivante pour lancer un nouveau shell avec le groupe effectif correct :

      ```
      newgrp nom_groupe
      ```
   b. Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   c. Accédez au répertoire temporaire qui contient les fichiers d'installation Installation Manager.
   d. Utilisez la commande suivante pour lancer l'installation :

      ```
      ./groupinstc -dL emplacement_données -acceptLicense
      ```

      Où *emplacement_données* spécifie le répertoire de données et l'option `-acceptLicense` indique que vous acceptez le contrat de licence.

      Vous devez spécifier un répertoire de données auquel tous les membres du groupe peuvent accéder. Chaque instance de Installation Manager nécessite un répertoire de données différent.

Résultats

Installation Manager est installé et peut maintenant être utilisé pour installer Tivoli Netcool/OMNIbus.

Que faire ensuite

Si nécessaire, ajoutez le chemin du répertoire d'installation Installation Manager à votre variable d'environnement `PATH`.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

Installation d'Installation Manager pour l'interface graphique Web

Vous pouvez installer Installation Manager s'il n'est pas déjà installé ou si vous n'avez pas installé la version requise.

Avant de commencer

Vérifiez que vous avez copié et extrait le contenu du répertoire `IM` du DVD ou téléchargée l'image d'installation dans le système de fichiers local. Les versions suivantes d'Installation Manager sont disponibles :

- Windows 32 et 64 bits
- UNIX Linux 32 et 64 bits
- AIX 64 bits

Pourquoi et quand exécuter cette tâche

Sur les systèmes Linux : lorsque vous exécutez la commande Installation Manager pour la première fois, assurez-vous que vous spécifiez l'option datalocation pour l'emplacement des données d'agent. L'emplacement des données d'agent est le répertoire qu'Installation Manager utilise pour les données qui sont associées à son référentiel.

Procédure

1. Ouvrez une fenêtre de commande et choisissez l'une des options suivantes :

Option	Description
Installer Installation Manager sur un système Windows	Accédez au répertoire IM\ *nom_plateforme.im*\ et exécutez **`install`** pour installer Installation Manager en mode administrateur.
Installer Installation Manager sur un système Linux/UNIX	Accédez au répertoire IM/ *nom_plateforme.im*/ et exécutez la commande d'installation : • Mode administrateur : `./install` • Mode non administrateur : `./userinst` • Mode groupe : `./groupinst` Par exemple : `./install -dataLocation /opt/ibm/im/data` où /opt/ibm/im/data est l'emplacement de données d'agent Installation Manager.

2. La fenêtre **Installation Manager > Install Packages** apparaît. Cliquez sur **Suivant**.
3. Le panneau **Installation Manager > Licenses** s'affiche. Lisez le contrat de licence et acceptez-en les dispositions, puis cliquez sur **Suivant**.
4. Le panneau **Installation Manager > Location** s'affiche. Acceptez l'emplacement d'installation spécifié par défaut ou modifiez-le ; cliquez sur **Suivant**.
5. Le panneau **Installation Manager > Summary** s'affiche. Lisez le panneau et cliquez sur **Install**.

Systèmes d'exploitation pris en charge

Tivoli Netcool/OMNIbus est pris en charge sous différentes versions d'UNIX, de Linux et de Windows. Ces informations indiquent quels systèmes d'exploitation sont pris en charge pour quel composant du produit, quels packages doivent être installés sur votre système d'exploitation avant que vous puissiez démarrer l'installation, et si des restrictions s'appliquent.

Les systèmes d'exploitation pris en charge pour Tivoli Netcool/OMNIbus sont spécifiés sur le site Web des rapports de compatibilité des produits logiciels IBM à l'adresse http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.jsp.

Conseil : Vous pouvez créer davantage de rapports, y compris des rapports détaillés pour chaque système d'exploitation, spécifiant les navigateurs, hyperviseurs et bases de données pris en charge ainsi que les produits compatibles.

Exigences supplémentaires en termes de système d'exploitation

Vérifiez que tous les correctifs recommandés sont installés sur votre système d'exploitation, y compris les derniers niveaux de modules de correction. Les exigences pour les packages des systèmes d'exploitation et toutes les éventuelles restrictions s'appliquant à des systèmes d'exploitation spécifiques sont documentés dans les sections suivantes.

AIX

Les ensembles de fichiers suivants sont requis pour l'exécution de Tivoli Netcool/OMNIbus sur les systèmes d'exploitation AIX :

- `bos.rte.bind_cmds`
- `bos.rte.iconv`
- `bos.rte.im`
- `bos.rte.libc`
- `bos.rte.libpthreads`
- `bos.rte.loc`
- `bos.rte.mlslib`
- `bos.rte.odm`
- `bos.rte.security`
- `xlC.rte`

Les ensembles de fichiers suivants ne sont requis que par le composant Outils de bureau :

- `X11.base.common`
- `X11.base.lib`
- `X11.base.rte`
- `X11.motif.lib`

Netcool MIB Manager nécessite les modules suivants :

- `atk-1.12.3-2.aix5.2.ppc.rpm` (ou versions ultérieures)
- `cairo-1.8.8-1.aix5.2.ppc.rpm` (ou versions ultérieures)
- `expat-2.0.1-2.aix5.3.ppc.rpm` (ou versions ultérieures)

- fontconfig-2.4.2-1.aix5.2.ppc.rpm (ou versions ultérieures)
- freetype2-2.3.9-1.aix5.2.ppc.rpm (ou versions ultérieures)
- gettext-0.10.40-8.aix5.2.ppc.rpm (ou versions ultérieures)
- glib2-2.12.4-2.aix5.2.ppc.rpm (ou versions ultérieures)
- gtk2-2.10.6-5.aix5.2.ppc.rpm (ou versions ultérieures)
- libjpeg-6b-6.aix5.1.ppc.rpm (ou versions ultérieures)
- libpng-1.2.32-2.aix5.2.ppc.rpm (ou versions ultérieures)
- libtiff-3.8.2-1.aix5.2.ppc.rpm (ou versions ultérieures)
- pango-1.14.5-4.aix5.2.ppc.rpm (ou versions ultérieures)
- pixman-0.12.0-3.aix5.2.ppc.rpm (ou versions ultérieures)
- xcursor-1.1.7-3.aix5.2.ppc.rpm (ou versions ultérieures)
- xft-2.1.6-5.aix5.1.ppc.rpm (ou versions ultérieures)
- zlib-1.2.3-4.aix5.2.ppc.rpm (ou versions ultérieures)

Consultez le site Web AIX suivant pour plus de détails sur l'utilisation de RPM Package Manager pour obtenir et installer les packages requis :

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/

HP-UX Itanium

La liste d'événements du bureau n'est pas prise en charge sur HP-UX Itanium.

Netcool MIB Manager nécessite les modules suivants :

- GTK
- GNU_C_C++

Linux

Les bibliothèques pour le système d'exploitation Linux 32 bits ne sont pas installées avec Tivoli Netcool/OMNIbus. Si vous souhaitez exécuter des sondes ou des passerelles 32 bits, vous aurez peut-être besoin de bibliothèques 32 bits. Consultez la documentation relative à la sonde ou à la passerelle pour connaître la configuration requise spécifique. Vous pouvez également exécuter IBM Prerequisite Scanner avec la fonction de sonde sélectionnée afin de déterminer si vous disposez de toutes les bibliothèques nécessaires. Les bibliothèques Tivoli Netcool/OMNIbus 32 bits principales qui sont requises pour exécuter des analyses et des passerelles 32 bits (par exemple, libOpl) sont installées par défaut avec Tivoli Netcool/OMNIbus.

Remarque : Les composants serveur et sonde Tivoli Netcool/OMNIbus ne sont pas pris en charge sur les éditions de bureau de Red Hat Enterprise Linux (RHEL) ou SUSE Linux.

Les tableaux suivants décrivent les packages RPM qui sont requis pour les systèmes d'exploitation Linux.

Tableau 13. Exigences pour Red Hat Enterprise Linux (RHEL) Server 5 64 bits

RPM minimum requis	Explication et commentaires
• audit-libs-1.7.18-2.el5 (ou versions ultérieures) • expat-1.95.8-8.3.el5_5.3 (ou versions ultérieures) • fontconfig-2.4.1-7.el5 (ou versions ultérieures) • freetype-2.2.1-28.el5_7.2 (ou versions ultérieures) • glibc-2.5-65.el5_7.1 (ou versions ultérieures) • libICE-1.0.1-2.1 (ou versions ultérieures) • libSM=libSM-1.0.1-3.1 (ou versions ultérieures) • libgcc-4.1.2-51.el5 (ou versions ultérieures) • libidn-0.6.5-1.1.el5 (ou versions ultérieures) • libjpeg-6b-37 (ou versions ultérieures) • libpng-1.2.10-7.1.el5_7.5 (ou versions ultérieures) • libstdc++-4.1.2-51.el5 (ou versions ultérieures) • pam-0.99.6.2-6.el5_5.2 (ou versions ultérieures) • zlib-1.2.3-4.el5 (ou versions ultérieures) Les packages suivants sont requis uniquement par le composant Outils de bureau : • libX11-1.0.3-11.el5_7.1 • libXau-1.0.1-3.1 (ou versions ultérieures) • libXdmcp-1.0.1-2.1 (ou versions ultérieures) • libXext-1.0.1-2.1 (ou versions ultérieures) • libXft-2.1.10-1.1 (ou versions ultérieures) • libXmu-1.0.2-5 (ou versions ultérieures) • libXp-1.0.0-8.1.el5 (ou versions ultérieures) • libXpm-3.5.5-3 (ou versions ultérieures) • libXrender-0.9.1-3.1 (ou versions ultérieures) • libXt-1.0.2-3.2.el5 (ou versions ultérieures) • openmotif-2.3.1-6.1.el5_8 (ou versions ultérieures) Le package suivant est requis par Netcool MIB Manager : • gtk2-2.10.4-21.el5_5.6 (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • compat-libstdc++-33-3.2.3-61 (ou versions ultérieures)

Tableau 14. Exigences pour Red Hat Enterprise Linux (RHEL) Server 6 64 bits

RPM minimum requis	Explication et commentaires
• audit-libs-2.0.4-1.el6.x86_64 (ou versions ultérieures) • expat-2.0.1-9.1.el6.x86_64 (ou versions ultérieures) • fontconfig-2.8.0-3.el6.x86_64 (ou versions ultérieures) • freetype-2.3.11-5.el6.x86_64 (ou versions ultérieures) • glibc-2.12-1.7.el6.x86_64 (ou versions ultérieures) • libICE-1.0.6-1.el6.x86_64 (ou versions ultérieures) • libSM-1.1.0-7.1.el6.x86_64 (ou versions ultérieures) • libgcc-4.4.4-13.el6.x86_64 (ou versions ultérieures) • libidn-1.18-2.el6.x86_64 (ou versions ultérieures) • libpng-1.2.44-1.el6.x86_64 (ou versions ultérieures) • libstdc++-4.4.4-13.el6.x86_64 (ou versions ultérieures) • libuuid-2.17.2-6.el6.x86_64 (ou versions ultérieures) • libxcb-1.5-1.el6.x86_64 (ou versions ultérieures) • nss-softokn-freebl-3.12.7-1.1.el6.x86_64 (ou versions ultérieures) • pam-1.1.1-4.el6.x86_64 (ou versions ultérieures) • zlib-1.2.3-25.el6.x86_64 (ou versions ultérieures) Le package suivant est requis par Red Hat Enterprise Linux (RHEL) Server 6.0, 6.1, 6.2 et 6.3 : • libjpeg-6b-46.el6.x86_64 (ou versions ultérieures) Le package suivant est requis par Red Hat Enterprise Linux (RHEL) Server 6.4 (ou versions ultérieures) : • libjpeg-turbo-1.2.1-1.el6.x86_64 (ou versions ultérieures) Les packages suivants sont requis uniquement par le composant Outils de bureau : • libX11-1.3-2.el6.x86_64 (ou versions ultérieures) • libXau-1.0.5-1.el6.x86_64 (ou versions ultérieures) • libXext-1.1-3.el6.x86_64 (ou versions ultérieures) • libXft-2.1.13-4.1.el6.x86_64 (ou versions ultérieures) • libXmu-1.0.5-1.el6.x86_64 (ou versions ultérieures) • libXp-1.0.0-15.1.el6.x86_64 (ou versions ultérieures) • libXpm-3.5.8-2.el6.x86_64 (ou versions ultérieures) • libXrender-0.9.5-1.el6.x86_64 (ou versions ultérieures) • libXt-1.0.7-1.el6.x86_64 (ou versions ultérieures) • openmotif-2.3.3-1.el6.x86_64 (ou versions ultérieures) Le package suivant est requis par Netcool MIB Manager : • gtk2-2.18.9-4.el6.x86_64 (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • compat-libstdc++-33-3.2.3-69.el6.i686 (ou versions ultérieures) • glibc-2.12-1.7.el6.i686 (ou versions ultérieures) • libgcc-4.4.4-13.el6.i686 (ou versions ultérieures) • libstdc++-4.4.4-13.el6.i686 (ou versions ultérieures)

Tableau 15. Exigences pour SUSE Linux Enterprise Server (SLES) 10 64 bits

RPM minimum requis	Explication et commentaires
• audit-libs-1.2.9-6.19 (ou versions ultérieures) • expat-2.0.0-13.9.1 (ou versions ultérieures) • fontconfig-2.3.94-18.23.16 (ou versions ultérieures) • freetype2-2.1.10-18.23.1 (ou versions ultérieures) • glibc-2.4-31.81.11 (ou versions ultérieures) • libgcc-4.1.2_20070115-0.32.53 (ou versions ultérieures) • libidn-0.6.0-14.2 (ou versions ultérieures) • libstdc++-4.1.2_20070115-0.32.53 (ou versions ultérieures) • pam-0.99.6.3-28.23.15 (ou versions ultérieures) • zlib-1.2.3-15.2 (ou versions ultérieures) Les packages suivants sont requis uniquement par le composant Outils de bureau : • openmotif-2.3.0-1 (ou versions ultérieures) • xorg-x11-libs-6.9.0-50.69.31 (ou versions ultérieures) Le package suivant est requis par Netcool MIB Manager : • gtk2-2.8.11-0.27.11 (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • glibc-32bit-2.4-31.81.11 (ou versions ultérieures) • libstdc++33-32bit-3.3.3-7.8.1 (ou versions ultérieures)

Tableau 16. Exigences pour SUSE Linux Enterprise Server (SLES) 11 64 bits

RPM minimum requis	Explication et commentaires
• audit-libs-1.7.7-5.16 (ou versions ultérieures) • fontconfig-2.6.0-10.6 (ou versions ultérieures) • freetype2-2.3.7-25.8 (ou versions ultérieures) • glibc-2.9-13.2 (ou versions ultérieures) • libexpat1-2.0.1-88.21 (ou versions ultérieures) • libidn-1.10-3.18 (ou versions ultérieures) • libuuid1-1.41.1-13.9 (ou versions ultérieures) • pam-1.0.2-20.1 (ou versions ultérieures) • zlib-1.2.3-106.34 (ou versions ultérieures) Les packages suivants sont requis par les installations SP1 : • libgcc43-4.3.3_20081022-11.18 (ou versions ultérieures) • libstdc++43-4.3.3_20081022-11.18 (ou versions ultérieures) Les packages suivants sont requis par les installations SP2 : • libgcc46-4.6.1_20110701-0.13.9 (ou versions ultérieures) • libstdc++46-4.6.1_20110701-0.13.9 (ou versions ultérieures) Les packages suivants sont requis uniquement par le composant Outils de bureau : • openmotif-2.3.0-1 (ou versions ultérieures) • xorg-x11-libICE-7.4-1.15 (ou versions ultérieures) • xorg-x11-libSM-7.4-1.18 (ou versions ultérieures) • xorg-x11-libX11-7.4-5.5 (ou versions ultérieures) • xorg-x11-libXau-7.4-1.15 (ou versions ultérieures) • xorg-x11-libXext-7.4-1.14 (ou versions ultérieures) • xorg-x11-libXmu-7.4-1.17 (ou versions ultérieures) • xorg-x11-libXp-7.4-1.14 (ou versions ultérieures) • xorg-x11-libXpm-7.4-1.17 (ou versions ultérieures) • xorg-x11-libXrender-7.4-1.14 (ou versions ultérieures) • xorg-x11-libXt-7.4-1.17 (ou versions ultérieures) • xorg-x11-libs-7.4-8.18 (ou versions ultérieures) • xorg-x11-libxcb-7.4-1.15 (ou versions ultérieures) Le package suivant est requis par Netcool MIB Manager : • gtk2-2.14.4-16.1 (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • glibc-32bit-2.9-13.2 (ou versions ultérieures) • libgcc43-32bit-4.3.3_20081022-11.18 (ou versions ultérieures) • libstdc++33-32bit-3.3.3-11.9 (ou versions ultérieures) • libstdc++43-32bit-4.3.3_20081022-11.18 (ou versions ultérieures)

Linux on System z

Remarque :

- La liste d'événements du bureau n'est pas prise en charge sur Linux on System z.
- Les composants serveur et sonde Tivoli Netcool/OMNIbus ne sont pas pris en charge sur les éditions de bureau de Red Hat Enterprise Linux (RHEL) ou SUSE Linux.

Les bibliothèques pour le système d'exploitation zLinux 32 bits ne sont pas installées avec Tivoli Netcool/OMNIbus. Si vous souhaitez exécuter des sondes ou des passerelles 32 bits, vous aurez peut-être besoin de bibliothèques 32 bits.

Consultez la documentation relative à la sonde ou à la passerelle pour connaître la configuration requise spécifique. Vous pouvez également exécuter IBM Prerequisite Scanner avec la fonction de sonde sélectionnée afin de déterminer si vous disposez de toutes les bibliothèques nécessaires. Les bibliothèques Tivoli Netcool/OMNIbus 32 bits principales qui sont requises pour exécuter des analyses et des passerelles 32 bits (par exemple, `libOpl`) sont installées par défaut avec Tivoli Netcool/OMNIbus.

Les tableaux suivants décrivent les packages RPM qui sont requis pour les systèmes d'exploitation System z.

Tableau 17. Exigences pour Red Hat Enterprise Linux (RHEL) Server 5.9 on zLinux.

RPM minimum requis	Explication et commentaires
• `audit-libs-1.8-2.el5` (ou versions ultérieures) • `glibc-2.5-107` (ou versions ultérieures) • `libgcc-4.1.2-54.el5` (ou versions ultérieures) • `libstdc++-4.1.2-54.el5` (ou versions ultérieures) • `pam-0.99.6.2-12.el5` (ou versions ultérieures) • `zlib-1.2.3-7.el5` (ou versions ultérieures) Les packages suivants sont requis par Netcool MIB Manager : • `gtk2-2.10.4-21.el5_5.6` (ou versions ultérieures) • `libX11-1.0.3-11.el5_7.1` (ou versions ultérieures) • `libXau-1.0.1-3.1` (ou versions ultérieures) • `libXdmcp-1.0.1-2.1` (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • `compat-libstdc++-33-3.2.3-61` (ou versions ultérieures)

Tableau 18. Exigences pour Red Hat Enterprise Linux (RHEL) Server 6.2 on zLinux.

RPM minimum requis	Explication et commentaires
• `audit-libs-2.2-2.el6.s390x` (ou versions ultérieures) • `glibc-2.12-1.80.el6.s390x` (ou versions ultérieures) • `libgcc-4.4.6-4.el6.s390x` (ou versions ultérieures) • `libstdc++-4.4.6-4.el6.s390x` (ou versions ultérieures) • `pam-1.1.1-10.el6_2.1.s390x` (ou versions ultérieures) • `zlib-1.2.3-27.el6.s390x` (ou versions ultérieures) • `nss-softokn-freebl-3.12.9-11.el6.s390x` (ou versions ultérieures) Les packages suivants sont requis par Netcool MIB Manager : • `gtk2-2.10.4-21.el5_5.6` (ou versions ultérieures) • `libX11-1.3-2.el6.s390x` (ou versions ultérieures) • `libXau-1.0.5-1.el6.s390x` (ou versions ultérieures) • `libxcb-1.5-1.el6.s390x` (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • `compat-libstdc++-33-3.2.3-69.el6.i686` (ou versions ultérieures) • `glibc-2.12-1.7.el6.i686` (ou versions ultérieures) • `libgcc-4.4.4-13.el6.i686` (ou versions ultérieures) • `libstdc++-4.4.4-13.el6.i686` (ou versions ultérieures)

Tableau 19. Exigences pour SUSE Linux Enterprise Server (SLES) 11 on zLinux.

RPM minimum requis	Explication et commentaires
• audit-libs-1.7.7-5.16 (ou versions ultérieures) • glibc-2.11.1-0.20.1 (ou versions ultérieures) • libgcc43-4.3.4_20091019-0.7.35 (ou versions ultérieures) • libstdc++43-4.3.4_20091019-0.7.35 (ou versions ultérieures) • pam-1.0.4-0.5.12 (ou versions ultérieures) • zlib-1.2.3-106.34 (ou versions ultérieures) Les packages suivants sont requis par SLES 11 SP2 (ou versions ultérieures) • libgcc46-4.6.1_20110701-0.13.9 (ou versions ultérieures) • libstdc++46-4.6.1_20110701-0.13.9 (ou versions ultérieures) Les packages suivants sont requis par Netcool MIB Manager : • gtk2-2.14.4-16.1 (ou versions ultérieures) • xorg-x11-libXau-7.4-1.15 (ou versions ultérieures) • xorg-x11-libxcb-7.4-1.20.34 (ou versions ultérieures) • xorg-x11-libX11-7.4-5.5 (ou versions ultérieures)	Si vous souhaitez exécuter des sondes ou des passerelles 32 bits ou d'autres produits 32 bits qui sont installés dans l'emplacement d'origine Netcool, les packages suivants sont requis. Cette liste n'est pas exhaustive : certains produits peuvent nécessiter des packages supplémentaires. • glibc-32bit-2.9-13.2 (ou versions ultérieures) • libgcc43-32bit-4.3.3_20081022-11.18 (ou versions ultérieures) • libstdc++33-32bit-3.3.3-11.9 (ou versions ultérieures) • libstdc++43-32bit-4.3.3_20081022-11.18 (ou versions ultérieures)

Solaris

Avant d'installer Tivoli Netcool/OMNIbus sur des systèmes d'exploitation Solaris, installez les packages suivants :

- Sur Solaris 10, les packages SUNWxwrtl et SUNWmfrun.
- Sur Solaris 11, le package SUNWmfrun est requis.

Lorsque vous accédez à l'aide en ligne de MIB Manager sur un système d'exploitation Solaris, vérifiez qu'un navigateur Web est en cours d'exécution avant de cliquer sur **Aide**. Sinon, l'aide en ligne ne s'ouvre pas. Ce comportement est provoqué par un défaut ouvert (376208) sur la plateforme Eclipse.

Exigences de l'environnement d'exécution Java (JRE)

L'interface graphique de Netcool/OMNIbus Administrator, l'utilitaire Confpack (**nco_confpack**) et un composant de notification d'événement accéléré exigent que l'environnement d'exécution Java (JRE) soit installé sur votre système.

L'environnement d'exécution Java 7.0 d'IBM est inclus dans l'ensemble d'installations de tous les systèmes d'exploitation et fournit un support pour la norme Federal Information Processing Standard 140-2 (FIPS 140-2). Sur les systèmes d'exploitation 64 bits, un environnement JRE 32 bits est fourni en plus du JRE 64 bits. Certaines sondes et passerelles Tivoli Netcool/OMNIbus ont besoin du JRE 32 bits pour fonctionner sur les systèmes d'exploitation 64 bits.

Navigateurs de l'Interface graphique Web, environnements JRE et périphériques mobiles

Pour pouvoir afficher l'Interface graphique Web, les postes de travail client ont besoin d'un navigateur pris en charge et d'un plug-in JRE (Java Runtime Environment). Les périphériques mobiles doivent figurer sur un système d'exploitation pris en charge. Configurez les navigateurs pour l'acceptation des cookies.

- «Navigateurs pris en charge»
- «Environnements d'exécution Java (JRE) pris en charge»
- «Périphériques mobiles pris en charge»

Navigateurs pris en charge

Les navigateurs pris en charge sont les suivants :

- Internet Explorer 9
- Internet Explorer 10
- Firefox ESR 17
- Firefox ESR 24
- Web GUI Fix Pack 1 Safari 6.1

Environnements d'exécution Java (JRE) pris en charge

L'Interface graphique Web prend en charge IBM JRE 7.0. Appliquez toujours les dernières mises à jour à l'environnement JRE sur l'hôte Interface graphique Web.

Périphériques mobiles pris en charge

Certaines fonctions de l'Interface graphique Web peuvent être affichées sur les périphériques mobiles. Ces fonctions sont présentées ci-après :

Liste d'événements mobiles

Les pages de la liste d'événements pour mobile (la page d'arrivée, le tableau de bord des événements, la liste d'événements et le détail des événements) sont prises en charge sur Android V2.3 et versions ultérieures, et iOS 5.0 et versions ultérieures pour les iPhones.

Jauges de mobiles

Pour pouvoir afficher une page Jauges sur un périphérique mobile, celui-ci doit être un smartphone, JavaScript et AJAX doivent être activés sur le navigateur et l'écran doit avoir une résolution minimale de 320 x 240 pixels. Avec cette résolution, la page Jauges peut afficher deux colonnes de jauges. La page Jauges est présentée sur les smartphones s'exécutant sur les systèmes d'exploitation Blackberry 4.6+ et iOS 4.0+ et versions ultérieures.

La fonction de zoom avant de la page Jauges utilise des actions de lancement URL. Si vous rencontrez des problèmes avec cette fonction sur un périphérique mobile, vérifiez que le navigateur prend en charge JavaScript et AJAX. Assurez-vous également qu'aucune action JavaScript définie n'est susceptible d'affecter le fonctionnement.

Exigences liées à l'interface utilisateur

Tivoli Netcool/OMNIbus prend en charge les environnements graphiques sur les systèmes d'exploitation AIX, Linux, Solaris et Windows. Les environnements graphiques ne sont pas pris en charge sur HP-UX Itanium ou Linux on System z.

Les composants du bureau Tivoli Netcool/OMNIbus sont pris en charge sur les environnements graphiques suivants :

- AIX, Linux et Solaris : `openmotif 2.2.4` et l'environnement CDE (Common Desktop Environment)
- Windows : Microsoft Windows 2008 Server, Windows Vista Enterprise Edition et Windows 7 Enterprise Edition

Exigences relatives à l'aide en ligne

L'aide en ligne de Tivoli Netcool/OMNIbus est déployée à l'aide d'IBM Eclipse Help System (IEHS), qui est une application Web. Tivoli Netcool/OMNIbus prend en charge IEHS V3.1.1.

L'aide en ligne s'affiche dans un navigateur Web et est disponible en mode autonome et en mode centre de documentation. Le mode autonome est activé par défaut.

En mode autonome, l'infrastructure préfabriquée de l'application IEHS et les fichiers d'aide en ligne s'exécutent sur un serveur Web local. Le **Système d'aide local** doit être sélectionné en tant que fonction installable afin d'obtenir les composants IEHS obligatoires. Après l'installation, vous pouvez accéder à l'aide en ligne, généralement sans avoir besoin d'une configuration supplémentaire. Lorsque vous tentez d'accéder à l'aide en ligne, un serveur Web démarre automatiquement et s'exécute localement jusqu'à ce que vous le mettiez manuellement hors tension.

En mode centre de documentation, l'infrastructure préfabriquée de l'application IEHS et les fichiers d'aide en ligne s'exécutent sur un serveur Web distant auquel les utilisateurs doivent se connecter afin d'accéder à l'aide en ligne. L'utilisation d'un serveur d'aide en ligne partagé diminue la charge sur les hôtes ou les postes de travail locaux. Un administrateur système doit prendre la responsabilité d'installer, de configurer et de gérer les composants IEHS sur ce serveur. La fonction **Système d'aide local** doit être installée sur ce serveur afin d'obtenir l'infrastructure préfabriquée de l'application IEHS et les fichiers d'aide en ligne. Pour accéder à l'aide en ligne sur le serveur distant, les utilisateurs doivent modifier un fichier de configuration IEHS local avec les détails de communication du serveur distant. Le fichier de configuration d'IEHS est installé, par défaut, dans le cadre d'une installation standard de Tivoli Netcool/OMNIbus. L'administrateur système doit exécuter un script de démarrage IEHS pour démarrer le serveur IEHS et ouvrir la connexion pour les utilisateurs.

Pour le composant de bureau Tivoli Netcool/OMNIbus (auquel vous avez généralement accès à l'aide de Conductor), le navigateur du système d'exploitation par défaut est utilisé pour afficher l'aide en ligne en mode autonome ou en mode centre de documentation. Si vous utilisez Netcool/OMNIbus Administrator ou le client de notification d'événement accéléré, vous devez indiquer un navigateur pour afficher l'aide en ligne.

Navigateurs pris en charge pour IEHS V3.1.1

Vous pouvez rencontrer une limitation des fonctionnalités de votre aide en ligne si votre navigateur ne prend pas complètement en charge les cookies ou JavaScript, ou si votre navigateur bloque les fenêtres en incrustation. Sur certains systèmes d'exploitation, certains navigateurs peuvent uniquement afficher l'interface du système d'aide en mode basique. Dans ce mode, seules les fonctions de base d'IEHS sont disponibles, notamment l'affichage du contenu et la fonction de recherche.

Les versions minimum de navigateur prises en charge pour IEHS V3.1.1 sont les suivants :

- Internet Explorer 6.0

  Remarque : Si les paramètres de sécurité d'Internet Explorer sont configurés de sorte que l'option **Autoriser l'actualisation des métafichiers** est définie sur `Désactiver`, la page d'index d'aide peut ne pas s'afficher. Dans un tel cas, définissez la valeur de l'option sur `Activer`.
- Mozilla 1.7
- Firefox 1.0
- Safari 1.2
- Konqueror (mode basique de l'interface utilisateur uniquement)

Remarque : Les navigateurs Web pris en charge qui sont répertoriés ici pour IEHS diffèrent des navigateurs Web pris en charge pour l'Interface graphique Web. Lorsque vous accédez à l'aide en ligne de Tivoli Netcool/OMNIbus MIB Manager sur un système d'exploitation Solaris, vous devez disposer d'un navigateur Web en cours d'exécution avant de cliquer sur **Aide**. Sinon, l'aide en ligne ne s'ouvre pas. Ce comportement est causé par un défaut ouvert (376208) sur la plateforme Eclipse.

.

Tâches associées:

«Configuration et exécution de l'aide en ligne», à la page 95
Après avoir installé Tivoli Netcool/OMNIbus, vous devrez peut-être configurer votre système pour accéder à l'aide en ligne. L'aide en ligne est déployée à l'aide d'IBM Eclipse Help System (IEHS) et elle est accessible en mode autonome ou en mode centre d'informations.

Prise en charge du protocole de réseau

Tivoli Netcool/OMNIbus prend en charge la communication via les réseaux IPv4 et IPv6.

Tivoli Netcool/OMNIbus prend en charge les configurations suivantes pour IPv4 et IPv6 :

- Installation et exécution dans un réseau s'exécutant dans un environnement IPv4 uniquement
- Installation et exécution dans un réseau s'exécutant dans un environnement IPv6 uniquement
- Maintien de l'interopérabilité avec IPv4, de sorte que le produit peut fonctionner et coexister sur un réseau prenant en charge une configuration IPv4 uniquement, IPv6 uniquement ou une configuration double IPv4 et IPv6

Un environnement double IPv4 et IPv6 peut être défini en tant qu'environnement dans lequel les deux protocoles peuvent être utilisés simultanément.

- Prise en charge du traitement des événements générés dans les deux environnements réseau IPv4 et IPv6 au sein d'un seul ObjectServer et d'une instance de bureau
- Fonctionnement et coexistence sur un réseau prenant en charge IPv4 uniquement, IPv6 uniquement ou un hybride d'IPv4 et d'IPv6 sur tous les systèmes d'exploitation pris en charge

Restrictions IPv6

La fonctionnalité d'égal à égal des sondes est disponible dans un environnement double IPv4 et IPv6. Les passerelles du serveur ObjectServer version 7 ou ultérieure (**nco_g_objserv_bi** et **nco_g_objserv_uni**) peuvent également se connecter à un serveur ObjectServer à l'aide d'IPv6 ou d'IPv4. Pour obtenir des détails sur la prise en charge de sondes et passerelles individuelles pour IPv6, voir la documentation fournie avec chaque sonde et passerelle.

IBM Eclipse Help System (IEHS) V3.1.1, qui est utilisé pour la distribution de l'aide en ligne, ne prend pas en charge IPv6. Par conséquent, lors de la configuration d'un serveur IEHS à utiliser en mode centre de documentation IEHS, n'indiquez pas d'adresse IPv6 pour accéder au serveur.

Internet Explorer version 6 ne prend pas en charge l'utilisation d'adresses IPv6 littérales dans les adresses URL. Sur les postes de travail client de l'Interface graphique Web, vous devez utiliser les noms d'hôte à la place.

Concepts associés:

Chapitre 15, «Configuration IPv6», à la page 413
Tivoli Netcool/OMNIbus offre la prise en charge des protocoles IPv4 et IPv6. Les composants peuvent à présent fonctionner et coexister sur un réseau prenant en charge une configuration IPv4 seulement, IPv6 seulement ou IPv4 et IPv6.

Tâches associées:

«Configuration et exécution de l'aide en ligne», à la page 95
Après avoir installé Tivoli Netcool/OMNIbus, vous devrez peut-être configurer votre système pour accéder à l'aide en ligne. L'aide en ligne est déployée à l'aide d'IBM Eclipse Help System (IEHS) et elle est accessible en mode autonome ou en mode centre d'informations.

Protocole de communication

Les composants Tivoli Netcool/OMNIbus utilisent la technologie client/serveur communicant via un réseau TCP/IP.

Vous pouvez installer les composants sur un seul système ou dans un environnement distribué. Par exemple, il peut être approprié d'installer une sonde sur le même système que sa source d'événement, alors que le serveur ObjectServer et le bureau sont installés sur d'autres systèmes du réseau.

Le serveur ObjectServer, le serveur proxy, les passerelles et le contrôle de processus doivent être configurés pour utiliser le protocole de communication de Tivoli Netcool/OMNIbus.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Compatibilité avec des versions antérieures

Tivoli Netcool/OMNIbus version 8.1 est compatible avec les versions précédentes du produit. Les exceptions et les solutions sont décrites ici.

Les composants du serveur sont compatibles avec les composants de Tivoli Netcool/OMNIbus versions 7.2, 7.2.1, 7.3, 7.3.1 et 7.4. Les composants serveur sont compatibles avec l'Interface graphique Web versions 7.3, 7.3.1 et 7.4 et IBM Tivoli Netcool/Webtop version 2.2. Les *composants serveur* désignent la sonde, la passerelle, le contrôle de processus et le bureau.

Dépendances des sondes et des passerelles

Vérifiez que vous téléchargez la dernière version des composants d'analyse et de passerelle à utiliser avec la version 8.1. N'utilisez pas la fonction **PINSTALL** de groupe de sondes V7.

Tous les modules de correction de dépendance requis pour les sondes et les passerelles sont documentés dans les fichiers `install.txt` disponibles dans les modules à télécharger. Ces informations sont également disponibles dans les publications individuelles d'analyse et de passerelle du Knowledge Center Tivoli Netcool/OMNIbus à l'adresse : http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Compatibilité des passerelles ObjectServer

Les passerelles du serveur ObjectServer Tivoli Netcool/OMNIbus version 8.1 contiennent des mappages de passerelle supplémentaires qui ne sont pas disponibles dans Tivoli Netcool/OMNIbus version 7.2.1 ou dans les versions inférieures, et ne peuvent par conséquent pas être répliquées. Pour utiliser une passerelle du serveur ObjectServer Tivoli Netcool/OMNIbus version 8.1 avec une version inférieure du serveur ObjectServer, vous devez commenter certaines des entrées du fichier de définition de réplication de la table et du fichier de définition de mappage.

Pour les passerelles unidirectionnelles, procédez comme suit :

- Editez le fichier `$NCHOME/omnibus/gates/objserv_uni/objserv_uni.reader.tblrep.def` en commentant les lignes suivantes, comme indiqué dans l'exemple :

  ```
  # REPLICATE ALL FROM TABLE 'iduc_system.iduc_stats'
  #  USING map 'IducMap';
  ```

- Editez le fichier `$NCHOME/omnibus/gates/objserv_uni/objserv_uni.map` en commentant les lignes suivantes, comme indiqué dans l'exemple :

  Dans la section `CREATE MAPPING StatusMap` :

  ```
  # 'ProbeSubSecondId' = '@ProbeSubSecondId',
  # 'BSM_Identity' = '@BSM_Identity'
  ```

  Plus loin dans le fichier :

```
# CREATE MAPPING IducMap
# (
#  'ServerName' = '@ServerName' ON INSERT ONLY,
#  'AppName' = '@AppName',
#  'AppDesc' = '@AppDesc' ON INSERT ONLY,
#  'ConnectionId' = '@ConnectionId' ON INSERT ONLY,
#  'LastIducTime' = '@LastIducTime'
# );
```

Pour les passerelles bidirectionnelles, procédez comme suit :

- Editez les fichiers $NCHOME/omnibus/gates/objserv_bi/objserv_bi.objectservera.tblrep.def et $NCHOME/omnibus/gates/objserv_bi/objserv_bi.objectserverb.tblrep.def en commentant les lignes suivantes, comme indiqué dans l'exemple :

  ```
  # REPLICATE ALL FROM TABLE 'iduc_system.iduc_stats'
  #  USING map 'IducMap';
  ```

- Editez le fichier $NCHOME/omnibus/gates/objserv_bi/objserv_bi.map en commentant les lignes suivantes, comme indiqué dans l'exemple :

  Dans la section CREATE MAPPING StatusMap :

  ```
  # 'ProbeSubSecondId' = '@ProbeSubSecondId',
  # 'BSM_Identity' = '@BSM_Identity'
  ```

  Plus loin dans le fichier :

  ```
  # CREATE MAPPING IducMap
  # (
  #  'ServerName' = '@ServerName' ON INSERT ONLY,
  #  'AppName' = '@AppName',
  #  'AppDesc' = '@AppDesc' ON INSERT ONLY,
  #  'ConnectionId' = '@ConnectionId' ON INSERT ONLY,
  #  'LastIducTime' = '@LastIducTime'
  # );
  ```

Compatibilité du contrôle de processus

L'agent de processus Windows version 8.1 ne peut pas communiquer avec un agent de processus Windows version 7.2 ou inférieure. L'agent de processus Windows version 8.1 ne peut par ailleurs pas communiquer avec les serveurs ObjectServer version 7.2 ou inférieure.

nco_postmsg

L'utilitaire **nco_postmsg** est compatible avec le serveur ObjectServer version 7.1 et les versions ultérieures. Vous pouvez installer cet utilitaire puis l'utiliser pour vous connecter, et envoyer des événements, au serveur ObjectServer version 7.1 ou versions ultérieures.

Compatibilité du kit d'outils Tivoli Event Integration Facility (EIF)

EIF est compatible avec les versions inférieures (notamment les expéditeurs et les récepteurs basés sur Tivoli Enterprise Console) uniquement lorsque le type de transfert SOCKET est utilisé. Les conditions suivantes s'appliquent :

- Un nouvel expéditeur EIF ne peut pas envoyer d'événements au serveur Tivoli Enterprise Console à l'aide du type de transfert SSL. Toutefois, un nouvel expéditeur peut envoyer des événements au serveur Tivoli Enterprise Console à l'aide du transfert SOCKET.

- Un nouveau récepteur EIF ne peut pas recevoir d'événements des adaptateurs Tivoli Enterprise Console via IPv4 ou IPv6. Cependant, un nouvel expéditeur peut recevoir des événements des adaptateurs Tivoli Enterprise Console via le type de transfert SOCKET.
- Les adaptateurs Tivoli Enterprise Console et le serveur Tivoli Enterprise Console ne sont pas liés à la nouvelle version des bibliothèques EIF.
- Un nouveau récepteur EIF ne peut pas recevoir d'événements des adaptateurs Tivoli Enterprise Console via IPv4 ou IPv6.
- Sans les mises à jour correspondantes, Probe for Tivoli EIF ne peut pas recevoir d'événements via le type de transfert SSL.
- Sans les mises à jour correspondantes, Probe for Tivoli EIF ne peut pas recevoir d'événements des nouveaux expéditeurs EIF via IPv6 car l'implémentation Java prend déjà en charge IPv6 via la machine virtuelle Java.
- Avec les mises à jour correspondantes, Probe for Tivoli EIF peut recevoir des événements envoyés via IPv4 provenant des versions précédentes des expéditeurs EIF, notamment les adaptateurs IBM Tivoli Monitoring et Tivoli Enterprise Console.

Formats d'horodatage dans les fichiers journaux

Les horodatages sont affichés au format ISO 8601 dans les fichiers journaux du serveur ObjectServer, du serveur proxy, de l'utilitaire **nco_dbinit**, de la sonde, de la passerelle du serveur ObjectServer et des autres passerelles. Pour la compatibilité avec les versions antérieures, vous pouvez utiliser la propriété **OldTimeStamp** pour passer à l'ancien format d'horodatage utilisé dans la version 7.2.1 ou dans les versions antérieures. Vous pouvez trouver cette propriété utile si des outils d'analyse syntaxique des fichiers journaux sont déjà en place dans votre système. Notez que les horodatages du fichier journal de l'utilitaire **nco_dbinit** ne peuvent pas être basculés vers l'ancien format car cet utilitaire ne possède pas de propriété **OldTimeStamp**.

Voici une comparaison des formats :

Ancien format dans la version 7.2.1 ou une version inférieure	**Format IS0 8601**
jj/MM/AAAA hh:mm:ss AM jj/MM/AAAA hh:mm:ss PM lorsque l'environnement local est défini sur en_GB sur un ordinateur Solaris 9 Exemple : 01/05/2009 07:15:04 AM	AAAA-MM-JJThh:mm:ss où T sépare la date de l'heure, hh représente l'heure au format 24 heures et les nombres sont affichés en chiffres arabes occidentaux (0-9). Exemple : 2001-10-21T13:43:11

Format et analyse des dates et heures

Dans Tivoli Netcool/OMNIbus version 7.2.1 ou inférieure, la fonction POSIX strftime() est utilisée dans les conversions de date et d'heure. Pour les fonctions SQL du serveur ObjectServer (to_char, to_date, et to_time) et les fonctions du fichier de règles de la sonde (datetotime et timetodate), vous pouvez définir un format de sortie en indiquant une chaîne de format qui consiste en zéro indicateur de conversion ou plus. Par exemple, le format POSIX pour la sortie peut être défini dans la fonction to_time du serveur ObjectServer de la manière suivante :

```
to_time('Thu Dec 11 2003', '%a %b %d %Y')
```

Dans Tivoli Netcool/OMNIbus version 7.3 et ultérieures, les bibliothèques ICU utilisent le langage LDML pour les modèles de date et d'heure. Les caractères utilisés dans ces modèles sont définis à l'adresse http://userguide.icu-project.org/formatparse/datetime. Utilisez ces modèles de date et d'heure lorsque possible dans vos fonctions SQL du serveur ObjectServer et dans les fonctions du fichier de règles de la sonde pour obtenir les résultats dont vous avez besoin.

Pour conserver une compatibilité amont, le format POSIX est toujours pris en charge dans les fonctions de date et d'heure des fichiers de règles du serveur ObjectServer et des sondes. Notez cependant que le format POSIX n'est pas entièrement compatible avec la technologie d'analyse syntaxique utilisée pour les modèles de date et d'heure LDML. Certains formats POSIX ne sont également pas pris en charge. Lors d'une compatibilité intégrale avec la technologie d'analyse syntaxique, une sortie identique est obtenue pour le format POSIX dans la version 7.3.1 (et ultérieures) et dans les versions inférieures. Lors d'une compatibilité partielle, des variations peuvent se produire dans la sortie obtenir pour le format POSIX dans les différentes versions du produit. Par exemple, les variations suivantes peuvent être obtenues pour la même date et la même heure :

Résultat pour le format POSIX %c dans la version 7.3.1 (et ultérieures) : Monday, July 20, 2009 10:18:43 AM Greenwich Mean Time
Résultat pour le format POSIX %c dans des versions inférieures : Mon Jul 20 10:18:43 2009

Résultat pour le format POSIX %x dans la version 7.3.1 (et ultérieures) : Monday, July 20, 2009
Résultat pour le format POSIX %x dans des versions inférieures : 07/20/09

Le tableau suivant fournit certains conseils sur les formats POSIX qui sont entièrement ou partiellement pris en charge dans la version 7.3.1 (et ultérieures). La première colonne présente les indicateurs de conversion POSIX standard pouvant être utilisés dans les fonctions de date et d'heure et le résultat prévu. Les deuxième et troisième colonnes indiquent si chaque indicateur de conversion est entièrement pris en charge dans la version 7.3.1 (et ultérieures) et si l'indicateur de conversion correspond au résultat attendu après l'analyse syntaxique. En outre, la deuxième colonne répertorie les résultats pour le format POSIX dans les environnements locaux C, en_GB et en_US, alors que la troisième colonne répertorie les résultats pour le format POSIX dans tous les autres environnements locaux, sauf Hindi et Arabe.

Remarque : Ces informations sont basées sur des vérifications exécutées sur un hôte Solaris 9. La sortie POSIX varie selon les systèmes d'exploitation, de sorte que vous pouvez observer certaines différences avec les résultats indiqués dans le tableau.

Tableau 20. Compatibilité pour le format POSIX dans les conversions de date et d'heure dans la version 7.3.1 (et ultéreures)

Format POSIX standard pris en charge dans l'analyse syntaxique de la date et de l'heure (et résultat prévu)	**Résultats de la version 7.3.1 (et ultérieures) pour les environnements locaux C, en_GB et en_US**	**Résultats pour la version 7.3.1 (et ultérieures) pour tous les autres environnements locaux, sauf l'Hindi et l'Arabe**
%a est remplacé par le nom du jour de semaine abrégé de l'environnement local.	Résultat identique	Non identique
%A est remplacé par le nom du jour de semaine complet de l'environnement local.	Résultat identique	Non identique
%b est remplacé par le nom du mois abrégé de l'environnement local.	Résultat identique	Non identique
%B est remplacé par le nom du mois complet de l'environnement local.	Résultat identique	Non identique
%c est remplacé par la représentation de l'heure et de la date appropriée pour l'environnement local.	Non identique	Non identique
%C est remplacé par le numéro de siècle (l'année divisée par 100 et tronquée sur un entier) en tant que nombre décimal [00-99].	Non pris en charge	Non pris en charge
%d est remplacé par le jour du mois en tant que nombre décimal [01,31].	Résultat identique	Résultat identique
%D identique à %m/%j/%a.	Résultat identique	Résultat identique
%e est remplacé par le jour du mois en tant que nombre décimal [1,31] ; un seul chiffre est précédé par un espace.	Résultat identique	Résultat identique
%h identique à %b.	Résultat identique	Résultat identique
%H est remplacé par l'heure (au format 24 heures) en tant que nombre décimal [00,23].	Résultat identique	Résultat identique
%I est remplacé par l'heure (au format 12 heures) en tant que nombre décimal [01,12].	Résultat identique	Résultat identique
%j est remplacé par le jour de l'année en tant que nombre décimal [001,366].	Résultat identique	Résultat identique
%m est remplacé par le mois en tant que nom décimal [01,12].	Résultat identique	Résultat identique

Tableau 20. Compatibilité pour le format POSIX dans les conversions de date et d'heure dans la version 7.3.1 (et ultéreures) (suite)

Format POSIX standard pris en charge dans l'analyse syntaxique de la date et de l'heure (et résultat prévu)	**Résultats de la version 7.3.1 (et ultérieures) pour les environnements locaux C, en_GB et en_US**	**Résultats pour la version 7.3.1 (et ultérieures) pour tous les autres environnements locaux, sauf l'Hindi et l'Arabe**
%M est remplacé par la minute en tant que nombre décimal [00,59].	Résultat identique	Résultat identique
%n est remplacé par un caractère de retour à la ligne.	Résultat identique	Résultat identique
%p est remplacé par un équivalent à a.m. ou p.m. au niveau de l'environnement local	Résultat identique	Résultat identique
%r est remplacé par l'heure au format a.m. et p.m. ; dans l'environnement local POSIX, %r est équivalent à %I:%M:%S %p.	Résultat identique	Non identique
%R est remplacé par l'heure au format 24 heures (%H:%M).	Résultat identique	Résultat identique
%S est remplacé par la seconde en tant que nombre décimal [00,61].	Résultat identique	Résultat identique
%t est remplacé par un caractère de tabulation.	Résultat identique	Résultat identique
%T est remplacé par l'heure (%H:%M:%S).	Résultat identique	Résultat identique
%U est remplacé par le numéro de la semaine de l'année (dimanche étant le premier jour de la semaine) en tant que nombre décimal [00,53].	Non pris en charge	Non pris en charge
%u est remplacé par le jour de la semaine en tant que nombre décimal [1,7], 1 représentant le lundi.	Résultat identique	Résultat identique
%V est remplacé par le numéro de la semaine de l'année (lundi étant le premier jour de la semaine) en tant que nombre décimal [01,53]. Si la semaine contenant le 1er janvier comporte quatre jours ou plus dans la nouvelle année, elle est considérée comme la semaine n°1. Sinon, il s'agit de la dernière semaine de l'année précédente et la semaine suivante est la semaine n°1.	Résultat identique	Résultat identique

Tableau 20. Compatibilité pour le format POSIX dans les conversions de date et d'heure dans la version 7.3.1 (et ultéreures) (suite)

Format POSIX standard pris en charge dans l'analyse syntaxique de la date et de l'heure (et résultat prévu)	**Résultats de la version 7.3.1 (et ultérieures) pour les environnements locaux C, en_GB et en_US**	**Résultats pour la version 7.3.1 (et ultérieures) pour tous les autres environnements locaux, sauf l'Hindi et l'Arabe**
%W est remplacé par le numéro de la semaine de l'année (lundi étant le premier jour de la semaine) en tant que nombre décimal [00,53]. Tous les jours d'une nouvelle année traitant le premier lundi sont considérés comme étant dans la semaine n°0.	Non pris en charge	Non pris en charge
%w est remplacé par le jour de la semaine en tant que nombre décimal [0,6], 0 représentant le dimanche.	Non pris en charge	Non pris en charge
%x est remplacé par la représentation de la date appropriée pour l'environnement local.	Non identique	Non identique
%X est remplacé par la représentation de l'heure appropriée pour l'environnement local.	Non identique	Non identique
%y est remplacé par l'année sans le siècle en tant que nombre décimal [00,99].	Résultat identique	Résultat identique
%Y est remplacé par l'année avec le siècle en tant que nombre décimal.	Résultat identique	Résultat identique
%Z est remplacé par le nom ou l'abréviation du fuseau horaire ou par aucun octet si aucune information de fuseau horaire n'existe.	Résultat identique	Résultat identique
%% est remplacé par %.	Résultat identique	Résultat identique

Remarques supplémentaires :

- Les formats POSIX suivants ne sont pas pris en charge dans Tivoli Netcool/OMNIbus version 7.3 ou versions ultérieures : %U, %w, %W, %C
- Pour les environnements locaux arabe et hindi, les chiffres de la sortie formatée sont au format numérique hindi au lieu des nombres arabes occidentaux. Le résultat est par conséquent différent du résultat POSIX.
- Les indicateurs de conversion modifiés au format POSIX, qui commencent par E ou O, ne sont pas pris en charge.
- Les formats associés à l'environnement local (%c, %r, %x et %X) peuvent être utilisés individuellement dans une chaîne de format ou ensemble, uniquement dans les associations suivantes :
  - `%x %X`
  - `%x %r`

Les autres associations comme %x %C ou %X %x provoquent une erreur "Invalid date/time format".

- Si les formats associés à l'environnement local (%c, %r, %x et %X) sont utilisés avec des caractères ordinaires ou d'autres formats n'appartenant pas à l'environnement local, notamment %a ou %b, les caractères ou les formats n'appartenant pas à l'environnement local sont ignorés en silence. Exemple :
  - %c YEAR est traité de la même manière que %c
  - %A %b %x est traité de la même manière que %x
- La version 7.2.1 ou les versions inférieures peuvent uniquement faire une analyse syntaxique des chaînes d'heures qui contiennent des informations de fuseau horaire local. L'exemple suivant explique comment une chaîne incluant des informations de fuseau horaire peut être analysée sur le plan syntaxique dans la version 7.3.1 (et ultérieures) :

Chaîne	Sortie

`select to_time( '2009-03-28:10:00:00 GMT+08:00', 'yyyy-MM-dd:HH:mm:ss ZZZZ' ) from alerts.status`	`FUNC`
	`-----------`
	`1238205600`

Traitement de chaînes de caractères codées sur plusieurs octets

Un support est fourni pour gérer les caractères non valides lors du traitement de chaînes de caractères chiffrées sur plusieurs octets. Si un caractère non valide est rencontré, il est remplacé par un point d'interrogation (?)et le traitement se poursuit. Un message d'avertissement est également enregistré dans le fichier journal à propos de ce caractère non valide.

VersionsConcentrateur des services d'application du tableau de bord

L'Interface graphique Web est basée sur Concentrateur des services d'application du tableau de bord version 2.2. Concentrateur des services d'application du tableau de bord version 2.2 peut coexister sur un serveur avec les versions précédentes de Concentrateur des services d'application du tableau de bord. Par exemple, vous pouvez exécuter des produits sur le serveur qui sont basés sur Concentrateur des services d'application du tableau de bord 2.1. Chaque version de Concentrateur des services d'application du tableau de bord doit être installée dans un chemin unique et doit être exécutée sur un numéro de port unique.

Concepts associés:

«Intégration à d'autres produits Tivoli», à la page 62
Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

Intégration à d'autres produits Tivoli

Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

IBM Tivoli Network Manager IP Edition et IBM Tivoli Business Service Manager requièrent une intégration à Tivoli Netcool/OMNIbus pour devenir entièrement opérationnels.

Les informations les plus à jour sur les produits pouvant être intégrés à Tivoli Netcool/OMNIbus sont fournies par les rapports de compatibilité des produits logiciels IBM à l'adresse suivante : http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.jsp Différents rapports sont fournis pour chaque système d'exploitation pris en charge.

Concepts associés:

«Compatibilité avec des versions antérieures», à la page 54
Tivoli Netcool/OMNIbus version 8.1 est compatible avec les versions précédentes du produit. Les exceptions et les solutions sont décrites ici.

Chapitre 17, «Extension des fonctionnalités de Tivoli Netcool/OMNIbus», à la page 429
Tivoli Netcool/OMNIbus inclut un ensemble de ressources qui vous permettent de développer les fonctionnalités du produit. L'intégration à d'autres produits Tivoli est requise pour certaines personnalisations.

«Authentification unique», à la page 573
L'authentification unique (SSO) est prise en charge par les produits Tivoli. Lorsque les utilisateurs se connectent à une application dans un environnement SSO, les informations d'identification utilisateur sont autorisées dans un référentiel central des utilisateurs. Ce référentiel peut être Tivoli Netcool/OMNIbus ObjectServer ou un répertoire LDAP. Après autorisation des informations d'identification utilisateur, les utilisateurs peuvent lancer des applications. L'authentification unique est prise en charge dans des environnements qui sont hébergés dans des serveurs Jazz for Service Management sur plusieurs hôtes, ou un seul hôte.

Tâches associées:

«Extension de la fonctionnalité de l'Interface graphique Web», à la page 587
Tivoli Netcool/OMNIbus inclut des ressources pouvant être utilisées pour étendre la fonctionnalité de l'Interface graphique Web lorsque Tivoli Netcool/OMNIbus est intégré avec d'autres produits.

«Configuration d'intégrations de lancement en contexte dans les produits Tivoli», à la page 591
Vous pouvez configurer l'Interface graphique Web pour qu'elle démarre dans des produits Tivoli compatibles.

Découverte setuid des exécutables de Tivoli Netcool/OMNIbus

Aucun des fichiers exécutables de Tivoli Netcool/OMNIbus ne reconnaissent setuid, sauf mention contraire dans la documentation relative au composant associé. Si un exécutable Tivoli Netcool/OMNIbus est utilisé avec l'attribut setuid, le fichier conserve ses privilèges émis pendant toute la durée de son exécution.

Chapitre 5. Installation et mise à jour de Tivoli Netcool/OMNIbus

Consultez les rubriques suivantes avant d'installer, mettre à jour ou désinstaller Tivoli Netcool/OMNIbus.

Important : Les composants côté serveur sont compatibles avec IBM Tivoli Business Service Manager (TBSM) V4.2.1. Toutefois, si vous avez l'intention d'installer les composants côté serveur sur un ordinateur qui héberge déjà TBSM V4.2.1, vous devez vous assurer que le groupe de correctifs 01 est au moins appliqué à l'installation de TBSM.

Préparation à l'installation

Consultez les rubriques suivantes avant d'installer Tivoli Netcool/OMNIbus.

Fonctions installables de Tivoli Netcool/OMNIbus

Vous pouvez choisir d'installer tout ou partie des fonctionnalités disponibles de Tivoli Netcool/OMNIbus. Par exemple, si vous voulez seulement utiliser des sondes sur un ordinateur particulier, vous pourriez seulement nécessiter les fonctionnalités **Support de sonde** et **Agent de processus**. Vous pouvez modifier votre installation à tout moment pour ajouter ou supprimer des fonctionnalités.

Le tableau suivant indique les fonctions installables pour les installations de composants de serveur de Tivoli Netcool/OMNIbus. La colonne **Fonction** indique la les noms de fonction tels qu'ils apparaissent dans l'interface graphique et la console IBM Installation Manager et leurs identifiants tels qu'utilisés avec les fichiers de réponses. Vous devez spécifier les identifiants de la fonction lors de la création d'un fichier de réponses IBM Installation Manager pour une installation silencieuse. Si vous enregistrez un fichier de réponses au cours d'une installation en mode graphique ou console, la sélection des fonctions est enregistrée à l'aide de ces identifiants.

Tableau 21. Fonctions de Tivoli Netcool/OMNIbus

Fonction	Description
Interface graphique d'administration `nco_admin_gui_feature`	Sélectionnez cette fonction pour installer l'interface graphique d'administration de Netcool/OMNIbus Administrator.
Outils d'administration `nco_admin_tools_feature`	Sélectionnez cette option pour installer les utilitaires de ligne de commande suivants pour une utilisation par les administrateurs système : • outil de création de packages de configuration (**`nco_confpack`**) Utilisez outil de création de packages de configuration pour importer et exporter des parties des configurations de l'ObjectServer. • ObjectServer Report Generator (**`nco_osreport`**) Utilisez ObjectServer Report Generator pour exporter des configurations d'ObjectServer complètes dans des fichiers SQL. Vous pouvez utiliser les fichiers générés pour créer des ObjectServers.

Tableau 21. Fonctions de Tivoli Netcool/OMNIbus (suite)

Fonction	Description
Migration TEC `nco_tec_migration`	Sélectionnez cette option pour installer l'outil de conversion BAROC (**`nco_baroc2sql`**). Vous pouvez utiliser cet outil pour faciliter la migration des fichiers BAROC Tivoli Enterprise Console (TEC) vers SQL.
Interface graphique de l'opérateur `nco_operator_gui_feature`	Sélectionnez cette option pour installer les applications et les utilitaires graphiques suivants pour une utilisation par les opérateurs : • Netcool/OMNIbus Conductor Utilisez Netcool/OMNIbus Conductor pour lancer d'autres applications, pour afficher les configurations, et pour modifier les fichiers de propriétés. • liste d'événements L'interface graphique liste d'événements affiche les événements à code couleur. • liste d'événements transitoires Utilisez l'outil liste d'événements transitoires pour exécuter directement des listes d'événements transitoires personnalisés à partir de la ligne de commande, dans un script, ou dans le cadre d'une liste d'événements. • notification d'événement accéléré L'application notification d'événement accéléré (AEN) permet d'accélérer les événements de priorité élevée afin de garantir une exécution des systèmes sans interruption. • éditeur de serveurs Utilisez l'éditeur de serveurs pour configurer et gérer les informations de communication pour les ObjectServers, les passerelles, les serveurs proxy, et les agents de processus.
ObjectServer `nco_objserv_feature`	Sélectionnez cette fonction pour installer le serveur ObjectServer. Le serveur ObjectServer se trouve sur le serveur de base de données en mémoire au coeur de Tivoli Netcool/OMNIbus. Utilisez le serveur ObjectServer pour stocker et traiter des informations d'alerte. Si vous n'installez pas le composant du serveur ObjectServer, vous devez disposer d'un serveur ObjectServer s'exécutant ailleurs sur votre réseau.
Passerelles ObjectServer `nco_g_objserv_feature`	Sélectionnez cette fonction pour installer les passerelles requises pour envoyer des événements entre les serveurs ObjectServer.
Serveur de pont `nco_bridgeserv_feature`	Sélectionnez cette fonction pour installer le serveur de pont pare-feu. Ce serveur active les sondes pour se connecter à un serveur ObjectServer à partir de l'extérieur d'un pare-feu.
Serveur proxy `nco_proxyserv_feature`	Sélectionnez cette fonction pour installer le serveur proxy. Vous pouvez utiliser le serveur proxy pour réduire le nombre de connexions directes de la sonde à un serveur ObjectServer afin d'améliorer les performances.
Agent de processus `nco_pa_feature`	Sélectionnez cette fonction pour installer l'agent de processus (PA). Utilisez l'agent de processus pour gérer les processus d'ObjectServers, de sondes et de passerelles, et pour exécuter des procédures externes.

Tableau 21. Fonctions de Tivoli Netcool/OMNIbus (suite)

Fonction	Description
Support de sonde `nco_probes_support _feature`	Sélectionnez cette fonction pour installer l'infrastructure requise pour exécuter des sondes. Lorsque vous sélectionnez cette option, les sondes suivantes sont également installées : • Vérificateur de syntaxe de règles de sonde (**nco_p_syntax**) Le vérificateur de syntaxe des règles de sonde vous permet de tester la syntaxe d'un fichier de règles. • Sonde Simnet (**nco_p_simnet**) Utilisez l'analyse Simnet pour générer automatiquement des incidents et simuler des événements de réseau.
Une prise en charge des passerelles `nco_gateways_support _feature`	Sélectionnez cette fonction pour installer l'infrastructure requise pour exécuter des passerelles. Utilisez la fonction **Passerelles ObjectServer** pour installer les passerelles ObjectServer.
Netcool MIB Manager `nco_mib_manager_feature`	Sélectionnez cette fonction pour installer Netcool MIB Manager. MIB Manager génère des fichiers de règles pour la sonde SNMP (**nco_p_mttrapd**) à partir de fichiers MIB SNMP.
Extensions `nco_extensions_feature`	Sélectionnez cette option pour installer des modèles et des fichiers pour étendre les fonctionnalités de Tivoli Netcool/OMNIbus. Les extensions disponibles incluent des configurations pour le contrôle des afflux d'événements, les événements prévisibles et les analyses, l'architecture multiniveau et la gestion des événements pour les environnements virtuels.

Référence associée:

«Migration des données BAROC d'IBM Tivoli Enterprise Console», à la page 136
Tivoli Netcool/OMNIbus fournit l'intégration avec Tivoli Enterprise Console.

Structure du répertoire d'installation

Les packages sont installés dans divers sous-répertoires du répertoire de base Netcool (`NCHOME`) lors d'une installation Tivoli Netcool/OMNIbus.

Les répertoires par défaut qui sont créés lors de l'installation sont décrits dans les sections suivantes :

- «Répertoire de base Netcool (NCHOME)»
- «Répertoires Tivoli Netcool/OMNIbus», à la page 69
- «Répertoires de sondes et de passerelles», à la page 71

Répertoire de base Netcool (NCHOME)

Le répertoire de base de Netcool est le répertoire d'origine dans lequel Tivoli Netcool/OMNIbus est installé. Il est défini par la variable d'environnement `NCHOME`.

UNIX Linux `$NCHOME` a comme valeur par défaut `/opt/IBM/tivoli/netcool`.

Windows `%NCHOME%` a comme valeur par défaut `C:\IBM\Tivoli\Netcool`.

Lorsqu'un répertoire ou un chemin de commande commence par la variable *NCHOME*, l'information s'applique à tous les systèmes d'exploitation pris en charge.

Remarque : N'installez pas de produit qui n'utilise pas Installation Manager dans le même répertoire que Tivoli Netcool/OMNIbus. L'utilisation de différents programmes d'installation pour gérer le même répertoire peut provoquer l'altération d'un ou plusieurs produits.

Remarque : Dans les versions précédentes du produit, la variable d'environnement `OMNIHOME` est utilisée dans les fichiers de configuration. Pour utiliser ces fichiers de configuration anciens dans la version actuelle, définissez `OMNIHOME` dans le répertoire suivant :

- UNIX Linux `$NCHOME/omnibus`
- Windows `%NCHOME%\omnibus`

Le tableau suivant répertorie les sous-répertoires du répertoire de base Netcool.

Remarque : *NCHOME* indique que le répertoire existe sur les systèmes d'exploitation Windows, UNIX et Linux. `$NCHOME` indique un répertoire spécifique d'UNIX ou de Linux. `%NCHOME%` indique un répertoire spécifique de Windows.

Tableau 22. Répertoire de base de Netcool

Répertoire	Description
NCHOME`/bin`	UNIX Linux Emplacement des fichiers binaires du portefeuille Netcool, y compris les utilitaires iKeyman et le script **`nco_run`** ainsi que les liens qui exécutent des applications communes. Windows Emplacement des utilitaires iKeyman.
`$NCHOME/etc`	Emplacement des fichiers de configuration générés ou utilisés par les applications communes ou les produits de tiers et du fichier de configuration de la localisation (`tds.dat`). Vous pouvez modifier ces fichiers.
`$NCHOME/etc/default`	Emplacement des versions de référence par défaut en lecture seule du fichier de configuration de la localisation (`tds.dat`) et d'autres fichiers de configuration.
`$NCHOME/etc/security`	Emplacement du fichier de configuration FIPS 140–2 (`fips.conf`) requis pour l'initialisation de FIPS 140–2 sous Tivoli Netcool/OMNIbus.
`$NCHOME/etc/security/keys`	Emplacement des fichiers de la base de données de clés, créés pour gérer les certificats numériques et les connexions Secure Sockets Layer (SSL).
`%NCHOME%\ini`	Emplacement du fichier de données de connexion (`sql.ini`) et du fichier de configuration (`tds.dat`).
`%NCHOME%\ini\default`	Emplacement des versions de référence par défaut du fichier de données de connexion (`sql.ini`) et du fichier de configuration de localisation (`tds.dat`).

Tableau 22. Répertoire de base de Netcool (suite)

Répertoire	Description
%NCHOME%\ini\security	Emplacement du fichier de configuration FIPS 140–2 (fips.conf) requis pour l'initialisation de FIPS 140–2 sous Tivoli Netcool/OMNIbus.
%NCHOME%\ini\security\keys	Emplacement des fichiers de la base de données de clés, créés pour gérer les certificats numériques et les connexions Secure Sockets Layer (SSL).
NCHOME/license	Emplacement des fichiers de licence IBM et non IBM.
%NCHOME%\locales	Emplacement des fichiers de langue pour les messages.
NCHOME/log	Emplacement du fichier journal de communication pour le serveur ObjectServer.
NCHOME/platform	Emplacement des programmes internes et des bibliothèques utilisés par Tivoli Netcool/OMNIbus.
$NCHOME/properties	Emplacement des fichiers de propriétés.
NCHOME/var	Emplacement des fichiers journaux de passerelle.

Répertoires Tivoli Netcool/OMNIbus

Un certain nombre de répertoires par défaut sont créés lorsque vous installez Tivoli Netcool/OMNIbus.

Le tableau suivant décrit les sous-répertoires du répertoire de base Netcool qui sont spécifiques de Tivoli Netcool/OMNIbus.

NCHOME indique que le répertoire existe sur les systèmes d'exploitation Windows, UNIX et Linux. $NCHOME indique un répertoire spécifique d'UNIX ou de Linux. %NCHOME% indique un répertoire spécifique de Windows.

Tableau 23. Structure de répertoire Tivoli Netcool/OMNIbus

Répertoire	Description
NCHOME/omnibus/bin	Contient des fichiers exécutables Tivoli Netcool/OMNIbus et des fichiers exécutables IEHS permettant de démarrer et d'arrêter un serveur IEHS exécuté localement en mode autonome ou en mode centre d'information. UNIX Linux Emplacement du script **nco_run** et liens qui exécutent des applications Tivoli Netcool/OMNIbus.
NCHOME/omnibus/db	Emplacement des fichiers de la base de données du serveur ObjectServer.
NCHOME/omnibus/desktop	UNIX Linux Emplacement des fichiers de ressource du bureau. **Restriction :** Le répertoire Bureau n'est pas disponible sur une installation Linux on System z ou HP-UX Integrity. Windows Emplacement des fichiers exécutables et des bibliothèques du bureau.

Tableau 23. Structure de répertoire Tivoli Netcool/OMNIbus (suite)

Répertoire	Description
NCHOME/omnibus/etc	Contient des fichiers de configuration requis par l'utilitaire d'initialisation de base de données (**nco_dbinit**) pour créer un serveur ObjectServer, et des fichiers de configuration permettant de mettre à niveau le schéma de base de données. Cet emplacement contient également les fichiers de propriétés et le fichier de configuration permettant de définir les valeurs pour l'exécution du système d'aide en ligne en mode centre d'information. Vous pouvez modifier ces fichiers. Windows Emplacement des fichiers de configuration requis par l'utilitaire d'initialisation de base de données (**nco_dbinit**) pour créer un serveur ObjectServer, et des fichiers de configuration permettant de mettre à niveau le schéma de base de données. Cet emplacement contient également des fichiers de propriétés. Vous pouvez modifier ces fichiers.
NCHOME/omnibus/etc/default	Emplacement des versions de référence par défaut des fichiers de propriétés en lecture seule, et des fichiers de configuration utilisés par l'utilitaire **nco_dbinit** et les utilitaires d'aide en ligne. Windows Emplacement des versions de référence par défaut des fichiers de propriétés et des fichiers de configuration utilisés par l'utilitaire **nco_dbinit**.
NCHOME/omnibus/etc/initial	Emplacement de la copie inscriptible du fichier de propriétés source du serveur ObjectServer (NCOMS.props), utilisée par **nco_dbinit**. Windows Emplacement de la copie inscriptible des fichiers de propriétés source du serveur ObjectServer (NCOMS.props), utilisée par l'utilitaire **nco_dbinit**.
$NCHOME/omnibus/etc/locale	Emplacement des fichiers de définition SQL de bureau traduits dans chaque langue prise en charge. Le fichier de définition SQL de bureau insère les valeurs par défaut dans les tables de bureau, à savoir les couleurs, les visuels de colonne, les conversions, les outils et les menus par défaut.
NCHOME/omnibus/extensions	Emplacement des ressources permettant d'étendre les fonctionnalités de Tivoli Netcool/OMNIbus.
%NCHOME%\omnibus\ini	Emplacement des fichiers de configuration du bureau. Cet emplacement contient également le fichier de configuration permettant de définir les valeurs pour l'exécution du système d'aide en ligne en mode centre d'information. Vous pouvez modifier ces fichiers.
%NCHOME%\omnibus\ini\default	Emplacement des versions de référence des fichiers de configuration du bureau et de l'aide en ligne.

Tableau 23. Structure de répertoire Tivoli Netcool/OMNIbus (suite)

Répertoire	Description
`$NCHOME/omnibus/install`	Emplacement des ressources d'installation des sondes et des passerelles. UNIX Linux Contient également le script de démarrage qui exécute automatiquement le démon de contrôle de processus lors du démarrage du système.
NCHOME`/omnibus/java`	Emplacement des fichiers `.jar` qui prennent en charge les applications Java.
`%NCHOME%\omnibus\locales`	Emplacement des fichiers de localisation des langues.
NCHOME`/omnibus/log`	Emplacement de la plupart des fichiers journaux du serveur ObjectServer. (Le fichier journal de communication du serveur ObjectServer se trouve dans `$NCHOME/log`.)
NCHOME`/omnibus/platform`	Emplacement des ressources dépendant de la plateforme telles que les catalogues, les bibliothèques, les modules et les fichiers IEHS de Tivoli Netcool/OMNIbus.
NCHOME`/omnibus/tsm`	Emplacement d'installation des TSM. Requis pour la compatibilité avec une version antérieure du programme d'installation de la sonde.
NCHOME`/omnibus/upgrade`	Emplacement du script de mise à niveau de Tivoli Netcool/OMNIbus`UPGRADE.SH`, qui migre les données de configuration de l'installation précédente vers une installation de version 8.1. Windows Emplacement des scripts de mise à niveau de Tivoli Netcool/OMNIbus, qui migrent les données de configuration d'une installation précédente vers une installation version 8.1.
NCHOME`/omnibus/utils`	Emplacement des utilitaires **`nco_mail`** et **`nco_functions`**. Peut être utilisé pour stocker des utilitaires similaires utilisés par des outils et des automatisations externes. Windows Emplacement des utilitaires migrés depuis une précédente installation. Le répertoire `utils` est uniquement présent si vous disposiez d'un répertoire `utils`, migré au cours d'une mise à niveau vers la version 8.1.
NCHOME`/omnibus/var`	Emplacement de stockage des informations d'exécution internes.

Répertoires de sondes et de passerelles

Le tableau suivant répertorie les répertoires où des sondes, des passerelles et leurs fichiers de configuration respectifs sont installés.

Remarque : *NCHOME* indique que le répertoire existe sur les systèmes d'exploitation Windows, UNIX et Linux. `$NCHOME` indique un répertoire spécifique d'UNIX ou de Linux. `%NCHOME%` indique un répertoire spécifique de Windows.

Tableau 24. Structure des répertoires de sondes et de passerelles

Répertoire	Description
32-bit `$NCHOME/omnibus/probes` 64-bit `$NCHOME/omnibus/platform/arch/probes64`.	Emplacement d'installation des sondes. Utilisez les scripts d'encapsuleur dans `$NCHOME/omnibus/probes` pour exécuter les sondes sur les systèmes d'exploitation 64 bits et 32 bits.
`%NCHOME%\omnibus\probes`	Emplacement d'installation des sondes.
`%NCHOME%\omnibus\probes\win32`	Emplacement de stockage des fichiers de configuration des sondes. Par exemple, les fichiers de propriétés et de règles.
NCHOME`/omnibus/gates`	Emplacement de stockage des données de configuration des nouvelles passerelles ObjectServer.

Installation de Tivoli Netcool/OMNIbus

Vous pouvez installer Tivoli Netcool/OMNIbus avec l'interface graphique ou la console d'IBM Installation Manager, ou vous pouvez effectuer une installation en mode silencieux. Le produit est disponible sous forme de distribution de fichier compressé sur DVD ou téléchargeable à partir d'IBM Passport Advantage.

La distribution de fichier compressé contient IBM Installation Manager. Utilisez cette option lorsque vous souhaitez installer Tivoli Netcool/OMNIbus sur un petit nombre d'ordinateurs. Vous installerez également le produit via cette option si vous n'avez pas accès à Internet et si vous ne voulez pas gérer votre propre référentiel de logiciels IBM.

Vous avez aussi l'option d'installer IBM Installation Manager séparément et d'utiliser celui-ci pour télécharger et installer le produit à partir d'un référentiel IBM ou d'un référentiel local sur votre réseau. Vous recourrez à cette option pour installer le logiciel ou pour le mettre à jour à la dernière version sans devoir copier les fichiers compressés sur chaque ordinateur. À moins que chaque ordinateur dispose d'un accès à Internet, il vous faudra conserver un ou plusieurs référentiels de logiciels. Pour plus de détails concernant l'utilisation de IBM Installation Manager pour Enterprise Deployment et concernant l'utilitaire Installation Manager Packaging Utility, voir http://www.ibm.com/support/knowledgecenter/SSDV2W_1.0.0/com.ibm.im.articles.doc/topics/entdeployment.htm.

Le tableau qui suit décrit les options disponibles pour l'installation du produit avec IBM Installation Manager.

Tableau 25. Options d'installation

Option d'installation	Description
Option 1	1. Téléchargez et installez IBM Installation Manager. 2. Utilisez IBM Installation Manager pour télécharger et installer Tivoli Netcool/OMNIbus à partir des référentiels IBM Passport Advantage.
Option 2	1. Téléchargez et installez IBM Installation Manager. 2. Utilisez IBM Installation Manager Packaging Utility pour copier Tivoli Netcool/OMNIbus à partir des référentiels IBM Passport Advantage vers un référentiel local. 3. Utilisez IBM Installation Manager pour installer Tivoli Netcool/OMNIbus.

Tableau 25. Options d'installation (suite)

Option d'installation	Description
Option 3	1. Obtenez le fichier de distribution compressé Tivoli Netcool/OMNIbus de IBM Passport Advantage ou sur DVD et extrayez le contenu dans un répertoire temporaire. 2. Utilisez l'un des scripts d'encapsuleur fournis pour installer IBM Installation Manager et Tivoli Netcool/OMNIbus simultanément. Les scripts disponibles sont : `install_gui.sh` (pour les installations via l'interface graphique), `install_console.sh` (pour les installations via la console) ou `install_silent.sh` (pour les installation en mode silencieux). **Remarque :** Ces scripts sélectionnent automatiquement Installation Manager Mode administrateur quand ils sont exécutés par un utilisateur root ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root. Si vous souhaitez utiliser Mode groupe, vous devez installer Installation Manager manuellement avec la commande `groupinst` ou `groupinstc`.
Option 4	1. Téléchargez et installez IBM Installation Manager. 2. Obtenez le fichier de distribution compressé Tivoli Netcool/OMNIbus de IBM Passport Advantage ou sur DVD et stockez le contenu dans un référentiel local. 3. Utilisez IBM Installation Manager pour installer Tivoli Netcool/OMNIbus.

Pour plus de détails concernant l'installation des produits avec IBM Installation Manager, voir http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Installation de Tivoli Netcool/OMNIbus (interface graphique)

Installation de Tivoli Netcool/OMNIbus à partir de l'interface graphique Installation Manager.

Avant de commencer

Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin. Pour l'option d'installation 3, les scripts d'installation sélectionnent automatiquement Installation Manager Mode administrateur quand ils sont exécutés par un utilisateur root, ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root.

Vérifiez que les droits d'accès utilisateur nécessaires sont en place pour vos répertoires d'installation prévus.

Si vous mettez à jour depuis une version précédente de Tivoli Netcool/OMNIbus, vous pouvez choisir de migrer vos données automatiquement vers votre nouvelle installation ou vous pouvez migrer vos données manuellement.

Pourquoi et quand exécuter cette tâche

Les étapes pour démarrer Installation Manager et installer Tivoli Netcool/OMNIbus sont différentes en fonction de l'option Installation que vous choisissez.

Windows Vous devez installer Tivoli Netcool/OMNIbus en tant qu'utilisateur administrateur. Un administrateur par ordinateur peut installer une seule instance de Tivoli Netcool/OMNIbus par ordinateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer Installation Manager, effectuez les vérifications suivantes.

Mode Installation Manager	Contrôle
Mode administrateur	Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur. Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode non-administrateur	Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode groupe	Utilisez l'utilitaire **`id`** pour vérifier que votre groupe utilisateur effectif est adapté à l'installation. Si nécessaire, utilisez la commande suivante pour lancer un nouveau shell avec le groupe effectif correct : `newgrp` *`nom_groupe`* Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask. **Remarque :** Mode groupe n'est pas disponible pour l'option d'installation 3.

2. Démarrez Installation Manager. Avec l'option d'installation 3, cette étape installe et exécute Installation Manager, qui démarre alors automatiquement l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Options d'installation 1 et 2	1. Accédez au sous-répertoire `/eclipse` du répertoire d'installation d'Installation Manager. 2. Utilisez la commande suivante pour démarrer Installation Manager : `./IBMIM`

Option	Description
Option d'installation 3	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus. 2. Accédez au répertoire décompressé et exécutez `./install_gui.sh`. Ce script installe et exécute Installation Manager, qui commence alors automatiquement l'installation de Tivoli Netcool/OMNIbus.
Option d'installation 4	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus dans un référentiel local. 2. Accédez au sous-répertoire `/eclipse` du répertoire d'installation d'Installation Manager et utilisez la commande suivante pour démarrer Installation Manager : UNIX Linux `./IBMIM`

Pour enregistrer les étapes d'installation dans un fichier de réponses à utiliser avec des installations en mode silencieux, utilisez l'option `-record` *`fichier_réponses`*. Exemple :

```
./IBMIM -record /tmp/install_1.xml
```

Cette fonction n'est pas applicable à l'option d'installation 3.

3. Configurez Installation Manager pour accéder aux fichiers d'installation Tivoli Netcool/OMNIbus.

Option	Description
Option d'installation 1	1. Dans le menu principal, sélectionnez **Fichier** > **Préférences**. 2. Vous pouvez définir vos préférences pour les serveurs proxy dans Installation Manager. Les serveurs proxy permettent l'établissement de connexions à des serveurs distants derrière un pare-feu. Dans la fenêtre Préférences, développez le nœud **Internet** : **Proxy FTP** Sélectionnez cette option pour spécifier une adresse hôte et un numéro de port pour le proxy SOCKS. **Proxy HTTP** Sélectionnez cette option pour activer un serveur HTTP ou un proxy SOCKS. Sélectionnez **Enable proxy server**. 3. Dans la fenêtre Préférences, sélectionnez le panneau **Passport Advantage**. 4. Sélectionnez **Se connecter à Passport Advantage**, cliquez sur **Appliquer**, puis cliquez sur **OK**.

Option	Description
Option d'installation 2	1. Dans le menu principal, sélectionnez **Fichier** > **Préférences**. 2. Vous pouvez définir vos préférences pour les serveurs proxy dans Installation Manager. Les serveurs proxy permettent l'établissement de connexions à des serveurs distants derrière un pare-feu. Dans la fenêtre Préférences, développez le nœud **Internet** : **Proxy FTP** Sélectionnez cette option pour spécifier une adresse hôte et un numéro de port pour le proxy SOCKS. **Proxy HTTP** Sélectionnez cette option pour activer un serveur HTTP ou un proxy SOCKS. Sélectionnez **Enable proxy server**. 3. Dans la fenêtre Préférences, sélectionnez le panneau **Référentiels**, puis cliquez sur **Ajouter un référentiel**. 4. Dans la fenêtre Ajouter un référentiel, entrez le chemin ou l'URL de votre référentiel local, puis cliquez sur **OK**. 5. Dans la fenêtre Préférences, cliquez sur **Appliquer**, puis sur **OK**.
Option d'installation 3	Cette étape n'est pas applicable à l'option d'installation 3.
Option d'installation 4	1. Dans le menu principal, sélectionnez **Fichier** > **Préférences**. 2. Dans la fenêtre Préférences, sélectionnez le panneau **Référentiels**, puis cliquez sur **Ajouter un référentiel**. 3. Dans la fenêtre Ajouter un référentiel, entrez le chemin vers le répertoire `OMNIbusRepository` dans le répertoire non compressé, puis cliquez sur **OK**. 4. Dans la fenêtre Préférences, cliquez sur **Appliquer**, puis sur **OK**.

4. Démarrez l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Options d'installation 1, 2 et 4	Dans la fenêtre principale d'Installation Manager, cliquez sur **Installer** et suivez les instructions de l'assistant d'installation pour terminer l'installation.
Option d'installation 3	Cette étape n'est pas applicable à l'option d'installation 3.

5. Suivez les instructions de l'assistant d'installation. Le programme d'installation nécessite l'entrée suivante à différentes étapes de l'installation :

- Lorsque vous y êtes invité(e), entrez votre ID utilisateur et votre mot de passe IBM.
- Lisez et acceptez le contrat de licence.
- Spécifiez un répertoire partagé pour Installation Manager ou acceptez le répertoire par défaut.
- Spécifiez un répertoire d'installation pour Tivoli Netcool/OMNIbus ou acceptez le répertoire par défaut.
- Sélectionnez les fonctions Tivoli Netcool/OMNIbus dont vous avez besoin.
- Si vous mettez à jour depuis une version précédente de Tivoli Netcool/OMNIbus, vous pouvez choisir de migrer vos données automatiquement vers votre nouvelle installation.

6. Une fois l'installation terminée :

   UNIX Linux Cliquez sur Terminer.

   Windows Redémarrez l'ordinateur. Sélectionnez **Redémarrer maintenant** ou **Redémarrer plus tard**, puis cliquez sur **Terminer**.

Résultats

Installation Manager installe Tivoli Netcool/OMNIbus.

Windows Les raccourcis **Netcool Conductor** et **Netcool Suite** sont ajoutés au menu **Démarrer** > **Tous les programmes**. Sous Windows 8 et Windows Server 2012, des raccourcis pour toutes les principales applications sont ajoutées à la vue **Apps**. Les variables d'environnement `NCHOME`, `OMNIHOME`, `SYBASE`, e `PATH` requises pour exécuter les fonctions installées sont définies ou modifiées automatiquement. Ne modifiez pas la valeur de la variable `SYBASE`.

Concepts associés:

«Migration de données», à la page 120
Quand vous effectuez une mise à niveau depuis Tivoli Netcool/OMNIbus V7.4 (ou version antérieure) vers V8.1, vous pouvez soit migrer vos données existantes manuellement, soit utiliser IBM Installation Manager pour une migration automatique.

Référence associée:

«Structure du répertoire d'installation», à la page 67
Les packages sont installés dans divers sous-répertoires du répertoire de base Netcool (`NCHOME`) lors d'une installation Tivoli Netcool/OMNIbus.

«Tâches de post-installation», à la page 86
Après l'installation de Tivoli Netcool/OMNIbus, vous devez réaliser un certain nombre de tâches de post-installation.

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

«Fonctions installables de Tivoli Netcool/OMNIbus», à la page 65
Vous pouvez choisir d'installer tout ou partie des fonctionnalités disponibles de Tivoli Netcool/OMNIbus. Par exemple, si vous voulez seulement utiliser des sondes sur un ordinateur particulier, vous pourriez seulement nécessiter les fonctionnalités **Support de sonde** et **Agent de processus**. Vous pouvez modifier

votre installation à tout moment pour ajouter ou supprimer des fonctionnalités.

«Assistant de configuration initiale», à la page 193
L'assistant de configuration initiale (**nco_icw** automatise certaines tâches de configuration initiale, telles que la création d'ObjectServers et de passerelles.

«IBM Prerequisite Scanner», à la page 30
IBM Prerequisite Scanner est un outil de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit IBM.

Installation de Tivoli Netcool/OMNIbus (console)

Installation de Tivoli Netcool/OMNIbus à partir de la console Installation Manager.

Avant de commencer

Déterminez le mode utilisateur Installation Manager dont vous avez besoin. Pour l'option d'installation 3, les scripts d'installation sélectionnent automatiquement Installation Manager Mode administrateur quand ils sont exécutés par un utilisateur root, ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root.

Vérifiez que les droits d'accès utilisateur nécessaires sont en place pour vos répertoires d'installation prévus.

Si vous mettez à jour depuis une version précédente de Tivoli Netcool/OMNIbus, vous pouvez choisir de migrer vos données automatiquement vers votre nouvelle installation ou vous pouvez migrer vos données manuellement.

Pourquoi et quand exécuter cette tâche

Les étapes pour démarrer Installation Manager et installer Tivoli Netcool/OMNIbus sont différentes en fonction de l'option Installation que vous choisissez.

Windows Vous devez installer Tivoli Netcool/OMNIbus en tant qu'utilisateur administrateur. Un administrateur par ordinateur peut installer une seule instance de Tivoli Netcool/OMNIbus par ordinateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer Installation Manager, effectuez les vérifications suivantes :

Mode Installation Manager	Vérifier
Mode administrateur	Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur. Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode non-administrateur	Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode groupe	Utilisez l'utilitaire **id** pour vérifier que votre groupe utilisateur effectif est adapté à l'installation. Si nécessaire, utilisez la commande suivante pour lancer un nouveau shell avec le groupe effectif correct : `newgrp` *nom_groupe* Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask. **Remarque :** Mode groupe n'est pas disponible pour l'option d'installation 3.

2. Démarrez Installation Manager. Avec l'option d'installation 3, cette étape installe et exécute Installation Manager, qui démarre alors automatiquement l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Options d'installation 1 et 2	1. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager. 2. Utilisez l'une des commandes suivantes pour démarrer Installation Manager : `./imcl -c` OR `./imcl -consoleMode`.
Option d'installation 3	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus. 2. Accédez au répertoire décompressé et exécutez `./install_console.sh`. Ce script installe et exécute Installation Manager, qui commence alors automatiquement l'installation de Tivoli Netcool/OMNIbus.
Option d'installation 4	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus dans un référentiel local. 2. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager. 3. Utilisez l'une des commandes suivantes pour démarrer Installation Manager : `./imcl -c` OR `./imcl -consoleMode`.

3. Configurez Installation Manager pour accéder aux fichiers d'installation Tivoli Netcool/OMNIbus.

Option	Description
Option d'installation 1	1. Dans le menu principal, sélectionnez Préférences. 2. Dans le menu Préférences, sélectionnez Passport Advantage. 3. Dans le menu Passport Advantage, sélectionnez Se connecter à Passport Advantage. 4. Lorsque vous y êtes invité, saisissez votre nom d'utilisateur et votre mot de passe IBM. 5. Revenez au menu principal.
Option d'installation 2	1. Dans le menu principal, sélectionnez Préférences. 2. Dans le menu Préférences, sélectionnez Référentiels. 3. Dans le menu Préférences, sélectionnez Ajouter un référentiel. 4. Entrez le chemin ou l'URL de votre référentiel local. 5. Revenez au menu principal.
Option d'installation 3	Cette étape n'est pas applicable à l'option d'installation 3.
Option d'installation 4	1. Dans le menu principal, sélectionnez Préférences. 2. Dans le menu Préférences, sélectionnez Référentiels. 3. Dans le menu Préférences, sélectionnez Ajouter un référentiel. 4. Entrez le chemin du répertoire `OMNIbusRepository` dans le répertoire décompressé. 5. Revenez au menu principal.

4. Démarrez l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Options d'installation 1, 2 et 4	Dans le menu principal, sélectionnez Installer.
Option d'installation 3	Cette étape n'est pas applicable à l'option d'installation 3.

5. Suivez les instructions de l'assistant d'installation. Le programme d'installation nécessite l'entrée suivante à différentes étapes de l'installation :
   - Lorsque vous y êtes invité, entrez un répertoire partagé Installation Manager ou acceptez le répertoire par défaut.
   - Lorsque vous êtes y invité, entrez un répertoire d'installation ou acceptez le répertoire par défaut.
   - Désélectionnez les fonctions dont vous n'avez pas besoin.

- Si vous mettez à jour depuis une version précédente de Tivoli Netcool/OMNIbus, vous pouvez choisir de migrer vos données automatiquement vers votre nouvelle installation.
- Si nécessaire, générez un fichier de réponses pour une utilisation avec des installations silencieuses sur d'autres ordinateurs. Entrez le chemin de répertoire et un nom de fichier avec une extension `.xml`. Le fichier de réponse est généré avant la fin de l'installation.

6. Une fois l'installation terminée :

   UNIX Linux Sélectionnez Terminé.

   Windows Redémarrez l'ordinateur. Sélectionnez Redémarrer maintenant ou Redémarrer plus tard, puis cliquez sur Terminer.

Résultats

Installation Manager installe Tivoli Netcool/OMNIbus.

Windows Les raccourcis **Netcool Conductor** et **Netcool Suite** sont ajoutés au menu **Démarrer** > **Tous les programmes**. Sous Windows 8 et Windows Server 2012, des raccourcis pour toutes les principales applications sont ajoutées à la vue **Apps**. Les variables d'environnement `NCHOME`, `OMNIHOME`, `SYBASE`, e `PATH` requises pour exécuter les fonctions installées sont définies ou modifiées automatiquement. Ne modifiez pas la valeur de la variable `SYBASE`.

Concepts associés:

«Migration de données», à la page 120
Quand vous effectuez une mise à niveau depuis Tivoli Netcool/OMNIbus V7.4 (ou version antérieure) vers V8.1, vous pouvez soit migrer vos données existantes manuellement, soit utiliser IBM Installation Manager pour une migration automatique.

Référence associée:

«Structure du répertoire d'installation», à la page 67
Les packages sont installés dans divers sous-répertoires du répertoire de base Netcool (`NCHOME`) lors d'une installation Tivoli Netcool/OMNIbus.

«Tâches de post-installation», à la page 86
Après l'installation de Tivoli Netcool/OMNIbus, vous devez réaliser un certain nombre de tâches de post-installation.

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

«Fonctions installables de Tivoli Netcool/OMNIbus», à la page 65
Vous pouvez choisir d'installer tout ou partie des fonctionnalités disponibles de Tivoli Netcool/OMNIbus. Par exemple, si vous voulez seulement utiliser des sondes sur un ordinateur particulier, vous pourriez seulement nécessiter les fonctionnalités **Support de sonde** et **Agent de processus**. Vous pouvez modifier votre installation à tout moment pour ajouter ou supprimer des fonctionnalités.

«Assistant de configuration initiale», à la page 193
L'assistant de configuration initiale (**`nco_icw`** automatise certaines tâches de configuration initiale, telles que la création d'ObjectServers et de passerelles.

«IBM Prerequisite Scanner», à la page 30
IBM Prerequisite Scanner est un outil de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit IBM.

Installation de Tivoli Netcool/OMNIbus (mode silencieux)

Vous pouvez installer Tivoli Netcool/OMNIbus en mode silencieux. Cette méthode d'installation est utile si vous souhaitez des configurations d'installation identiques sur plusieurs postes de travail. L'installation silencieuse nécessite un fichier de réponse qui définit la configuration de l'installation.

Avant de commencer

Effectuez les actions suivantes :

- Créez ou enregistrez un fichier de réponse Installation Manager.

  Vous pouvez spécifier un référentiel de packages local ou distant Tivoli Netcool/OMNIbus dans le fichier de réponse. Vous pouvez également spécifier que Installation Manager télécharge le package de IBM Passport Advantage. Pour plus d'informations sur la spécification de référentiels authentifiés dans les fichiers de réponse, recherchez la rubrique «Storing credentials» dans le centre d'information de Installation Manager :

  http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin. Pour l'option d'installation 3, les scripts d'installation sélectionnent automatiquement Installation Manager Mode administrateur quand ils sont exécutés par un utilisateur root, ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root.
- Lisez le contrat de licence. Le contrat de licence peut être consulté sur le site Web IBM Passport Advantage ou à l'aide de Installation Manager en mode graphique ou console.
- Veillez à ce que les autorisations utilisateur nécessaires soient en place pour les répertoires d'installation prévus.

Pourquoi et quand exécuter cette tâche

Windows Vous devez installer Tivoli Netcool/OMNIbus en tant qu'utilisateur administrateur. Un administrateur par ordinateur peut installer une seule instance de Tivoli Netcool/OMNIbus par ordinateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de commencer l'installation, effectuez les contrôles suivants.

Mode Installation Manager	Contrôle
Mode administrateur	Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur. Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode non-administrateur	Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
Mode groupe	Utilisez l'utilitaire **`id`** pour vérifier que votre groupe utilisateur effectif est adapté à l'installation. Si nécessaire, utilisez la commande suivante pour lancer un nouveau shell avec le groupe effectif correct : `newgrp` *`nom_groupe`* Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask. **Remarque :** Mode groupe n'est pas disponible pour l'option d'installation 3.

2. Démarrez Installation Manager. Avec l'option d'installation 3, cette étape installe et exécute Installation Manager, qui démarre alors automatiquement l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Options d'installation 1 et 2	1. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager. 2. Utilisez la commande suivante pour installer Tivoli Netcool/OMNIbus : UNIX Linux `./imcl -input` *`fichier_réponse`* `-acceptlicense [-log chemin_complet_vers_fichier_journal]` Windows `imcl -input` *`fichier_réponse`* `-acceptlicense [-log chemin_complet_vers_fichier_journal]` Où *`fichier_réponse`* est le chemin du répertoire vers le fichier de réponse.
Option d'installation 3	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus. 2. Accédez au répertoire décompressé et exécutez `./install_silent.sh fichier_réponse -acceptLicense`. Ce script installe et exécute Installation Manager, qui commence alors automatiquement l'installation de Tivoli Netcool/OMNIbus.

Option	Description
Option d'installation 4	1. Décompressez le fichier de distribution compressé Tivoli Netcool/OMNIbus dans un référentiel local. 2. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager. 3. Utilisez la commande suivante pour installer Tivoli Netcool/OMNIbus : UNIX Linux `./imcl -input` *`fichier_réponse`* `-acceptlicense [-log chemin_complet_vers_fichier_journal]` Windows `imcl -input` *`fichier_réponse`* `-acceptlicense [-log chemin_complet_vers_fichier_journal]` Où *`fichier_réponse`* est le chemin du répertoire vers le fichier de réponse.

Résultats

Installation Manager installe Tivoli Netcool/OMNIbus.

Windows Les raccourcis **Netcool Conductor** et **Netcool Suite** sont ajoutés au menu **Démarrer** > **Tous les programmes**. Sous Windows 8 et Windows Server 2012, des raccourcis pour toutes les principales applications sont ajoutées à la vue **Apps**. Les variables d'environnement `NCHOME`, `OMNIHOME`, `SYBASE`, e `PATH` requises pour exécuter les fonctions installées sont définies ou modifiées automatiquement. Ne modifiez pas la valeur de la variable `SYBASE`.

Référence associée:

«Structure du répertoire d'installation», à la page 67
Les packages sont installés dans divers sous-répertoires du répertoire de base Netcool (`NCHOME`) lors d'une installation Tivoli Netcool/OMNIbus.

«Tâches de post-installation», à la page 86
Après l'installation de Tivoli Netcool/OMNIbus, vous devez réaliser un certain nombre de tâches de post-installation.

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

«Fonctions installables de Tivoli Netcool/OMNIbus», à la page 65
Vous pouvez choisir d'installer tout ou partie des fonctionnalités disponibles de Tivoli Netcool/OMNIbus. Par exemple, si vous voulez seulement utiliser des sondes sur un ordinateur particulier, vous pourriez seulement nécessiter les fonctionnalités **Support de sonde** et **Agent de processus**. Vous pouvez modifier votre installation à tout moment pour ajouter ou supprimer des fonctionnalités.

«Mise à niveau à partir de V7.4 (et versions précédentes)», à la page 120
Utilisez IBM Installation Manager pour installer Tivoli Netcool/OMNIbus V8.1. En cours d'installation, vous pouvez utiliser Installation Manager pour migrer automatiquement vos données existantes. Il vous est également possible de migrer

ces données manuellement après installation de la version V8.1.

«IBM Prerequisite Scanner», à la page 30
IBM Prerequisite Scanner est un outil de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit IBM.

Collecte des détails d'installation

Après avoir installé les composants côté serveur de Tivoli Netcool/OMNIbus, vous pouvez exécuter l'outil d'affichage de version de serveur d'objets (**nco_id**) pour vérifier que l'installation des composants a abouti. Les informations recueillies sont également utiles pour le dépannage.

Pourquoi et quand exécuter cette tâche

L'outil d'affichage de version de serveur d'objets est un utilitaire de ligne de commande qui peut recueillir et afficher des informations de base ou détaillées sur votre installation Tivoli Netcool/OMNIbus. Il peut écrire les informations recueillies dans un fichier `.html` ou vous pouvez rediriger la sortie de ligne de commande vers un fichier.

L'ensemble d'informations de base inclut les répertoires d'installation, les produits installés, les composants et les groupes de correctifs.

L'ensemble détaillé des informations comprend l'ensemble des informations de base et les informations suivantes :

- Informations sur le système d'exploitation.
- Informations sur IBM Installation Manager collectées de Tivoli Netcool/OMNIbus ainsi que de toutes les sondes qui sont installées sur l'ordinateur hôte. Le compte d'utilisateur qui exécute **nco_id** doit avoir accès en lecture au répertoire de données Installation Manager et son contenu.
- Liste des fichiers binaires installés dans les répertoires suivants, y compris les sommes SHA1 de tous les fichiers :

  UNIX Linux 32-bit

  – `$NCHOME/omnibus/arch/bin`
  – `$NCHOME/omnibus/arch/lib`

  UNIX Linux 64-bit

  – `$NCHOME/omnibus/arch/bin64`
  – `$NCHOME/omnibus/arch/lib64`

  Windows

  – `%NCHOME%\omnibus\win32\bin`
  – `%NCHOME%\omnibus\win32\lib`
- Heure à laquelle les bibliothèques de produits ont été compilées.

Vous pouvez lancer l'outil d'affichage de version de serveur d'objets avec l'une des commandes suivantes :

- *NCHOME*`/bin/nco_id`
- *NCHOME*`/omnibus/bin/nco_id`

Vous pouvez spécifier les options de ligne de commande suivantes lorsque vous démarrez l'outil.

Option de ligne de commande	Description
`-?`	Affiche des informations d'aide sur les options disponibles.
`-o` *chaîne*	Indique le nom et l'emplacement d'un fichier `.html` dans lequel les informations recueillies sont écrites. Si vous spécifiez uniquement un nom de fichier, le fichier est créé dans le répertoire de travail.
`-s`	Affiche des informations de base sur l'installation. Il s'agit de l'option par défaut.
`-v`	Affiche des informations détaillées sur l'installation.

Procédure

1. Pour écrire les informations détaillées dans un fichier `.html`, utilisez la commande suivante :

   ```
   NCHOME/omnibus/bin/nco_id -o PackageTest.html -v
   ```

2. Pour rediriger les informations détaillées dans un fichier texte, utilisez la commande suivante:

   ```
   NCHOME/omnibus/bin/nco_id -v > PackageTest.txt
   ```

Que faire ensuite

Si un composant que vous avez choisi d'installer est absent des informations recueillies, cela pourrait indiquer qu'un ou plusieurs composants n'ont pas été installés avec succès. Vérifiez les fichiers journaux d'installation et relisez les messages d'installation pour identifier tout problème survenu au cours de l'installation.

Tâches de post-installation

Après l'installation de Tivoli Netcool/OMNIbus, vous devez réaliser un certain nombre de tâches de post-installation.

En fonction de votre environnement d'exploitation, effectuez les tâches suivantes :

- UNIX Linux Définissez des variables d'environnement (le cas échéant).
- Configurez le serveur IEHS pour l'accès à l'aide en ligne.
- Si vous souhaitez fonctionner en mode FIPS 140–2, configurez votre environnement JRE pour FIPS 140–2. Configurez également la prise en charge FIPS 140–2 pour les composants serveur.
- Si vous avez installé la fonction Administrateur, vous pouvez sélectionner un navigateur pour l'aide en ligne de Netcool/OMNIbus Administrator.
- Installez les sondes et les passerelles.
- Windows Si nécessaire, installez des ObjectServers, des serveurs proxy, des agents de processus, des sondes ou des passerelles, comme des services Windows.

Pour obtenir une assistance supplémentaire avec Tivoli Netcool/OMNIbus et pour vous aider à identifier les problèmes, vous pouvez également installer IBM Support Assistant.

Pour utiliser IBM Tivoli Monitoring afin de surveiller et de gérer les ressources Tivoli Netcool/OMNIbus, installez l'agent IBM Tivoli Monitoring for Tivoli

Netcool/OMNIbus. Pour obtenir plus d'informations sur cet agent, voir le manuel *IBM Tivoli Monitoring for Tivoli Netcool/OMNIbus Agent User's Guide*.

Référence associée:

«Fonctions installables de Tivoli Netcool/OMNIbus», à la page 65
Vous pouvez choisir d'installer tout ou partie des fonctionnalités disponibles de Tivoli Netcool/OMNIbus. Par exemple, si vous voulez seulement utiliser des sondes sur un ordinateur particulier, vous pourriez seulement nécessiter les fonctionnalités **Support de sonde** et **Agent de processus**. Vous pouvez modifier votre installation à tout moment pour ajouter ou supprimer des fonctionnalités.

«IBM Support Assistant», à la page 673
IBM Support Assistant (ISA) est un outil de maintenabilité logicielle local gratuit qui vous aide à résoudre les problèmes liés aux applications logicielles IBM. ISA permet d'accéder rapidement aux informations de support et aux outils de maintenabilité pour identifier les problèmes.

Définition des variables d'environnement

UNIX Linux

Une fois l'installation de Tivoli Netcool/OMNIbus sur les systèmes d'exploitation UNIX et Linux terminée, il se peut que vous deviez définir un certain nombre de variables d'environnement.

Le tableau suivant décrit les variables d'environnement que vous pouvez devoir définir. Le format de syntaxe POSIX est obsolète.

Tableau 26. Variables d'environnement

Variable d'environnement	Description
NCHOME	La variable d'environnement spécifie l'emplacement d'origine de Tivoli Netcool/OMNIbus. Vous ne devez pas obligatoirement définir cette variable d'environnement manuellement avant d'exécuter le programme d'installation de Tivoli Netcool/OMNIbus. Il est prévu cette variable d'environnement soit définie automatiquement lorsque vous exécutez une application Tivoli Netcool/OMNIbus qui contient le préfixe `nco_`. **Remarque :** Si vous utilisez plusieurs installations de Netcool, ne définissez pas cette variable. Cette variable peut forcer les programmes d'une installation à utiliser des fichiers d'une autre installation. Cependant, il est utile de définir cette variable lorsque vous utilisez certains utilitaires qui ne font pas partie d'une installation.
OMNIHOME	Cette variable d'environnement était précédemment utilisée pour indiquer l'emplacement d'une installation Tivoli Netcool/OMNIbus. Elle est maintenant utilisée pour fournir le support existant des scripts, des applications tierces et des sondes qui continuent à utiliser la variable d'environnement `$OMNIHOME`. Lorsque vous utilisez de telles applications avec Tivoli Netcool/OMNIbus 8.1, `$OMNIHOME` est automatiquement remplacé par `$NCHOME/omnibus`.

Tableau 26. Variables d'environnement (suite)

Variable d'environnement	Description
PATH	Cette variable d'environnement indique le chemin d'accès aux fichiers exécutables. Pour exécuter des programmes Tivoli Netcool/OMNIbus sans entrer leur chemin d'accès complet chaque fois, vous pouvez ajouter les emplacements de répertoire de ces programmes à votre variable d'environnement `PATH`. Les valeurs de chemin que vous ajoutez peuvent inclure : `$NCHOME/omnibus/bin` et `$NCHOME/omnibus/probes`.
AIX LIBPATH Linux Solaris LD_LIBRARY_PATH	Cette variable d'environnement est spécifique du système d'exploitation. Elle indique le chemin d'accès aux bibliothèques partagées utilisées pour fournir une taille de distribution totale plus faible pour Tivoli Netcool/OMNIbus. Le module de chargement dynamique d'exécution recherche automatiquement des bibliothèques partagées dans le répertoire par défaut suivant : • Sur les systèmes d'exploitation 32 bits : `$NCHOME/platform/`*`arch`*`/lib` • Sur les systèmes d'exploitation 64 bits : `$NCHOME/platform/`*`arch`*`/lib64` Où *arch* est le répertoire qui correspond à votre système d'exploitation. Par exemple, l'emplacement d'installation par défaut des bibliothèques partagées sur un système d'exploitation Solaris 32 bits est `/opt/IBM/tivoli/netcool/platform/solaris2/lib`. AIX Solaris En règle générale, il est inutile de vérifier ou de modifier ce paramètre de variable d'environnement. Toutefois, si un autre utilisateur ou une autre application a modifié cette variable, Tivoli Netcool/OMNIbus peut mal fonctionner ou échouer. Dans cette situation, vérifiez les chemins d'accès aux bibliothèques partagées. Linux L'installation de Netcool/OMNIbus fournit des liens dynamiques (et non statiques) vers la bibliothèque Open Motif 2.2.3. Si cette bibliothèque est installée dans son répertoire système par défaut, (par exemple, `/usr/X11R6/lib/libXm.so.3`), la variable d'environnement LD_LIBRARY_PATH est automatiquement définie sur son chemin d'accès. Cependant, si la bibliothèque est installée dans un emplacement différent, vous devez mettre à jour manuellement la variable d'environnement avec son emplacement. Comme pour les autres systèmes d'exploitation UNIX, vous pouvez vérifier les chemins d'accès aux bibliothèques partagées.

Tableau 26. Variables d'environnement (suite)

Variable d'environnement	Description
NDE_LOGFILE_MAXSIZE	Cette variable d'environnement contrôle la taille maximale des fichiers journaux, en octets, pour le serveur ObjectServer, la passerelle ObjectServer, les serveurs proxy, l'utilitaire **nco_postmsg** et l'utilitaire **nco_bridgeserve**. Lorsque le fichier journal atteint la taille maximale spécifiée, l'application ,par exemple le serveur ObjectServer, renomme le fichier journal, par exemple *nom_serveur*.log en *nom_serveur*.log_old. Elle démarre ensuite un nouveau fichier *nom_serveur*.log. Lorsque le nouveau fichier *nom_serveur*.log atteint la taille maximale, *nom_serveur*.log_old est écrasé, etc. Concernant la variable d'environnement NDE_LOGFILE_MAXSIZE, vous pouvez également utiliser les variables d'environnement NDE_LOGFILE_ROTATION_FORMAT et NDE_LOGFILE_ROTATION_TIME pour imposer la rotation du fichier journal.

Tableau 26. Variables d'environnement (suite)

Variable d'environnement	Description
NDE_LOGFILE_ROTATION_FORMAT	Cette variable d'environnement indique si une rotation de fichier journal a lieu pour le serveur ObjectServer, la passerelle ObjectServer, les serveurs proxy, l'utilitaire **nco_postmsg** et l'utilitaire **nco_bridgeserve**. Cette variable d'environnement indique également un horodatage, qui est ajouté à l'ancien fichier journal après la rotation. Utilisez cette variable d'environnement en parallèle avec la variable d'environnement NDE_LOGFILE_ROTATION_TIME. Si vous définissez la variable NDE_LOGFILE_ROTATION_FORMAT sur une valeur définie, une rotation quotidienne du journal est imposée. Si vous spécifiez une valeur dans une syntaxe au format POSIX ou Local Data Markup Language (LDML), un horodatage est ajouté à l'ancien fichier journal après la rotation. L'horodatage garantit que chaque ancien fichier journal ait un nom unique, de façon à ne pas être écrasé. Un horodatage génère un nom de fichier journal qui respecte le format suivant : *nom_objectserver*.log_201004301356. Pour plus d'informations sur la syntaxe au format LDML, consultez http://userguide.icu-project.org/formatparse/datetime. Si vous ne souhaitez pas d'horodatage, vous pouvez définir la valeur de la variable NDE_LOGFILE_ROTATION_FORMAT en caractères littéraux, par exemple : «rotation.» Après la rotation, cette valeur est ajoutée à l'ancien fichier journal et génère un nom de fichier journal qui respecte le format suivant : *nom_objectserver*.log_rotated. Si vous définissez la variable en caractères littéraires, les anciens fichiers ayant subi une rotation sont écrasés par les fichiers qui ont subi un rotation plus récente, à l'heure spécifiée par la variable d'environnement NDE_LOGFILE_ROTATION_TIME. **Important :** Les caractères littéraux doivent être placés entre des guillemets simples d'échappement (' '), comme il est décrit dans http://userguide.icu-project.org/formatparse/datetime. Si vous définissez la variable d'environnement NDE_LOGFILE_ROTATION_FORMAT, l'environnement NDE_LOGFILE_MAXSIZE est ignoré.
NDE_LOGFILE_ROTATION_TIME	Cette variable d'environnement indique l'heure à laquelle une rotation de fichier journal a lieu, si vous définissez la variable d'environnement NDE_LOGFILE_ROTATION_FORMAT de sorte qu'elle impose une rotation de fichier journal. Cette variable d'environnement affecte le serveur ObjectServer, la passerelle ObjectServer, les serveurs proxy, l'utilitaire **nco_postmsg** et l'utilitaire **nco_bridgeserve**. La variable NDE_LOGFILE_ROTATION_TIME est définie pour indiquer l'heure de la journée la rotation du fichier journal en heures et en minutes. Le format est hhmm, où hh est au format 24 heures.

Exemples

Les exemples suivants montrent comment définir manuellement les variables d'environnement NCHOME, OMNIHOME, PATH, NDE_LOGFILE_MAXSIZE et NDE_LOGFILE_ROTATION_FORMAT, ainsi que NDE_LOGFILE_ROTATION_TIME. Ces exemples supposent que le répertoire de base de Netcool (/opt/IBM/tivoli/netcool) est utilisé pour Solaris, HP-UX, et Red Hat Linux, et que /usr/IBM/tivoli/netcool est utilisé pour AIX.

Exemple : paramètres NCHOME, OMNIHOME et PATH sous Solaris, HP-UX et Red Hat Linux

Chaque utilisateur csh peut ajouter les lignes suivantes à son fichier $HOME/.login :

```
setenv NCHOME /opt/IBM/tivoli/netcool
setenv OMNIHOME $NCHOME/omnibus
setenv PATH $NCHOME/omnibus/bin:$PATH
```

Chaque utilisateur ksh et sh peut ajouter les lignes suivantes à son fichier $HOME/.profile :

```
NCHOME=/opt/IBM/tivoli/netcool;export NCHOME
OMNIHOME=$NCHOME/omnibus;export OMNIHOME
PATH=$PATH:$NCHOME/omnibus/bin;export PATH
```

Exemple : paramètre NCHOME, OMNIHOME et PATH sous AIX

Chaque utilisateur csh peut ajouter les lignes suivantes à son fichier $HOME/.login :

```
setenv NCHOME /usr/IBM/tivoli/netcool
setenv OMNIHOME $NCHOME/omnibus
setenv PATH $NCHOME/omnibus/bin:$PATH
```

Chaque utilisateur ksh et sh peut ajouter les lignes suivantes à son fichier $HOME/.profile :

```
NCHOME=/usr/IBM/tivoli/netcool;export NCHOME
OMNIHOME=$NCHOME/omnibus;export OMNIHOME
PATH=$PATH:$NCHOME/omnibus/bin;export PATH
```

Exemple : Configuration de NDE_LOGFILE_MAXSIZE

L'exemple suivant montre comment définir la taille maximale des fichiers du serveur ObjectServer sur 102 400 octets :

```
setenv NDE_LOGFILE_MAXSIZE 102400
nco_objserv
```

Exemple : Configuration de NDE_LOGFILE_ROTATION_FORMAT et de NDE_LOGFILE_ROTATION_TIME à l'aide de POSIX

L'exemple suivant montre comment faire subir une rotation aux fichiers journaux chaque jour à minuit et comment ajouter l'année, le mois, le jour, l'heure et les minutes au nom des anciens fichiers journaux en utilisant la syntaxe au format POSIX :

```
setenv NDE_LOGFILE_ROTATION_FORMAT %Y%m%d-%H%M
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

Exemple : Configuration de NDE_LOGFILE_ROTATION_FORMAT et de NDE_LOGFILE_ROTATION_TIME à l'aide du format LDML

L'exemple suivant montre comment faire subir une rotation aux fichiers journaux chaque jour à minuit et comment ajouter l'année, le mois, le jour, l'heure et les minutes au nom des anciens fichiers journaux en utilisant la syntaxe au format LDML :

```
setenv NDE_LOGFILE_ROTATION_FORMAT yyyyMMdd-HHmm
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

Exemple : Configuration de NDE_LOGFILE_ROTATION_FORMAT et de NDE_LOGFILE_ROTATION_TIME à l'aide d'une chaîne littérale

L'exemple suivant montre comment faire subir une rotation aux fichiers journaux chaque jour à minuit et comment ajouter «old» (ancien) au nom des anciens fichiers journaux à l'aide de la chaîne de caractère littéraux :

```
setenv NDE_LOGFILE_ROTATION_FORMAT \'old\'
setenv NDE_LOGFILE_ROTATION_TIME 0000
```

Tâches associées:

«Vérification des chemins d'accès de la bibliothèque partagée»
Sur les systèmes d'exploitation UNIX et Linux, Tivoli Netcool/OMNIbus utilise des bibliothèques partagées, qui sont spécifiées par une variable d'environnement, pour fournir une taille de distribution totale plus petite. Si cette variable d'environnement est modifiée, Tivoli Netcool/OMNIbus risque de ne pas fonctionner correctement. Vous devez vérifier que toutes les bibliothèques partagées peuvent être trouvées.

Vérification des chemins d'accès de la bibliothèque partagée

UNIX Linux

Sur les systèmes d'exploitation UNIX et Linux, Tivoli Netcool/OMNIbus utilise des bibliothèques partagées, qui sont spécifiées par une variable d'environnement, pour fournir une taille de distribution totale plus petite. Si cette variable d'environnement est modifiée, Tivoli Netcool/OMNIbus risque de ne pas fonctionner correctement. Vous devez vérifier que toutes les bibliothèques partagées peuvent être trouvées.

Pourquoi et quand exécuter cette tâche

Les variables d'environnement spécifiques au système d'exploitation suivantes sont utilisées pour spécifier l'emplacement des bibliothèques partagées :

- AIX LIBPATH
- Linux Solaris LD_LIBRARY_PATH

AIX Solaris En règle générale, il est inutile de vérifier ou de modifier ce paramètre de variable d'environnement. Toutefois, si un autre utilisateur ou une autre application a modifié cette variable, Tivoli Netcool/OMNIbus peut mal fonctionner ou échouer. Dans ce cas, vous devez vérifier que toutes les bibliothèques partagées peuvent être trouvées.

Procédure

Pour vérifier que les bibliothèques partagées peuvent être trouvées exécutez la commande suivante :

- AIX `dump -H`
- Linux Solaris `ldd`

Ces commandes répertorient les dépendances dynamiques des fichiers exécutables.

Exemple

Le tableau suivant montre comment utiliser ces commandes pour répertorier toutes les dépendances de tous les fichiers binaires installés qui se trouvent dans le répertoire suivant :

- 32-bit `$NCHOME/omnibus/platform/arch/bin/`
- 64-bit `$NCHOME/omnibus/platform/arch/bin64/`

Où *arch* représente le répertoire de votre système d'exploitation.

Tableau 27. Vérification des chemins d'accès de la bibliothèque partagée

Système d'exploitation	Commande	Description de la sortie
Solaris et Linux	32-bit `ldd $NCHOME/omnibus/platform/arch/bin/nco_*` 64-bit `ldd $NCHOME/omnibus/platform/arch/bin64/nco_*`	La sortie de cette commande répertorie les dépendances dynamiques et indique les bibliothèques introuvables.
AIX	32-bit `dump -H $NCHOME/omnibus/platform/arch/bin/nco_*` 64-bit `dump -H $NCHOME/omnibus/platform/arch/bin64/nco_*`	La sortie de cette commande répertorie les dépendances dynamiques et indique les bibliothèques introuvables.

Référence associée:

«Définition des variables d'environnement», à la page 87
Une fois l'installation de Tivoli Netcool/OMNIbus sur les systèmes d'exploitation UNIX et Linux terminée, il se peut que vous deviez définir un certain nombre de variables d'environnement.

Installation des sondes et des passerelles

Les sondes et les passerelles font partie de la suiteTivoli Netcool/OMNIbus et peuvent être installées avecIBM Installation Manager.

UNIX Linux Les sondes et les passerelles 32 bits nécessitent des bibliothèques de système d'exploitation 32 bits qui, si vous utilisez un système d'exploitation 64 bits, peuvent ne pas être déjà installées. Consultez la documentation relative à la sonde ou à la passerelle pour connaître la configuration requise spécifique. Vous pouvez également exécuter IBM Prerequisite Scanner avec la fonction de sonde sélectionnée afin de déterminer si vous disposez de toutes les bibliothèques nécessaires. Les bibliothèques Tivoli Netcool/OMNIbus 32 bits principales qui sont requises pour exécuter des analyses et des passerelles 32 bits (par exemple, `libOpl`) sont installées par défaut.

Sondes

La fonction Support de sonde de Tivoli Netcool/OMNIbus doit être installée avant de procéder à l'installation de la sonde.

Les sondes suivantes sont installées dans le cadre de la fonction Probe Support :

- La sonde Simnet (**nco_p_simnet**) génère automatiquement des incidents et simule les événements réseau.
- Le vérificateur de syntaxe des règles de sonde (**nco_p_syntax**) est utilisé pour tester la syntaxe des fichiers de règles.

Remarque : Ne téléchargez et n'utilisez que des sondes et passerelles nouvelles ou mises à jour dans votre installation version 8.1.

Les sondes sont généralement installées sur un poste de travail distinct de l'hôte ObjectServer. Pour plus d'informations sur l'installation d'une sonde spécifique, voir la documentation de chaque sonde. Vous pouvez également effectuer un déploiement à partir d'un seul ordinateur centralisé sur un ou plusieurs ordinateurs distants à l'aide du mécanisme de déploiement distant fourni par IBM Tivoli Monitoring.

Les sondes sont installées dans le répertoire suivant :

- UNIX Linux 32-bit `$NCHOME/omnibus/probes/arch`
- UNIX Linux 64-bit `$NCHOME/omnibus/platform/arch/probes64`
- Windows `%NCHOME%\omnibus\probes\win32`

Pour lancer une sonde, utilisez son script d'encapsuleur`nco_p_*` dans le répertoire *NCHOME*`/omnibus/probes`.

Passerelles

La fonction Gateway Support de Tivoli Netcool/OMNIbus doit être installée avant de procéder à l'installation de la passerelle.

Les passerelles sont généralement installées sur le serveur principal ou les autres serveurs. Pour plus d'informations sur l'installation d'une passerelle spécifique, voir la documentation de chaque passerelle. Vous pouvez installer des passerelles du serveur ObjectServer dans le cadre de l'installation de Tivoli Netcool/OMNIbus.

Les passerelles sont installées sur les répertoires suivants :

- Fichiers binaires de passerelle : *NCHOME*`/omnibus/bin`
- Fichiers de configuration de passerelle : *NCHOME*`/omnibus/gates`

Référence associée:

«IBM Prerequisite Scanner», à la page 30
IBM Prerequisite Scanner est un outil de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit IBM.

Configuration et exécution de l'aide en ligne

Après avoir installé Tivoli Netcool/OMNIbus, vous devrez peut-être configurer votre système pour accéder à l'aide en ligne. L'aide en ligne est déployée à l'aide d'IBM Eclipse Help System (IEHS) et elle est accessible en mode autonome ou en mode centre d'informations.

Procédure

1. UNIX Linux Utilisez les informations du tableau suivant pour configurer IEHS sur votre système.

Paramètre	Description
Variables d'environnement du navigateur	Ajoutez l'emplacement du répertoire de votre navigateur Web dans les variables d'environnement suivantes (le cas échéant) : • `PATH` • Linux Solaris `LD_LIBRARY_PATH` • AIX `LIBPATH` • Variables d'environnement spécifiques au navigateur , par exemple: `MOZILLA_FIVE_HOME` Le navigateur par défaut du système d'exploitation est utilisé.
Mode autonome Fonction **Local Help System** (Système d'aide local) installée sur un poste de travail client (Fichiers d'aide en ligne installés sur un serveur Web IEHS local)	La configuration est uniquement nécessaire si le numéro de port par défaut d'IEHS, 8888, est utilisé par un autre service local. Si tel est le cas, éditez le fichier de configuration d'IEHS `$NCHOME/omnibus/etc/nco_IEHS.cfg` comme suit : • IEHSMode: 0 • IEHSHost: *laissez vide* • IEHSPort: *numéro de port inutilisé* **Remarque :** Après avoir modifié le numéro de port dans le fichier de configuration, vous devez arrêter le serveur IEHS local pour que vos modifications entrent en vigueur. Exécutez la commande `$NCHOME/omnibus/bin/help_end` pour arrêter le serveur. Il redémarre automatiquement lorsque vous accédez à l'aide en ligne. (Si vous modifiez la définition de vos variables d'environnement pour le navigateur, vous devez également arrêter le serveur IEHS pour que vos modifications entrent en vigueur.)

Paramètre	Description
Mode centre d'informations Fonction **Local Help System** (Système d'aide local) installée sur un serveur distant (Fichiers d'aide en ligne installés sur un serveur Web IEHS distant, généralement géré par un administrateur système)	Sur l'ordinateur désigné comme serveur IEHS, éditez le fichier de configuration IEHS `$NCHOME/omnibus/etc/nco_IEHS.cfg` comme suit : • IEHSMode: 1 • IEHSHost: *laissez vide ou spécifiez l'adresse IP ou le nom d'hôte du serveur IEHS* **Remarque :** IEHS V3.1.1 ne prend pas en charge les adresses IPv6. • IEHSPort: *numéro de port inutilisé pour le serveur IEHS* Le numéro de port par défaut est 8888. Si nécessaire, mettez à jour vos paramètres de pare-feu pour ouvrir le port. Le nom de l'hôte sur lequel le serveur IEHS est exécuté se trouve dans le fichier `$NCHOME/omnibus/platform/arch/nco_IEHS/eclipse/workspace/.metadata/.connection`. Notez que ce fichier est uniquement disponible lorsque le serveur IEHS est en cours d'exécution. Il est supprimé lorsque vous arrêtez le serveur IEHS. Sur chaque poste de travail client, éditez le fichier de configuration IEHS `$NCHOME/omnibus/etc/nco_IEHS.cfg` comme suit : • IEHSMode: 1 • IEHSHost: *adresse IP ou nom d'hôte du serveur IEHS* • IEHSPort: *numéro de port sur lequel le serveur IEHS est exécuté* **Important :** Vous devez dire aux utilisateurs d'effectuer cette tâche.

2. Windows Utilisez les informations du tableau suivant pour configurer IEHS sur votre système.

Paramètre	Description
Mode autonome Fonction **Local Help System** (Système d'aide local) installée sur un poste de travail client (Fichiers d'aide en ligne installés sur un serveur Web IEHS local)	La configuration est uniquement nécessaire si le numéro de port par défaut d'IEHS, 8888, est utilisé par un autre service local. Si tel est le cas, éditez le fichier de configuration d'IEHS `%NCHOME%\omnibus\ini\nco_IEHS.cfg` comme suit : • IEHSMode: 0 • IEHSHost: *laissez vide* • IEHSPort: *numéro de port inutilisé* **Remarque :** Après avoir modifié le numéro de port dans le fichier de configuration, vous devez arrêter le serveur IEHS local pour que vos modifications entrent en vigueur. Exécutez la commande `%NCHOME%\omnibus\bin\help_end.bat` ou cliquez deux fois sur le fichier dans l'Explorateur Windows. (Le serveur redémarre automatiquement lorsque vous accédez à l'aide en ligne.)

Paramètre	Description
Mode centre d'informations Fonction **Local Help System** (Système d'aide local) installée sur un serveur distant (Fichiers d'aide en ligne installés sur un serveur Web IEHS distant, généralement géré par un administrateur système)	Sur l'ordinateur désigné comme serveur IEHS, éditez le fichier de configuration d'IEHS `%NCHOME%\omnibus\ini\nco_IEHS.cfg` comme suit : • IEHSMode: 1 • IEHSHost: *laissez vide ou spécifiez l'adresse IP ou le nom d'hôte du serveur IEHS* **Remarque :** IEHS V3.1.1 ne prend pas en charge les adresses IPv6. • IEHSPort: *numéro de port inutilisé pour le serveur IEHS* Le numéro de port par défaut est 8888. Si nécessaire, mettez à jour vos paramètres de pare-feu pour ouvrir le port. Le nom de l'hôte sur lequel le serveur IEHS est exécuté se trouve dans le fichier `%NCHOME%\omnibus\platform\win32\nco_IEHS\eclipse\workspace\.metadata\.connection`. Notez que ce fichier est uniquement disponible lorsque le serveur IEHS est en cours d'exécution. Il est supprimé lorsque vous arrêtez le serveur IEHS. Sur chaque poste de travail client, éditez le fichier de configuration d'IEHS `%NCHOME%\omnibus\ini\nco_IEHS.cfg` comme suit : • IEHSMode: 1 • IEHSHost: *adresse IP ou nom d'hôte du serveur IEHS* • IEHSPort: *numéro de port sur lequel le serveur IEHS est exécuté* **Important :** Vous devez dire aux utilisateurs d'effectuer cette tâche.

Mode centre d'informations

3. Utilisez les commandes suivantes pour démarrer et arrêter IEHS.
   - Démarrez IEHS : *NCHOME*`/omnibus/bin/IC_start`
   - Arrêtez IEHS : *NCHOME*`/omnibus/bin/IC_end`

Mode autonome

4. En mode autonome, le serveur IEHS local démarre lors de votre première demande d'aide. Utilisez la commande suivante pour l'arrêter.

   NCHOME`/omnibus/bin/help_end`

Concepts associés:

«Exigences relatives à l'aide en ligne», à la page 51
L'aide en ligne de Tivoli Netcool/OMNIbus est déployée à l'aide d'IBM Eclipse Help System (IEHS), qui est une application Web. Tivoli Netcool/OMNIbus prend en charge IEHS V3.1.1.

Configuration de l'environnement d'exécution Java pour FIPS 140–2

Pour configurer l'environnement d'exécution Java (JRE) fourni avec Tivoli Netcool/OMNIbus pour utiliser le chiffrement FIPS 140-2, modifiez la configuration du fichier `java.security`. Vous pouvez également télécharger et ajouter des fichiers de règles pour utiliser des algorithmes de chiffrement étendus.

Procédure

Editez le fichier de sécurité Java

1. En fonction de votre système d'exploitation, ouvrez le fichier suivant `java.security` pour édition.

- UNIX Linux 32-bit `$NCHOME/platform/arch/jre_1.7.0/jre/lib/security/java.security`
- UNIX Linux 64-bit `$NCHOME/platform/arch/jre64_1.7.0/jre/lib/security/java.security`
- Windows `%NCHOME%\platform\win32\jre_1.7.0\jre\lib\security\java.security`

2. Ajoutez les lignes suivantes au début de la section du fichier `List of providers and their preference orders.`

```
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
```

3. Pour chaque entrée de fournisseur existante, incrémentez le nombre `security.provider.x` par deux. Lorsque les modifications sont terminées, la section se présente comme suit :

Linux AIX

```
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.sasl.IBMSASL
security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.11=sun.security.provider.Sun
security.provider.12=com.ibm.security.cmskeystore.CMSProvider
```

HP-UX Solaris

```
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
security.provider.4=sun.security.provider.Sun
security.provider.5=com.ibm.crypto.provider.IBMJCE
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.ibm.security.sasl.IBMSASL
security.provider.9=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.10=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.11=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.12=com.ibm.security.cmskeystore.CMSProvider
```

Windows

```
security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.sasl.IBMSASL
security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.11=sun.security.provider.Sun
security.provider.12=com.ibm.security.cmskeystore.CMSProvider
```

4. Définissez la clé par défaut et les algorithmes de fabrique du gestionnaire d'accréditation pour le module javax.net.ssl :

```
ssl.KeyManagerFactory.algorithm=IbmX509
ssl.TrustManagerFactory.algorithm=IbmX509
```

5. Définissez les implémentations de fournisseur par défaut SSLSocketFactory et SSLServerSocketFactory pour le module javax.net.ssl :

   ```
   ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
   ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
   ```

6. Enregistrez et fermez le fichier.

Résultats

Le JRE est configuré pour fonctionner avec le chiffrement FIPS 140-2.

Référence associée:

«Basculement de votre installation vers le mode FIPS 140-2», à la page 289
Si vous souhaitez changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2, suivez les étapes décrites dans la liste de contrôle de la configuration de FIPS 140-2.

Configuration du chiffrement renforcé : Pourquoi et quand exécuter cette tâche

Pour activer le chiffrement renforcé, vous devez télécharger et installer les fichiers de règles nécessaires qui permettent cette fonctionnalité. Les téléchargements nécessitent un ID IBM et l'acceptation des dispositions du contrat de licence.

Procédure

1. Allez sur le site IBM JCE à l'adresse suivante :

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   Pour plus d'informations sur la sécurité IBM Java, voir le site Web suivant :

   http://www.ibm.com/support/knowledgecenter/api/content/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/introduction.html

2. Si vous avez déjà un identifiant IBM, connectez-vous. Sinon, cliquez sur le lien **register here** (S'enregistrer ici) pour créer un ID IBM.
3. Sélectionnez **Unrestricted JCE Policy files for SDK** pour toutes les versions les plus récentes et cliquez sur **Continue**.
4. Lisez et acceptez les dispositions du contrat de licence et téléchargez le fichier d'archive des fichiers de règles.
5. Sur l'ordinateur hôte Tivoli Netcool/OMNIbus extrayez les fichiers `local_policy.jar` et `US_export_policy.jar` de l'archive et copiez-les dans le répertoire suivant (remplacez les fichiers existants).
   - UNIX Linux 32-bit `$NCHOME/platform/arch/jre_1.7.0/jre/lib/security`
   - UNIX Linux 64-bit `$NCHOME/platform/arch/jre64_1.7.0/jre/lib/security`
   - Windows `%NCHOME%\platform\win32\jre_1.7.0\jre\lib\security`
6. Mettez à jour les fichiers de règles sur chaque ordinateur.

Configuration des composants Tivoli Netcool/OMNIbus comme services Windows

Les composants serveur et sondes de Tivoli Netcool/OMNIbus peuvent être installés pour être exécutés en tant que services sur un hôte Windows. Les composants serveur que vous installez en tant que services incluent le serveur ObjectServer, l'agent de processus, le serveur proxy et les passerelles.

Pourquoi et quand exécuter cette tâche

Vous pouvez installer, configurer et désinstaller des services en exécutant un utilitaire de ligne de commande. Vous pouvez également configurer des services installés dans la fenêtre Services du Panneau de configuration.

La pratique standard sous Windows consiste à configurer vos services Tivoli Netcool/OMNIbus avec le démarrage automatique.

Vous pouvez également configurer les composants Tivoli Netcool/OMNIbus pour qu'ils soient exécutés comme processus Tivoli Netcool/OMNIbus dans un système de contrôle des processus. Si vous prévoyez d'utiliser le contrôle des processus, l'approche privilégiée est d'installer vos agents de processus en tant que services Windows puis de configurer les autres composants pour l'exécution en tant que processus dans le système de contrôle des processus. Pour obtenir plus d'informations sur le contrôle du processus, voir le manuel *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Installation, configuration et désinstallation des services pour les composants serveur :

Pour installer, configurer ou désinstaller les composants serveur de Tivoli Netcool/OMNIbus en tant que services, vous devez exécuter le fichier exécutable du composant avec une ou plusieurs options de ligne de commande supplémentaires.

Pourquoi et quand exécuter cette tâche

La procédure suivante décrit comment installer des ObjectServers, des serveurs proxy, des agents de processus et des passerelles en tant que services Windows. Pour plus d'informations sur l'installation de sondes en tant que services Windows, voir la documentation de chaque sonde.

Procédure

Pour installer, configurer ou désinstaller un service Tivoli Netcool/OMNIbus :

1. Dans une invite de commande, entrez la commande suivante :

   ```
   %NCHOME%\omnibus\bin\nco_nom [option [valeur]...]
   ```

   Dans cette commande :

   - **nco_***nom* représente un des noms de fichier exécutable indiqué dans le tableau ci-dessous.

Tableau 28. Noms de fichiers exécutables pour les composants serveur

Type de composant	Nom du fichier exécutable
ObjectServer	**nco_objserv**
Serveur proxy	**nco_proxyserv**
Agent de processus	**nco_pad**
Passerelle	**nco_g_***nom_passerelle* *nom_passerelle* est le nom abrégé d'un type de passerelle.

- Les crochets représentent des entrées facultatives pour les options de ligne de commande que vous pouvez utiliser avec la commande **nco_***nom*. Le tableau suivant répertorie chaque *option* ainsi que sa *valeur* (le cas échéant).

Tableau 29. Options de ligne de commande pour installer, configurer et désinstaller les services Tivoli Netcool/OMNIbus

Option de ligne de commande	Fonction
`/INSTALL`	Installe un composant serveur ou une sonde Tivoli Netcool/OMNIbus en tant que service.
`/REMOVE`	Supprime un service installé.
`/NOAUTO`	Installe le service avec un démarrage manuel. Ignorez cette option pour exécuter le service avec le démarrage automatique.
`/DEPEND` *srv @grp...*	Spécifie les autres services ou groupes dont dépend le service installé. Si vous utilisez cette option, ce service ne démarre pas avant l'exécution des services (*srv*) et groupes (*@ grp*) que vous spécifiez. **Remarque :** La valeur de *srv* doit être le **Nom du service** et *pas* le **Nom d'affichage**. Pour afficher le **Nom du service**, ouvrez le Panneau de configurationWindows puis cliquez deux fois sur **Outils d'administration** puis sur **Services**. Cliquez deux fois sur l'entrée du service concerné pour ouvrir la fenêtre Propriétés. Le **Nom du service** est affiché dans l'onglet **Général** de la fenêtre Propriétés.
`/GROUP` *nom*	Installe le service comme membre d'un groupe, où *nom* représente le nom du groupe. Cette option est utilisée avec l'option de ligne de commande `/DEPEND`. Vous pouvez par exemple regrouper toutes les sondes sous le même nom de groupe. Vous pouvez ensuite forcer la dépendance de ce groupe à un autre service.

Tableau 29. Options de ligne de commande pour installer, configurer et désinstaller les services Tivoli Netcool/OMNIbus (suite)

Option de ligne de commande	Fonction
/ACCOUNT [*domaine*\]*utilisateur*	Spécifie que le service se connecte à un compte utilisateur. Dans cette syntaxe de commande, *domaine* représente le nom du domaine, qui est facultatif (comme indiqué par les crochets), et *utilisateur* représente le nom d'utilisateur. Si vous utilisez l'option de ligne de commande /ACCOUNT, vous devez également spécifier l'option /PASSWORD. Si vous omettez l'option de ligne de commande /ACCOUNT, le service se connecte au compte système local. Par exemple, si vous souhaitez installer un service d'agent de processus en tant qu'utilisateur du poste de travail local (c'est-à-dire, Administrateur), *domaine* n'est pas requis. Entrez : `nco_pad /INSTALL /ACCOUNT Administrator` **Conseil :** Tenez compte du fait que le compte requiert des droits "connexion comme service", automatiquement octroyés lorsque vous spécifiez un compte de connexion pour le service dans la fenêtre Services du Panneau de configuration. Cela n'est pas le cas si vous utilisez l'option /ACCOUNT avec l'option /INSTALL lorsque vous installez le service depuis la ligne de commande.
/PASSWORD *mot_de_passe*	Spécifie une chaîne *mot_de_passe* pour le compte utilisateur.
/INSTANCE *ID*	Spécifie un identificateur d'instance unique pour un service, où *ID* représente l'identificateur. Par exemple, si vous installez plusieurs services d'agent de processus, le deuxième service et les services suivants requièrent chacun un ID unique.

Tableau 29. Options de ligne de commande pour installer, configurer et désinstaller les services Tivoli Netcool/OMNIbus (suite)

Option de ligne de commande	Fonction
`/CMDLINE "`*option*`"`	Spécifie une ou plusieurs options de ligne de commande à définir dès que le service est redémarré. Veillez à inclure les options de ligne de commande entre guillemets. Utilisez des options de ligne de commande disponibles pour le type de composant qui est configuré. Par exemple, pour le serveur ObjectServer, spécifiez une ou plusieurs options de ligne de commande pouvant être utilisées avec la commande **nco_objserv**, ou pour l'agent de processus, spécifiez une ou plusieurs options de ligne de commande pouvant être utilisées avec la commande**nco_pad**. Exemples : • Pour spécifier l'agent de processus qui doit être exécuté au démarrage d'un service pour l'agent de processus NCO_PA, définissez la valeur de *option* sur `"-name NCO_PA"`. • Pour spécifier un autre fichier journal `/tmp/my_pafile.log` dans lequel les messages sont écrits, définissez la valeur *option* sur `"-logfile /tmp/my_pafile.log"`.
`/BACKOFF` *n*	Définit le nombre maximum de tentatives de démarrage ou de connexion du service, où *n* est un entier représentant ce nombre. Par exemple, pour spécifier le nombre maximum de tentatives de connexion d'une sonde au serveur ObjectServer NCOMS, incluez les options suivantes lors de l'installation du service de sonde : `/CMDLINE "-server NCOMS" /BACKOFF 3`

Conseil : Vous pouvez afficher les options de ligne de commande pour l'installation, la configuration et la désinstallation de ces services Windows en utilisant la commande suivante :
`%NCHOME%\omnibus\bin\nco_`*nom*`.exe /?`

2. Après avoir installé les services, redémarrez l'ordinateur.

Que faire ensuite

Une fois qu'un composant serveur est installé en tant que service, vous devez utiliser l'éditeur de serveurs pour définir l'hôte et le numéro de port du service avant de le démarrer.

Utilisez également la fenêtre Services du Panneau de configuration pour affecter un des comptes utilisateur suivants au service :

- Compte système local (LocalSystem). Il s'agit de l'option par défaut et privilégiée. Ce compte n'a pas de mot de passe.
- Un compte qui appartient au groupe Administrateurs sur l'ordinateur local. Avec cette option, il est recommandé d'utiliser des comptes dont les mots de passe n'expirent pas.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Affichage et reconfiguration des services installés :

Vous pouvez afficher et reconfigurer les services Windows que vous avez installé pour les composants serveur et les sondes Tivoli Netcool/OMNIbus.

Pourquoi et quand exécuter cette tâche

Pour afficher et reconfigurer les services installés :

Procédure

1. Ouvrez le Panneau de configuration Windows.
2. Cliquez deux fois sur **Outils d'administration** puis sur **Services**. La fenêtre Services s'ouvre avec une liste de tous les services Windows actuellement installés sur votre ordinateur. Les noms d'affichage et de service de tous les services Tivoli Netcool/OMNIbus commencent par `Netcool` ou `NCO`, comme indiqué dans le tableau suivant.

Tableau 30. Noms d'affichage et de service

Type de composant	Nom d'affichage	Nom du service
ObjectServer	**Netcool/OMNIbus Object Server** **Remarque :** Si plusieurs services ObjectServer sont installés, le deuxième service et les services suivants sont affichés comme : **Netcool/OMNIbus Object Server (*ID*)**. Dans ce cas, *ID* est l'identificateur spécifié par l'option de ligne de commande `/INSTANCE` lors de l'installation du service.	**NCOObjectServer** Les noms de service supplémentaires sont au format : **NCOObjectServer$*ID*** Où, *ID* est l'identificateur spécifié par l'option de ligne de commande `/INSTANCE` lors de l'installation du service.
Agent de processus	**NCO Process Agent** (NCO Agent de processus)	**NCOProcessAgent**
Serveur proxy	**NCO Proxy Server** (NCO Serveur proxy)	**NCOProxyServer**
Passerelle ObjectServer (unidirectionnelle)	u**Netcool/OMNIbus Uni-Directional ObjectServer Gateway** (Netcool/OMNIbus passerelle ObjectServer unidirectionnelle)	**NCOObjectServerGatewayUni**

Tableau 30. Noms d'affichage et de service (suite)

Type de composant	Nom d'affichage	Nom du service
Passerelle ObjectServer (bidirectionnelle)	u**Netcool/OMNIbus Bi-Directional ObjectServer Gateway** (Netcool/OMNIbus passerelle ObjectServer bidirectionnelle)	**NCOObjectServerGatewayBi**
Sonde	**NCO Sonde *nom*** Où *nom* est le nom unique abrégé de la sonde. Par exemple : **NCO SimNet Probe** (NCO Sonde SimNet)	**NCO Sonde *nom***

3. Utilisez la fenêtre Services pour démarrer et arrêter les services en fonction de vos besoins.
4. Utilisez la fenêtre Propriétés de chaque service pour configurer les propriétés suivantes :
   - Le type de démarrage du service. Il peut être `Automatique`, `Manuel` ou `Désactivé`.
   - Le compte de connexion pour le service
   - L'action de reprise à effectuer en cas d'échec du service

Résultats

Remarque : Si un serveur ObjectServer et une sonde sont démarrés en tant que services, la sonde peut démarrer en premier mais ne peut pas se connecter au serveur ObjectServer avant que celui-ci ne soit en cours d'exécution.

Exemples : configuration de composants en tant que services :

Ces exemples présentent comment installer, exécuter et désinstaller des composants Tivoli Netcool/OMNIbus en tant que services Windows.

Exemple : installation et exécution de l'agent de processus en tant que service :

Cet exemple présente comment installer, exécuter et désinstaller l'agent de processus en tant que service Windows.

Pour installer l'agent de processus en tant que service Windows procédez comme suit :

1. Exécutez l'éditeur de serveur pour définir les détails de connexion de l'agent de processus.
2. Exécutez les commandes suivantes dans l'ordre pour ouvrir une fenêtre d'invite de commande et installer l'agent de processus en tant que service :

   ```
   cmd.exe
   cd %NCHOME%\omnibus\bin
   nco_pad /install
   ```

   Le service est installé avec le nom de service **NCOProcessAgent**.

   Voici un autre exemple de commande pour installer l'agent de processus en tant que service :

```
nco_pad /install /noauto /cmdline "-secure -debug 1 -cryptalgorithm
AES_FIPS -keyfile \"%OMNIHOME%/bin/fichier-de-clés1\""
```

Dans cet exemple, le service est installé avec un démarrage manuel. L'agent de processus est configuré pour s'exécuter en mode sécurisé et consigner des informations sur les processus qu'il démarre dans son fichier journal. L'algorithme et le fichier de clés, qui peuvent être utilisés pour déchiffrer les mots de passe dans le fichier de configuration de l'agent de processus, sont également indiqués. Un tel déchiffrement des mots de passe est obligatoire si votre fichier de configuration contient des mots de passe chiffrés qui ont été générés avec la commande **nco_aes_crypt**. Notez que vous devez échapper les guillemets imbriqués avec des barres obliques inversées, comme indiqué avec la valeur `-keyfile`.

Pour démarrer l'agent de processus en tant que service, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net start NCOProcessAgent
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service d'agent de processus de Tivoli Netcool/OMNIbus et démarrez-le. Vous pouvez également configurer le type de démarrage du service sur `Automatique`.

Pour arrêter le service d'agent de processus, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net stop NCOProcessAgent
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service d'agent de processus de Tivoli Netcool/OMNIbus et arrêtez-le.

Pour désinstaller le service, exécutez la commande suivante :

```
nco_pad /remove
```

Exemple : installation, exécution et désinstallation d'un serveur ObjectServer appelé MYSERV en tant que service Windows :

Cet exemple présente comment installer, exécuter et désinstaller un serveur ObjectServer appelé MYSERV en tant que service Windows.

Pour installer un serveur ObjectServer appelé MYSERV en tant que service, procédez comme suit :

1. Exécutez l'éditeur de serveur pour définir les détails de connexion du nouveau serveur.
2. Exécutez les commandes suivantes dans l'ordre pour ouvrir une fenêtre d'invite de commande, initialiser la base de données et installer le serveur ObjectServer en tant que service :

   ```
   cmd.exe
   cd %NCHOME%\omnibus\bin
   nco_dbinit -server MYSERV
   nco_objserv /install /cmdline "-name MYSERV"
   ```

   Le service est installé avec le nom de service **NCOObjectServer**.

Pour démarrer le serveur ObjectServer en tant que service, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net start NCOObjectServer
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service du serveur ObjectServer de Tivoli Netcool/OMNIbus et démarrez-le.

Pour arrêter le service du serveur ObjectServer, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net stop NCOObjectServer
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service du serveur ObjectServer de Tivoli Netcool/OMNIbus et arrêtez-le.

Pour désinstaller le service, exécutez la commande suivante :

```
nco_objserv /remove
```

Référence associée:

Windows «Exemple: installation, exécution et désinstallation d'un deuxième ObjectServer appelé OSTWO sur le même hôte»
Cet exemple présente comment installer, exécuter et désinstaller un service Windows pour un deuxième ObjectServer appelé OSTWO sur le même hôte que le premier ObjectServer.

Exemple: installation, exécution et désinstallation d'un deuxième ObjectServer appelé OSTWO sur le même hôte :

Cet exemple présente comment installer, exécuter et désinstaller un service Windows pour un deuxième ObjectServer appelé OSTWO sur le même hôte que le premier ObjectServer.

Pour installer un deuxième ObjectServer appelé OSTWO en tant que service, procédez comme suit :

1. Exécutez l'éditeur de serveur pour définir les détails de connexion du nouveau serveur.
2. Exécutez les commandes suivantes dans l'ordre pour ouvrir une fenêtre d'invite de commande, initialiser la base de données et installer le serveur ObjectServer en tant que service :

   ```
   cmd.exe
   cd %NCHOME%\omnibus\bin
   nco_dbinit -server OSTWO
   nco_objserv /install /instance TWO /cmdline "-name OSTWO"
   ```

   Le service est installé avec le nom de service **NCOObjectServer$TWO**.

Pour démarrer le serveur ObjectServer en tant que service, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net start NCOObjectServer$TWO
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service du serveur ObjectServer de Tivoli Netcool/OMNIbus et démarrez-le.

Pour arrêter le service du serveur ObjectServer, utilisez l'une des méthodes suivantes :

- Dans la ligne de commande, exécutez la commande suivante :

  ```
  net stop NCOObjectServer$TWO
  ```

- Dans le Panneau de configuration de Windows, cliquez deux fois sur **Outils d'administration**, puis sur **Services**. Recherchez le service du serveur ObjectServer de Tivoli Netcool/OMNIbus et arrêtez-le.

Pour désinstaller le service, exécutez la commande suivante :

```
nco_objserv /remove /instance TWO
```

Référence associée:

Windows «Exemple : installation, exécution et désinstallation d'un serveur ObjectServer appelé MYSERV en tant que service Windows», à la page 106
Cet exemple présente comment installer, exécuter et désinstaller un serveur ObjectServer appelé MYSERV en tant que service Windows.

Exemple : installation et exécution du serveur proxy en tant que service :

Cet exemple présente comment installer et exécuter le serveur proxy en tant que service Windows.

Pour installer et exécuter le serveur proxy en tant que service, exécutez les commandes suivantes dans l'ordre :

```
cmd.exe

cd %NCHOME%\omnibus\bin

nco_proxyserv /install

net start NCOProxyServer
```

Exemple : installation et exécution de passerelles du serveur ObjectServer en tant que services :

Cet exemple présente comment installer et exécuter les passerelles du serveur ObjectServer en tant que services Windows.

Pour installer et exécuter une passerelle bidirectionnelle appelée BI_GATE en tant que service, exécutez les commandes suivantes dans l'ordre :

```
cmd.exe

cd %NCHOME%\omnibus\bin

nco_g_objserv_bi /install /cmdline "-name BI_GATE"

net start NCOObjectServerGatewayBi
```

Pour installer et exécuter une passerelle unidirectionnelle appelée UNI_GATE en tant que service, exécutez les commandes suivantes dans l'ordre :

```
cmd.exe

cd %NCHOME%\omnibus\bin

nco_g_objserv_uni /install /cmdline "-name UNI_GATE"

net start NCOObjectServerGatewayUni
```

Exemple : installation de services avec des dépendances :

Cet exemple présente comment installer les composants Tivoli Netcool/OMNIbus centraux en tant que services dans un groupe appelé OmniCore, puis installer une passerelle bidirectionnelle qui dépend de ce groupe.

Exécutez les commandes suivantes dans l'ordre :

```
cmd.exe

cd %NCHOME%\omnibus\bin

nco_objserv /install /group OmniCore

nco_pad /install /group OmniCore

nco_proxyserv /install /group OmniCore

nco_g_objserv_bi /install /depend @OmniCore
```

Retrait de Tivoli Netcool/OMNIbus

Utilisez IBM Installation Manager pour supprimer Tivoli Netcool/OMNIbus ainsi que les sondes ou les passerelles. Vous ne pouvez pas supprimer Tivoli Netcool/OMNIbus sans supprimer toutes les sondes ou les passerelles installées au même moment. Vous pouvez supprimer une ou plusieurs sondes ou passerelles sans retirer Tivoli Netcool/OMNIbus.

Avant de commencer

Effectuez les actions suivantes :

- Sauvegardez tous les fichiers de données ou de configuration qui ont été créés depuis l'installation initiale et que vous voulez conserver.
- Pour effectuer une suppression en mode silencieux, créez ou enregistrez un fichier de réponses Installation Manager. Utilisez l'option `-record` *`fichier_réponses`*. Par exemple :

  ```
  ./IBMIM -record /tmp/install_1.xml
  ```

Procédure

1. Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
2. Retirez tous les services Tivoli Netcool/OMNIbus qui ont été installés manuellement :
   a. Arrêtez le service.

b. Retirez les services de sonde en exécutant le fichier exécutable pour la sonde avec l'option de ligne de commande `-remove`.

c. Supprimez d'autres services Tivoli Netcool/OMNIbus en exécutant le fichier exécutable approprié avec l'option de ligne de commande `/REMOVE`. Si vous avez installé le service avec un identificateur d'instance, vous devez également inclure l'option de ligne de commande `/INSTANCE`.

Suppression via l'interface graphique

3. Pour supprimer Tivoli Netcool/OMNIbus avec l'interface graphique d'Installation Manager :
   a. Accédez au sous-répertoire `/eclipse` du répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour démarrer l'assistant Installation Manager :

      UNIX Linux `./IBMIM`

      Windows `IBMIM`

   c. Dans la fenêtre principale d'Installation Manager, cliquez sur **Désinstaller**.
   d. Sélectionnez les offres que vous voulez supprimer et suivez les instructions de l'assistant d'installation pour effectuer la suppression.

Suppression via la console

4. Pour supprimer Tivoli Netcool/OMNIbus avec la console d'Installation Manager :
   a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour démarrer Installation Manager :

      UNIX Linux `./imcl -c`

      Windows `imcl -c`

   c. Dans le menu principal, sélectionnez Désinstaller.
   d. Sélectionnez les offres que vous voulez supprimer et suivez les instructions d'Installation Manager pour effectuer la suppression.

Suppression en mode silencieux

5. Pour supprimer Tivoli Netcool/OMNIbus en mode silencieux :
   a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour lancer la suppression :

      UNIX Linux `./imcl -input` *`fichier_réponses`*

      Windows `imcl -input` *`fichier_réponses`*

      Où *`fichier_réponses`* est le chemin de répertoire vers le fichier de réponses qui définit la configuration de la suppression.

Résultats

Installation Manager supprime les fichiers et les répertoires qu'il a installés.

Que faire ensuite

Les fichiers qui n'ont pas été installés par Installation Manager et les fichiers de configuration qui ont été modifiés sont laissées en place. Examinez ces fichiers et supprimez-les ou sauvegardez-les de façon appropriée.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Mise à jour de Tivoli Netcool/OMNIbus

Vous devez utiliser IBM Installation Manager pour mettre à jour votre installation Tivoli Netcool/OMNIbus. Vous pouvez mettre à jour vers une nouvelle version du produit, modifier une installation existante, ou appliquer des groupes de correctifs sur une installation existante.

Préparation à la mise à niveau

Avant de mettre à jour votre installation Tivoli Netcool/OMNIbus, vous devez arrêter tous les processus en cours d'exécution ou les services Windows et sauvegarder vos ObjectServers existants.

Procédure

1. Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours d'exécution.
2. Arrêtez le serveur IBM Eclipse Help System (IEHS) qui exécute l'aide en ligne.
3. Windows Si des services de votre installation existante ont été installés manuellement, entrez la commande suivante pour les désinstaller manuellement.

   ```
   %OMNIHOME%\bin\nco_nom /remove [/instance ID]
   ```

   Dans cette commande, %OMNIHOME% représente %NCHOME%\omnibus. Remplacez nco_*nom* par le nom du fichier exécutable d'un composant serveur, d'une sonde ou d'une passerelle. Remplacez *ID* par un identificateur d'instance unique qui peut avoir été spécifié lors de l'installation du service. Par exemple, pour désinstaller un service ObjectServer avec un ID OBJTWO, entrez `%OMNIHOME%\bin\nco_objserv /remove /instance OBJTWO`
4. Utilisez l'interface interactive SQL pour sauvegarder le serveur ObjectServer existant.

   La syntaxe est `ALTER SYSTEM BACKUP 'répertoire_sauvegarde';`.

   Par exemple :

   ```
   1> alter system backup 'tmp/backups/NCOMS';
   2> go
   ```

   La commande `ALTER SYSTEM BACKUP` génère des copies des fichiers `.tab` du serveur ObjectServer dans le répertoire spécifié. Le répertoire de sauvegarde ne peut pas être l'emplacement en cours des fichiers de données ObjectServer (par défaut : *NCHOME*/omnibus/db/*nom_ObjectServer*).
5. Sauvegardez l'Interface graphique Web.

   Exportation les données de configuration à partir du serveur Interface graphique Web. Les données sélectionnées sont écrites dans un fichier `.zip` que vous pouvez copier dans un emplacement sécurisé.
6. Pour restaurer l'ObjectServer, copiez les fichiers `.tab` dans le répertoire de fichiers de données de l'ObjectServer.

7. Pour restaurer Interface graphique Web, importez les données précédemment exportées.

Tâches associées:

«Configuration et exécution de l'aide en ligne», à la page 95
Après avoir installé Tivoli Netcool/OMNIbus, vous devrez peut-être configurer votre système pour accéder à l'aide en ligne. L'aide en ligne est déployée à l'aide d'IBM Eclipse Help System (IEHS) et elle est accessible en mode autonome ou en mode centre d'informations.

Mise à jour de Tivoli Netcool/OMNIbus (interface graphique)

Vous pouvez utiliser l'interface graphique Installation Manager pour mettre à jour votre installation de Tivoli Netcool/OMNIbus.

Avant de commencer

Vous devez avoir un ID IBM pour télécharger le logiciel de IBM Passport Advantage.

Effectuez les actions suivantes :

- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin.
- Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
- Sauvegardez votre installation et vos données Tivoli Netcool/OMNIbus existants.

Pourquoi et quand exécuter cette tâche

La procédure de démarrage d'Installation Manager est différente selon le mode utilisateur avec lequel vous l'avez installé. Les étapes de la mise à jour de Tivoli Netcool/OMNIbus avec l'interface graphique Installation Manager sont communes à tous les modes d'utilisateur et tous les systèmes d'exploitation.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer Installation Manager, effectuez les vérifications suivantes :
   a. Mode administrateur:
      1) Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
      2) Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Mode non-administrateur ou Mode groupe :

      Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
2. Placez-vous dans le répertoire d'installation d'Installation Manager.
3. Utilisez la commande suivante pour démarrer Installation Manager :

- UNIX Linux `./IBMIM`
- Windows `IBMIM`

Pour enregistrer les étapes de mise à jour dans un fichier de réponses à utiliser avec des mises à jour en mode silencieux, utilisez l'option `-record` *`fichier_réponses`*. Exemple :

```
IBMIM -record C:\fichier_réponses\update_1.xml
```

4. Si Installation Manager n'est pas déjà configuré pour télécharger des paquets de IBM Passport Advantage, utilisez les étapes suivantes pour ce faire :
   a. Dans le menu principal, sélectionnez **Fichier** > **Préférences**.
   b. Dans la fenêtre Préférences, sélectionnez le panneau **Référentiels**.
   c. Sélectionnez **Search service repositories during installation and updates**, cliquez sur **Appliquer**, puis cliquez sur **OK**.
5. Dans la fenêtre principale d'Installation Manager, cliquez sur **Mettre à jour**.
6. Suivez les instructions de l'assistant pour réaliser la mise à jour. L'assistant nécessite la saisie suivante à différents stades de la mise à jour :
   - Si vous y êtes invité, saisissez votre nom d'utilisateur et votre mot de passe IBM.
   - Sélectionnez tout ou partie des packages ou des correctifs disponibles.
   - Lisez et acceptez chaque contrat de licence.
   - Vérifiez la liste des mises à jour à appliquer.
   - Vérifiez que la taille totale de l'installation ne dépasse pas l'espace disque disponible.
7. Une fois la mise à jour terminée :
   - UNIX Linux Cliquez sur **Finish (Terminer)**.
   - Windows L'ordinateur doit être redémarré. Sélectionnez **Redémarrer maintenant** ou **Redémarrer plus tard**, puis cliquez sur **Terminer**.

Résultats

Installation Manager met à jour Tivoli Netcool/OMNIbus.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Mise à jour de Tivoli Netcool/OMNIbus (console)

Vous pouvez utiliser la console Installation Manager pour mettre à jour votre installation de Tivoli Netcool/OMNIbus.

Avant de commencer

Vous devez avoir un ID IBM pour télécharger le logiciel de IBM Passport Advantage.

Effectuez les actions suivantes :

- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin.
- Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
- Sauvegardez votre installation et vos données Tivoli Netcool/OMNIbus existants.

Pourquoi et quand exécuter cette tâche

Les étapes de démarrage de Installation Manager sont différentes selon le mode utilisateur d'installation. Les étapes de la mise à jour de Tivoli Netcool/OMNIbus avec la console Installation Manager sont communes à tous les modes d'utilisateur et tous les systèmes d'exploitation.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer Installation Manager, effectuez les vérifications suivantes :
   a. Mode administrateur:
      1) Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
      2) Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Mode non-administrateur ou Mode groupe :
      Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
2. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager.
3. Utilisez la commande suivante pour démarrer Installation Manager :
   - UNIX Linux `./imcl -c`
   - Windows `imcl -c`
4. Si Installation Manager n'est pas déjà configuré pour télécharger des paquets de IBM Passport Advantage, utilisez les étapes suivantes pour ce faire :
   a. Dans le menu principal, sélectionnez Préférences.
   b. Dans le menu Préférences, sélectionnez Référentiels.

c. Dans le menu Référentiels, sélectionnez les référentiels de service de recherche lors de l'installation et des mises à jour.
d. Revenez au menu principal.

5. Dans le menu principal, sélectionnez Mettre à jour.

   Suivez les instructions d'Installation Manager pour terminer la mise à jour. Installation Manager nécessite l'entrée suivante à différentes étapes de l'installation :

   - Si vous y êtes invité, saisissez votre nom d'utilisateur et votre mot de passe IBM.
   - Sélectionnez tout ou partie des packages ou des correctifs disponibles. Installation Manager prépare, décide et valide les packages sélectionnés. Cette opération peut prendre un certain temps.
   - Lisez et acceptez le contrat de licence qui apparaît.
   - Sélectionnez les fonctions Tivoli Netcool/OMNIbus dont vous n'avez pas besoin.
   - Si nécessaire, générer un fichier de réponses à utiliser avec des mises à jour sur d'autres ordinateurs. Entrez le chemin du répertoire et un nom de fichier avec une extension `.xml`. Le fichier de réponse est généré avant la fin de la mise à jour.

6. Une fois la mise à jour terminée :

   - UNIX Linux Sélectionnez Terminé.
   - Windows L'ordinateur doit être redémarré. Sélectionnez Redémarrer maintenant ou Redémarrer plus tard, puis cliquez sur Terminer.

Résultats

Installation Manager met à jour Tivoli Netcool/OMNIbus.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Mise à jour de Tivoli Netcool/OMNIbus (mode silencieux)

Vous pouvez mettre à jourTivoli Netcool/OMNIbus en mode silencieux. Ceci est utile si vous voulez des configurations de mise à jour identiques sur plusieurs postes de travail. La mise à jour silencieuse nécessite un fichier de réponse qui définit la configuration de la mise à jour.

Avant de commencer

Effectuez les actions suivantes :

- Créez ou enregistrez un fichier de réponses Installation Manager.
- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin.
- Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
- Sauvegardez votre installation et vos données Tivoli Netcool/OMNIbus existants.

Pourquoi et quand exécuter cette tâche

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer la mise à jour, effectuez les vérifications suivantes :
   a. Mode administrateur:
      1) Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
      2) Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Mode non-administrateur ou Mode groupe :

      Utilisez l'utilitaire **umask** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
2. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager.
3. Utilisez la commande suivante pour mettre à jour Tivoli Netcool/OMNIbus :
   - UNIX Linux `./imcl input` *`fichier_réponses`*
   - Windows `imcl input` *`fichier_réponses`*

   où *`fichier_réponses`* est le chemin du répertoire vers le fichier de réponses.

Résultats

Installation Manager met à jour Tivoli Netcool/OMNIbus.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Collecte des détails d'installation

Après avoir installé les composants côté serveur de Tivoli Netcool/OMNIbus, vous pouvez exécuter l'outil d'affichage de version de serveur d'objets (**nco_id**) pour vérifier que l'installation des composants a abouti. Les informations recueillies sont également utiles pour le dépannage.

Pourquoi et quand exécuter cette tâche

L'outil d'affichage de version de serveur d'objets est un utilitaire de ligne de commande qui peut recueillir et afficher des informations de base ou détaillées sur

votre installation Tivoli Netcool/OMNIbus. Il peut écrire les informations recueillies dans un fichier `.html` ou vous pouvez rediriger la sortie de ligne de commande vers un fichier.

L'ensemble d'informations de base inclut les répertoires d'installation, les produits installés, les composants et les groupes de correctifs.

L'ensemble détaillé des informations comprend l'ensemble des informations de base et les informations suivantes :

- Informations sur le système d'exploitation.
- Informations sur IBM Installation Manager collectées de Tivoli Netcool/OMNIbus ainsi que de toutes les sondes qui sont installées sur l'ordinateur hôte. Le compte d'utilisateur qui exécute **nco_id** doit avoir accès en lecture au répertoire de données Installation Manager et son contenu.
- Liste des fichiers binaires installés dans les répertoires suivants, y compris les sommes SHA1 de tous les fichiers :

  UNIX Linux 32-bit

  – `$NCHOME/omnibus/arch/bin`
  – `$NCHOME/omnibus/arch/lib`

  UNIX Linux 64-bit

  – `$NCHOME/omnibus/arch/bin64`
  – `$NCHOME/omnibus/arch/lib64`

  Windows

  – `%NCHOME%\omnibus\win32\bin`
  – `%NCHOME%\omnibus\win32\lib`
- Heure à laquelle les bibliothèques de produits ont été compilées.

Vous pouvez lancer l'outil d'affichage de version de serveur d'objets avec l'une des commandes suivantes :

- *NCHOME*`/bin/nco_id`
- *NCHOME*`/omnibus/bin/nco_id`

Vous pouvez spécifier les options de ligne de commande suivantes lorsque vous démarrez l'outil.

Option de ligne de commande	Description
`-?`	Affiche des informations d'aide sur les options disponibles.
`-o` *chaîne*	Indique le nom et l'emplacement d'un fichier `.html` dans lequel les informations recueillies sont écrites. Si vous spécifiez uniquement un nom de fichier, le fichier est créé dans le répertoire de travail.
`-s`	Affiche des informations de base sur l'installation. Il s'agit de l'option par défaut.
`-v`	Affiche des informations détaillées sur l'installation.

Procédure

1. Pour écrire les informations détaillées dans un fichier `.html`, utilisez la commande suivante :

   NCHOME`/omnibus/bin/nco_id -o PackageTest.html -v`

2. Pour rediriger les informations détaillées dans un fichier texte, utilisez la commande suivante:

   NCHOME/omnibus/bin/nco_id -v > PackageTest.txt

Que faire ensuite

Si un composant que vous avez choisi d'installer est absent des informations recueillies, cela pourrait indiquer qu'un ou plusieurs composants n'ont pas été installés avec succès. Vérifiez les fichiers journaux d'installation et relisez les messages d'installation pour identifier tout problème survenu au cours de l'installation.

Rétrogradation de mises à jour

Installation Manager peut annuler des mises à jour appliquées. Vous pouvez annuler une mise à jour dans l'interface graphique ou la console Installation Manager ou vous pouvez effectuer une rétromigration silencieuse.

Avant de commencer

Effectuez les actions suivantes :

- Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
- Sauvegardez tous les fichiers de données ou de configuration qui ont été créés depuis la mise à jour initiale et que vous voulez conserver.
- Pour effectuer une rétromigration en mode silencieux, créez ou enregistrez un fichier de réponses Installation Manager.

Pourquoi et quand exécuter cette tâche

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. UNIX Linux Avant de lancer Installation Manager, effectuez les vérifications suivantes :
   a. Mode administrateur:
      1) Si vous n'êtes pas déjà connecté en tant que root, utilisez la commande `su` ou `sudo sh` pour démarrer un shell superutilisateur.
      2) Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.
   b. Mode non-administrateur ou Mode groupe :

      Utilisez l'utilitaire **`umask`** pour vérifier la valeur umask. Si nécessaire, modifiez la valeur de umask.

Rétromigration dans l'interface graphique

2. Pour annuler une mise à jour dans l'interface graphique Installation Manager :
   a. Placez-vous dans le répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour démarrer l'assistant Installation Manager :

- UNIX Linux `./IBMIM`
- Windows `IBMIM`

c. Dans la fenêtre principale d'Installation Manager, cliquez sur **Annulation**.
d. Suivez les instructions de l'assistant pour réaliser la rétromigration.
e. Une fois la rétromigration terminée :
   - UNIX Linux Cliquez sur **Finish (Terminer)**.
   - Windows L'ordinateur doit être redémarré. Sélectionnez **Redémarrer maintenant** ou **Redémarrer plus tard**, puis cliquez sur **Terminer**.

Rétromigration à partir de la console

3. Pour annuler une mise à jour dans la console Installation Manager :
   a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager.
   b. Utilisez la commande suivante pour démarrer Installation Manager :
      - UNIX Linux `./imcl -c`
      - Windows `imcl -c`
   c. Dans le menu principal, sélectionnez Annulation.
   d. Suivez les instructions d'Installation Manager pour terminer la la rétromigration.
   e. Une fois la rétromigration terminée :
      - UNIX Linux Sélectionnez Terminé.
      - Windows L'ordinateur doit être redémarré. Sélectionnez Redémarrer maintenant ou Redémarrer plus tard, puis cliquez sur Terminer.

Rétromigration en mode silencieux

4. Pour annuler une mise à jour en mode silencieux :
   a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation Installation Manager.
   b. Utilisez la commande suivante pour démarrer la rétromigration :
      - UNIX Linux `./imcl input` *`fichier_réponses`*
      - Windows `imcl input` *`fichier_réponses`*

      Où *`fichier_réponses`* est le chemin de répertoire vers le fichier de réponses qui définit la configuration de la rétromigration.

Résultats

Installation Manager annule la mise à jour.

Référence associée:

«Présentation d'IBM Installation Manager», à la page 32
Vous pouvez installer IBM Installation Manager avec une interface graphique ou une console ou vous pouvez effectuer une installation en mode silencieux. Avant l'installation, vous devez déterminer le mode d'utilisation dont vous avez besoin.

«Fichiers de réponses Installation Manager», à la page 35
Pour effectuer une installation silencieuse de Tivoli Netcool/OMNIbus, vous devez créer ou enregistrer un fichier de réponses Installation Manager.

Mise à niveau à partir de V7.4 (et versions précédentes)

Utilisez IBM Installation Manager pour installer Tivoli Netcool/OMNIbus V8.1. En cours d'installation, vous pouvez utiliser Installation Manager pour migrer automatiquement vos données existantes. Il vous est également possible de migrer ces données manuellement après installation de la version V8.1.

Remarque : À partir de la version 8.1 de Tivoli Netcool/OMNIbus, utilisez la fonction de mise à jour de IBM Installation Manager pour la mise à niveau vers les nouvelles versions du produit.

Sous les systèmes d'exploitation UNIX et Linux, vous pouvez continuer à exécuter votre installation Tivoli Netcool/OMNIbus existante en parallèle avec l'installation nouvellement mise à niveau. Toutefois, vous devez vous assurer que les deux installations utilisent des jeux de ports différents. Vous pouvez changer les ports utilisés par la version mise à niveau en modifiant les valeurs par défaut qui apparaissent dans le fichier de connexions de données `$NCHOME/etc/omni.dat`. Une fois les ports changés, exécutez l'utilitaire **`nco_igen`** pour générer le fichier d'interfaces qui stocke les informations de communication avec le serveur.

Migration de données

Quand vous effectuez une mise à niveau depuis Tivoli Netcool/OMNIbus V7.4 (ou version antérieure) vers V8.1, vous pouvez soit migrer vos données existantes manuellement, soit utiliser IBM Installation Manager pour une migration automatique.

Pour mettre à niveau votre version précédente afin qu'elle s'exécute en mode FIPS 140-2, vous devrez peut-être configurer certaines de vos données avant ou après la mise à niveau.

Quand vous optez pour une migration automatique de vos données au cours du processus de mise à niveau, les informations de migration sont écrites dans le fichier journal suivant :

NCHOME`/omnibus/log/migrate.log`

UNIX Linux

Migration de données sous UNIX et Linux

IBM Installation Manager offre le choix de migrer automatiquement des données depuis une installation existante vers l'installation mise à niveau. Sur le panneau de migration des données, vous devez indiquer l'emplacement où Installation Manager pourra trouver les fichiers à migrer - c'est-à-dire l'emplacement de votre installation existante ou d'une sauvegarde de cette installation.

Vous pouvez également migrer vos données manuellement après mise à niveau, ce qui nécessite une sauvegarde de votre ancienne installation pour utilisation avec le script de mise à niveau.

Pour une migration manuelle de données :

1. Accédez au répertoire `$NCHOME/omnibus/upgrade`.
2. Exécutez la commande suivante :

   `UPGRADE.SH -old` *`ANCIEN_CHEMIN`* `-new` *`NOUVEAU_CHEMIN`* `[-log` *`CHEMIN_FICHIER_JOURNAL`*`]`

où *ANCIEN_CHEMIN* est l'emplacement dans lequel vous avez sauvegardé votre ancienne installation et où *NOUVEAU_CHEMIN* est le nouvel emplacement de `$NCHOME/omnibus`.

Pour sauvegarder les informations de migration dans un fichier journal, utilisez l'option `-log` avec la variable *CHEMIN_FICHIER_JOURNAL* représentant le répertoire dans lequel vous voulez enregistrer le fichier journal. Si vous n'utilisez pas l'option `-log`, les détails sont écrits dans la sortie standard.

Windows

Migration de données sous Windows

Sous les systèmes d'exploitation Windows, une seule installation de Tivoli Netcool/OMNIbus par ordinateur est autorisée. Au démarrage, Installation Manager vérifie s'il existe déjà une installation. S'il en trouve une, vous devez la supprimer avant de poursuivre la mise à niveau.

Pour supprimer l'installation existante :

1. Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
2. Supprimez tout service Tivoli Netcool/OMNIbus qui a été installé manuellement.
3. Facultatif : Pour sauvegarder vos données et vos fichiers de configuration existants, appliquez l'une des méthodes suivantes :
   a. Exécutez **nco_config_save.bat** qui se trouve dans la distribution de fichier .zip ESD pour sauvegarder un ensemble prédéfini de fichiers.
   b. Copiez manuellement le contenu du répertoire `%NCHOME%` existant vers un emplacement de sauvegarde.
4. Supprimez toutes les sondes et passerelles mises en place.
5. Exécutez `%NCHOME%\_uninst\OMNIbus\uninstall.exe -i console`.

Une fois l'ancienne installation de Tivoli Netcool/OMNIbus supprimée, vous pouvez poursuivre la mise à niveau.

Si vous avez sauvegardé votre ancienne installation, vous pouvez migrer les données et la configuration existantes. Dans le panneau de migration de données d'Installation Manager, indiquez l'emplacement de votre sauvegarde. Il vous est également possible de copier manuellement vos fichiers de données et de configuration vers la nouvelle installation.

Tâches associées:

«Préparation des chiffrements de valeur de propriété pour la mise à niveau (en mode FIPS 140-2)», à la page 129
Si vous souhaitez que votre installation mise à niveau s'exécute en mode FIPS 140-2, vous devrez peut-être déchiffrer toutes les propriétés et tous les mots de passe chiffrés de vos fichiers de propriétés et de configuration avant la mise à niveau. Effectuez cette tâche si votre installation existante utilise le chiffrement des valeurs de propriété avec l'algorithme AES ou utilise les programmes **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe . Ignorez cette tâche si vous ne souhaitez pas exécuter votre installation en mode FIPS 140-2. Vous pouvez également ignorer cette tâche si vous effectuez une mise à niveau d'un système version 7.3 ou version ultérieure et si votre système fonctionne déjà en mode FIPS 140-2.

Fichiers migrés pendant une mise à niveau

Lorsque vous mettez à niveau depuis une version précédente de Tivoli Netcool/OMNIbus vers la version 8.1, vous pouvez choisir de migrer les fichiers existants dans la nouvelle installation.

Important :

- Examinez tous les fichiers de propriétés migrés pour les nouvelles conditions :
  - Lorsque des chemins de fichier sont indiqués dans une propriété, vérifiez que le chemin fait référence à l'emplacement correct de la nouvelle installation, et non pas à l'ancien emplacement à partir duquel le fichier a été migré.
  - Si vous avez utilisé la variable d'environnement *OMNIHOME* ou *NCHOME* (plutôt que la valeur développée de la variable), il n'est pas nécessaire de modifier les chemins de fichier car la variable d'environnement se résout automatiquement sur le nouvel emplacement.
- Si l'installation précédente contenait des fichiers ObjectServer, créés en tant qu'objets de stockage pour consigner ou rapporter des données, ces fichiers logiques ont été stockés dans la base de données ObjectServer. Les fichiers ont été stockés avec une référence vers le chemin de répertoire complet de l'emplacement physique. Si le chemin de mise à niveau est différent du chemin de l'installation précédente, vérifiez si vos objets de fichier font référence à l'ancien emplacement, et mettez à jour les chemins pour qu'ils désignent le nouvel emplacement. Vous pouvez vérifier les chemins dans la table catalog.files. En outre, dans la fenêtre Netcool/OMNIbus Administrator, sélectionnez le bouton de menu **Système**, puis cliquez sur **Log Files** (Fichiers journaux) pour afficher les détails des fichiers.

UNIX Linux

Le tableau suivant répertorie les fichiers migrés et leurs emplacements dans la nouvelle installation.

Tableau 31. Emplacements des fichiers migrés sur UNIX et Linux

Type de fichier	Emplacement migré
Fichiers de données de connexions	`$NCHOME/etc/omni.dat`
Fichiers de configuration	`$NCHOME/omnibus/etc/*.conf` Vous devez copier manuellement tous les autres fichiers de configuration dans leur emplacement équivalent `$NCHOME/omnibus`.

Fichiers de configuration de la passerelle ObjectServer	`$NCHOME/omnibus/etc/*GATE.props`
	
	`$NCHOME/omnibus/etc/*.tblrep.def`
	
	`$NCHOME/omnibus/etc/*.map`
	
	`$NCHOME/omnibus/etc/*.startup.cmd`

Fichiers de base de données	`$NCHOME/omnibus/db`
Fichiers de propriétés Netcool/OMNIbus Administrator	`$NCHOME/omnibus/etc/nco_config.props`
Fichier de règles	`$NCHOME/omnibus/etc/admin.policy`

Tableau 31. Emplacements des fichiers migrés sur UNIX et Linux (suite)

Type de fichier	Emplacement migré
Fichier d'exclusions	`$NCHOME/omnibus/etc/exclusions.old.xml` Si vous avez préalablement modifié le fichier d'exclusions de votre ancienne installation, copiez ces modifications à partir du fichier `exclusions.old.xml` migré dans le fichier `$NCHOME/omnibus/etc/exclusions.xml` de la nouvelle installation.
Fichier de propriétés pour l'utilitaire **`nco_confpack`**	`$NCHOME/omnibus/etc/nco_confpack.props`
Fichiers du bureau	`$NCHOME/omnibus/desktop/default.elc` La liste d'événements UNIX ou Linux utilise les fichiers `default.elc` et `minimal.elc` spécifiques à l'environnement local à l'emplacement `$NCHOME/omnibus/desktop/locale/`*`arch`*`/`*`env_local`*.
Fichiers MIB Manager	Si l'installation précédente contient un répertoire `$NCHOME/omnibus/platform/arch/mibmanager/workspace`, son contenu est copié dans `$NCHOME/omnibus/var/mibmanager.migrated`. Vous pouvez utiliser le contenu de ce répertoire pour vous aider à configurer MIB Manager.
Fichiers de base de données de clés pour SSL (V7.3 ou versions ultérieures)	`$NCHOME/etc/security/keys/migrated`
Fichier de configuration FIPS 140-2	`$NCHOME/etc/security/fips.conf`
Utilitaires	`$NCHOME/omnibus/utils`
Fichiers de règles et de propriétés de sonde (`*.rules` et `*.props`)	`$NCHOME/omnibus/probes/migrated` **Important :** Toutes les sondes doivent être réinstallées. Copiez les anciennes données dans `$NCHOME/omnibus/probes/migrated` vers le nouvel emplacement de la sonde.
Fichiers de configuration Telco Service Monitors	`$NCHOME/omnibus/tsm/migrated`
Fichiers de configuration RestOS JSON	`$NCHOME/omnibus/etc/restos/`
Fichiers RestOS uipreview	`$NCHOME/omnibus/etc/restos/uipreview.migrated` **Remarque :** Si des fichiers ont été modifiés dans le répertoire `uipreview` de l'ancienne installation, vous devez migrer ces fichiers manuellement vers le nouveau répertoire `$NCHOME/omnibus/etc/restos/uipreview/`.
Fichiers RestOS docroot	`$NCHOME/omnibus/etc/restos/docroot.migrated` **Remarque :** Si des fichiers ont été modifiés dans le répertoire `docroot` de l'ancienne installation, vous devez migrer ces fichiers manuellement vers le nouveau répertoire `$NCHOME/omnibus/etc/restos/docroot/`.

Windows

Le tableau suivant répertorie les fichiers migrés et leurs emplacements dans la nouvelle installation.

Tableau 32. Emplacements des fichiers migrés sous Windows

Type de fichier	Emplacement migré
Fichiers de données de connexions	`%NCHOME%\ini\sql.ini`

Fichiers de configuration	`%NCHOME%\omnibus\ini\*.props`
	
	`%NCHOME%\omnibus\*\*.conf`
	
	`%NCHOME%\omnibus\*\*.props`
	
	La mise à niveau copie uniquement les fichiers de configuration qui utilisent des noms par défaut ; par exemple, `nco_pa.props`, `*GATE.conf`, et `*GATE.props`. Tous les autres fichiers de configuration doivent être copiés manuellement dans l'emplacement `%NCHOME%\omnibus` équivalent.

Fichiers de configuration de la passerelle ObjectServer	`%NCHOME%\omnibus\etc\*GATE.props`
	
	`%NCHOME%\omnibus\etc\*.tblrep.def`
	
	`%NCHOME%\omnibus\etc\*.map`
	
	`%NCHOME%\omnibus\etc\*.startup.cmd`

Fichiers de base de données	`%NCHOME%\omnibus\db`
Fichiers de propriétés Netcool/OMNIbus Administrator	`%NCHOME%\omnibus\etc\nco_config.props`
Fichier de règles	`%NCHOME%\omnibus\etc\admin.policy`
Fichier d'exclusions	`%NCHOME%\omnibus\etc\exclusions.old.xml` Si vous avez apporté des modifications précédemment dans le fichier d'exclusions de votre ancienne installation, vous devez copier ces modifications à partir du fichier `exclusions.old.xml` migré dans le fichier `%NCHOME%\omnibus\etc\exclusions.xml` de la nouvelle installation.
Fichier de propriétés de Confpack	`%NCHOME%\omnibus\etc\nco_confpack.props`
Fichiers de Desktop	`%NCHOME%\omnibus\ini\default.elc`
Fichiers de base de données de clés pour SSL (V7.3 ou versions ultérieures)	`%NCHOME%\ini\security\keys\migrated`
Fichier de configuration FIPS 140-2	`%NCHOME%\ini\security\fips.conf`
Utilitaires et scripts	Si l'installation précédente contenait un répertoire `utils`, le processus de mise à niveau copie ce répertoire ainsi que son contenu dans : `%NCHOME%\omnibus\utils` Si l'installation précédente contenait un répertoire `scripts`, le processus de mise à niveau copie ce répertoire ainsi que son contenu dans : `%NCHOME%\omnibus\scripts`

Tableau 32. Emplacements des fichiers migrés sous Windows (suite)

Type de fichier	Emplacement migré
Fichiers de règles et de propriétés de sonde (`*.rules` et `*.props`)	`%NCHOME%\omnibus\probes\migrated` **Remarque :** Toutes les sondes doivent être réinstallées et les anciennes données migrées dans le répertoire ci-dessus doivent être copiées dans le nouvel emplacement de la sonde.

Mise à jour du schéma de ObjectServer

Après la mise à niveau vers une nouvelle version de Tivoli Netcool/OMNIbus, vous pouvez mettre à jour le schéma pour chaque instance ObjectServer que vous exécutez. Certaines nouvelles fonctionnalités de l'installation mise à niveau peuvent nécessiter la mise à jour du schéma. Tous les nouveaux ObjectServers que vous créez dans votre installation mise à niveau sont créés avec le schéma le plus récent.

Avant de commencer

L'ObjectServer doit être en cours d'exécution lorsque vous appliquez une mise à jour de schéma.

Pourquoi et quand exécuter cette tâche

Les fichiers de mise à jour de schéma SQL suivants se trouvent dans le répertoire *NCHOME*`/omnibus/etc` :

Fichier de mise à jour de schéma	Description
`update70to71.sql`	Ce fichier met à jour un schéma ObjectServer V7.0 vers un schéma V7.1.
`update71to72.sql`	Ce fichier met à jour un schéma ObjectServer V7.1 vers un schéma V7.2 ou V7.2.1. Les schémas version 7.2 et 7.2.1 sont identiques.
`update72xto73.sql`	Ce fichier met à jour un schéma ObjectServer V7.2 ou V7.2.1 vers un schéma V7.3.
`update73to731.sql`	Ce fichier met à jour un schéma ObjectServer V7.3 vers un schéma V7.3.1.
`update731to74.sql`	Ce fichier met à jour un schéma ObjectServer V7.3.1 vers un schéma V7.4.
`update74to74fp3.sql`	Cette mise à jour a été fournie avec Tivoli Netcool/OMNIbus V7.4 groupe de correctifs 3.
`update74fp3to81.sql`	Ce fichier met à jour un schéma ObjectServer V7.4 vers un schéma V8.1.

Si vous mettez à jour depuis une ancienne version de l'Tivoli Netcool/OMNIbus vers V8.1, appliquez les mises à jour de schéma dans l'ordre de la version d'édition. Par exemple, pour mettre à jour de V7.3.1 vers V8.1, appliquez d'abord `update731to74.sql`, puis appliquez `update74to74fp3.sql`, et `update74fp3to81.sql`.

Remarque : L'initialisation de la base de données n'est pas nécessaire après une mise à jour de schéma.

Procédure

1. Consultez le fichier de mise à jour de schéma afin de vérifier si il modifie une configuration personnalisée dans votre environnement d'exploitation. Si nécessaire, modifiez le fichier de mise à jour de schéma pour résoudre les conflits avec votre configuration existante. Retirez du fichier toutes les mises à jour dont vous n'avez pas besoin.

   En fonction de votre configuration existante, les modifications de schéma décrites dans le tableau ci-dessous pourraient exiger une attention particulière.

Fichier de mise à jour de schéma	Notes sur la mise à niveau
`update70to71.sql`	Les automatisations connection_watch_disconnect et connection_watch_connect sont modifiées dans le module d'installation de la version 7.1. Lorsque vous mettez à niveau le schéma, les nouveaux déclencheurs sont importés avec les noms connection_watch_disconnect2 et connection_watch_connect2, et sont désactivés par défaut. Si vous souhaitez utiliser les nouveaux déclencheurs, activez-les puis désactivez les déclencheurs connection_watch_disconnect et connection_watch_connect originaux, disponibles dans la version 7.0.
`update71to72.sql`	Si vous avez créé vos propres outils et les avez ajouté aux menus, recherchez d'éventuels conflits dans les tables tools.*. Plusieurs modifications de schéma et de nouvelles automatisations prennent en charge les fonctions de IBM Tivoli Network Manager IP Edition V3.7 (précédemment Netcool Precision IP). Si vous utilisez déjà Network Manager, les modifications sont peut-être déjà ajoutées au serveur ObjectServer. Dans ce cas, supprimez la configuration en double du fichier de mise à jour de schéma.
`update72xto73.sql`	Les automatisations deduplication et new_row sont modifiées dans le module d'installation de la version 7.3. Une fois le schéma mis à niveau, les nouveaux déclencheurs sont importés en tant que deduplication_73 et new_row_73, et sont désactivés par défaut. Si vous souhaitez utiliser les nouveaux déclencheurs, activez-les, puis désactivez les déclencheurs deduplication et new_row d'origine installés dans la version 7.2 ou 7.2.1.
`update73to731.sql`	Le déclencheur disconnect_iduc_missed est mis à jour pour augmenter à 100 le nombre maximal de signaux iduc_missed avant que le client ne soit déconnecté. Ce déclencheur remplace le déclencheur disconnect_iduc_missed de la version V7.3. Si vous voulez utiliser le nouveau déclencheur, désactivez le déclencheur disconnect_iduc_missed initial qui a été installé avec V7.3 puis activez le nouveau déclencheur.

Fichier de mise à jour de schéma	Notes sur la mise à niveau

update731to74.sql	Une nouvelle colonne NmosDomainName est ajoutée aux tables precision.entity_service et precision.service_details. La nouvelle colonne active les événements affectant le service (SAE) à partir de plusieurs domaines IBM Tivoli Network Manager IP Edition devant être ajoutés au serveur ObjectServer.
	
	Cette fonction était précédemment disponible dans les groupes de correctifs pour Tivoli Netcool/OMNIbus V7.3.0 et V7.3.1. Si vous avez déjà ajouté cette fonction dans V7.3.0 ou v7.3.1, et que vous appliquez le fichier de mise à jour de schéma sans modification, les erreurs suivantes sont enregistrées dans le fichier journal d'ObjectServer :
	`ERROR=Object exists on line 13 of statement`
	`'--...', at or near 'NmosDomainName'`
	`ERROR=Object exists on line 2 of statement`
	`'alter table precision.service_details`
	`add column NmosDomainName varchar(255);...',`
	`at or near 'NmosDomainName'`
	
	Le reste de la mise à jour du schéma est traité normalement.

update74to74fp3.sql	Cette mise à jour ajoute deux nouvelles tables à la base de registre et crée un certain nombre de nouveaux déclencheurs dans un nouveau groupe de déclenchement appelé oslc. Aucune table ou automatisation existante n'est mise à jour.
update74fp3to81.sql	La table registry.probes devient persistante dans V8.1. Si vous avez une instance virtuelle existante du registry.probes, elle est supprimée, avec tous les déclencheurs dépendants, et une nouvelle table persistante est créée. **Remarque :** Toutes les données contenues dans la table virtuelle sont perdues lors de cette mise à jour. Les données de la sonde sont mises à jour de nouveau dans la nouvelle table persistante alors que les sondes se reconnectent à l'ObjectServer. Dans la version 8.1, la configuration par défaut inclut des commandes SQL qui configurent le canal AEN et les déclencheurs de post-insertion pour l'intégration de la recherche d'événements à IBM SmartCloud Analytics - Log Analysis. Les déclencheurs de post-insertion sont désactivés par défaut. Vous devez les activer si vous souhaitez utiliser la transmission d'événements AEN dans Message Bus Gateway.

2. Utilisez l'interface interactive SQL pour sauvegarder le serveur ObjectServer existant.

   La syntaxe est `ALTER SYSTEM BACKUP '`*`répertoire_sauvegarde`*`';`.

   Exemple :

   ```
   1> alter system backup 'tmp/74to81Upgrade/NCOMS';
   2> go
   ```

3. Utilisez l'interface interactive SQL pour appliquer la mise à jour. Exemple :

   UNIX Linux `f$NCHOME/omnibus/bin/nco_sql -user` *`nom_utilisateur`* `-password` *`mot_de_passe`* `-server` *`nom_ObjectServer`* `< update74to81.sql`

   Windows `%NCHOME%\omnibus\bin\isql -U` *`nom_utilisateur`* `-P` *`mot_de_passe`* `-S` *`nom_ObjectServer`* `-i update74to81.sql`

Où *nom_ObjectServer* est le nom de l'ObjectServer et *nom_utilisateur* et *mot_de_passe* sont des données d'identification valides pour cet ObjectServer.

4. Une fois la mise à jour terminée, consultez le fichier journal de l'ObjectServer pour y rechercher des erreurs.
5. En cas d'erreurs, corrigez-les et apportez les corrections nécessaires dans le fichier de mise à jour de schéma ou à votre système. Puis, revenez à l'ObjectServer sauvegardé et réappliquez la mise à jour.
6. Si vous demandez deux ou plusieurs mises à jour de schéma dans l'ordre, effectuez une sauvegarde de chaque ObjectServer mis à jour avec succès avant d'appliquer la mise à jour suivante.

Mise à niveau d'un ObjectServer connecté à une passerelle de base de données

Lorsque vous mettez à niveau un ObjectServer et conservez le même nom ObjectServer, ou récupérez un ObjectServer sauvegardé, l'ObjectServer mis à niveau ou récupéré a une valeur de série inférieure à l'ancien ObjectServer. Cela peut poser des problèmes si l'ObjectServer est connecté à une passerelle de base de données qui est utilisée pour les rapports d'historique (comme Gateway for Oracle ou Gateway for JDBC).

Pourquoi et quand exécuter cette tâche

Si l'ObjectServer est connecté à une passerelle de base de données qui est utilisée pour des rapports d'historique, la passerelle traite les alertes dans l'ObjectServer mis à niveau ou récupéré comme des réinsertions.

La passerelle tente de réinsérer les lignes existantes en tant que nouvelles lignes, ce qui peut provoquer une erreur de contrainte d'unicité ou de ligne en double à partir de la base de données si ServerName et ServerSerial existent déjà dans la base de données. Cela se produit parce la passerelle utilise ServerName et ServerSerial en tant que clés uniques. Lorsque la base de données génère une erreur de contrainte d'unicité ou de ligne en double, la passerelle supprime la réinsertion.

Lorsque cela se produit, une erreur est consignée dans le fichier journal de la passerelle. L'erreur est différente en fonction de la base de données. Ce qui suit est un exemple d'erreur consignée par une base de données Oracle :

```
10/03/07 03:14:48 PM: Warning: W-UNK-000-000: Oracle Error: [ORA-00001: unique
 constraint (REPORTER.STATUS) violated] - sqlcode[-1]
```

Procédure

Pour résoudre ce problème, utilisez les étapes suivantes pour modifier la valeur Serial après avoir mis à niveau ou récupéré l'ObjectServer :

1. Vérifiez la valeur actuelle de Serial dans la base de données.

   Par exemple, utilisez la commande suivante pour vérifier la valeur Serial dans une base de données Oracle :

   ```
   SQL*PLUS> MAX(SERVERSERIAL)
   ```

2. Utilisez la commande ALTER TABLE SET INCR pour mettre à jour Serial à une valeur appropriée dans alerts.status.

   Par exemple, si la valeur actuelle de Serial dans la base de données est 49369, utilisez la commande ObjectServer SQL suivante pour la définir sur 50000 :

   ```
   alter table alerts.status set incr 50000;
   ```

Remarque : Pour éviter les doublons, vous ne pouvez pas définir une valeur d'incrément qui est identique à la valeur d'une ligne existante. En outre, vous ne pouvez pas définir une valeur `INCR` qui entraîne les insertions suivantes à avoir les mêmes valeurs que les lignes existantes.

Préparation des chiffrements de valeur de propriété pour la mise à niveau (en mode FIPS 140-2)

Si vous souhaitez que votre installation mise à niveau s'exécute en mode FIPS 140-2, vous devrez peut-être déchiffrer toutes les propriétés et tous les mots de passe chiffrés de vos fichiers de propriétés et de configuration avant la mise à niveau. Effectuez cette tâche si votre installation existante utilise le chiffrement des valeurs de propriété avec l'algorithme AES ou utilise les programmes **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe . Ignorez cette tâche si vous ne souhaitez pas exécuter votre installation en mode FIPS 140-2. Vous pouvez également ignorer cette tâche si vous effectuez une mise à niveau d'un système version 7.3 ou version ultérieure et si votre système fonctionne déjà en mode FIPS 140-2.

Pourquoi et quand exécuter cette tâche

En mode FIPS 140–2, les valeurs de propriété doivent être chiffrées par un algorithme et le mode de fonctionnement défini sur AES_FIPS. Le chiffrement des valeurs de propriété est utilisé pour chiffrer des valeurs de chaîne dans un fichier de propriétés ou dans un fichier de configuration de sorte que les chaînes ne puissent pas être lues sans clé.

Si votre installation existante utilise le chiffrement de valeur de propriété avec l'algorithme AES, ou utilise les utilitaires **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe, ces valeurs chiffrées ne répondent pas aux critères requis pour FIPS 140–2.

Pour exécuter votre système mis à niveau en mode FIPS 140–2, vous devez déchiffrer ces valeurs puis les chiffrer à nouveau à l'aide de l'algorithme AES_FIPS. Exécutez cette tâche pour chaque ObjectServer, serveur proxy, agent de processus, sonde et passerelle utilisant des valeurs de propriété chiffrées, dont des mots de passe.

Procédure

Pour mettre à niveau la valeur de la propriété et le chiffrement du mot de passe :

1. Dans votre installation existante, identifiez toutes les clés générées à l'aide du générateur de clés de la ligne de commande **nco_keygen**. L'utilitaire **nco_keygen** stocke des clés dans des fichiers de clés. Pour identifier les fichiers de clés, vérifiez les paramètres de la propriété **ConfigKeyFile** dans vos fichiers de propriétés.
2. A l'aide des clés de votre installation existante, déchiffrez toutes les propriétés et tous les mots de passe codés de vos fichiers de propriétés et de configuration en exécutant l'utilitaire **nco_aes_crypt** avec l'option de la ligne de commande `-d`.
3. Répétez ces étapes pour chaque ObjectServer, serveur proxy, agent de processus, sonde et passerelle utilisant des valeurs de propriété chiffrées, dont des mots de passe.

Que faire ensuite

Exécutez les tâches suivantes :

1. Effectuez une mise à niveau vers Tivoli Netcool/OMNIbus version 8.1.
2. Configurez Tivoli Netcool/OMNIbus pour opérer en mode FIPS 140–2.
3. Chiffrez de nouveau les valeurs à l'aide de l'utilitaire **nco_keygen** afin de générer une ou plusieurs nouvelles clés, puis à l'aide de l'utilitaire **nco_aes_crypt** avec le paramètre de fichier de clés approprié et l'algorithme de cryptographie AES_FIPS.

Concepts associés:

Chapitre 10, «Configuration de la prise en charge de FIPS 140–2 pour les composants serveur», à la page 283
Vous pouvez exécuter les composants serveur suivants en mode FIPS 140–2 : les serveurs ObjectServer, les agents de processus, les serveurs proxy et les passerelles du serveur ObjectServer. Dans ce mode, les fonctions cryptographiques de Tivoli Netcool/OMNIbus utilisent les modules cryptographiques approuvés par la norme FIPS 140–2.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

«Options de ligne de commande nco_aes_crypt», à la page 370
Vous pouvez utiliser l'utilitaire **nco_aes_crypt** pour chiffrer et déchiffrer les valeurs de chaîne ou les données contenues dans un fichier.

Instructions de mise à niveau vers le codage UTF-8 (Windows)

Si vous avez précédemment exécuté vos serveurs ObjectServer, passerelles ObjectServer ainsi que les sondes et passerelles prises en charge dans le codage système par défaut sous Windows, mais que vous souhaitez passer au codage UTF-8, vous devez convertir certains de vos fichiers de configuration existants ainsi que les données ObjectServer en codage UTF-8.

Vous devez convertir les fichiers suivants s'ils contiennent des caractères non-ASCII, pour vous assurer qu'ils seront analysés correctement :

- Convertir vos fichiers de propriétés existants pour le serveur ObjectServer la passerelle ObjectServer, les sondes et **nco_dbinit**.
- Convertir vos fichiers de règles de sonde existants.
- Convertir vos fichiers de mappe de passerelle existants.
- Convertir tout fichier `.sql` personnalisé existant pour l'utilitaire **nco_dbinit**. Par exemple, lors de la création du serveur ObjectServer, vous pouvez avoir utilisé l'option de ligne de commande `-desktopfile` pour spécifier un fichier différent du fichier par défaut `$NCHOME/omnibus/etc/desktop.sql`, qui contient les données de configuration pour le bureau UNIX et Windows.

Vous devez également convertir les données existantes dans le serveur ObjectServer à partir du codage système par défaut. Cela implique la création d'un nouveau serveur ObjectServer en codage UTF-8 puis l'utilisation d'un passerelle pour transférer les données depuis l'ancien ObjectServer vers le nouveau serveur ObjectServer.

Avant de commencer

Vous devez avoir terminé le processus de mise à niveau et migré vos données. Vous devez également avoir mis à niveau le schéma ObjectServer.

Pourquoi et quand exécuter cette tâche

Pour mettre à niveau vers le codage UTF-8 :

Procédure

1. Convertissez vos fichiers de propriétés non ASCII, fichiers de règles de sonde, fichiers de mappe de passerelle et fichier `.sql` en codage UTF-8. Vous pouvez utiliser des outils tels que **iconv** et **uconv**, qui peuvent convertir les fichiers d'un codage à un autre :
   - Pour plus d'informations sur l'utilisation d'**iconv** sous Windows, accédez à http://gnuwin32.sourceforge.net/summary.html.
   - L'outil **uconv** est disponible en distribution binaire ICU4C 4.0.1 qui peut être téléchargée à partir de http://icu-project.org/download/. L'application se trouve dans le répertoire `bin`.
2. Dans votre emplacement mis à jour, écrasez les fichiers non ASCII avec les fichiers convertis.
3. Convertissez vos données ObjectServer comme suit :
   a. Créez un nouveau serveur ObjectServer en codage UTF-8 en exécutant l'utilitaire **nco_dbinit** avec l'option de ligne de commande `-utf8enabled` définie sur TRUE, et l'option `-desktopfile` définie sur l'emplacement du fichier `.sql` converti (le cas échéant).
   b. Si vous avez utilisé l'option de ligne de commande `-desktopfile` pour créer le serveur ObjectServer, comme spécifié à l'étape 3a, vous devez mettre à niveau le schéma ObjectServer car il a été créé à l'aide d'un des fichiers `.sql` d'une version de produit antérieure. Exécutez les scripts `update*.sql` pertinents dans le répertoire `$NCHOME/omnibus/etc`.
   c. Si nécessaire, installez une passerelle ObjectServer unidirectionnelle. Configurez ensuite la passerelle pour lire les données de l'ancien ObjectServer non UTF-8 et écrire les données dans le nouveau serveur ObjectServer UTF-8.
   d. Configurez les communications serveur entre les composants à l'aide de la commande **nco_xigen** de `$NCHOME/omnibus/bin` ou de l'éditeur de serveurs.
   e. Démarrez l'ancien ObjectServer non UTF-8, qui contient les données d'événement à convertir.
   f. Démarrez le nouveau serveur ObjectServer en codage UTF-8 en exécutant la commande **nco_objserv** avec l'option de ligne de commande `-utf8enabled` définie sur `TRUE`.
   g. Démarrez la passerelle ObjectServer :
      - Si la passerelle est exécutée dans le même codage système par défaut que l'ancien ObjectServer non-UTF-8, elle peut être exécutée avec l'option de ligne de commande `-utf8enabled` définie sur `TRUE` ou `FALSE`.
      - Si la passerelle est exécutée dans un codage différent de celui du serveur ObjectServer, vous devez l'exécuter avec l'option `-utf8enabled` définie sur `TRUE`.

      Pour plus d'informations sur la passerelle ObjectServer, allez sur le centre de documentation IBM Tivoli Network Management à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp.

)Recherchez et développez le nœud *IBM Tivoli Netcool/OMNIbus* puis allez sur le nœud *TivoliNetcool/OMNIbus gateways* (Passerelles TivoliNetcool/OMNIbus). Recherchez la publication sur la passerelle ObjectServer.

Pendant le processus de synchronisation, les données sont transférées de l'ancien ObjectServer vers le nouveau serveur.

Le nouveau serveur ObjectServer sera prêt pour l'utilisation après avoir exécuté les autres étapes de post-installation requises. Notez que la mise à jour de certains fichiers de configuration avec le nom du nouveau serveur ObjectServer, et éventuellement avec les différents chemins d'accès spécifiés peut être nécessaire.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Tâches associées:

«Création d'un serveur ObjectServer», à la page 197
Vous créez un ou plusieurs serveurs ObjectServer sur un poste de travail hôte en exécutant l'utilitaire d'initialisation de base de données (**nco_dbinit**).

«Mise à jour du schéma de ObjectServer», à la page 125
Après la mise à niveau vers une nouvelle version de Tivoli Netcool/OMNIbus, vous pouvez mettre à jour le schéma pour chaque instance ObjectServer que vous exécutez. Certaines nouvelles fonctionnalités de l'installation mise à niveau peuvent nécessiter la mise à jour du schéma. Tous les nouveaux ObjectServers que vous créez dans votre installation mise à niveau sont créés avec le schéma le plus récent.

«Démarrage manuel du serveur ObjectServer», à la page 204
Utilisez la commande **nco_objserv** pour démarrer manuellement le serveur ObjectServer.

Mise à niveau d'une architecture à plusieurs niveaux

La procédure décrite ici vous montre comment mettre à niveau un déploiement à plusieurs niveaux existant. Si vous installez une nouvelle configuration multiniveau Tivoli Netcool/OMNIbus version 8.1, n'utilisez pas cette procédure.

Avant de commencer

Pour éviter de perdre toute personnalisation de votre configuration, réalisez des copies de sauvegarde de tous les fichiers qui sont écrasés dans le cadre de cette procédure.

Pourquoi et quand exécuter cette tâche

Si vous mettez à niveau à partir d'une architecture multiniveau version 7.3 ou version 7.3.1 existante, exécutez d'abord les étapes 1 à 10, et ensuite les étapes 11 à 14. Si vous mettez à niveau à partir d'une architecture multiniveau version 7.4 existante, ignorez les étapes 1 à 10 et exécutez uniquement les étapes 11 à 14.

Procédure

Mise à niveau depuis la version 7.3 ou 7.3.1 vers la version 7.4

1. Ajoutez la propriété **Gate.Reader.IgnoreStatusFilter** à chaque fichier de propriétés de passerelle Collection-to-Aggregation (C_TO_A_GATE) et définissez-la sur TRUE.

   Par exemple : `Gate.Reader.IgnoreStatusFilter : TRUE`

2. Selon le nombre de passerelles définies dans votre architecture, copiez et renommez les fichiers de définition de réplication de table Collection-to-Aggregation de *NCHOME*/omnibus/extensions/multitier/gateway/ en *NCHOME*/omnibus/etc/.

   Par exemple, `C_TO_A_GATE_P_2.tblrep.def` et `C_TO_A_GATE_B_2.tblrep.def`.

   Remarque : Si vous répliquez des tables personnalisées, ajoutez-les aux fichiers de définition de réplication copiés.

3. Utilisez les commandes suivantes avec l'interface interactive SQL pour réactiver le déclencheur de changement d'état par défaut sur⌂tous les ObjectServers.
   - Pour les ObjectServers de la couche Collection et de la couche Agrégation :

     ```
     1> ALTER TRIGGER state_change SET ENABLED TRUE;
     2> go
     ```

   - Pour les ObjectServers de la couche Affichage :

     ```
     1> ALTER TRIGGER dsd_state_change SET ENABLED TRUE;
     2> go
     ```

4. Utilisez les commandes suivantes avec l'interface interactive SQL pour permettre aux déclencheurs de nettoyage sur les ObjectServers de la couche Affichage de nettoyer les journaux et les détails orphelins.

   ```
   1> ALTER TRIGGER clean_journal_table SET GROUP dsd_triggers;
   2> ALTER TRIGGER clean_details_table SET GROUP dsd_triggers;
   3> go
   ```

5. Supprimez les déclencheurs suivants de chaque type d'ObjectServer :
   - A partir des ObjectServers de la couche Collection : `col_state_change`
   - A partir des ObjectServers de la couche Agrégation : `agg_state_change`
   - A partir des ObjectServers de la couche Affichage : `dsd_state_change_2`

   L'exemple suivant utilise l'interface interactive SQL pour supprimer le déclencheur `col_state_change` :

   ```
   1> DROP TRIGGER col_state_change;
   2> go
   ```

6. Supprimez les lignes suivantes dans tous les fichiers de définition de mappe :

   ```
   'SourceStateChange' = '@SourceStateChange' ON INSERT ONLY,
   'SourceServerName' = '@SourceServerName' ON INSERT ONLY,
   'SourceServerSerial' = '@SourceServerSerial' ON INSERT ONLY,
   ```

7. Redémarrez toutes les passerelles pour lesquelles vous avez modifié les fichiers de configuration.
8. Utilisez l'interface interactive SQL pour importer les nouveaux fichiers ObjectServer SQL dans vos ObjectServers en cours d'exécution.

   UNIX Linux

   - Exemple d'ObjectServer de la couche Collection :

     ```
     $NCHOME/omnibus/bin/nco_sql -server COL_P_1 -user root <
     $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
     ```

   - Exemple d'ObjectServer de la couche Agrégation :

     ```
     $NCHOME/omnibus/bin/nco_sql -server AGG_P -user root <
     $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
     ```

   - Exemple d'ObjectServer de la couche Affichage :

```
$NCHOME/omnibus/bin/nco_sql -server DIS_1 -user root <
$NCHOME/omnibus/extensions/multitier/objectserver/display.sql
```

Windows

- Exemple d'ObjectServer de la couche Collection :

```
%NCHOME%\omnibus\bin\isql -S COL_P_1 -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\collection.sql
```

- Exemple d'ObjectServer de la couche Agrégation :

```
%NCHOME%\omnibus\bin\isql -S AGG_P -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\aggregation.sql
```

- Exemple d'ObjectServer de la couche Affichage :

```
%NCHOME%\omnibus\bin\isql -S DIS_1 -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\display.sql
```

Remarque : L'application de ces scripts SQL provoque des erreurs lorsque l'interface tente de créer des zones qui sont déjà présentes. Vous pouvez ignore ces erreurs en toute sécurité. Le but de réimporter le SQL est de mettre à jour les déclencheurs.

9. Facultatif : Supprimez des zones de configuration multiniveau redondantes en supprimant les colonnes suivantes de tous les ObjectServers :
   - `SourceStateChange`
   - `SourceServerName`
   - `SourceServerSerial`

   L'exemple suivant utilise l'interface interactive SQL pour supprimer la colonne `SourceStateChange` :

```
1> ALTER TABLE alerts.status DROP COLUMN SourceStateChange;
2> go
```

   Remarque : Avant de supprimer ces colonnes, vérifiez qu'aucune fonction personnalisée dans votre environnement ne dépend de ces colonnes.

10. Appliquez le script SQL suivant à tous les serveurs ObjectServer inclus dans votre configuration multiniveau :

    NCHOME`/omnibus/etc/update731to74.sql`

Mise à niveau depuis la version 7.4 vers la version 8.1

11. Appliquez les scripts SQL suivants, dans l'ordre indiqué, à tous les serveurs ObjectServer inclus dans votre configuration multiniveau.
    a. *NCHOME*`/omnibus/etc/update74to74fp3.sql`
    b. *NCHOME*`/omnibus/etc/update74fp3to81.sql`
12. Ajoutez la section suivante à tous les fichiers de définition de mappe ObjectServer Gateway.

```
##############################################################################
# Mappe de registre de sonde
#
# NOTE:
# 'ConnectionID'   Only set on the original ObjectServer that probes are
#   connected to. Elsewhere it defaults to '0'.
##############################################################################
CREATE MAPPING ProbeMap
(
 'Name'  = '@Name'  ON INSERT ONLY,
 'Hostname' = '@Hostname' ON INSERT ONLY,
 'ProbeType' = '@ProbeType',
 'HTTP_port' = '@HTTP_port',
 'HTTPS_port' = '@HTTPS_port',
```

```
 'RulesChecksum' = '@RulesChecksum',
 'PID'  = '@PID',
 'Status' = '@Status',
 'StartTime' = '@StartTime',
 'LastUpdate' = '@LastUpdate',
 'ApiReleaseID' = '@ApiReleaseID',
 'ApiVersion' = '@ApiVersion'
);
```

13. Ajoutez la commande REPLICATE suivante au fichier de définition de réplication de table AGG_GATE.tblrep.def.

```
REPLICATE ALL FROM TABLE 'registry.probes'
 USING map 'ProbeMap'
 WITH NORESYNC;
```

14. Ajoutez la commande REPLICATE suivante à tous les fichiers de définition de réplication de table de passerelles unidirectionnelles (exemple : A_TO_D_GATE.tblrep.def, C_TO_A_GATE_B_1.tblrep.def et C_TO_A_GATE_P_1.tblrep.def).

```
REPLICATE ALL FROM TABLE 'registry.probes'
 USING map 'ProbeMap';
```

Résultats

Votre architecture multiniveau est mise à niveau pour utiliser la fonction de registre de la sonde.

Concepts associés:

Chapitre 8, «Configuration et déploiement d'une architecture à plusieurs niveaux», à la page 223
Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

Installation de sondes et de passerelles dans un environnement Tivoli Netcool/OMNIbus mis à niveau

La réinstallation des sondes est nécessaire lors de la mise à niveau à la version 8.1 de toute version précédente de Tivoli Netcool/OMNIbus.

Avant de commencer

Les sondes et les passerelles 32 bits nécessitent des bibliothèques de système d'exploitation 32 bits qui, si vous utilisez un système d'exploitation 64 bits, peuvent ne pas être déjà installées. Consultez la documentation relative à la sonde ou à la passerelle pour connaître la configuration requise spécifique. Vous pouvez également exécuter IBM Prerequisite Scanner avec la fonction de sonde sélectionnée afin de déterminer si vous disposez de toutes les bibliothèques nécessaires. Les bibliothèques Tivoli Netcool/OMNIbus 32 bits principales qui sont requises pour exécuter des analyses et des passerelles 32 bits (par exemple, libOpl) sont installées par défaut.

Pourquoi et quand exécuter cette tâche

Lorsque vous migrez des données, manuellement ou avec IBM Installation Manager, vos anciens fichiers de configuration de sonde et de passerelle sont copiés dans les endroits suivants :

UNIX Linux

- Fichiers de configuration de sonde : `$NCHOME/omnibus/probes/migrated`
- Fichiers de configuration de passerelle : `$NCHOME/omnibus/etc`

Windows

- Fichiers de configuration de sonde : `%NCHOME%\omnibus\probes\migrated`
- Fichiers de configuration de passerelle : `%NCHOME%\omnibus\etc`

Procédure

1. Installez les sondes et les passerelles dans le nouvel environnement Tivoli Netcool/OMNIbus.
2. Une fois l'installation terminée, copiez les fichiers de configuration de sonde migrés du répertoire `$NCHOME/omnibus/probes/migrated` vers les emplacements appropriés de `$NCHOME/omnibus/probes`.

Remarques supplémentaires sur la mise à niveau et la migration

Lisez les remarques suivantes pour obtenir des informations supplémentaires sur les processus de mise à niveau et de migration de Tivoli Netcool/OMNIbus et sur toutes les actions que vous devrez peut-être effectuer.

Migration des données BAROC d'IBM Tivoli Enterprise Console

Tivoli Netcool/OMNIbus fournit l'intégration avec Tivoli Enterprise Console.

Le produit Tivoli Enterprise Console est une application de gestion des événements basée sur des règles qui intègre la gestion du système, du réseau, de la base de données et de l'application pour permettre de garantir une disponibilité optimale des services informatiques d'une organisation.

Dans Tivoli Enterprise Console, un événement est un objet créé en se basant sur des données obtenues depuis une source surveillée par un adaptateur d'événements. Chaque événement est identifié par un nom de classe défini par un adaptateur d'événements. Les noms de classe sont utilisés pour donner un intitulé aux événements, mais chaque événement contient des informations supplémentaires qui aident à définir et à situer un incident potentiel. Les classes d'événement peuvent avoir des sous-classes pour permettre une analyse plus approfondie des informations afin de leur appliquer des règles plus détaillées. Un adaptateur formate les informations d'événement en attributs qui contiennent un nom et une valeur puis envoie ces informations au serveur d'événements pour traitement.

Un adaptateur utilise différents fichiers pour ses opérations. Un de ces fichiers est le fichier de Basic recorder of objects in C (BAROC), qui décrit les classes d'événements prises en charge par l'adaptateur pour le serveur d'événements. Ce serveur doit charger le fichier pour pouvoir comprendre les événements qu'il reçoit de l'adaptateur. Un fichier BAROC a l'extension `.baroc`.

Dans Tivoli Netcool/OMNIbus, le serveur ObjectServer stocke et traite les événements dans une représentation "à plat" normalisée, incompatible avec la hiérarchie des classes et le format d'attribut étendu adopté pour les événements de Tivoli Enterprise Console.

Pour prendre en charge la migration des données d'événement de Tivoli Enterprise Console, Tivoli Netcool/OMNIbus fournit un outil BAROC pour convertir les données. Le schéma du serveur ObjectServer fournit également les objets suivants pour la prise en charge de la migration des données de Tivoli Enterprise Console :

- Une table master.class_membership est utilisée pour stocker les détails de toutes les classes Tivoli Enterprise Console avec l'ID classe, le nom et l'ID parent. L'outil BAROC renseigne cette table.
- Une colonne ExtendedAttr de type de données VARCHAR(4096) dans la table alerts.status, qui stocke plusieurs paires valeur-nom dans une colonne et dans un format compatible avec les chaînes d'événement Tivoli Enterprise Console.
- Fonctions de règles de sonde et SQL :
  - Une fonction SQL instance_of : renvoie true si la classe est une sous-classe de classe_parent ou si elles sont égales, à l'aide de la hiérarchie définie dans la table master.class_membership.
  - Une fonction SQL nvp_exists() : vérifie si la paire valeur-nom existe.
  - Une fonction SQL nvp_get() : extrait la valeur d'une paire valeur-nom spécifique.
  - Une fonction SQL nvp_set() : ajoute ou remplace les clés d'une paire valeur-nom et renvoie la nouvelle chaîne valeur-nom.
  - Une fonction de règle de sonde nvp_add() : ajoute ou remplace des variables et leurs valeurs dans une liste de paires valeur-nom ou crée une telle liste de toutes les variables.
  - Une fonction de règle de sonde nvp_remove() : supprime les clés d'une paire valeur-nom et renvoie la nouvelle chaîne de paire valeur-nom.

A propos de l'outil de conversion BAROC (nco_baroc2sql) :

Pour prendre en charge la migration des données depuis Tivoli Enterprise Console vers Tivoli Netcool/OMNIbus, l'outil de conversion BAROC est fourni dans Tivoli Netcool/OMNIbus pour convertir les fichiers BAROC de Tivoli Enterprise Console en fichiers SQL du serveur ObjectServer, que vous pouvez ensuite importer dans la base de données.

L'outil BAROC (**nco_baroc2sql**) est installé lorsque vous sélectionnez la fonction **Serveurs** lors de l'installation de Tivoli Netcool/OMNIbus. Cet outil se trouve dans le répertoire *NCHOME*/omnibus/bin. Vous devez d'abord exécuter l'outil sur votre fichier de charge .baroc pour créer des instructions SQL INSERT qui sont conformes aux instructions SQL du serveur ObjectServer. Ces instructions sont sauvegardées dans un fichier que vous indiquez. Après la génération de la sortie SQL, vous devez importer les données qui sont définies dans les instructions INSERT dans la base de données du serveur ObjectServer.

Lorsque vous exécutez l'outil **nco_baroc2sql**, il écrit une instruction INSERT pour la table master.class_membership du serveur ObjectServer pour chaque relation classe-parent existant dans le fichier BAROC. Lorsque la classe BAROC possède plusieurs relations d'héritage dans ses classes parent, l'outil **nco_baroc2sql** écrit une instruction INSERT pour chaque relation classe/parent existant dans le fichier BAROC. Le format de l'instruction INSERT que l'outil **nco_baroc2sql** génère est le suivant :

```
insert into master.class_membership ( Class, ClassName, Parent ) values (entier, 'chaîne', entier );
```

Où :

- La valeur Class contient un identificateur numérique unique pour la classe. Les identificateurs de classe générés commencent à partir de 76000, à moins que indiquiez une valeur de départ différente lorsque vous exécutez l'outil à partir de la ligne de commande.
- La valeur ClassName contient le nom de la classe comme elle apparaît dans le fichier BAROC.
- La valeur Parent contient la valeur de classe numérique de la classe parent. Si aucune classe parent n'est définie dans le fichier BAROC, une instruction INSERT est créée pour la classe dont la zone Parent est définie sur -1. (Ces entrées sont connues sous le nom de nœuds root.)

Par exemple :

```
insert into master.class_membership (Class, ClassName, Parent ) values ( 76000, 'ABC_Base', 76001);
```

La table master.class_membership n'autorise pas les mappages en double des noms de classe aux numéros de classe. Elle n'autorise également pas plusieurs entrées avec le même nom de classe ou le même numéro de classe.

L'outil **nco_baroc2sql** crée également une entrée de conversion de classe pour chaque classe des fichiers `.baroc`. Cela permet d'écrire les outils spécifiques à la classe pour la liste d'événements de Tivoli Netcool/OMNIbus. Le format de l'instruction INSERT que l'outil génère est le suivant :

```
insert into alerts.conversions values
('Class+ID de classe', 'Class', ID de classe, 'nom de classe' );
```

Par exemple :

```
insert into alerts.conversions values ( 'Class76000', 'Class', 76000, 'ABC_Base');
```

Remarque : La table master.class_membership n'autorise pas les mappages en double des noms de classe aux numéros de classe. Elle n'autorise également pas plusieurs entrées avec le même nom de classe ou le même numéro de classe.

Les deux types d'instructions INSERT sont sauvegardés dans le même fichier de sortie.

Remarque : L'outil **nco_baroc2sql** n'exécute pas de validation pour vérifier si les identificateurs de classe qu'il alloue sont disponibles sur le système cible. L'outil n'insère pas non plus de limite supérieure pour les valeurs d'identificateur de classe.

Les classes de Tivoli Enterprise Console sont mappées aux classes du serveur ObjectServer. 10 000 identificateurs de classe sont réservés pour ce mappage, compris entre 76000 et 86000.

Pour mapper des événements entrants Tivoli Enterprise Console aux identificateurs de classe ObjectServer, l'outil **nco_baroc2sql** peut facultativement générer un fichier de table de recherche insérable dans le fichier de règles d'une sonde. La table de recherche contient les valeurs class-name Tivoli Enterprise Console mappées aux classes ObjectServer. La table de recherche respecte le format suivant :

```
class-name ID de classe
```

Chaque classe est définie sur une ligne séparée, avec une définition dans chaque ligne ajoutée à la table alerts.conversions par le langage SQL généré par l'outil **nco_baroc2sql**.

Migration de données BAROC :

Avant de migrer des données Tivoli Enterprise Console, vous devez préparer un fichier de chargement définissant les fichiers BAROC à traiter. Les fichiers BAROC spécifiés dans le fichier de chargement doivent se trouver dans le même répertoire que le fichier de chargement.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez la migration, l'outil **nco_baroc2sql** lit le fichier de chargement spécifié et traite les fichiers BAROC en suivant leur ordre de présentation dans le fichier de chargement.

Procédure

1. Entrez la commande suivante dans la ligne de commande :

   NCHOME/omnibus/bin/nco_baroc2sql -baroc *fichier_chargement_baroc* -sql *fichier_sortie* -lookup *ficher_recherche*

   Où :

   - *fihcier_chargment_baroc* représente le nom et le chemin du fichier du fichier de chargement BAROC
   - *fichier_sortie* représente le nom et le chemin de fichier du fichier de sortie, généré sous forme de fichier SQL
   - *fichier_recherche* (facultatif) représente le nom du fichier de la table de recherche à destination duquel le mappage des valeurs class-name aux classes ObjectServer est écrit.

   La commande **nco_baroc2sql** dispose des options de ligne de commande suivantes : Soit l'option de ligne de commande –sql, soit l'option -lookup doit être spécifiée - ou les deux. Si aucune de ces deux options de ligne de commande n'est spécifiée, l'outil **nco_baroc2sql** échoue.

Tableau 33. Options de ligne de commande pour la commande nco_baroc2sql

Option de ligne de commande	Description
-baroc *fichier*	Chemin d'accès au fichier de chargement BAROC, qui répertorie les fichiers BAROC à traiter.
-sql *fichier*	Chemin d'accès dans lequel le fichier de sortie SQL sera écrit.
-help	Affiche le texte d'aide.
-version	Affiche les informations de version sur l'outil.
-classno *ent*	Numéro de classe de base à utiliser pour les conversions de classe. La valeur par défaut est 76000. Modifiez uniquement cette valeur si vous avez des conversions existantes dans la plage de 76 000 à 86 000.
-lookup *fichier*	Facultatif : Le nom du fichier de la table de recherche à destination duquel le mappage des valeurs class-name aux classes ObjectServer est écrit.

   Attendez la fin du processus.

2. Connectez-vous à l'interface SQL interactive et importez le fichier de sortie SQL sur le serveur ObjectServer en procédant comme suit :

   UNIX Linux $NCHOME/omnibus/bin/nco_sql -server *nom_serveur* -username root -password ""< *fichier_sortie*

Windows `%NCHOME%\omnibus\bin\isql -S nom_serveur -U root -P mot_de_passe -i fichier_sortie.sql`

Où *nom_serveur* représente le nom du serveur ObjectServer dans lequel les données sont importées et *fichier_sortie* représente le chemin d'accès et le nom du fichier de sortie SQL.

Résultats

Les messages de traitement sont affichés à l'écran et ne sont pas générés dans un fichier journal. Vous pouvez rediriger les messages dans un fichier journal, le cas échéant.

Probe for Tivoli EIF offre l'intégration du flux d'événements entre Tivoli Enterprise Console et Tivoli Netcool/OMNIbus. Les informations sur cette sonde sont disponibles dans le centre de documentation Tivoli Network Management à l'adresse http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/common/kc_welcome-444.html.

Que faire ensuite

Si vous devez effectuer des changements sur la table master.class_membership après avoir exécuté l'outil **nco_baroc2sql**, procédez comme suit :

- Pour ajouter de nouvelles entrées à la table master.class_membership, déterminez le nombre maximal des conversions de classes que la table contient actuellement. Puis, réexécutez l'outil **nco_baroc2sql** et utilisez l'option `-classno` pour spécifier un numéro de classe basique pour les conversions de classes qui soit plus élevé que le nombre maximal actuel.
- Pour changer le mappage du nom de classe au numéro de classe, supprimez les entrées existantes dans la table master.class_membership. Réexécutez ensuite l'outil **nco_baroc2sql** et utilisez l'option `-classno` pour spécifier un numéro de classe basique différent à utiliser pour les conversions de classes.

Vous pouvez à présent réimporter le fichier de sortie SQL dans le serveur ObjectServer en répétant l'étape 2, à la page 139 de cette tâche.

Si vous avez utilisé l'option de ligne de commande `-lookup`, vous pouvez à présent insérer le fichier de table de recherche généré dans le fichier de règles de la sonde requise. L'exemple suivant vous montre comment définir la table de recherche `tec_class` dans le fichier de règles :

```
table tec_class = "table_recherche"
default = "Unknown"
```

Où *table_recherche* correspond au chemin d'accès vers la table de recherche générée par l'outil **nco_baroc2sql**. L'exemple suivant indique comment utiliser la fonction `lookup` (recherche) pour remplir l'élément de classe avec le nom de classe Tivoli Enterprise Console :

```
$Class = lookup($ClassName,tec_class)
```

Migration des certificats et des clés SSL

Si votre environnement est protégé par le chiffrement SSL (Secure Socket Layer), vous pourriez devoir migrer les certificats existants vers une nouvelle base de données clés après une mise à niveau vers une nouvelle version de l'Tivoli Netcool/OMNIbus. Cela garantit que les ObjectServers continuent de fonctionner correctement.

Pourquoi et quand exécuter cette tâche

Remarque : Les certificats créés dans Tivoli Netcool/OMNIbus V7.2 (et versions antérieures) sont stockés dans un format qui est incompatible avec V8.1. Vous devez créer ou régénérer manuellement les certificats et les clés SSL requis dans votre installation V8.1. Les instructions suivantes s'appliquent uniquement aux mises à niveau à partir de V7.2.1.

Vous devez créer une base de données de clés et importer les certificats de la base de données de clés précédente vers la nouvelle. Effectuez cette procédure sur chaque ordinateur hôte sur lequel ObjectServer, un agent de processus ou un serveur proxy est configuré pour SSL, ainsi que sur chaque ordinateur client utilisant des connexions SSL.

Les bases de données de clés se trouvent dans le répertoire *NCHOME*`/etc/security/keys`. Le fichier de base de données de clés Tivoli Netcool/OMNIbus est nommé `omni.kdb`.

Procédure

Répétez la procédure suivante sur chaque ordinateur hôte sur lequel ObjectServer, un agent de processus ou un serveur proxy est configuré pour SSL, ainsi que sur chaque ordinateur client utilisant des connexions SSL.

1. Si vous avez effectué la mise à niveau en installant Tivoli Netcool/OMNIbus V8.1 dans le même répertoire que la version précédente deTivoli Netcool/OMNIbus, déplacez la base de données de clés `omni.kdb` vers un répertoire temporaire (*temp*).

   Si vous avez installé V8.1 dans un autre répertoire de la version précédente et que vous avez migré les données à partir de la version précédente, vous pouvez ignorer cette étape. `omni.kdb` est automatiquement copié dans le répertoire *NCHOME*`/etc/security/keys/migrated` pendant la mise à niveau.
2. Utilisez la commande suivante pour créer une base de données de clés, également appelée `omni.kdb`, dans l'installation V8.1 :

   NCHOME`/bin/nc_gskcmd -keydb -create -db` *NCHOME*`/etc/security/keys/omni.kdb -pw` *mot_de_passe* `-type cms -stash`

   Utilisez le même mot de passe que l'ancienne base de données `omni.kdb`.
3. Utilisez la commande suivante pour importer les certificats contenus dans l'ancienne base de données de clés vers la nouvelle base de données de clés version 8.1 :

   NCHOME`/bin/nc_gskcmd -cert -import -db` *chemin*`/omni.kdb -pw` *mot_de_passe* `-type cms -target` *NCHOME*`/etc/security/keys/omni.kdb -target_pw` *mot_de_passe* `-target_type cms`

   Où *chemin* est l'emplacement de l'ancienne base de données de clés temporaire (*temp*`/omni.kdb`) ou l'emplacement de l'ancienne base de données de clés migrée (*NCHOME*`/etc/security/keys/migrated`). *mot_de_passe* est l'ancien mot de passe de la base de données de clés.

Tâches associées:

«Création d'une base de données de clés», à la page 381
Sur chaque ordinateur sur lequel un composant serveur (ObjectServer, agent de processus ou serveur proxy) est installé, créez une base de données de clés pour stocker les certificats numériques. Créez également une base de données de clés sur chaque ordinateur à partir duquel les clients se connectent au serveur à l'aide d'un port SSL. Utilisez un fichier de la base de données de clés dédié (`omni.kdb`) pour chaque installation Tivoli Netcool/OMNIbus sur un serveur ou un ordinateur client.

«Configuration d'un réseau protégé SSL», à la page 380
Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

«Gestion des certificats numériques», à la page 401
Exécutez ces tâches dans le cadre de la gestion d'un réseau protégé SSL.

Mise à niveau des mots de passe à chiffrement DES vers AES

Les versions précédentes de Tivoli Netcool/OMNIbus utilisent Data Encryption Standard (DES) pour chiffrer les mots de passe stockés dans l'ObjectServer. Si vous voulez utiliser le chiffrement FIPS 140-2 dans votre installation mise à niveau Tivoli Netcool/OMNIbus, vous devez vous assurer que tous les mots de passe sont chiffrés avec Advanced Encryption Standard (AES).

Pourquoi et quand exécuter cette tâche

Après mise à niveau vers Tivoli Netcool/OMNIbus version 8.1, modifiez la norme de chiffrement des mots de passe AES, changez ou réinitialisez tous les mots de passe, puis redémarrez Tivoli Netcool/OMNIbus.

La propriété ObjectServer **PasswordEncryption** spécifie le type de chiffrement utilisé.

Procédure

1. Remplacez la valeur de la propriété ObjectServer **PasswordEncryption** par AES.
2. Pour appliquer le chiffrement AES, modifiez ou réinitialisez tous les mots de passe ou contactez les utilisateurs et demandez-leur de modifier ou réinitialiser leurs mots de passe.

   Vous pouvez réinitialiser les mots de passe de l'utilisateur avec l'interface interactive SQL. Par exemple :

   ```
   1> alter user 'nom d'utilisateur' set password 'mot de passe';
   2> go
   ```

   Où *mot de passe* est le nouveau mot de passe.
3. Pour vérifier avec l'interface interactive SQL que tous les mots de passe ont été modifiés, utilisez la commande suivante :

   ```
   1> select UserName,Passwd from security.users;
   2> go
   ```

   Les mots de passe à chiffrement DES contiennent 11 caractères. Les mots de passe à chiffrement AES contiennent 24 caractères.
4. Pour vérifier avec l'Netcool/OMNIbus Administrator (**nco_config**) que tous les mots de passe ont été modifiés, utilisez les étapes suivantes :
   a. Démarrez Netcool/OMNIbus Administrator.
   b. Connectez-vous à l'ObjectServer.

c. Cliquez sur **Système**, puis cliquez sur **Databases** (Bases de données) pour ouvrir le panneau >Databases, Tables and Columns (Bases de données, tables et colonnes)..
d. Sélectionnez la base de données **sécurité** et la table **utilisateurs**, puis cliquez sur l'onglet **Data View** (Vue des données) dans le panneau Databases, Tables and Columns (Bases de données, tables et colonnes) pour visualiser les données utilisateur.

Dans la colonne **Passwd** (Mot de passe), les mots de passe à chiffrement DES contiennent 11 caractères et les mots de passe à chiffrement AES contiennent 24 caractères.

5. Configurez Tivoli Netcool/OMNIbus pour opérer en mode FIPS 140–2.
6. Redémarrez Tivoli Netcool/OMNIbus.

Concepts associés:

Chapitre 10, «Configuration de la prise en charge de FIPS 140–2 pour les composants serveur», à la page 283
Vous pouvez exécuter les composants serveur suivants en mode FIPS 140–2 : les serveurs ObjectServer, les agents de processus, les serveurs proxy et les passerelles du serveur ObjectServer. Dans ce mode, les fonctions cryptographiques de Tivoli Netcool/OMNIbus utilisent les modules cryptographiques approuvés par la norme FIPS 140–2.

Tâches associées:

«Configuration de l'environnement d'exécution Java pour FIPS 140–2», à la page 97
Pour configurer l'environnement d'exécution Java (JRE) fourni avec Tivoli Netcool/OMNIbus pour utiliser le chiffrement FIPS 140-2, modifiez la configuration du fichier `java.security`. Vous pouvez également télécharger et ajouter des fichiers de règles pour utiliser des algorithmes de chiffrement étendus.

Chapitre 6. Installation et mise à niveau du composantInterface graphique Web

Cette rubrique présente comment installer, mettre à niveau et désinstaller le composant Interface graphique Web. Les processus d'installation, de mise à niveau et de désinstallation sont identiques pour tous les systèmes d'exploitation.

Avant de commencer

- Aménagez suffisamment d'espace disque sur le volume que vous prévoyez pour l'installation de l'Interface graphique Web. Si vous avez l'intention d'installer d'autres produits Concentrateur des services d'application du tableau de bord, l'espace disponible dans l'emplacement d'installation doit être suffisant pour contenir ces produits. Les performances de l'Interface graphique Web sont supérieures lorsque Concentrateur des services d'application du tableau de bord a l'usage exclusif des ressources système. Les performances du système peuvent être réduites si Concentrateur des services d'application du tableau de bord partage des ressources avec d'autres produits.
- Installez les composants du serveur Tivoli Netcool/OMNIbus, puis créez et démarrez un ou plusieurs serveurs ObjectServer. Afin d'éviter le recours à des utilisateurs root ObjectServer, créez de nouveaux utilisateurs pour la connexion à l'Interface graphique Web. Cette dernière doit être en mesure de communiquer avec le ou les serveurs ObjectServer. Si le serveur Concentrateur des services d'application du tableau de bord doit communiquer avec d'autres systèmes à l'aide d'un serveur proxy, il pourra être nécessaire d'ajouter les droits de transaction de données appropriés au système intermédiaire.
- Windows Affectez les privilèges d'administrateur à l'utilisateur auquel vous souhaitez faire appel pour l'installation.
- Assurez-vous que l'ordinateur hôte dispose d'une capacité disque suffisante et que les données qu'il contient peuvent être sauvegardées régulièrement. Le système du serveur Concentrateur des services d'application du tableau de bord peut nécessiter une grande quantité d'espace de stockage pour répondre aux exigences de la page d'accueil d'un grand nombre d'utilisateurs de l'Interface graphique Web.

Pourquoi et quand exécuter cette tâche

Le produit est disponible sous forme de distribution de fichier compressé sur DVD ou téléchargeable à partir d'IBM Passport Advantage. Ce produit est installé par IBM Installation Manager. Trois modes d'installation sont pris en charge : Interface graphique, Console et Silencieux. Vous pouvez créer un nouveau répertoire pour y installer l'Interface graphique Web ou utiliser une installation Concentrateur des services d'application du tableau de bord existante. En cours d'installation, vous indiquerez le serveur ObjectServer auquel l'Interface graphique Web doit se connecter, et éventuellement, vous identifierez un serveur ObjectServer secondaire pour protéger la reprise en ligne.

La distribution de fichier compressé contient IBM Installation Manager. Utilisez cette option lorsque vous souhaitez installer Tivoli Netcool/OMNIbus sur un petit nombre d'ordinateurs. Vous installerez également le produit via cette option si vous n'avez pas accès à Internet et si vous ne voulez pas gérer votre propre référentiel de logiciels IBM.

Vous avez aussi l'option d'installer IBM Installation Manager séparément et d'utiliser celui-ci pour télécharger et installer le produit à partir d'un référentiel IBM ou d'un référentiel local sur votre réseau. Vous recourrez à cette option pour installer le logiciel ou pour le mettre à jour à la dernière version sans devoir copier les fichiers compressés sur chaque ordinateur. À moins que chaque ordinateur dispose d'un accès à Internet, il vous faudra conserver un ou plusieurs référentiels de logiciels. Pour plus de détails concernant l'utilisation de IBM Installation Manager pour Enterprise Deployment et concernant l'utilitaire Installation Manager Packaging Utility, voir http://www.ibm.com/support/knowledgecenter/SSDV2W_1.0.0/com.ibm.im.articles.doc/topics/entdeployment.htm.

Le tableau qui suit décrit les options disponibles pour l'installation du produit avec IBM Installation Manager.

Tableau 34. Options d'installation

Option d'installation	**Description**
Option 1	1. Téléchargez et installez IBM Installation Manager. 2. Utilisez IBM Installation Manager pour télécharger et installer l'Interface graphique Web à partir des référentiels IBM Passport Advantage.
Option 2	1. Téléchargez et installez IBM Installation Manager. 2. Utilisez IBM Installation Manager Packaging Utility pour copier l'Interface graphique Web depuis les référentiels IBM Passport Advantage vers un référentiel local. 3. Utilisez IBM Installation Manager pour installer l'Interface graphique Web.
Option 3	1. Procurez-vous le fichier de distribution compressé Interface graphique Web à partir de IBM Passport Advantage ou sur un DVD et extrayez le contenu dans un répertoire temporaire. 2. Utilisez les commandes disponibles dans le répertoire IBM Installation Manager mis en package (exemple : **im.linux.x86_64**) pour installer IBM Installation Manager et l'Interface graphique Web en même temps. Les commandes disponibles sont les suivantes : • **install** : pour les installations via l'interface graphique • **installc** : pour les installations à partir de la console • `tools/imcl` : pour les installations en mode silencieux **Remarque :** Ces scripts sélectionnent automatiquement IBM Installation Manager Mode administrateur quand ils sont exécutés par un utilisateur root ou Mode non-administrateur quand ils sont exécutés par un utilisateur non-root. Si vous souhaitez utiliser Mode groupe, installez IBM Installation Manager manuellement avec la commande **groupinst** ou **groupinstc**.
Option 4	1. Téléchargez et installez IBM Installation Manager. 2. Procurez-vous le fichier de distribution compressé Interface graphique Web à partir de IBM Passport Advantage ou sur un DVD et stockez le contenu dans un référentiel local. 3. Utilisez IBM Installation Manager pour installer l'Interface graphique Web.

Pour plus de détails concernant l'installation des produits avec IBM Installation Manager, voir http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Concepts associés:

«Exigences d'espace disque», à la page 29
Vérifiez que l'espace disque disponible est suffisant sur le volume pour le système d'exploitation sur lequel vous installez Tivoli Netcool/OMNIbus.

Tâches associées:

«Mise à niveau à partir d'IBM Tivoli Netcool/Webtop version 2.2 ou de l'Interface graphique Web version 7.3.0», à la page 167
Pour mettre à niveau Netcool/Webtop version 2.2 ou l'Interface graphique Web version 7.3.0 vers l'Interface graphique Web version 8.1, mettez à niveau l'interface utilisateur Web vers la version 7.4, puis mettez à niveau vers l'Interface graphique Web version 8.1.

Information associée:

Gestion du domaine dans une configuration de référentiel fédéré

Préparation de l'installation ou de la mise à niveau de l'Interface graphique Web

Avant d'installer ou de mettre à niveau l'Interface graphique Web, il peut être nécessaire d'effectuer une ou plusieurs tâches de préinstallation, en fonction des fonctions à installer. Vous devez également obtenir le module d'installation pour votre système d'exploitation.

Regroupement d'informations sur l'installation

Avant d'exécuter le programme d'installation de l'Interface graphique Web, rassemblez les informations dont vous avez besoin pour installer le produit.

Informations concernant toutes les installations

Regroupez les informations suivantes pour toutes les installations de l'Interface graphique Web :

Tableau 35. Information pour une installation

Elément	Valeur par défaut	Description
Répertoire d'installation de Concentrateur des services d'application du tableau de bord		
Créer une nouvelle instance de Concentrateur des services d'application du tableau de bord ou réutiliser une instance qui existe déjà ?	Créer	Indique si vous voulez créer une nouvelle instance de Concentrateur des services d'application du tableau de bord pour l'Interface graphique Web ou en utiliser une existante.
Répertoire	`/opt/IBM/JazzSM`	Lorsque vous créez une nouvelle instance de Concentrateur des services d'application du tableau de bord, choisissez quel répertoire d'installation vous souhaitez utiliser pour l'Interface graphique Web et Concentrateur des services d'application du tableau de bord. UNIX Linux Le nom du chemin ne peut pas contenir d'espace.

Tableau 35. Information pour une installation (suite)

Elément	Valeur par défaut	Description
Concentrateur des services d'application du tableau de bord instance		Lorsque votre réutilisez une instance Concentrateur des services d'application du tableau de bord, le répertoire contient l'instance à utiliser.
Répertoire d'installation de l'Interface graphique Web		
Répertoire	`/ibm/netcool/omnibus_webgui`	Choisissez dans quel répertoire vous souhaitez mettre l'Interface graphique Web. Ce répertoire est également appelé le répertoire de base du produit. UNIX Linux Le nom du chemin ne peut pas contenir d'espace.
Répertoire d'installation du serveur Websphere Application Server		
Répertoire	`/opt/IBM/Websphere/AppServer`	Quand vous créez une nouvelle instance de Concentrateur des services d'application du tableau de bord, choisissez le répertoire d'installation à utiliser pour le serveur Websphere Application Server.
Administrateur		
User ID (ID utilisateur)	smadmin	Identifiants de connexion de l'administrateur de l'Interface graphique Web. **Restriction :** Le mot de passe de l'administrateur ne doit pas commencer par un trait d'union (-).
Password		
Ports de communication		
Interface graphique Webport	16310	Port non sécurisé utilisé par l'Interface graphique Web pour être en mode écoute des demandes de connexion des utilisateurs. La procédure d'installation réserve également le port supérieur d'une unité (16311 par défaut) pour les connexions sécurisées. Vérifiez que ces deux ports ne sont pas en cours d'utilisation sur le serveur que l'Interface graphique Web doit utiliser.
Caractéristiques principales du serveur ObjectServer		
User ID (ID utilisateur)	root	Identité et accréditations du serveur ObjectServer principal dans une configuration ObjectServer double ou du serveur ObjectServer unique qui alimentent l'Interface graphique Web en données. Ce nom peut contenir un maximum de 29 caractères.
Password	*****	
Nom	OMNIbus	
Nom d'hôte	myobjectserver.ibm.com	
Port	4100	
Caractéristiques du serveur ObjectServer secondaire		

Tableau 35. Information pour une installation (suite)

Elément	Valeur par défaut	Description
Faut-il activer le serveur secondaire pour la reprise en ligne ?	Non	Détermine si votre site utilise un serveur ObjectServer secondaire pour protéger la reprise en ligne. Si votre site a un serveur ObjectServer secondaire, regroupez l'identité et les accréditations de ce serveur. Ce nom peut contenir un maximum de 29 caractères.
Nom		
Nom d'hôte		
Port		

Installation et mise à niveau de l'Interface graphique Web dans un environnement d'équilibrage de charge

Lorsque vous installez ou mettez à niveau l'Interface graphique Web dans un environnement d'équilibrage de la charge existante, effectuez l'installation ou la mise à niveau comme décrit ici. N'effectuez pas d'installation ou de mise à niveau dans un environnement d'équilibrage de charge avant d'avoir lu ces instructions.

Ces instructions s'appliquent dans les situations suivantes :

- Vous souhaitez mettre à niveau une installation existante de l'Interface graphique Web qui est dans un environnement d'équilibrage de charge.
- Vous souhaitez installer l'Interface graphique Web dans un environnement d'équilibrage de charge qui ne contient pas encore l'Interface graphique Web.

Procédure

1. Installez l'Interface graphique Web sur chaque nœud tour à tour et migrez les données depuis la version précédente. Assurez-vous d'avoir configuré chaque installation de la même manière.
2. Recréer le cluster et chaque nœud un à un. Lors de cette procédure, vous ne devez pas recréer ou éditer les fichiers de configuration ni la base de données. Au lieu de cela :
   a. Exécutez les commandes pour définir le cluster sur un nœud.
   b. Sur les autres nœuds, exécutez les commandes permettant de joindre les clusters.
   c. Préparez le serveur HTTP pour l'équilibrage de charge
   d. Démarrez les opérations d'équilibrage de charge de l'Interface graphique Web sur chaque nœud.

Tâches associées:

«Installation de l'interface graphique Web», à la page 151
Utilisez l'une de ces trois méthodes pour installer l'Interface graphique Web.

«Mise à niveau de l'Interface graphique Web et migration de données», à la page 158
Vous pouvez mettre à niveau vers la version 7.4 l'Interface graphique Web version 7.4, 7.3.1 ou 7.3. Vous pouvez également effectuer une mise à niveau à partir de IBM Tivoli Netcool/Webtop. Si vous effectuez une mise à niveau à partir de l'Netcool/Webtop, vous devez migrer les données vers la version 7.4 de l'Interface graphique Web.

«Exécution des tâches post-installation», à la page 178
Après l'installation, un certain nombre de tâches de configuration (obligatoires ou facultatives) sont nécessaires pour terminer la configuration initiale de votre

environnement de produit.

«Configuration d'un environnement d'équilibrage de charge», à la page 603
Vous pouvez configurer un cluster d'équilibrage de charge composé de noeuds de portail ayant des configurations identiques pour répartir uniformément les sessions utilisateur. L'équilibrage de charge est idéal pour les environnements avec un grand nombre d'utilisateurs. En cas d'échec d'un noeud dans un cluster, les nouvelles sessions utilisateur sont dirigées vers les autres noeuds actifs. L'équilibrage de charge est fourni dans Concentrateur des services d'application du tableau de bord.

Structure du répertoire d'installation Interface graphique Web

Le tableau suivant décrit la structure du répertoire d'installation de l'Interface graphique Web.

L'Interface graphique Web n'utilise pas le répertoire de base Netcool.

Windows Remplacez la barre oblique (/) par une barre oblique inversée (\).

Tableau 36. Répertoires Interface graphique Web

Répertoire	Description
REP_INSTALL_JazzSM/bin	Contient les scripts de démarrage et d'arrêt du serveur Concentrateur des services d'application du tableau de bord.
REP_INSTALL_WEBGUI/etc	Contient les fichiers de configuration de l'Interface graphique Web, notamment le fichier configurable par l'utilisateur server.init.
REP_INSTALL_WEBGUI/etc/cgi	Contient les options de configuration pour le registre CGI.
REP_INSTALL_WEBGUI/etc/cgi-bin	Contient les scripts CGI.
REP_INSTALL_WEBGUI/etc/charts	Contient les fichiers XML graphiques.
REP_INSTALL_WEBGUI/etc/configstore	Contient les fichiers de configuration des menus, outils, invites, métriques et collectes de filtres.
REP_INSTALL_WEBGUI/etc/data	Contient les définitions de filtre et de vue spécifiques à l'utilisateur et globales.
REP_INSTALL_WEBGUI/etc/datasources	Contient des informations sur les sources de données.
REP_INSTALL_WEBGUI/etc/default	Contient une copie des fichiers de configuration de l'Interface graphique Web par défaut.
REP_INSTALL_WEBGUI/etc/deprecated	Pour les installations mises à niveau de IBM Tivoli Netcool/Webtop V2.2 uniquement : contient les artefacts de configuration de Interface graphique Web migrés, par exemple les entités.
REP_INSTALL_WEBGUI/etc/maps	Contient les fichiers de carte.
REP_INSTALL_WEBGUI/etc/resources	Contient les ressources utilisées dans les cartes.
REP_INSTALL_WEBGUI/etc/system	Contient les fichiers HTML et les ressources système.
REP_INSTALL_WEBGUI/etc/templates	Contient les modèles HTML système.

Tableau 36. Répertoires Interface graphique Web (suite)

Répertoire	Description
REP_INSTALL_JazzSM/installedApps/Cellule_Noeud01_JazzSM/isc.ear/OMNIbusWebGUI.war	Contient les fichiers d'application Web Interface graphique Web.
REP_INSTALL_JazzSM/logs	Contient les fichiers journaux des applications.
REP_INSTALL_WAS/java/jre	Contient l'environnement d'exécution Java (JRE).
REP_INSTALL_WEBGUI	Contient les fichiers spécifiques à l'Interface graphique Web.
REP_INSTALL_WEBGUI/bin	Contient les scripts de l'Interface graphique Web.
REP_INSTALL_WEBGUI/integration/migration_tool	Contient les fichiers de l'utilitaire de migration de l'Interface graphique Web.
REP_INSTALL_WEBGUI/waapi	Contient les fichiers WAAPI.

Installation de l'interface graphique Web

Utilisez l'une de ces trois méthodes pour installer l'Interface graphique Web.

Installation de l'Interface graphique Web (interface graphique)

Installation du composant Interface graphique Web avec l'interface graphique Installation Manager.

Avant de commencer

- Obtenir un ID IBM et un droit de télécharger Tivoli Netcool/OMNIbus de IBM Passport Advantage. Les packages que vous êtes autorisé(e) à installer sont répertoriés dans Installation Manager.
- Déterminez le mode utilisateur d'Installation Manager dont vous avez besoin.
- Déterminez quelles fonctions des packages d'installation vous voulez installer et rassemblez les informations requises pour ces fonctions.
- Vérifiez que les droits d'accès utilisateur nécessaires sont en place pour vos répertoires d'installation prévus.
- Configurez `localhost` sur l'ordinateur où l'Interface graphique Web doit être installée.
- Si vous avez installé la version 8.1 bêta de Interface graphique Web vous devez sauvegarder et supprimer la version bêta avant d'installer la V8.1 complète de l'Interface graphique Web.
- Si vous installez l'Interface graphique Web dans un environnement Jazz for Service Management existant, sauvegardez la branche de répertoire *JazzSM_HOME* en cours pour le cas où vous souhaiteriez revenir à cette installation.

Pourquoi et quand exécuter cette tâche

Les étapes de démarrage d'Installation Manager diffèrent selon le mode utilisateur d'installation. Les étapes d'installation de l'Interface graphique Web avec l'assistant Installation Manager sont communes à tous les modes utilisateur et à tous tous les systèmes d'exploitation.

Windows Vous devez installer Interface graphique Web en tant qu'utilisateur administrateur.

UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.

Procédure

1. Accédez au sous-répertoire `/eclipse` du répertoire d'installation d'Installation Manager et utilisez la commande suivante pour démarrer Installation Manager :
   - UNIX Linux `./IBMIM`
   - Windows `IBMIM.exe`

   Pour enregistrer les étapes d'installation dans un fichier de réponses à utiliser avec des installations en mode silencieux, utilisez l'option `-record` *`fichier_réponses`*. Par exemple :

   ```
   IBMIM.exe -record C:\fichier_réponses\install_1.xml
   ```
2. Configurez Installation Manager pour télécharger les référentiels de packages depuis IBM Passport Advantage :
   a. Dans le menu principal, sélectionnez **Fichier** > **Préférences**.
   b. Vous pouvez définir des préférences pour les serveurs proxy dans IBM Installation Manager. Les serveurs proxy permettent d'établir des connexions à des serveurs distants derrière un pare-feu. Dans la fenêtre Préférences, développez le nœud **Internet** :

      Proxy FTP
      Sélectionnez cette option pour spécifier une adresse hôte et un numéro de port pour le proxy SOCKS.

      Proxy HTTP
      Sélectionnez cette option pour activer un serveur HTTP ou un proxy SOCKS.

      Sélectionnez **Enable proxy server**.
   c. Dans la fenêtre Préférences, sélectionnez le panneau **Passport Advantage**.
   d. Sélectionnez **Se connecter à Passport Advantage**, cliquez sur **Appliquer**, puis cliquez sur **OK**.
3. Dans la fenêtre principale d'Installation Manager, cliquez sur **Installer**. Suivez ensuite les instructions de l'assistant pour réaliser l'installation. Si vous y êtes invité, entrez votre ID utilisateur IBM et votre mot de passe. Les packages installables sont les suivants. Sélectionnez les packages dont vous avez besoin, en fonction de ce que vous souhaitez installer.

Package	Description
IBM WebSphere Application Server	Composant WebSphere Application Server sur lequel est basé Jazz for Service Management. Requis uniquement pour une nouvelle installation de Jazz for Service Management.

Package	Description
Jazz for Service Management extension for IBM WebSphere 8.5	Requis uniquement pour une nouvelle installation de Jazz for Service Management. **Remarque :** Vous devez sélectionner la version 8.5 de Jazz for Service Management extension for IBM WebSphere.
IBM Dashboard Application Services Hub	Requis uniquement pour une nouvelle installation de Jazz for Service Management.
IBMinterface graphique Web de Tivoli Netcool/OMNIbus	Contient l'Interface graphique Web. Si vous installez l'Interface graphique Web sur un produit Jazz for Service Management, existant, ce package est le seul dont vous avez besoin.
Environnement Reporting Services	Requis uniquement si vous avez besoin des fonctions de rapport incluses dans Jazz for Service Management.

Une fois que vous avez sélectionné les packages, l'assistant nécessite les entrées ci-après. Vous êtes invité à fournir certaines de ces informations.

- Lisez et acceptez le contrat de licence.
- Spécifiez un répertoire partagé pour Installation Manager ou acceptez le répertoire par défaut.
- Indiquez un répertoire d'installation pour le produit ou acceptez le répertoire par défaut.
- Sélectionnez les fonctions Interface graphique Web dont vous avez besoin :

  IBM interface graphique Web de Tivoli Netcool/OMNIbus
  interface graphique Web de Tivoli Netcool/OMNIbus et plugin Virtual Member Manager (VMM) pour Netcool ObjectServer sur IBM WebSphere Application Server (cette fonction est installée automatiquement).

  Installer les fonctions de base
  Installez les fonctions de base de l'interface graphique Web de Tivoli Netcool/OMNIbus avec déploiement sur le profil Jazz for Service Management.

  Installer des outils et des menus pour la recherche d'événements avec IBM SmartCloud Analytics - Log Analysis
  Installez les outils et menus de l'interface graphique Web de Tivoli Netcool/OMNIbus pour la recherche d'événements avec IBM SmartCloud Analytics - Log Analysis afin de disposer d'informations sur les événements Tivoli Netcool/OMNIbus.
- Entrez les informations nécessaires sur WebSphere Application Server, Jazz for Service Management, et les serveurs ObjectServer.

4. Une fois l'installation terminée, redémarrez l'ordinateur.

Résultats

Installation Manager installe l'Interface graphique Web.

Que faire ensuite

- Facultatif Pur configurer le produit, cliquez sur **Exécutez l'outil de configuration de l'interface graphique Web OMNIbus** et utilisez cet outil pour configurer les sources de données, créer des utilisateurs et des groupes, etc. Une

la configuration effectuée, le produit est prêt à l'emploi. Si vous n'utilisez pas l'outil, vous pouvez exécuter toutes les étapes de configuration séparément.

- Facultatif :Pur vous connecter à Concentrateur des services d'application du tableau de bord, cliquez sur **Connectez-vous à l'interface graphique Web OMNIbus**.

Tâches associées:

«Exécution des tâches post-installation», à la page 178
Après l'installation, un certain nombre de tâches de configuration (obligatoires ou facultatives) sont nécessaires pour terminer la configuration initiale de votre environnement de produit.

Installation de l'Interface graphique Web en mode console

L'utilisation du mode console pour l'installation de l'Interface graphique Web n'est possible que dans un environnement Jazz for Service Management existant. Jazz for Service Management et IBM WebSphere Application Server ne prennent pas en charge les installations en mode console. Pour une installation complète de l'Interface graphique Web et des composants Jazz for Service Management et IBM WebSphere Application Server sous-jacents, utilisez le mode interface graphique ou le mode silencieux.

Avant de commencer

- Obtenir un ID IBM et un droit de télécharger Tivoli Netcool/OMNIbus de IBM Passport Advantage. Les packages que vous êtes autorisé(e) à installer sont répertoriés dans Installation Manager.
- Téléchargez et installez Jazz for Service Management et IBM WebSphere Application Server. Ces composants peuvent aussi être installés en mode silencieux plutôt qu'en mode console. Voir http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.0/com.ibm.psc.doc_1.1.0/install/psc_c_install_silently_overview.html. Avant d'installer l'Interface graphique Web sur Jazz for Service Management, sauvegardez le répertoire *JazzSM_HOME*.
- Déterminez le mode utilisateur de l'Installation Manager dont vous avez besoin.
- Définissez les droits utilisateur nécessaires pour les répertoires d'installation prévus. Voir «Présentation d'IBM Installation Manager», à la page 32 ainsi que les informations sous «A propos de cette tâche».
- Déterminez quelles fonctions des packages d'installation vous allez installer et rassemblez les informations requises pour ces fonctions. Voir «Regroupement d'informations sur l'installation», à la page 147.
- Configurez `localhost` sur l'hôte.
- Supprimez toute version de test bêta de l'Interface graphique Web installée sur l'hôte.

Pourquoi et quand exécuter cette tâche

Les étapes de démarrage de Installation Manager différent selon le mode utilisateur appliqué pour son installation. Les étapes d'installation avec la console Installation Manager sont communes à tous les modes utilisateur et à tous les systèmes d'exploitation. Prenez bien note des informations qui suivent concernant les droits sur les systèmes d'exploitation pris en charge :

- UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`.

Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de 2 si la valeur résultante est 0.

- Windows Vous devez installer Tivoli Netcool/OMNIbus en tant qu'utilisateur administrateur.

Procédure

1. Accédez au sous-répertoire /eclipse/tools du répertoire d'installation d'Installation Manager.
2. Utilisez la commande suivante pour démarrer Installation Manager :
   - UNIX Linux ./imcl -c or ./imcl -consoleMode
   - Windows imcl.exe -c
3. Configurez Installation Manager pour télécharger les référentiels de packages depuis IBM Passport Advantage :
   a. Dans le menu principal, cliquez sur **Préférences** > **Passport Advantage** > **Se connecter à Passport Advantage**.
   b. Lorsque vous y êtes invité, entrez votre ID utilisateur et votre mot de passe IBM.
   c. Retournez au menu principal.
4. À partir des options disponibles dans le programme d'installation, ajoutez le référentiel que vous voulez installer.
5. Dans le menu principal, cliquez sur **Installer**. Suivez ensuite les instructions du programme d'installation pour terminer l'installation. Ce programme nécessite les entrées suivantes à différents stades de l'installation :
   - Sélectionnez Interface graphique Web.
   - Lorsque vous y êtes invité, indiquez un répertoire partagé Installation Manager ou acceptez le répertoire par défaut.
   - Lorsque vous êtes y invité, indiquez un répertoire d'installation ou acceptez le répertoire par défaut.
   - Générez un fichier de réponses à utiliser pour des installations en mode silencieux sur d'autres ordinateurs. Entrez le chemin du répertoire et un nom de fichier avec une extension .xml. Le fichier de réponses est généré avant que l'installation soit terminée.
6. Une fois l'installation terminée, cliquez sur **Terminer** puis redémarrez l'ordinateur.

Que faire ensuite

Exécutez les tâches de post-installation et configurez l'Interface graphique Web pour l'utilisation.

Tâches associées:

«Exécution des tâches post-installation», à la page 178
Après l'installation, un certain nombre de tâches de configuration (obligatoires ou facultatives) sont nécessaires pour terminer la configuration initiale de votre environnement de produit.

Installation de l'Interface graphique Web en mode silencieux

L'installation en mode silencieux nécessite un fichier de réponses qui définit la configuration de l'installation. Ce mode est utile si vous voulez avoir des configurations d'installation identiques sur plusieurs postes de travail.

Avant de commencer

- Définissez les droits utilisateur nécessaires pour les répertoires d'installation prévus. Voir «Présentation d'IBM Installation Manager», à la page 32 ainsi que les informations sous «A propos de cette tâche».
- Configurez `localhost` sur l'hôte.
- Supprimez toute version de test bêta de l'Interface graphique Web installée sur l'hôte.

Pourquoi et quand exécuter cette tâche

Les étapes de démarrage de Installation Manager différent selon le mode utilisateur appliqué pour son installation. Les étapes d'installation avec la console Installation Manager sont communes à tous les modes utilisateur et à tous les systèmes d'exploitation. Prenez bien note des informations qui suivent concernant les droits sur les systèmes d'exploitation pris en charge :

- UNIX Linux Installation Manager prend en compte vos paramètres umask en cours lorsqu'il définit le mode de droit d'accès des fichiers et répertoires qu'il installe. Si vous utilisez Mode administrateur ou Mode non-administrateur et umask est `0`, Installation Manager utilise un umask de `22`. Si vous utilisez Mode groupe, Installation Manager ignore les bits de groupe qui sont définis et utilise un umask de `2` si la valeur résultante est `0`.
- Windows Vous devez installer Tivoli Netcool/OMNIbus en tant qu'utilisateur administrateur.

La procédure à appliquer pour l'enregistrement d'un fichier de réponses silencieux va différer selon que vous voulez installer une nouvelle instance de Jazz for Service Management et WebSphere Application Server en tant que partie intégrante de l'installation de l'Interface graphique Web, ou que vous disposez déjà d'une instance de Jazz for Service Management dans laquelle l'Interface graphique Web sera installée.

- Dans le cas d'une instance existante de Jazz for Service Management, il vous faut un fichier de réponses silencieux pour les paramètres d'installation de l'Interface graphique Web uniquement. Un exemple de fichier de réponses est disponible dans le package d'installation à l'emplacement `cdimage/responsefiles/`*`plateforme`*`/OMNIbusWebGUI_install_response.xml`, où *plateforme* représente `unix` ou `windows`.
- Dans le cas d'une nouvelle installation de Jazz for Service Management, des paramètres de fichiers de réponses silencieux doivent être définis pour Jazz for Service Management et pour WebSphere Application Server. Selon votre environnement, vous aurez les options suivantes :
  - Enregistrez des fichiers de réponses silencieux pour Jazz for Service Management et pour WebSphere Application Server. Pour plus d'informations, voir http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.0.1/com.ibm.psc.doc_1.1.0.1/install/psc_c_install_silently_overview.html. Des exemples de fichiers de réponses sont fournis pour Jazz for Service Management et pour WebSphere Application Server.

– Exécutez une installation en mode interface de l'Interface graphique Web de telle sorte que les paramètres d'installation soient enregistrés sans installation du produit. Exemple :

```
IBMIM.exe -record C:\response_files\install_1.xml -skipInstall
 C:\Temp\skipInstall
```

Le fichier de réponses inclut l'emplacement du référentiel à partir duquel le package d'installation a été obtenu.

- Vous pouvez spécifier un référentiel local ou distant.
- Vous pouvez demander à ce que Installation Manager télécharge le package à partir de IBM Passport Advantage.

Procédure

1. Enregistrez le ou les fichier(s) de réponses.
2. Lisez le fichier de contrat de licence `license.txt` qui se trouve dans le package d'installation (`/native/license_version.zip`).
3. Pour chiffrer le mot de passe utilisé par l'administrateur pour la connexion initiale à Concentrateur des services d'application du tableau de bord, passez sur `/eclipse/tools` dans le répertoire d'installation de Installation Manager, puis entrez la commande suivante :
   - UNIX Linux `./imutilsc encryptString` *mot_passe*
   - Windows `imutilsc encryptString` *mot_passe*

   où *mot_passe* représente le mot de passe à chiffrer.
4. Pour démarrer l'installation en mode silencieux, entrez la commande suivante :
   - UNIX Linux `./imcl -input` *fichier_réponses* `-silent -acceptlicense [-log` *chemin_complet_vers_fichier_journal*`]`
   - Windows `imcl.exe -input` *fichier_réponses* `-silent -acceptlicense [-log` *chemin_complet_vers_fichier_journal*`]`

   Où *fichier_réponses* représente le chemin d'accès au répertoire du fichier de réponses enregistré à l'étape 1, et où *chemin_complet_vers_fichier_journal* représente l'emplacement de création du journal d'installation.

Tâches associées:

«Installation de l'Interface graphique Web (interface graphique)», à la page 151
Installation du composant Interface graphique Web avec l'interface graphique Installation Manager.

«Exécution des tâches post-installation», à la page 178
Après l'installation, un certain nombre de tâches de configuration (obligatoires ou facultatives) sont nécessaires pour terminer la configuration initiale de votre environnement de produit.

Information associée:

IBM Installation Manager : Stockage de données d'identification pour les installations en mode silencieux
Vous pouvez stocker des données d'identification pour les adresses URL qui requièrent une authentification, ce qui est le cas par exemple pour les référentiels, les serveurs proxy ou les fichiers de réponses. Ces fichiers de stockage sont utilisés lors de l'exécution de scripts d'installation en mode silencieux pour l'accès à des serveurs protégés par un mot de passe. Lorsque vous utilisez un fichier de stockage, une liste des adresses URL des référentiels et des serveurs proxy est nécessaire dans les préférences de votre fichier de réponses. Le fichier de stockage ne dispense pas de ces préférences.

Mise à niveau de l'Interface graphique Web et migration de données

Vous pouvez mettre à niveau vers la version 7.4 l'Interface graphique Web version 7.4, 7.3.1 ou 7.3. Vous pouvez également effectuer une mise à niveau à partir de IBM Tivoli Netcool/Webtop. Si vous effectuez une mise à niveau à partir de l'Netcool/Webtop, vous devez migrer les données vers la version 7.4 de l'Interface graphique Web.

Avant de commencer

Remarque :

1. Les noms de sources de données sur les systèmes source et cible doivent correspondre. Si les noms ne sont pas identiques, tous les fichiers de configuration contenant les informations de source de données doivent être modifiés manuellement pour utiliser la source de données appropriée.
2. Si vous avez fait des modifications au fichier de transformation ($TIP_HOME/tipv2/profiles/TIPProfile/installedApps/TIPCell/isc.ear/ISCWire.war/Transformations) dans Interface graphique Web version 7.4 groupe de correctifs 2, vous devez rétablir manuellement vos modifications après la migration vers la version 8.1.
3. Si vous avez installé la version 8.1 bêta de Interface graphique Web vous devez sauvegarder et supprimer la version bêta avant d'installer la V8.1 complète de l'Interface graphique Web.

Procédure

Le chemin de mise à niveau diffère selon la version de l'Interface graphique Web ou de l'Netcool/Webtop que vous souhaitez mettre à niveau. Si vous souhaitez effectuer une mise à niveau à partir de la version 7.3.1, le processus diffère selon la version de Concentrateur des services d'application du tableau de bord qui héberge l'installation de l'Interface graphique Web. Le tableau suivant décrit le chemin de mise à niveau pour la version de chaque produit et la version de Concentrateur des services d'application du tableau de bord.

Tableau 37. Chemins de mise à niveau à partir de versions différentes de l'Interface graphique Web et l'Netcool/Webtop, différenciés par la version de Concentrateur des services d'application du tableau de bord

Version du produit	Version de Tivoli Integrated Portal	Chemin de mise à niveau
7.4	2.2	Mise à niveau côte à côte uniquement. Installation propre de la version 8.1, suivie par la migration des données, laquelle se compose de : 1. Installation de la version 8.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.4.0. 2. Utilisation du programme **consolecli** pour exporter les données, les fichiers et les options de configuration de la version 7.4.0 et importation de ces éléments dans l'installation de la version 8.1.

Tableau 37. Chemins de mise à niveau à partir de versions différentes de l'Interface graphique Web et l'Netcool/Webtop, différenciés par la version de Concentrateur des services d'application du tableau de bord (suite)

Version du produit	Version de Tivoli Integrated Portal	Chemin de mise à niveau
7.3.1	2.2	Mise à niveau côte à côte uniquement. Installation propre de la version 8.1, suivie par la migration des données, laquelle se compose de : 1. Installation de la version 8.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.3.1. 2. Utilisation du programme **consolecli** pour exporter les données, les fichiers et les options de configuration de la version 7.3.1 et importation de ces éléments dans l'installation de la version 8.1.
7.3.1	2.1	Mise à niveau côte à côte uniquement. Installation propre de la version 8.1, suivie par la migration des données, laquelle se compose de : 1. Installation de la version 8.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.3.1. 2. Utilisation du programme **consolecli** pour exporter les données, les fichiers et les options de configuration de la version 7.3.1 et importation de ces éléments dans l'installation de la version 8.1.
7.3	1.1	Mettez à niveau Interface graphique Web à la version 7.4 ou 7.3.1, puis mettez à niveau à Interface graphique Web version 8.1, qui se compose de : 1. Installation de la version 7.4 ou 7.3.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.3. 2. Installation de la version 8.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.4 ou 7.3.1. 3. Utilisation du programme **consolecli** pour exporter les données, les fichiers et les options de configuration de la version 7.4 ou 7.3.1 et importation de ces éléments dans l'installation de la version 8.1.
Netcool/ Webtop V2.2	1.1	Mettez à niveau Interface graphique Web à la version 7.4 ou 7.3.1, puis mettez à niveau à Interface graphique Web version 8.1, qui se compose de : 1. Installation de la version 7.4 ou 7.3.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.3. 2. Installation de la version 8.1 de l'Interface graphique Web dans un emplacement différent de l'instance 7.4 ou 7.3.1. 3. Utilisation du programme **consolecli** pour exporter les données, les fichiers et les options de configuration de la version 7.4 ou 7.3.1 et importation de ces éléments dans l'installation de la version 8.1.
Netcool/ Webtop V2.1, V2.0 ou V1.3.1	Non disponible	1. Utilisation du programme de migration pour exporter les données, les fichiers et les options de configuration et importation de ces éléments dans l'installation de la version 7.4 ou 7.3.1. 2. Mise à niveau de l'Interface graphique Web vers la version 8.1.

Mise à niveau de la version 7.4.0 ou 7.3.1 sur Tivoli Integrated Portal version 2.2 ou 2.1

Si votre installation de la version 7.4.0 ou 7.3.1 de l'Interface graphique Web s'exécute sur une instance de Tivoli Integrated Portal version 2.2 ou 2.1, vous devez effectuer une mise à niveau côte-à-côte.

Avant de commencer

Vérifiez que tous les groupes de correctifs sont appliqués à la version 7.4.0 ou 7.3.1. Vérifiez que le module d'installation de l'interface graphique Web que vous utilisez pour effectuer la mise à niveau possède le nombre de bits requis. Par exemple, si vous souhaitez effectuer une mise à niveau à partir d'une installation 7.4.0 qui se trouve dans un environnement 64 bits, le module d'installation de l'interface graphique Web 64 bits est nécessaire. Si vous souhaitez effectuer une mise à niveau à partir d'une installation 7.4.0 qui se trouve dans un environnement 32 bits, vous devez utiliser le module d'installation 32 bits.

Pourquoi et quand exécuter cette tâche

Remarque : Cette procédure suppose que l'Interface graphique Web et Tivoli Integrated Portal sont installés dans leurs emplacements par défaut. Si votre installation utilise des emplacements différents pour un ou les deux composants, modifiez ces instructions en conséquence.

Procédure

Pour effectuer la mise à niveau côte-à-côte :

1. Vérifiez que vous avez appliqué tous les groupes de correctifs disponibles à l'Interface graphique Web et à Tivoli Integrated Portal.
2. Vérifiez que tous les utilisateurs sont déconnectés de l'Interface graphique Web.
3. Arrêtez le serveur.
4. Sauvegardez l'installation existante :
   - UNIX Linux Utilisez **tar** ou un outil d'archivage similaire à créer des copies de sauvegarde des répertoires suivants et de tous leurs sous-répertoires dans le fichier indiqué :

Tableau 38. Répertoires à sauvegarder sous UNIX et Linux

Répertoire	Nom du fichier de sauvegarde
opt/IBM/tivoli/netcoool/omnibus_webgui	webgui.tar
opt/IBM/tivoli/tipv2	tipv2.tar
opt/IBM/tivoli/tipv2Components	tipv2Components.tar

   - Windows Utilisez un utilitaire d'archivage approprié pour créer des fichiers `.zip` des dossiers suivants et de tous leurs sous-dossiers dans le fichier spécifié :

Tableau 39. Répertoires à sauvegarder sous Windows

Répertoire	Nom du fichier de sauvegarde
C:\IBM\tivoli\netcool\omnibus_webgui	webgui.zip
C:\IBM\tivoli\tipv2	tipv2.zip
C:\IBM\tivoli\tipv2Components	tipv2Components.zip

UNIX Linux Par exemple, la commande suivante sauvegarde le répertoire `omnibus_webgui`. Utilisez une commande similaire pour les autres répertoires.

```
tar cvf webgui.tar opt/IBM/tivoli/netcool/omnibus_webgui
```

5. Sauvegardez le moteur de déploiement (Deployment Engine (DE)) :
   - UNIX Linux Selon que le moteur de déploiement a été installé par l'utilisateur root ou l'utilisateur non-root, sauvegardez les répertoires suivants et tous leurs sous-répertoires dans le fichier spécifié.

Tableau 40. Répertoires DE à sauvegarder sous UNIX et Linux

Type d'installation	Répertoire	Nom du fichier de sauvegarde
root	`/usr/ibm/common/acsi`	`acsi.tar`
non-root	*`rép_principal_utilisateur`*`/.acsi_`*`nom_utilisateur`* Remplacez *rép_principal_utilisateur* par le répertoire de base de l'utilisateur non-root et *nom_utilisateur* par le nom de l'utilisateur non-root	`acsi_`*`nom_utilisateur`*`.tar` Remplacez *nom_utilisateur* par le nom d'utilisateur non-root.

   - Windows Utilisez un utilitaire d'archivage approprié pour créer des fichiers `.zip` du dossier suivant et de tous leurs sous-dossiers dans le fichier spécifié.

Tableau 41. Dossiers DE à sauvegarder sous Windows

Répertoire	Nom du fichier de sauvegarde
`C:\Program Files\IBM\Common\acsi`	`acsi.zip`

6. Copiez tous les fichiers `.tar` ou `.zip` dans un emplacement sécurisé.
7. Installez Interface graphique Web version 8.1 à un emplacement différent de l'instance version 7.4.0 ou 7.3.1.
8. Utilisez le programme **`tipcli`** pour exporter les données, les fichiers et les options de configuration de la version 7.4 ou 7.3.1.

Concepts associés:

«Exigences d'espace disque», à la page 29
Vérifiez que l'espace disque disponible est suffisant sur le volume pour le système d'exploitation sur lequel vous installez Tivoli Netcool/OMNIbus.

Tâches associées:

«Obtention du module d'installation», à la page 31
Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

«Installation de l'interface graphique Web», à la page 151
Utilisez l'une de ces trois méthodes pour installer l'Interface graphique Web.

Référence associée:

«Obtention de correctifs», à la page 682
Un correctif du produit peut être disponible pour résoudre les problèmes que vous rencontrez.

Exécution d'une installation propre et migration de données version 7.4.0 ou 7.3.1

Installez l'Interface graphique Web 8.1 dans une instance distincte de Concentrateur des services d'application du tableau de bord, puis copiez des données à partir de l'instance version 7.4.0 ou 7.3.1 à l'aide de l'outil de mise à niveau.

Procédure

La procédure de mise à niveau de l'Interface graphique Web vers la version 8.1 comprend les étapes suivantes :

1. Installez l'Interface graphique Web version 8.1.
2. Utilisez l'outil de mise à niveau pour exporter des données à partir de l'Interface graphique Web version 7.4.0 ou 7.3.1.
3. Copiez les données vers le serveur de l'Interface graphique Web version 8.1.
4. Importation des données.

Installation de l'Interface graphique Web version 8.1 :

Installez l'Interface graphique Web version 8.1. Lors de l'installation, une nouvelle instance de Concentrateur des services d'application du tableau de bord version est créée. Il est important que vous conserviez le même nom de source de données lors de l'installation Interface graphique Web version 8.1. Ceci est nécessaire afin que les données migrées importées de l'installation précédente correspondent à la source de données définie dans la version 8.1.

Avant de commencer

Veillez à effectuer une installation propre et vérifiez que tous les autres produits Concentrateur des services d'application du tableau de bord installés sur votre machine sont compatibles avec la version de Concentrateur des services d'application du tableau de bord que vous installez.

Concepts associés:

«Exigences d'espace disque», à la page 29
Vérifiez que l'espace disque disponible est suffisant sur le volume pour le système d'exploitation sur lequel vous installez Tivoli Netcool/OMNIbus.

Tâches associées:

«Obtention du module d'installation», à la page 31
Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

«Installation de l'interface graphique Web», à la page 151
Utilisez l'une de ces trois méthodes pour installer l'Interface graphique Web.

Exportation des données à partir de l'instance source de l'Interface graphique Web :

Pour exporter les données de l'instance de l'Interface graphique Web qui s'exécute sur Tivoli Integrated Portal V2.1, utilisez le programme **tipcli** fourni avec l'Interface graphique Web.

Dans ces étapes, l'instance de l'Interface graphique Web qui s'exécute sur Tivoli Integrated Portal version 2.2 ou 2.1 est appelée *serveur source*.

Procédure

1. Assurez-vous que le serveur source s'exécute et connectez-vous en tant qu'utilisateur d'administration de Tivoli Integrated Portal.
2. Si votre installation de Tivoli Integrated Portal ne comprend pas le serveur ESS, procédez comme suit :
   a. Dans l'instance d'Interface graphique Web version 7.4, copiez les fichiers `OMNIbusWebGUI_TIP_clone.properties` et `OMNIbusWebGUI_clone_settings.properties` les plus récents vers le répertoire *REP_INSTALL_WEBGUI*`/integration/upgrade/plugins` de l'Interface graphique Web version 7.4 ou 7.3.1.
   b. Accédez au répertoire *REP_INSTALL_WEBGUI*`/integration/upgrade/plugins` et éditez le fichier `OMNIbusWebGUI_TIP_clone.properties`.
   c. Recherchez la ligne suivante et insérez un marqueur de commentaire (#) au début de la ligne.
      ```
      components=ESSServer
      ```
   d. Enregistrez le fichier et quittez l'éditeur de texte.

   Le serveur ESS est un composant facultatif de Tivoli Integrated Portal utilisé par la version existante de l'Interface graphique Web ou de Netcool/Webtop.
3. Si l'Interface graphique Web source n'est pas installée dans l'emplacement par défaut, procédez comme suit. L'emplacement d'installation par défaut est `ibm/tivoli/netcool/omnibus_webgui` sur les systèmes d'exploitation UNIX et `C:\IBM\tivoli\netcool\omnibus_webgui` sur les systèmes d'exploitation Windows.
   a. Dans le répertoire *REP_INSTALL_WEBGUI*`/integration/upgrade/plugins`, éditez le fichier `OMNIbusWebGUI_clone_settings.properties`.
   b. Recherchez la ligne ci-après :
      ```
      TIP.Cellname=TIPCell
      ```
   c. Immédiatement après cette ligne, ajoutez la ligne suivante :
      ```
      product.home=REP_INSTALL_WEBGUI
      ```

      Où *REP_INSTALL_WEBGUI* est le répertoire d'installation réel de l'Interface graphique Web.
   d. Enregistrez le fichier et quittez l'éditeur de texte.
4. Accédez au répertoire *rép_principal_tip*`/profiles/TIPProfile/bin` et exécutez la commande export pour votre système d'exploitation :
   - UNIX Linux `./tipcli.sh Export --username` *admin_tip* `--password` *mot_de_passe_tip* `--settingFile` *REP_INSTALL_WEBGUI*`/integration/plugins/OMNIbusWebGUI_TIP_clone.properties`
   - Windows `tipcli.bat Export --username tipadmin --password tippass --settingFile webgui-home\integration\plugins\OMNIbusWebGUI_TIP_clone.properties`

Où *administrateur_tip* est le nom d'utilisateur d'administration Concentrateur des services d'application du tableau de bord et *mot_de_passe_tip* est le mot de passe associé.

Résultats

L'utilitaire **tipcli** crée les fichiers suivants sur le serveur source :

- Fichier de données dans `data.zip`, dans le *rép_principal_tip*`/profiles/TIPProfile/output`.
- Fichier journal dans *rép_principal_tip*`/profiles/TIPProfile/logs/tipcli.log`.

Copie des données :

Faites une copie du fichier `data.zip` qui a été créé sur le serveur de l'Interface graphique Web source par la commande d'exportation **consolecli**. Ensuite, connectez-vous au serveur cible et placez le fichier `data.zip` dans un répertoire d'importation, le répertoire par défaut est *REP_INSTALL_JazzSM*`/ui/input`.

Importation des données :

Copiez le fichier `data.zip` du serveur source vers le répertoire *REP_INSTALL_JazzSM*`/ui/input` du serveur cible.

Procédure

1. Assurez-vous que le serveur cible est en cours d'exécution et connectez-vous en tant qu'utilisateur d'administration de Concentrateur des services d'application du tableau de bord.
2. Le cas échéant, modifiez le niveau de journalisation. Par défaut, l'utilitaire **consolecli** écrit des messages d'information, d'avertissement et d'erreur dans le fichier journal.
3. Si votre installation de Concentrateur des services d'application du tableau de bord ne comprend pas le serveur ESS, procédez comme suit :
   a. Accédez au répertoire *REP_INSTALL_WEBGUI*`/integration/plugins` et éditez le fichier `OMNIbusWebGUI_DASH_clone.properties`.
   b. Recherchez la ligne suivante et insérez un marqueur de commentaire (#) au début de la ligne.
      ```
      components=ESSServer
      ```
   c. Enregistrez le fichier et quittez l'éditeur de texte.

   Le serveur ESS est un composant facultatif de Concentrateur des services d'application du tableau de bord utilisé par la version existante de l'Interface graphique Web ou de Netcool/Webtop.
4. Si l'instance de l'Interface graphique Web n'est pas installée dans l'emplacement par défaut, procédez comme suit. L'emplacement d'installation par défaut est `ibm/tivoli/netcool/omnibus_webgui` sur les systèmes d'exploitation UNIX et `C:\IBM\tivoli\netcool\omnibus_webgui` sur les systèmes d'exploitation Windows.
   a. Dans le répertoire *REP_INSTALL_WEBGUI*`/integration/plugins`, éditez le fichier `OMNIbusWebGUI_clone_settings.properties`.
   b. Recherchez la ligne ci-après :
      ```
      JazzSM.cell.name=
      ```
   c. Immédiatement après cette ligne, ajoutez la ligne suivante :
      ```
      product.home=REP_INSTALL_WEBGUI
      ```

Où *REP_INSTALL_WEBGUI* est le répertoire d'installation réel de l'Interface graphique Web.

d. Enregistrez le fichier et quittez l'éditeur de texte.

5. Accédez au répertoire contenant l'utilitaire *REP_INSTALL_JazzSM*/ui/bin et exécutez la commande import pour votre système d'exploitation :

   - UNIX Linux `./consolecli.sh Import --username smadmin --password mot_de_passe --settingFile REP_INSTALL_WEBGUI/integration/plugins/OMNIbusWebGUI_DASH_clone.properties`
   - Windows `consolecli.bat Import --username smadmin --password mot_de_passe --settingFile webgui-home\integration\plugins\OMNIbusWebGUI_DASH_clone.properties`

   Où *smadmin* est le nom d'utilisateur d'administration Concentrateur des services d'application du tableau de bord et *mot_de_passe* est le mot de passe associé.

   Remarque : Incluez l'option --importFile <*import directory*>/data.zip dans les lignes de commande, si vous n'utilisez pas le répertoire d'importation par défaut.

6. Vérifiez que l'utilitaire a ajouté ou mis à jour les fichiers correctement :

   a. Consultez le fichier journal *REP_INSTALL_JazzSM*/ui/logs/consolecli.log et vérifiez qu'aucune erreur ne s'est produite.

   b. Vérifiez que les copies de sauvegarde des fichiers d'origine sur le serveur de l'Interface graphique Web version 7.4 se trouvent dans un fichier .zip dans *REP_INSTALL_JazzSM*/ui/backups.

7. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.

   Important : Si le serveur fait partie d'un cluster d'équilibrage de charges, attendez jusqu'à ce que s'achève la prochaine planification de tâche temporisée avant de redémarrer le serveur. De la sorte, les données importées seront répliquées vers d'autres noeuds du cluster et de la base de données.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Référence associée:

«Référence ncwDataSourceDefinitions.xml», à la page 565
Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration ncwDataSourceDefinitions.xml se trouvant dans *REP_INSTALL_WEBGUI*/etc/datasources. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

Migration de l'Interface graphique Web dans un environnement de cluster (configuration de l'équilibrage de charge) :

Suivez ces procédures lors de la migration d'une Interface graphique Web dans un cluster.

Avant de commencer

Pour éviter la perte d'informations en cas de catastrophe, et de reprise après sinistre, sauvegardez votre installation de l'interface graphique Web et Concentrateur des services d'application du tableau de bord avant d'effectuer l'importation.

Procédure

- Migration de l'Interface graphique Web (exportation / importation) pour l'Interface graphique Web dans un environnement de cluster (configuration de l'équilibrage de charge) vers un serveur autonome.
  1. Effectuez l'exportation (système source) d'un noeud dans un environnement de cluster.
  2. Effectuez l'importation (système cible).
  3. Modifiez le fichier suivant :
     WEBGUI_HOME/etc/server.init

     Localisez la propriété `cluster.mode` et définissez-la par la valeur `cluster.mode:off`.
  4. Sauvegardez le fichier.
  5. Redémarrez le serveur.
- Migration de l'Interface graphique Web (exportation / importation) pour l'Interface graphique Web dans un environnement de cluster (configuration de l'équilibrage de charge) vers un noeud dans un environnement de cluster.
  1. Effectuez l'exportation (système source) d'un noeud dans un environnement de cluster.
  2. Détachez le serveur du cluster (système cible).
  3. Effectuez l'importation (système cible).
  4. Reconnectez le cluster.

Tâches associées:

«Importation des données», à la page 164
Copiez le fichier `data.zip` du serveur source vers le répertoire *REP_INSTALL_JazzSM*/ui/input du serveur cible.

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Mise à niveau à partir d'IBM Tivoli Netcool/Webtop version 2.2 ou de l'Interface graphique Web version 7.3.0

Pour mettre à niveau Netcool/Webtop version 2.2 ou l'Interface graphique Web version 7.3.0 vers l'Interface graphique Web version 8.1, mettez à niveau l'interface utilisateur Web vers la version 7.4, puis mettez à niveau vers l'Interface graphique Web version 8.1.

Tâches associées:

«Obtention du module d'installation», à la page 31
Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145
Cette rubrique présente comment installer, mettre à niveau et désinstaller le composant Interface graphique Web. Les processus d'installation, de mise à niveau et de désinstallation sont identiques pour tous les systèmes d'exploitation.

Migration à partir de IBM Tivoli Netcool/Webtop version 2.0 ou 2.1

Utilisez le programme de migration pour exporter les données, les fichiers et les options de configuration et importer ces éléments dans l'installation de la version 7.4. Lorsque ce processus est terminé, vous mettez à niveau l'interface graphique Web vers la version 8.1. Pour plus d'informations, voir *Exécution d'une installation propre et migration de données version 7.4.0 ou 7.3.1*. Pour migrer vos données Netcool/Webtop version 2.0 ou 2.1 existantes vers l'Interface graphique Web version 7.4, exécutez les scripts du module d'exportation de l'outil de migration sur les serveurs sur lesquels IBM Tivoli Netcool Security Manager et Netcool GUI Foundation sont installés. Importez ensuite les données de migration dans l'Interface graphique Web.

Avant de commencer

Installez l'Interface graphique Web version 7.4 de Tivoli Netcool/OMNIbus. Une fois l'installation de l'Interface graphique Web effectuée, l'outil de migration se trouve dans *REP_INSTALL_WEBGUI*`/integration/migration_tool/migration_tool_export.zip`.

Pourquoi et quand exécuter cette tâche

Procédure

La procédure de migration de Netcool/Webtop vers l'Interface graphique Web comprend les étapes suivantes :

1. Installation de l'outil de migration.
2. Exportation des données depuis le serveur Netcool/Webtop.
3. Copie des données vers le serveur de l'Interface graphique Web.
4. Configuration du module d'importation.
5. Importation des données.
6. Suppression de l'outil de migration.

Tâches associées:

Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145
Cette rubrique présente comment installer, mettre à niveau et désinstaller le composant Interface graphique Web. Les processus d'installation, de mise à niveau et de désinstallation sont identiques pour tous les systèmes d'exploitation.

Installation de l'outil de migration

Procédure

1. Sur le serveur de l'Interface graphique Web, copiez le fichier *REP_INSTALL_WEBGUI*/integration/migration_tool/migration_tool_export.zip vers le serveur de l'Netcool/Webtop.

   Si les composants Netcool Security Manager et Netcool GUI Foundation sont installés sur des serveurs différents, vous devez copier le fichier migration_tool_export.zip vers chacun de ces serveurs.
2. Sur chaque serveur Webtop, extrayez le fichier migration_tool_export.zip vers un répertoire adapté.

   Ce répertoire est nommé *REP_BASE_OUTIL_MIGRATION*.

Exportation des données

Avant de commencer

Vérifiez que les noms de tous les rôles utilisateur contiennent uniquement des lettres, des nombres et le caractère de soulignement. Veillez en particulier à ce que les noms de rôle ne contiennent pas le signe moins (-).

Procédure

Sur le serveur IBM Tivoli Netcool/Webtop :

1. Connectez-vous au serveur sur lequel Netcool Security Manager est installé en tant qu'administrateur.
2. Définissez *NCHOME* sur le répertoire d'installation de Netcool Security Manager.
3. Entrez :

   MIGRATION_TOOL_HOME/bin/sm_migration_export Les données utilisateur sont exportées dans le fichier nommé SecurityMigration.xml dans *MIGRATION_TOOL_HOME*/output/SecurityManager.xml
4. Facultatif : S'il y a un problème avec les noms des rôles, le script **sm_migration_export** peut échouer. Le cas échéant, allez dans *REP_INSTALL_OUTIL_MIGRATION*/etc et ouvrez le fichier rolesRenaming.properties pour y définir les mappages de rôles. Répétez ensuite l'étape 3.
5. Si Netcool GUI Foundation se situe sur un serveur distinct, paramétrez *NCHOME* de ce serveur sur le répertoire d'installation Netcool GUI Foundation.
6. Modifiez settings.properties dans *MIGRATION_TOOL_HOME*/etc et définissez les valeurs suivantes :

Tableau 42. Paramètres de l'outil de migration pour exportation des données Netcool GUI Foundation

Propriété	Valeur
NGF.Server.URL	Adresse URL de Netcool GUI Foundation.

Tableau 42. Paramètres de l'outil de migration pour exportation des données Netcool GUI Foundation (suite)

Propriété	Valeur
NGF.Admin.user	ID utilisateur de l'administrateur Netcool GUI Foundation.
NGF.Admin.password	Mot de passe de l'administrateur Netcool GUI Foundation.

7. Si l'interface WAAPI de l'Interface graphique Web n'est pas installée, éditez `export.lst` dans le même répertoire et mettez en commentaire la ligne suivante :

   ```
   com.ibm.tivoli.nc.migration.plugin.webtop.WAAPIInit2xExportPlugin
   ```

8. Accédez à *REP_INSTALL_OUTIL_MIGRATION*`/bin` et entrez `migration_export`. Les données sont exportées dans le fichier nommé `data.zip` dans *REP_INSTALL_OUTIL_MIGRATION*`/output`

Copie de données sur le serveur de l'interface graphique Web

Procédure

Copiez `SecurityMigration.xml` et `data.zip` sur le serveur de l'Interface graphique Web.

- Déposez `SecurityMigration.xml` dans *REP_INSTALL_WEBGUI*`/integration/migration_tool/output/SecurityManager`.
- Déposez `data.zip` dans *REP_INSTALL_WEBGUI*`/integration/migration_tool/output`.

Configuration du module d'importation

Pourquoi et quand exécuter cette tâche

Dans cette tâche, *MIGRATION_TOOL_HOME* fait référence à *REP_INSTALL_WEBGUI*`/integration/migration_tool`

Procédure

Sur le serveur de l'Interface graphique Web :

1. Définissez les variables suivantes :

Tableau 43. Variables d'environnement pour l'importation des données

Variable	Valeur
PROD_HOME	Répertoire d'installation de l'Interface graphique Web de Tivoli Netcool/OMNIbus version 8.1.0.

2. Modifiez `settings.properties` dans *MIGRATION_TOOL_HOME*`/etc` et définissez les valeurs suivantes :

Tableau 44. Paramètres de l'outil de migration pour importation des données

Propriété	Valeur
TIP.WSAdmin.user	Administrateur Concentrateur des services d'application du tableau de bord, tel que smadmin.

Tableau 44. Paramètres de l'outil de migration pour importation des données (suite)

Propriété	Valeur
TIP.WSAdmin.password	Mot de passe de l'administrateur Concentrateur des services d'application du tableau de bord, tel que smadmin.
Importer.Destination.Choice	Registre dans lequel Netcool Security Manager est importé. utilisez l'une des valeurs suivantes : **FBAUTH** Importe les données dans le référentiel basé sur fichier Concentrateur des services d'application du tableau de bord par défaut. **NCOS** Importe les données dans ObjectServer. Les utilisateurs sont créés automatiquement dans ObjectServer. **NONE** N'importe pas les données. **LDAP** Importe les données dans le registre LDAP. Les données utilisateur sont importées dans un fichier `.ldiff`, que vous devez ensuite dans LDAP.
Définissez les propriétés suivantes si la valeur de **Importer.Destination.Choice** est `NCOS` :	
Importer.NCOS.Server	Nom du serveur exécutant ObjectServer.
Importer.NCOS.Port	Numéro de port utilisé par ObjectServer.
Importer.NCOS.Admin	Superutilisateur ObjectServer.
Importer.NCOS.Password	Mot de passe du superutilisateur ObjectServer.
Importer.NCOS.defaultPassword	Mot de passe par défaut de l'Interface graphique Web à générer pour tous les utilisateurs importés.
Définissez les propriétés suivantes si la valeur de **Importer.Destination.Choice** est `FBAuth` :	
Importer.FBAUTH.defaultPassword	Mot de passe par défaut de l'Interface graphique Web à générer pour tous les utilisateurs importés.
Importer.FBAUTH.DefaultWIMRealm	Ne modifiez pas cette propriété.
Définissez la propriété suivante si la valeur de **Importer.Destination.Choice** est `LDAP` :	
Importer.LDAP.BaseDn	Nom distinctif du serveur LDAP.

3. Si WAAPI n'est pas installé sur le serveur Netcool/Webtop, modifiez `import.lst` dans *MIGRATION_TOOL_HOME*`/etc` et mettez en commentaire la ligne suivante :

   ```
   com.ibm.tivoli.nc.migration.plugin.webtop.WAAPIInitImportPlugin
   ```

Importation des données

Pourquoi et quand exécuter cette tâche

Dans cette tâche, *MIGRATION_TOOL_HOME* fait référence à *REP_INSTALL_WEBGUI*/integration/migration_tool

Procédure

Sur le serveur de l'Interface graphique Web :

1. Vérifiez que l'Interface graphique Web et le serveur Concentrateur des services d'application du tableau de bord sont en cours d'exécution.
2. Consultez le fichier *REP_INSTALL_WEBGUI*/etc/illegalChar.prop et vérifiez qu'il est approprié pour votre installation.

   Pour la plupart des installations, il suffit de supprimer le caractère d'espace de la liste des caractères non autorisés.
3. Accédez au répertoire *MIGRATION_TOOL_HOME*/bin et entrez :

   ```
   migration_import -migration
   ```
4. Si vous définissez la propriété **Importer.Destination.Choice** de settings.properties dans le protocole LDAP, importez le fichier generatedUsersAndGroups.ldif dans le serveur LDAP.

   Reportez-vous à la documentation de votre serveur LDAP pour les instructions relatives à l'importation d'un fichier .ldif.
5. Pour importer les utilisateurs et les groupes de Netcool/Webtop, accédez au répertoire *REP_INSTALL_OUTIL_MIGRATION*/import/roles. Exécutez la commande suivante correspondant à votre système d'exploitation :

   - UNIX Linux `addAllRolesAndRelationships` *REP_INSTALL_TIP administrateur_tip mot_de_passe_tip*
   - Windows `addAllRolesAndRelationships "`*REP_INSTALL_TIP*`"` *administrateur_tip mot_de_passe_tip*

   Remplacez *REP_INSTALL_TIP* par le répertoire d'installation de Concentrateur des services d'application du tableau de bord, *administrateur_tip* par l'ID utilisateur de l'administrateur Concentrateur des services d'application du tableau de bord et *mot_de_passe_tip* par le mot de passe de cet utilisateur.
6. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Résultats

Après avoir redémarré le serveur, les utilisateurs et les groupes migrés depuis Netcool Security Manager ainsi que les pages migrées depuis Netcool GUI Foundation sont visibles. Les utilisateurs ont les mêmes rôles que dans Netcool Security Manager.

Que faire ensuite

Pour obtenir l'ensemble des artefacts de configuration par défaut de l'Interface graphique Web version 7.4, fusionnez les fichiers contenus dans le dossier *REP_INSTALL_WEBGUI*/etc/default avec les artefacts de configuration qui ont été migrés depuis Netcool/Webtop. Par exemple, pour obtenir les filtres globaux par défaut, fusionnez le fichier *REP_INSTALL_WEBGUI*/etc/default/data/global/filter.xml avec le fichier *REP_INSTALL_WEBGUI*/etc/data/global/filter.xml.

Suppression de l'outil de migration
Procédure

Une fois que la migration aboutit, supprimez le fichier `settings.properties` qui contient les informations de connexion et de mot de passe. Vous pouvez également supprimer l'outil de migration de tous les hôtes.

Réexécution de l'outil de migration
Procédure

Si nécessaire, vous pouvez réexécuter l'outil de migration. Avant de pouvoir réexécuter l'outil, vous devez supprimer les fichiers et répertoires suivants :

1. Annulez la migration sur le serveur de l'Interface graphique Web.
2. Supprimez les fichiers et répertoires suivants :
   a. Sur le serveur Netcool Security Manager, vous supprimez le répertoire *MIGRATION_TOOL_HOME*`/output/SecurityManager` pour pouvoir réexécuter la commande **`sm_migration_export`**.
   b. Sur le serveur de l'Netcool GUI Foundation, vous supprimez le fichier *MIGRATION_TOOL_HOME*`/output` pour pouvoir réexécuter la commande **`migration_export`**.
   c. Sur le serveur de l'Interface graphique Web, vous supprimez le fichier *MIGRATION_TOOL_HOME*`/output` pour pouvoir réexécuter la commande **`migration_import`**. Supprimez également le fichier `migratedRoles.war` avant de réexécuter le script `addAllRolesAndRelationships`.

Migration à partir de IBM Tivoli Netcool/Webtop version 1.3.1

Utilisez le programme de migration pour exporter les données, les fichiers et les options de configuration et importer ces éléments dans l'installation de la version 7.4 ou 7.3.1. Lorsque ce processus est terminé, vous mettez à niveau l'interface graphique Web vers la version 8.1. Pour migrer les données de Netcool/Webtop version 1.3.1 vers l'Interface graphique Web V7.4, exécutez le module d'exportation de l'outil de migration sur l'hôte sur lequel Netcool/Webtop version 1.3.1 est installé. Vous importez ensuite les données de migration dans l'Interface graphique Web Tivoli Netcool/OMNIbus version 7.4.

Avant de commencer

Installez l'Interface graphique Web version 7.4.

Pourquoi et quand exécuter cette tâche

Procédure

La procédure de migration de Netcool/Webtop version 1.3.1 vers l'Interface graphique Web comprend les étapes suivantes :

1. Installation de l'outil de migration.
2. Exportation des données à partir du serveur Netcool/Webtop.
3. Copie des données vers le serveur de l'Interface graphique Web.
4. Configuration du module d'importation.
5. Importation des données.
6. Suppression de l'outil de migration.

Tâches associées:

Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145
Cette rubrique présente comment installer, mettre à niveau et désinstaller le composant Interface graphique Web. Les processus d'installation, de mise à niveau et de désinstallation sont identiques pour tous les systèmes d'exploitation.

Installation de l'outil de migration

Procédure

1. Sur l'hôte de l'Interface graphique Web, copiez le fichier *REP_INSTALL_WEBGUI*/integration/migration_tool/migration_tool_export.zip vers l'hôte de Netcool/Webtop.
2. Extrayez le fichier migration_tool_export.zip vers un répertoire adapté.

   Ce répertoire est nommé *MIGRATION_TOOL_HOME*.

Exportation des données

Procédure

1. En tant qu'administrateur, connectez-vous au serveur sur lequel Netcool/Webtop est installé en tant qu'administrateur.
2. Définissez *WEBTOP_HOME* sur le répertoire d'installation de Netcool/Webtop.
3. Si WAAPI n'est pas installé, modifiez export.lst dans *MIGRATION_TOOL_HOME*/etc et mettez en commentaire la ligne suivante :

   com.ibm.tivoli.nc.migration.plugin.webtop.WAAPIInit13ExportPlugin
4. Accédez à *MIGRATION_TOOL_HOME*/bin et entrez :

   UNIX Linux webtop13_migration_export

   Windows webtop13_migration_export.cmd

   Les données sont exportées dans le fichier nommé data.zip dans *MIGRATION_TOOL_HOME*/output

Copie de données sur le serveur de l'interface graphique Web

Procédure

Copiez data.zip sur le serveur de l'Interface graphique Web.
Déposez le fichier dans *REP_INSTALL_WEBGUI*/integration/migration_tool/output.

Configuration du module d'importation

Pourquoi et quand exécuter cette tâche

Dans cette tâche, *MIGRATION_TOOL_HOME* fait référence à *REP_INSTALL_WEBGUI*/integration/migration_tool.

Procédure

Sur le serveur de l'Interface graphique Web :

1. Définissez les variables suivantes :

Tableau 45. Variables d'environnement pour l'importation des données

Variable	Valeur
TIPHOME	Répertoire d'installation de Concentrateur des services d'application du tableau de bord.

Tableau 45. Variables d'environnement pour l'importation des données (suite)

Variable	Valeur
WEBTOP_HOME	Répertoire d'installation de l'Interface graphique Web de Tivoli Netcool/OMNIbus V7.4.0

2. Modifiez `settings.properties` dans *`MIGRATION_TOOL_HOME`*`/etc` et définissez les valeurs suivantes :

Tableau 46. Paramètres de l'outil de migration pour importation des données

Propriété	Valeur
`TIP.WSAdmin.user`	Administrateur Concentrateur des services d'application du tableau de bord, tel que tipadmin.
`TIP.WSAdmin.password`	Mot de passe de l'administrateur Concentrateur des services d'application du tableau de bord, tel que tippass.
`Importer.Destination.Choice`	Registre dans lequel Netcool Security Manager est importé. utilisez l'une des valeurs suivantes : **`FBAUTH`** Importe les données dans le référentiel basé sur fichier Concentrateur des services d'application du tableau de bord par défaut. **`NCOS`** Importe les données dans ObjectServer. Les utilisateurs sont créés automatiquement dans ObjectServer. **`NONE`** N'importe pas les données. **`LDAP`** Importe les données dans le registre LDAP. Les données utilisateur sont importées dans un fichier `.ldiff`, que vous devez ensuite dans LDAP.
Définissez les propriétés suivantes si la valeur de **`Importer.Destination.Choice`** est `NCOS` :	
`Importer.NCOS.Server`	Nom du serveur exécutant ObjectServer.
`Importer.NCOS.Port`	Numéro de port utilisé par ObjectServer.
`Importer.NCOS.Admin`	Superutilisateur ObjectServer.
`Importer.NCOS.Password`	Mot de passe du superutilisateur ObjectServer.
`Importer.NCOS.defaultPassword`	Mot de passe par défaut de l'Interface graphique Web à générer pour tous les utilisateurs importés.
Définissez les propriétés suivantes si la valeur de **`Importer.Destination.Choice`** est `FBAuth` :	
`Importer.FBAUTH.defaultPassword`	Mot de passe par défaut de l'Interface graphique Web à générer pour tous les utilisateurs importés.
`Importer.FBAUTH.DefaultWIMRealm`	Ne modifiez pas cette propriété.

Tableau 46. Paramètres de l'outil de migration pour importation des données (suite)

Propriété	Valeur
Définissez la propriété suivante si la valeur de **Importer.Destination.Choice** est LDAP :	
Importer.LDAP.BaseDn	Nom distinctif du serveur LDAP.

3. Si WAAPI n'est pas installé sur le serveur Netcool/Webtop, modifiez `import.lst` dans *MIGRATION_TOOL_HOME*`/etc` et mettez en commentaire la ligne suivante :

   `com.ibm.tivoli.nc.migration.plugin.webtop.WAAPIInitImportPlugin`

Importation des données

Pourquoi et quand exécuter cette tâche

Dans cette tâche, *MIGRATION_TOOL_HOME* fait référence à *REP_INSTALL_WEBGUI*`/integration/migration_tool`

Procédure

Sur le serveur de l'Interface graphique Web :

1. Vérifiez que l'Interface graphique Web et le serveur Concentrateur des services d'application du tableau de bord sont en cours d'exécution.
2. Consultez le fichier *REP_INSTALL_WEBGUI*`/etc/illegalChar.prop` et vérifiez qu'il est approprié pour votre installation.

   Pour la plupart des installations, il suffit de supprimer le caractère d'espace de la liste des caractères non autorisés.
3. Accédez au répertoire *MIGRATION_TOOL_HOME*`/bin` et exécutez la commande suivante correspondant à votre système d'exploitation :

   UNIX Linux `webtop13_migration_import -migration`

   Windows `webtop13_migration_import.cmd -migration`
4. Si vous définissez la propriété **Importer.Destination.Choice** de `settings.properties` dans le protocole LDAP, importez le fichier `generatedUsersAndGroups.ldif` dans le serveur LDAP.

   Reportez-vous à la documentation de votre serveur LDAP pour les instructions relatives à l'importation d'un fichier `.ldif`.
5. Pour importer les utilisateurs et les groupes de Netcool/Webtop, accédez au répertoire *REP_INSTALL_OUTIL_MIGRATION*`/import/roles` et exécutez la commande suivante correspondant à votre système d'exploitation :

   - UNIX Linux `addAllRolesAndRelationships.sh` *REP_INSTALL_TIP admintip mdptip*
   - Windows `addAllRolesAndRelationships.bat "`*REP_INSTALL_TIP*`"` *admintip mdptip*

   Remplacez *REP_INSTALL_TIP* par le répertoire d'installation de Concentrateur des services d'application du tableau de bord. Remplacez *admintip* par l'ID utilisateur de l'administrateur Concentrateur des services d'application du tableau de bord et remplacez *mdptip* par le mot de passe de cet utilisateur.
6. Redémarrez l'Interface graphique Web et le serveur Concentrateur des services d'application du tableau de bord

Résultats

Après avoir redémarré le serveur, les données de configuration migrées depuis Netcool/Webtop sont mises en place avec les utilisateurs migrés.

Que faire ensuite

Pour obtenir l'ensemble des artefacts de configuration par défaut de l'Interface graphique Web version 7.4, fusionnez les fichiers contenus dans le dossier *REP_INSTALL_WEBGUI*/etc/default avec les artefacts de configuration qui ont été migrés depuis Netcool/Webtop. Par exemple, pour obtenir les filtres globaux par défaut, fusionnez le fichier *REP_INSTALL_WEBGUI*/etc/default/data/global/filter.xml avec le fichier *REP_INSTALL_WEBGUI*/etc/data/global/filter.xml.

Suppression de l'outil de migration

Procédure

Une fois que la migration aboutit, supprimez le fichier settings.properties qui contient les informations de connexion et de mot de passe. Vous pouvez également supprimer l'outil de migration de tous les hôtes.

Réexécution de l'outil de migration

Procédure

Si nécessaire, vous pouvez réexécuter l'outil de migration. Avant de pouvoir réexécuter l'outil :

1. Annulez la migration sur le serveur de l'Interface graphique Web.
2. Supprimez les fichiers et répertoires suivants :
   a. Sur le serveur Netcool/Webtop, vous devez supprimer le répertoire *MIGRATION_TOOL_HOME*/output pour pouvoir réexécuter la commande **webtop13_migration_export**.
   b. Sur le serveur de l'Interface graphique Web, vous devez supprimer le fichier *REP_BASE_OUTIL_MIGRATION*/output avant de pouvoir réexécuter la commande **migration_import**. Vous devez également supprimer le fichier migratedRoles.war avant de réexécuter le script **addAllRolesAndRelationships**.

Sauvegarde d'une installation V8.1

Pour empêcher la perte d'informations au cours de l'installation, de la mise à niveau, de l'application d'un groupe de correctifs ou en cas d'incident, et pour pouvoir récupérer ces informations, sauvegardez votre installation de l'Interface graphique Web.

Avant de commencer

Assurez-vous que vous êtes connecté en tant qu'utilisateur d'administration.

Procédure

- UNIX Linux Procédez de la manière suivante :
  1. Arrêtez le serveur Concentrateur des services d'application du tableau de bord.
  2. Utilisez un utilitaire d'archivage approprié pour compresser le contenu des fichiers suivants, et effectuez une copie à un emplacement sécurisé :

- opt/IBM/netcoool/omnibus_webgui
- opt/IBM/JazzSM
- opt/IBM/WebSphere/AppServer

3. Lancez le serveur Concentrateur des services d'application du tableau de bord.

- Windows Procédez de la manière suivante :
  1. Arrêtez le serveur Concentrateur des services d'application du tableau de bord.
  2. Utilisez un utilitaire d'archivage approprié pour compresser le contenu des fichiers suivants, et effectuez une copie à un emplacement sécurisé :
     - C:\IBM\netcool\omnibus_webgui
     - C:\IBM\JazzSM
     - C:\IBM\WebSphere\AppServer
  3. Lancez le serveur Concentrateur des services d'application du tableau de bord.

Restauration d'une installation V8.1

Si la mise à niveau vers la version V8.1 échoue, vous pouvez restaurer votre instance V8.1 sauvegardée.

Avant de commencer

Vérifiez que vous êtes connecté en tant qu'administrateur et que vous disposez des fichiers de sauvegarde que vous avez créés lorsque vous avez mis à niveau vers la version 8.1.

Procédure

- UNIX Linux Procédez de la manière suivante :
  1. Arrêtez le serveur Concentrateur des services d'application du tableau de bord.
  2. Renommez les répertoires de serveur de l'Interface graphique Web et Concentrateur des services d'application du tableau de bord comme suit :

Tableau 47. Renommer les répertoires existants sous UNIX et Linux

Répertoire	Renommer par
opt/IBM/netcoool/omnibus_webgui	opt/IBM/netcoool/omnibus_webgui.old
opt/IBM/JazzSM	opt/IBM/JazzSM.old
opt/IBM/WebSphere/websphere_AppServer	opt/IBM/WebSphere/websphere_AppServer.old

  3. Restaurez le contenu des fichiers suivants à leur emplacement d'origine :
     omnibus_webgui.tar
     jazzSM.tar
     websphere_AppServer.tar
  4. Démarrez Concentrateur des services d'application du tableau de bord.

- Windows Procédez de la manière suivante :
  1. Arrêtez le serveur Concentrateur des services d'application du tableau de bord.

2. Renommez les dossiers Interface graphique Web et Concentrateur des services d'application du tableau de bord comme suit :

Tableau 48. Renommer les dossiers existants sous Windows

Dossier	Renommer par
C:\IBM\netcool\omnibus_webgui	C:\IBM\netcool\omnibus_webgui.old
C:\IBM\JazzSM	C:\IBM\JazzSM.old
C:\IBM\WebSphere\websphere_AppServer	C:\IBM\WebSphere\websphere_AppServer.old

3. Utilisez un programme d'archivage approprié pour restaurer le contenu des fichiers suivants à leur emplacement d'origine :

   omnibus_webgui.zip

   jazzSM.zip

   websphere_AppServer.zip

4. Lancez le serveur Concentrateur des services d'application du tableau de bord.

Exécution des tâches post-installation

Après l'installation, un certain nombre de tâches de configuration (obligatoires ou facultatives) sont nécessaires pour terminer la configuration initiale de votre environnement de produit.

Tâches associées:

«Installation de l'Interface graphique Web (interface graphique)», à la page 151
Installation du composant Interface graphique Web avec l'interface graphique Installation Manager.

«Connexion», à la page 182
Connectez-vous au portail chaque fois que vous voulez démarrer une session de travail.

Chapitre 18, «Configuration de l'Interface graphique Web», à la page 501
Le niveau de configuration que vous appliquez à l'Interface graphique Web après l'installation dépend de votre mode d'authentification des utilisateurs et du niveau de sécurité que vous souhaitez appliquer. Il est également important de tenir compte de la façon dont vous souhaitez utiliser l'Interface graphique Web dans votre environnement de production. Par exemple, considérez de quelles sources de données vous souhaitez recevoir des événements, si vous souhaitez effectuer une intégration à d'autres produits IBM et si vous souhaitez utiliser le haut niveau de résilience dans votre environnement qui est fourni par la fonctionnalité d'équilibrage de charge.

Exécution des tâches postinstallation pour l'Interface graphique Web

Un fois l'Interface graphique Web installée, vous pouvez lancer un outil qui effectue une configuration de post-installation. Vous pouvez également configurer l'interface graphique Web en mode silencieux.

Si vous n'avez pas exécuté l'utilitaire de configuration de post-installation, vous pouvez effectuer toutes les tâches manuellement.

L'outil crée une source de données unique qui est appelée «OMNIBUS». Vous devez spécifier l'hôte et le numéro de port et le nom d'utilisateur et mot de passe

pour cet ObjectServer. L'outil utilise l'ObjectServer pour l'authentification des utilisateurs et crée des utilisateurs et groupes par défaut Interface graphique Web dans cet ObjectServer.

Lorsque l'outil termine la configuration du produit, le serveur redémarre automatiquement.

Le mot de passe initial pour les comptes d'utilisateur par défaut, par exemple ncoadmin et ncouser, est **netcool**. Vous devez modifier ce mot de passe dans un environnement de production.

Démarrage de Outil de configuration de l'interface graphique Web OMNIbus

Démarrez le Outil de configuration de l'interface graphique Web OMNIbus pour configurer l'interface graphique Web.

Avant de commencer

Si vous rencontrez un problème lors de l'exécution du Outil de configuration de l'interface graphique Web OMNIbus, vous pouvez faire référence au fichier `ncwConfigUI_<horodatage>.log` pour plus d'informations. Le fichier journal se trouve dans le répertoire d'accueil `omnibus_webgui` sous `/configtools/logs`. Par exemple : `/opt/IBM/netcool/omnibus_webgui/configtool/logs`.

Procédure

1. Accédez au répertoire de l'outil de configuration pour votre plateforme : `WEBGUI_HOME/configtool/<$PLATFORM>`
2. Exécutez la commande ncwConfigUI.

Exemple

UNIX Linux Procédez de la manière suivante :

1. Accédez à `WEBGUI/HOME/configtool/linux.gtk.x86_64`
2. Exécutez la commande suivante :

```
./ncwConfigUI -WASUserID <WAS_ADMIN_ID> -WASPassword <WAS_ADMIN_PASSWORD>
```

Windows Procédez de la manière suivante :

1. Accédez à `C:\IBM\netcool\omnibus_webgui\configtool\win32.win32.x86_64`
2. Exécutez la commande suivante :

```
ncwConfigUI.exe -WASUserID <WAS_ADMIN_ID> -WASPassword <WAS_ADMIN_PASSWORD>
```

Que faire ensuite

- Si vous avez spécifié l'option pour créer des utilisateurs et groupes par défaut, utilisez les informations d'identification de ces utilisateurs pour vous connecter. Le mot de passe initial pour les comptes d'utilisateur par défaut, par exemple ncoadmin et ncouser, est le même que le mot de passe administrateur WebSphere Server.
- Si vous n'avez pas spécifié l'option pour créer des utilisateurs et des groupes, connectez-vous en tant qu'utilisateur par défaut Jazz for Service Management. Les informations d'identification cet utilisateur ont été spécifiées lors de l'installation.

Remarque : Si un nom d'utilisateur ou mot de passe incorrect est entré dans le Outil de configuration de l'interface graphique Web OMNIbus, un message d'erreur s'affiche lorsque vous créez des utilisateurs par défaut, ou lorsque WebSphere Application Server est redémarré. Pour corriger cela, vous pouvez relancer le Outil de configuration de l'interface graphique Web OMNIbus et entrez les informations d'identification correctes.

Configuration de l'interface graphique Web en mode silencieux

Vous pouvez configurer l'Interface graphique Web en mode silencieux. Cette méthode de configuration est utile si vous souhaitez des configurations identiques sur plusieurs postes de travail. La configuration en mode silencieux nécessite un fichier de propriétés qui définit la configuration de l'Interface graphique Web.

Avant de commencer

Vous devez avoir installé Jazz for Service Management. Pour plus d'informations, voir http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

Pourquoi et quand exécuter cette tâche

Le fichier de propriétés `OMNIbusWebGUI.properties` est inclus dans le répertoire d'installation Interface graphique Web, par exemple `<WEBGUI_HOME>/bin/OMNIbusWebGUI.properties`.

Procédure

1. Accédez au répertoire contenant le fichier `OMNIbusWebGUI.properties`.
2. Modifiez le fichier `OMNIbusWebGUI.properties` selon le cas.
3. Exécutez le script de post-configuration en mode silencieux :
   - Windows **<profil_JazzSM>\bin\ws_ant.bat**
   - Linux UNIX **<profil_JazzSM>/bin/ws_ant.sh**

   Utilisez une ou plusieurs des options suivantes lorsque vous exécutez cette commande :

   configureOS
   Utilisez cette option si vous souhaitez configurer le serveur ObjectServer pour l'interface graphique Web :
   - Enregistrez VMM_NCOS.
   - Configurez le référentiel d'utilisateur par défaut.
   - Créez/mettez à jour le fichier de source de données.
   - Redémarrez le serveur.

   resetVMM
   Utilisez cette option si vous souhaitez réinitialiser Virtual Member Manager :
   - Configurez le fichier comme référentiel d'utilisateur par défaut.

   configureVMM
   Utilisez cette option si vous souhaitez configurer VMM :
   - Enregistrez VMM_NCOS.
   - Configurez le référentiel d'utilisateur par défaut.

   restartServer
   Utilisez cette option si vous souhaitez redémarrer le serveur :
   - Arrêtez le serveur.

- Démarrez le serveur.

Ce qui suit est un exemple de base de la commande pour configurer Interface graphique Web en mode silencieux :

```
<profil_JazzSM>/bin/ws_ant.sh configureOS
```

Que faire ensuite

Vérifiez que l'Interface graphique Web est reconfigurée.

Utilisateurs et groupes fournis

Outil de configuration de l'interface graphique Web OMNIbus peut créer deux utilisateurs et deux groupes par défaut, de sorte que vous pouvez commencer à utiliser le produit dès que l'outil redémarre le serveur. Ils fournissent également un moyen pratique pour accéder au produit, que ce soit temporairement ou pour faire des démonstrations.

Les groupes facilitent l'attribution des privilèges d'utilisateur ou d'administration pour tous les utilisateurs que vous créez. Par exemple, lorsque vous créez des utilisateurs en lecture seule, vous devez les affecter au groupe Utilisateur_Netcool_OMNIbus.

Le tableau suivant répertorie les utilisateurs par défaut qui sont créés et les groupes qui leur sont attribués, et donne le mot de passe par défaut pour les utilisateurs. Assurez-vous que vous modifiez ce mot de passe lorsque vous vous connectez pour la première fois.

Tableau 49. Utilisateurs fournis par défaut

User ID (ID utilisateur)	Type d'utilisateur	Groupes	Mot de passe par défaut
ncouser	Lecture seule	Utilisateur_Netcool_OMNIbus	Identique au mot de passe administrateur de WebSphere Server.
ncoadmin	Administrator	Admin_Netcool_OMNIbus et Utilisateur_Netcool_OMNIbus	Identique au mot de passe administrateur de WebSphere Server.

Le tableau suivant répertorie les rôles qui sont attribués aux utilisateurs par défaut.

Tableau 50. Rôles affectés aux groupes fournis par défaut

Nom du groupe	Rôles affectés
Admin_Netcool_OMNIbus	ncw_admin ncw_dashboard_editor ncw_gauges_editor ncw_user netcool_rw
Utilisateur_Netcool_OMNIbus	ncw_user netcool_ro

Connexion

Connectez-vous au portail chaque fois que vous voulez démarrer une session de travail.

Avant de commencer

Jazz for Service Management doit être activé pour que vous puissiez vous y connecter à partir de votre navigateur.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour vous connecter :

Procédure

1. Dans un navigateur Web, entrez l'URL de Jazz for Service Management : `http://`*`domaine.hôte`*`:16310/ibm/console` ou `https://`*`domaine.hôte`*`:16311/ibm/console` s'il est configuré pour l'accès sécurisé.
   - *`host.domain`* est le nom de système hôte qualifié complet ou l'adresse IP de Jazz for Service Management (par ex. *MyServer.MySubdomain.MyDomain.com* ou 9.51.111.121 ou `localhost` si vous utilisez Jazz for Service Management localement).
   - `16310` est le numéro de port non sécurisé par défaut pour le portail et `16311` est le numéro de port sécurisé par défaut. Si votre environnement a été configuré avec un numéro de port autre que la valeur par défaut, entrez ce numéro en lieu et place. Si vous avez un doute quant au numéro de port utilisé, reportez-vous au profil du serveur d'applications afin de déterminer le numéro approprié.
   - `ibm/console` est le chemin par défaut vers Jazz for Service Management, cependant ce chemin est configurable et peut varier selon la valeur par défaut de votre environnement.
2. Sur la page de connexion, entrez votre ID utilisateur et votre mot de passe puis cliquez sur **Log in (Connexion)**. Il s'agit de l'ID utilisateur et du mot de passe stockés sur le Jazz for Service Management.

   Avertissement : Après authentification, le conteneur Web utilisé par Jazz for Service Management revient à la dernière URL demandée. Il s'agit généralement de `https://<host>:<port>/ibm/console`, mais vous pouvez être redirigé de façon inattendue si vous changez manuellement l'adresse URL de la page après avoir été d'abord redirigé vers la page de connexion, ou si vous avez fait une demande séparée au serveur dans une fenêtre de navigateur discrète avant de vous connectez.

   Remarque : Si plusieurs instances de Jazz for Service Management sont installées sur votre ordinateur, n'exécutez pas plus d'une instance à la fois au cours d'une session de navigation ; en d'autres termes, ne vous connectez pas à plusieurs instances sur des onglets de navigateur séparés.

Résultats

Après vérification de vos données d'identification, la page Accueil s'affiche. Si vous avez entré une valeur incorrecte pour le système hôte local ou le numéro de port, l'adresse URL ne peut pas être résolue. Consultez le profil du serveur d'applications pour vous assurer des valeurs entrées pour le système hôte local, le port et l'ID utilisateur.

Que faire ensuite

Sélectionnez l'un des éléments dans l'arborescence de navigation pour commencer à travailler sur la console.

Lorsque vous êtes connecté au Jazz for Service Management, évitez de cliquer sur le bouton **Précédent** du navigateur car vous serez automatiquement déconnecté. Si vous cliquez sur **Suivant**, vous constaterez que vous êtes déconnecté et que vous devez soumettre à nouveau vos données d'identification pour vous reconnecter.

Remarque : Si vous souhaitez utiliser l'authentification unique (SSO), vous devez utiliser le nom de domaine qualifié complet de l'hôte Tivoli Integrated Portal.

Acceptation du certificat de sécurité

Lorsque vous vous connectez, il peut arriver qu'une alerte de sécurité s'affiche avec un message signalant un problème au niveau du certificat de sécurité. Ceci indique que l'application du navigateur est en train de vérifier le certificat de sécurité du serveur d'applications.

Certificat auto-signé ou signé par une autorité d'accréditation

Le serveur d'applications utilise un certificat de sécurité auto-signé. Lors de votre première connexion au portail, il peut arriver qu'une alerte de sécurité s'affiche pour vous signaler un problème au niveau du certificat de sécurité. Vous pouvez être averti d'une éventuelle invalidité du certificat avec recommandation de renoncer à la connexion.

Toutefois, malgré cet avertissement, le certificat est bien valide et vous pouvez accepter la connexion. Ou bien, si vous préférez, une autre option consiste à installer votre propre certificat signé par une autorité d'accréditation. Pour des informations sur la création de votre propre certificat CA signé, allez à : http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tsec_sslcreateCArequest.html

Pour plus d'informations sur les certificats, allez sur le site IBM WebSphere Application Server Community Edition Documentation Project à l'adresse http://publib.boulder.ibm.com/wasce/V2.1.1/en/overview.html, et consultez les rubriques *Managing trust* et *Managing SSL certificates*.

Protection du fichier de clés du coffre

La clé de chiffrement du mot de passe administrateur est conservée dans le fichier de clés de coffre. Etablissez un accès en lecture seule strict à ce fichier.

Pourquoi et quand exécuter cette tâche

Pour restreindre l'accès au fichier, procédez comme suit :

Procédure

1. Accédez au répertoire *REP_INSTALL_WEBGUI*`/etc/encrypt`.
2. Utilisez la méthode mise à disposition par votre système d'exploitation pour vous assurer que le fichier `vault.key` n'est accessible qu'en lecture seule.

Exemple

UNIX Linux Utilisez les commandes suivantes :

```
cd opt/IBM/tivoli/netcool/omnibus_webgui/etc/encrypt
chmod 444 vault.key
```

Windows Utilisez l'explorateur Windows pour accéder au fichier `C:\IBM\tivoli\netcool\omnibus_webgui\etc\encrypt`. Cliquez avec le bouton droit de la souris sur le fichier `vault.key` et sélectionnez **Propriétés**. Cochez ensuite la case **Lecture seule** et cliquez sur **OK**.

Affectation de rôles d'Interface graphique Web à l'utilisateur administrateur

Pour permettre à l'utilisateur administrateur créé pendant le processus d'installation d'accéder aux pages et aux widgets de l'Interface graphique Web vous devez lui affecter des rôles supplémentaires.

Pourquoi et quand exécuter cette tâche

Vous spécifiez le nom d'utilisateur et le mot de passe de l'administrateur pendant l'installation. Le nom d'utilisateur par défaut est smadmin.

Pour affecter des rôles d'Interface graphique Web à l'utilisateur administrateur :

Procédure

1. Connectez-vous à l'Interface graphique Web avec les droit d'accès de l'utilisateur administrateur que vous avez entrés pendant l'installation.
2. Attribuez les rôles d'administration à cet utilisateur ou ajoutez l'utilisateur au groupe Admin_Netcool_OMNIbus.

Tableau 51. Ajout de rôles ou de groupes à l'administrateur

Activité	Procédure
Attribuez des rôles d'administration à l'utilisateur.	1. Cliquez sur **Paramètres de la console** > **Rôles utilisateur**. 2. Cliquez sur **Rechercher**. 3. Recherchez l'utilisateur (par exemple, smadmin) dans la grille au bas de la page et cliquez sur son nom unique. 4. Dans la page Rôles utilisateur, cochez les cases suivantes : • **ncw_admin** • **ncw_user** **Avertissement :** Ne décochez pas de case qui est déjà cochée. 5. Cliquez sur **Enregistrer**.

Tableau 51. Ajout de rôles ou de groupes à l'administrateur (suite)

Activité	Procédure
Ajoutez l'utilisateur au groupe Admin_Netcool_OMNIbus.	1. Connectez-vous à **WebSphere Integrated Solutions Console**. 2. Cliquez sur **Utilisateurs et groupes** > **Manage Users (Gérer les utilisateurs)**. 3. Cliquez sur **Rechercher**. 4. Recherchez l'utilisateur (par exemple, tipadmin) dans la grille au bas de la page et cliquez sur son ID utilisateur. 5. Dans la page Propriétés de l'utilisateur, cliquez sur l'onglet **Groupes** et sur **Ajouter**. 6. Dans la page Add User to groups (Ajouter un utilisateur aux groupes), cliquez sur **Rechercher**. 7. Cliquez sur le nom de groupe Admin_Netcool_OMNIbus, sur **Ajouter**, puis sur **Fermer**. 8. Cliquez sur l'onglet **General (Général)**, puis sur **OK**.

3. Déconnectez-vous et reconnectez-vous à l'Interface graphique Web.

Résultats

Après vous être reconnecté, les widgets et pages de l'Interface graphique Web sont affichés dans le panneau de navigation.

Que faire ensuite

Cliquez sur les liens suivants dans le panneau de navigation pour accéder à l'Interface graphique Web :

- Pour accéder aux fonction d'administration, par exemple aux ressources Générateur de filtres, Générateur de vues, Editeur d'outils et Création de mappe, cliquez sur **Administration** > **Outils de gestion d'événements**.
- Pour accéder aux fonctions d'affichage d'événement, cliquez sur **Incident** > **Evénements**.

Changement des mots de passe des utilisateurs fournis

A l'origine, les utilisateurs fournis (ncouser et ncoadmin) ont le même mot de passe que l'administrateur. Pour des raisons de sécurité, vous pouvez souhaiter changer les mots de passe de ces noms d'utilisateur.

Procédure

Pour modifier les mots de passe des comptes ncouser et ncoadmin, procédez comme suit :

1. Connectez-vous à **WebSphere Integrated Solutions Console**.
2. Assurez-vous d'être connecté en tant qu'administrateur (par exemple, smadmin).
3. Cliquez sur **Utilisateurs et groupes** > **Manage Users (Gérer les utilisateurs)**.
4. Cliquez sur **Rechercher**.
5. Pour chaque mot de passe à changer, procédez comme suit :
   a. Cliquez sur l'ID utilisateur en bas de la page.

b. Saisissez le nouveau mot de passe dans les zones **Mot de passe** et **Confirmer le mot de passe**.
c. Cliquez sur **OK**.

Configuration du client WAAPI

Pour configurer l'utilisation des événements prévisibles et la surveillance des événements IBM Tivoli Application Dependency Discovery Manager (TADDM), vous devez effectuer une configuration minimale du client WAAPI en spécifiant un utilisateur et un mot de passe.

Avant de commencer

Vous devez avoir attribué le rôle ncw_admin à l'administrateur ou à l'utilisateur du client WAAPI requis.

Pourquoi et quand exécuter cette tâche

Important : Vous devez effectuer au moins l'étape 1 avant de pouvoir configurer l'Interface graphique Web pour les événements prévisibles ou pour la surveillance des événements TADDM. Cette configuration requiert l'utilisation de la commande **runwaapi**, dans laquelle un utilisateur et un mot de passe doivent être spécifiés.

Pour configurer le client WAAPI :

Procédure

1. Editez le fichier *REP_INSTALL_WEBGUI*/waapi/etc/waapi.init et définissez les valeurs des propriétés suivantes :

   waapi.user
   Entrez votre nom d'utilisateur. L'utilisateur doit avoir le rôle ncw_admin.

   waapi.password
   Entrez votre mot de passe.

   waapi.port
   Facultatif : si, pendant l'installation, vous avez modifié le port du serveur de l'Interface graphique Web par défaut au serveur 16310, saisissez le port.
2. Facultatif : Définissez les valeurs des propriété restantes du fichier.

   Remarque : Vous n'avez pas besoin de spécifier les propriétés restantes immédiatement ; les propriétés **waapi.user** et **waapi.password** sont suffisantes pour configurer les événements prévisibles ou la surveillance des événements TADDM.
3. Enregistrez et fermez le fichier.

Résultats

L'utilisateur et le mot de passe du client WAAPI sont maintenant définis et vous pouvez exécuter la commande **runwaapi**.

Pour plus d'informations sur l'utilisation du client WAAPI pour administrer l'Interface graphique Web, voir le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Tâches associées:

«Affectation de rôles d'Interface graphique Web à l'utilisateur administrateur», à la page 184
Pour permettre à l'utilisateur administrateur créé pendant le processus d'installation d'accéder aux pages et aux widgets de l'Interface graphique Web vous devez lui affecter des rôles supplémentaires.

«Activation des événements prévisibles dans l'Interface graphique Web», à la page 587
Vous exécuterez un fichier de commandes WAAPI, fourni avec le composant serveur, sur le serveur Interface graphique Web afin de créer les configurations nécessaires pour afficher les événements prévisibles qui sont générés par IBM Tivoli Monitoring dans les listes d'événements.

«Activation de la prise en charge des événements TADDM dans l'Interface graphique Web», à la page 590
Vous pouvez ajouter un menu, des outils et un filtre pour les événements TADDM sur le serveur de l'Interface graphique Web pour vous permettre d'afficher des détails supplémentaires sur ces événements lorsqu'ils sont affichés dans la liste des événements actifs.

Activation du support multiculturel de l'Interface graphique Web

Il peut être nécessaire d'effectuer des étapes de configuration supplémentaires pour afficher l'Interface graphique Web dans votre langue.

Configuration de l'Interface graphique Web pour les caractères GB18030

Pour que votre installation de l'Interface graphique Web en chinois soit conforme à la norme GB18030 pour les caractères chinois, vous devez installer le jeu de caractères GB18030 sur votre système client et configurer les systèmes clients de façon à ce qu'ils affichent ces caractères.

Avant de commencer

Assurez-vous que votre système d'exploitation remplisse les conditions requises suivantes :

- UNIX Linux L'environnement local zh_CN.utf8 doit être installé sur les systèmes d'exploitation du client et du serveur de l'Interface graphique Web.
- Tous les systèmes d'exploitation : les polices qui prennent en charge GB18030 doivent être installées comme suit :
  - UNIX Linux Vous devrez peut-être télécharger les polices séparément.
  - Windows Le package de prise en charge qui contient la prise en charge des polices GB18030 doit être installé.

Pour plus d'informations sur les exigences de votre système d'exploitation, reportez-vous à la documentation de son fournisseur.

Pourquoi et quand exécuter cette tâche

Ces étapes de configuration concernent le composant d'Interface graphique Web uniquement. Vous devez également configurer les autres composants de Tivoli Netcool/OMNIbus pour pouvoir utiliser GB18030.

Pour configurer l'Interface graphique Web afin d'assurer la conformité à GB18030, procédez comme suit :

Procédure

1. UNIX Linux Sur les systèmes d'exploitation du client et du serveur, définissez les variables d'environnement LANG et LC_ALL sur LC_ALL=zh_CN.utf8.
2. Windows Sur les systèmes d'exploitation client, définissez la liaison de polices avec la police SimSun-18030.
3. Activez la détection automatique de chiffrement de langue sur votre navigateur Web.

Concepts associés:

«Navigateurs de l'Interface graphique Web, environnements JRE et périphériques mobiles», à la page 50
Pour pouvoir afficher l'Interface graphique Web, les postes de travail client ont besoin d'un navigateur pris en charge et d'un plug-in JRE (Java Runtime Environment). Les périphériques mobiles doivent figurer sur un système d'exploitation pris en charge. Configurez les navigateurs pour l'acceptation des cookies.

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Définition du fuseau horaire par défaut pour les nouveaux utilisateurs

Pour garantir que les nouveaux utilisateurs ont les paramètres de fuseau horaire corrects, vous devez spécifier le fuseau horaire appliqué lors de leur création.

Pourquoi et quand exécuter cette tâche

Lorsqu'un utilisateur est créé, les valeurs initiales ou par défaut sont renseignées à partir du fichier ci-dessous : *REP_INSTALL_WEBGUI*/etc/system/userdefaults.props. Le paramètre de fuseau horaire par défaut pour les nouveaux utilisateurs est GMT+00:00. Les valeurs de fuseau horaire autorisées sont spécifiées dans la base de données tz. Pour plus d'informations sur cette base de données, visitez le site Web suivant :

http://www.twinsun.com/tz/tz-link.htm

Pour connaître les valeurs de fuseau horaire autorisées, voir le site Web :

http://twiki.org/cgi-bin/xtra/tzdatepick.html

Une fois le fichier userdefaults.props modifié, vous devez redémarrer le serveur.

Conseil : Les paramètres de fuseau horaire des utilisateurs existants sont stockés dans le fichier suivant : *REP_INSTALL_WEBGUI*/etc/configstore/ncwUserPreferences/*nom_utilisateur*.nova, où *nom_utilisateur* désigne l'utilisateur.

Pour modifier le fuseau horaire par défaut pour les nouveaux utilisateurs :

Procédure

1. Ouvrez le fichier *REP_INSTALL_WEBGUI*/etc/system/userdefaults.props.
2. Définissez la valeur de la propriété **timezone** sur le fuseau horaire requis.

Conseil : Sélectionnez le nom d'un fuseau horaire basé sur les paramètres régionaux (par exemple Amérique/Chicago) plutôt qu'un fuseau horaire basé sur GMT (par exemple, etc/GMT-6).

3. Définissez la valeur du paramètre **ael_user_properties_timezone_updated** sur `true`.
4. Redémarrez le serveur.

Résultats

Lors de la création de nouveaux utilisateurs, le fuseau horaire des fichiers *REP_INSTALL_WEBGUI*/etc/configstore/ncwUserPreferences/*nom_utilisateur*.nova est défini sur la valeur de la propriété **timezone**.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Identification et résolution des problèmes d'installation

Les informations suivantes vous aident à résoudre les problèmes d'installation que vous pouvez rencontrer.

La migration échoue avec des erreurs "Out of Memory"

Comment récupérer d'une erreur Out of memory lors de la migration.

La phase d'importation d'une migration échoue si la machine virtuelle Java (JVM) n'a pas suffisamment de mémoire et que des erreurs Out of memory s'affichent dans les fichiers journaux de la migration. Si ceci se produit, augmentez la mémoire de la machine virtuelle Java, annulez la migration puis recommencez la phase d'importation.

Tâches associées:

«Migration à partir de IBM Tivoli Netcool/Webtop version 2.0 ou 2.1», à la page 167
Utilisez le programme de migration pour exporter les données, les fichiers et les options de configuration et importer ces éléments dans l'installation de la version 7.4. Lorsque ce processus est terminé, vous mettez à niveau l'interface graphique Web vers la version 8.1. Pour plus d'informations, voir *Exécution d'une installation propre et migration de données version 7.4.0 ou 7.3.1*. Pour migrer vos données Netcool/Webtop version 2.0 ou 2.1 existantes vers l'Interface graphique Web version 7.4, exécutez les scripts du module d'exportation de l'outil de migration sur les serveurs sur lesquels IBM Tivoli Netcool Security Manager et Netcool GUI Foundation sont installés. Importez ensuite les données de migration dans l'Interface graphique Web.

«Migration à partir de IBM Tivoli Netcool/Webtop version 1.3.1», à la page 172
Utilisez le programme de migration pour exporter les données, les fichiers et les options de configuration et importer ces éléments dans l'installation de la version 7.4 ou 7.3.1. Lorsque ce processus est terminé, vous mettez à niveau l'interface graphique Web vers la version 8.1. Pour migrer les données de Netcool/Webtop version 1.3.1 vers l'Interface graphique Web V7.4, exécutez le module d'exportation de l'outil de migration sur l'hôte sur lequel Netcool/Webtop version 1.3.1 est installé. Vous importez ensuite les données de migration dans l'Interface graphique Web Tivoli Netcool/OMNIbus version 7.4.

Retrait de l'Interface graphique Web

Utilisez IBM Installation Manager pour retirer l'Interface graphique Web.

Avant de commencer

Effectuez les actions suivantes :

- Arrêtez tous les processus Tivoli Netcool/OMNIbus en cours.
- Sauvegardez tous les fichiers de données ou de configuration qui ont été créés depuis l'installation initiale et que vous voulez conserver.
- Pour effectuer une suppression en mode silencieux, créez ou enregistrez un fichier de réponses Installation Manager. Utilisez l'option `-record` *`fichier_réponses`*. Par exemple :
  1. Créez ou enregistrez un skipInstall :

     ```
     IBMIM.exe -record C:\fichier_réponses\install_1.xml -skipInstall
      C:\Temp\skipInstall
     ```

  2. Pour créer un fichier de réponses de désinstallation à l'aide du skipInstall créé :

     ```
     IBMIM.exe -record C:\fichier_réponses\uninstall_1.xml -skipInstall
      C:\Temp\skipInstall
     ```

Procédure

Suppression via l'interface graphique

1. Pour supprimer l'Interface graphique Web avec l'interface graphique d'Installation Manager :
   a. Accédez au sous-répertoire `/eclipse` du répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour démarrer l'assistant Installation Manager :
      - UNIX Linux `./IBMIM`
      - Windows `IBMIM.exe`
   c. Dans la fenêtre principale d'Installation Manager, cliquez sur **Désinstaller**.
   d. Sélectionnez les offres que vous voulez supprimer et suivez les instructions de l'assistant d'installation pour effectuer la suppression.

Suppression via la console

2. Pour supprimer le composant d'Interface graphique Web dans la console d'Installation Manager :
   a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation d'Installation Manager.
   b. Utilisez la commande suivante pour démarrer Installation Manager :
      - UNIX Linux `./imcl -c`
      - Windows `imcl.exe -c`
   c. Dans le menu principal, sélectionnez Désinstaller.
   d. Sélectionnez les offres que vous voulez supprimer et suivez les instructions d'Installation Manager pour effectuer la suppression.

Suppression en mode silencieux

3. Pour supprimer l'Interface graphique Web en mode silencieux :

a. Accédez au sous-répertoire `/eclipse/tools` du répertoire d'installation d'Installation Manager.
b. Utilisez la commande suivante pour lancer la suppression :
   - UNIX Linux `./imcl -input fichier_réponses -silent -log /tmp/install_log.xml -acceptLicense`
   - Windows `imcl.exe -input fichier_réponses -silent -log \Temp\install_log.xml -acceptLicense`

   Où *fichier_réponses* est le chemin de répertoire vers le fichier de réponses qui définit la configuration de la suppression.

Résultats

Installation Manager supprime les fichiers et les répertoires qu'il a installés.

Que faire ensuite

- Les fichiers qui n'ont pas été installés par Installation Manager et les fichiers de configuration qui ont été modifiés sont laissées en place. Examinez ces fichiers et supprimez-les ou sauvegardez-les de façon appropriée.
- Pour plus d'informations sur la désinstallation de Jazz for Service Management, recherchez *uninstalling* dans le centre de documentation de Jazz SM à l'adresse http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html.

Chapitre 7. Configuration du système Tivoli Netcool/OMNIbus

Après avoir installé Tivoli Netcool/OMNIbus, vous pouvez créer et configurer un ou plusieurs ObjectServers et configurer les informations de communications de vos composants serveur Tivoli Netcool/OMNIbus.

Assistant de configuration initiale

L'assistant de configuration initiale (**nco_icw** automatise certaines tâches de configuration initiale, telles que la création d'ObjectServers et de passerelles.

L'assistant présente une série de panneaux dans lesquels vous pouvez créer les éléments communs d'une installation Tivoli Netcool/OMNIbus installation pour un ou plusieurs ordinateurs. Lorsque votre configuration est terminée, elle est enregistrée dans un fichier descripteur de déploiement. Vous pouvez appliquer le fichier descripteur de déploiement sur⌂n'importe quel ordinateur où l'Assistant est installé.

Vous pouvez configurer un déploiement distribué complet en une seule session et attribuer chaque composant à un ordinateur spécifique. Lorsque vous appliquez le descripteur de déploiement sur chaque ordinateur, seuls les composants qui sont définis pour cet ordinateur y seront installés.

Pour démarrer l'interface graphique de l'assistant, utilisez la commande suivante :`$NCHOME/omnibus/bin/nco_icw`

Pour démarrer la console de l'assistant, utilisez la commande suivante : `$NCHOME/omnibus/bin/nco_icw -console`

Chaque panneau de l'assistant contient une assistance embarquée pour vous aider à effectuer chaque tâche. Avant de tenter de créer une configuration prête pour la production, familiarisez-vous avec les concepts et les instructions de configuration liés ci-dessous.

Tâches associées:

«Installation de Tivoli Netcool/OMNIbus (interface graphique)», à la page 73
Installation de Tivoli Netcool/OMNIbus à partir de l'interface graphique Installation Manager.

Création et exécution de serveurs ObjectServer

Chaque installation Tivoli Netcool/OMNIbus peut avoir au moins un serveur ObjectServer pour stocker et gérer les informations d'alerte. Vous pouvez également configurer plusieurs serveurs ObjectServer sur un ou plusieurs ordinateurs hôtes.

Tâches associées:

«Importation des rapports récapitulatifs des événements dans Tivoli Common Reporting», à la page 484
Pour exécuter les rapports récapitulatifs des événements, connectez Tivoli Common Reporting à une base de données relationnelle via une passerelle. Puis, importez le module de rapports qui est fourni avec Tivoli Netcool/OMNIbus dans Tivoli Common Reporting.

Présentation du serveur ObjectServer

Le serveur ObjectServer est le serveur de la base situé au coeur de Tivoli Netcool/OMNIbus. Les données sur l'événement sont réacheminées vers le serveur ObjectServer à partir de programmes externes, notamment des sondes et des passerelles. Le serveur ObjectServer stocke et gère ces informations dans des tables de base de données et affiche les informations dans la liste d'événements.

Dans une configuration standard, les événements sont réacheminés directement vers le serveur ObjectServer. Vous pouvez utiliser le serveur proxy pour réduire le nombre de connexions de sonde à un serveur ObjectServer.

Vous pouvez exécuter le serveur ObjectServer et le serveur proxy en mode sécurisé. Dans ce mode, le serveur ObjectServer et le serveur proxy authentifient les demandes de connexion provenant de sondes, passerelles et serveurs proxy en demandant un nom d'utilisateur et un mot de passe.

Le serveur ObjectServer prend en charge la conservation des données à l'aide de points de contrôle et de journaux sur disque. Les points de contrôle écrivent toutes les données sur le disque à des intervalles définis par le système afin de permettre la récupération des données si le serveur s'arrête de manière imprévue. Entre les points de contrôles, les modifications supplémentaires de la base de données sont consignées sur le disque.

Initialisation de la base de données du serveur ObjectServer

Pour créer un nouveau serveur ObjectServer, vous devez exécuter l'utilitaire d'initialisation de la base de données (**nco_dbinit**).

L'utilitaire **nco_dbinit** exécute les fonctions suivantes :

- Crée un fichier de propriétés pour le nouveau serveur ObjectServer

  Le fichier de propriétés contient les paramètres de configuration du serveur ObjectServer. Il a pour nom `$NCHOME/omnibus/etc/`*`nom de serveur`*`.props`, où *nom de serveur* est le nom que vous indiquez lors de la création du serveur ObjectServer.
- Crée des tables de base de données et des données par défaut pour le nouveau serveur ObjectServer
- Crée les utilisateurs, groupes et rôles par défaut pour le nouveau serveur ObjectServer

  Les utilisateurs par défaut du serveur ObjectServer, `root` et `nobody`, sont créés ainsi que les groupes et les rôles par défaut pour vous aider à gérer les droits.

L'utilitaire **nco_dbinit** utilise un certain nombre de fichiers d'initialisation de la base de données par défaut pour créer les données par défaut.

Fichiers d'initialisation de la base de données

L'utilitaire d'initialisation de bases de données (nco_dbinit) utilise des fichiers SQL pour créer les tables de base de données et les données par défaut pour un nouveau serveur ObjectServer.

Ces fichiers SQL sont les suivants :

- `application.sql` : Ce fichier crée les tables initiales pour les bases de données `alerts` et `tools`.
- `automation.sql` : Ce fichier crée les groupes de déclencheurs initiaux, les déclencheurs et les procédures.

- `desktop.sql` : ce fichier indique les valeurs initiales des tables de bureau, y compris les couleurs, les conversions, les outils et les menus par défaut.
- `system.sql` : ce fichier indique la base de données et les tables de sécurité, les utilisateurs système, les groupes, les rôles ainsi que les autorisations. Vous ne devez pas l'éditer.
- `security.sql` : ce fichier indique les rôles opérateur et administrateur supplémentaires.

Ces fichiers se trouvent dans le répertoire `$NCHOME/omnibus/etc`.

Répertoire de bases de données du serveur ObjectServer

Les tables de base de données du serveur ObjectServer sont stockées dans un répertoire par défaut.

Le serveur ObjectServer utilise `$NCHOME/omnibus/db` sur les systèmes UNIXet `%NCHOME%\omnibus\db` sur les systèmes Windows.

Conventions de dénomination des serveurs ObjectServer

Lorsqu'une installation inclut plusieurs serveurs ObjectServer, chaque ObjectServer doit posséder un nom unique. Ce nom est utilisé dans la configuration pour identifier le serveur ObjectServer.

Les sondes, passerelles et clients de bureau utilisent le nom du serveur ObjectServer pour s'y connecter.

Le nom d'un serveur ObjectServer doit se composer d'un maximum de 29 lettres majuscules et ne peut pas commencer par un entier. Le préfixe du nom d'un ObjectServer ou d'une passerelle ne doit contenir que des caractères ASCII imprimables et ne doit pas inclure les caractères suivants :

- tabulation
- retour chariot
- à la ligne
- espace
- {
- }
- #
- +
- "
- !
- '

N'utilisez pas de nom se terminant par _PA, _GATE ou _PROXY. Ces chaînes sont réservées à l'identification d'un agent de processus (_PA), d'une passerelle (_GATE) ou d'un serveur proxy (_PROXY).

Configuration de la reprise en ligne et de la reprise par restauration automatisées

Tivoli Netcool/OMNIbus prend en charge la reprise en ligne et la reprise par restauration automatisées des serveurs ObjectServer. Dans ce mode, un serveur ObjectServer de sauvegarde contient une réplique des données d'événement et reprend automatiquement toutes les opérations du serveur ObjectServer principal, notamment un contrôle d'automatisation, lorsque ce dernier est en panne.

La reprise en ligne se produit lorsque des applications se connectent à un serveur ObjectServer de sauvegarde lorsque la connexion au serveur ObjectServer principal est perdue. La fonction de reprise par restauration permet aux applications de se reconnecter au serveur ObjectServer principal lorsqu'il est à nouveau actif.

Une passerelle du serveur ObjectServer bidirectionnelle est utilisée pour répliquer les données d'événement entre les serveurs ObjectServer principal et de sauvegarde. La passerelle possède des connexions actives avec les deux serveurs ObjectServer et connaît le statut de chaque ObjectServer. Cette passerelle utilise les notifications de signaux pour informer chaque ObjectServer dans la configuration de la paire de reprise en ligne, lorsque son équivalent échoue ou redémarre. Lorsque les signaux sont émis, les messages sont également écrits dans le fichier journal du serveur ObjectServer. Le niveau de journalisation des messages est ERROR lors de la reprise en ligne, et INFO pour la reprise par restauration.

Une reprise en ligne et une reprise par restauration automatiques sont prises en charge avec les signaux, procédures et déclencheurs suivants :

- Signaux : gw_counterpart_down et gw_counterpart_up
- Procédures : automation_disable et automation_enable
- Déclencheurs : backup_startup, backup_counterpart_down et backup_counterpart_up. Ces déclencheurs sont désactivés dans le fichier `$NCHOME/omnibus/etc/automation.sql`, qui est un des fichiers d'initialisation de base de données.

Pour activer la reprise en ligne et la reprise par restauration automatisées, les déclencheurs backup_startup, backup_counterpart_down et backup_counterpart_up du fichier `$NCHOME/omnibus/etc/automation.sql` doivent être activés avant ou après avoir exécuté **`nco_dbint`** pour créer les serveurs ObjectServer. Pour activer les déclencheurs avant d'exécuter **`nco_dbint`**, modifiez le fichier `automation.sql`. Pour activer les déclencheurs dans un serveur ObjectServer existant, utilisez la commande ALTER TRIGGER ou l'outil Netcool/OMNIbus Administrator. Pour plus d'informations sur l'activation des déclencheurs, consultez le *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Remarque : Si vous configurez vos serveurs ObjectServer principal et de sauvegarde de façon à ce qu'ils s'exécutent comme une paire virtuelle dans la couche d'agrégation d'une architecture à plusieurs niveaux standard, les déclencheurs backup_startup, backup_counterpart_down et backup_counterpart_up sont automatiquement activés dans la configuration.

Concepts associés:

«Fichiers d'initialisation de la base de données», à la page 194
L'utilitaire d'initialisation de bases de données (nco_dbinit) utilise des fichiers SQL pour créer les tables de base de données et les données par défaut pour un nouveau serveur ObjectServer.

Chapitre 8, «Configuration et déploiement d'une architecture à plusieurs niveaux», à la page 223
Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

Création d'un serveur ObjectServer

Vous créez un ou plusieurs serveurs ObjectServer sur un poste de travail hôte en exécutant l'utilitaire d'initialisation de base de données (**nco_dbinit**).

Pourquoi et quand exécuter cette tâche

Remarques importantes pour le support multiculturel :

- Vous devez exécuter **nco_dbinit** dans l'environnement local dans lequel vous allez démarrer et exécuter le serveur ObjectServer.
- Si vous tentez d'exécuter le serveur ObjectServer avec le chiffrement UTF-8 sous Windows (ce qui garantit la conformité GB18030), exécutez l'utilitaire **nco_dbinit** avec l'option de ligne de commande `-utf8enabled` définie sur `TRUE`.
- Lorsque vous créez un serveur ObjectServer, vous pouvez le configurer pour que les données de configuration du bureau UNIX et Windows soient affichées dans votre environnement local. Ces données sont généralement affichées dans la liste d'événements et Conductor et incluent les couleurs par défaut, les visuels de colonne, les conversions, les outils et les menus. Lorsque vous exécutez **nco_dbinit**, les données de configuration sont lues à partir du fichier de définition SQL par défaut du bureau, mais vous pouvez spécifier un fichier différent pour votre environnement local en utilisant l'option de ligne de commande `-desktopfile` avec la commande **nco_dbinit**.

Pour créer un serveur ObjectServer :

Procédure

A partir de la ligne de commande, entrez la commande appropriée à votre système d'exploitation :

Option	Description
UNIX	`$NCHOME/omnibus/bin/nco_dbinit -server` *nom_serveur*
Windows	`%NCHOME%\omnibus\bin\nco_dbinit -server` *nom_serveur*

Dans cette commande, *nom_serveur* est le nom du serveur ObjectServer que vous voulez créer. Des options et propriétés de ligne de commande supplémentaires sont disponibles pour l'utilitaire **nco_dbinit**.

Résultats

Le fichier de propriétés `$NCHOME/omnibus/etc/`*nom_serveur*`.props` est créé pour le nouveau serveur ObjectServer. De plus, les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. Vous pouvez créer des objets ObjectServer supplémentaires en utilisant Netcool/OMNIbus Administrator ou ObjectServer SQL.

Concepts associés:

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Tâches associées:

«Configuration du serveur ObjectServer pour utiliser le texte d'interface utilisateur traduit dans le bureau», à la page 426
La base de données ObjectServer contient des données de configuration affichées dans le bureau UNIX et Windows (c'est-à-dire dans la liste d'événements et Conductor). Lorsque vous initialisez la base de données ObjectServer, ces données de configuration sont lues dans le fichier de définitions SQL, qui insère les valeurs par défaut dans les tables du bureau, y compris les couleurs par défaut, les visuels de colonne, les conversions, les outils et les menus.

Propriétés et options de ligne de commande de nco_dbinit

Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

L'emplacement par défaut du fichier de propriétés est `$NCHOME/omnibus/etc/nco_dbinit.props`.

Les propriétés et les options de ligne de commande prises en charge par **nco_dbinit** sont décrites dans le tableau suivant.

Tableau 52. Propriétés et options de ligne de commande de nco_dbinit

Propriété	Option de ligne de commande	Description
AlertsData TRUE | FALSE	-alertsdata	Contrôle si le fichier indiqué par la propriété **AlertsDataFile** est lu. La valeur par défaut est FALSE ; c'est-à-dire que le fichier n'est pas lu.
AlertsDataFile *chaîne*	-alertsdatafile*chaîne*	Un fichier de définition d'applications SQL supplémentaire est lu après le fichier indiqué par la propriété **ApplicationFile**. Si vous voulez que ce fichier soit lu, définissez la propriété **AlertsData** sur TRUE. Le fichier par défaut est `$NCHOME/etc/alertsdata.sql`. Les instructions INSERT qui contiennent les zones de type INCR sont traitées différemment dans ce fichier et dans le fichier indiqué par la propriété **ApplicationFile**. De ce fichier, de telles zones ne sont *pas* incrémentées, mais elles sont affectées aux valeurs données dans les instructions INSERT. Par exemple, la table alerts.journal contient une clé externe basée sur la zone Serial de la table alerts.status. Pour maintenir cette référence, les valeurs de la zone Serial doivent être insérées sans être changées. Utilisez ce fichier uniquement pour les données créées par des outils automatiques, par exemple, l'utilitaire **nco_osreport**.

Tableau 52. Propriétés et options de ligne de commande de nco_dbinit (suite)

Propriété	Option de ligne de commande	Description
ApplicationFile *chaîne*	-applicationfile *chaîne*	Fichier de définition SQL de l'application qui crée les tables par défaut des bases de données d'alertes et d'outils. Le fichier par défaut est $NCHOME/omnibus/etc/application.sql.
AutomationFile *chaîne*	-automationfile *chaîne*	Fichier de définition SQL de l'automatisation qui crée les déclencheurs et les groupes de déclencheurs par défaut. Le fichier par défaut est $NCHOME/omnibus/etc/automation.sql.
CopyPropsFile TRUE | FALSE	-nopropsfile	Détermine si un nouveau fichier de propriétés est créé pour le serveur ObjectServer cible. Si l'option de ligne de commande -nopropsfile est indiquée ou la propriété **CopyPropsFile** est définie sur FALSE, le fichier de propriétés par défaut n'est pas copié vers le serveur ObjectServer cible. La valeur par défaut est TRUE. En d'autres termes, le fichier de propriétés par défaut est copié et renommé pour le nouveau serveur ObjectServer.
CustomConfigFile *chaîne*	-customconfigfile *chaîne*	Contient une liste séparée par des virgules des chemins d'accès aux fichiers SQL d'importation (.sql) qui peut être utilisée pour mettre à jour le schéma de base de données avec la configuration supplémentaire lorsque le serveur ObjectServer est créé.
DesktopFile *chaîne*	-desktopfile *chaîne*	Fichier de définition SQL du bureau qui insère des valeurs par défaut dans les tables du bureau, y compris les couleurs par défaut, les conversions, les outils et les menus. Le fichier par défaut est $NCHOME/omnibus/etc/desktop.sql.
DesktopPrimaryServer *chaîne*	-dsdprimary *chaîne*	Indique le nom du serveur ObjectServer principal dans une architecture à deux serveurs. Cette valeur est entrée dans la zone MasterServer de la table master.national. Si la propriété **DesktopServer** n'est pas définie sur TRUE, cette propriété est ignorée.
DesktopServer TRUE | FALSE	-desktopserver	Indique que le serveur ObjectServer doit être créé en tant que serveur ObjectServer de bureau.
DesktopServerDualWrite 0 | 1	-dsddualwrite	Indique que le serveur ObjectServer de bureau doit être créé avec le mode écriture double activé. Cette valeur est entrée dans la zone DualWrite de la table master.national. Si la propriété **DesktopServer** n'est pas définie sur TRUE, cette propriété est ignorée.

Tableau 52. Propriétés et options de ligne de commande de nco_dbinit (suite)

Propriété	Option de ligne de commande	Description
DesktopServerFile *chaîne*	-desktopserverfile *chaîne*	Configure le serveur ObjectServer en tant que serveur ObjectServer de bureau à l'aide de ce fichier de définition SQL, qui crée la table master.national pour le serveur de bureau et la colonne MasterSerial correspondante dans la table alerts.status. Le fichier par défaut est $NCHOME/omnibus/etc/desktopserver.sql.
Force TRUE | FALSE	-force	Force l'écrasement des fichiers base de données existants. **Avertissement :** Toutes les modifications sont perdues.
N/D	-help	Affiche l'aide sur les options de ligne de commande et quitte.
Memstore.DataDirectory *chaîne*	-memstoredatadirectory *chaîne*	Indique le chemin du serveur ObjectServer à utiliser pour les fichiers base de données. La valeur par défaut est $NCHOME/omnibus/db.
MessageLevel *chaîne*	-messagelevel*chaîne*	Indique le niveau de consignation du message. Les valeurs possibles sont les suivantes : fatal, error, warn, info et debug. Le niveau par défaut est info. Les messages qui sont consignés à chaque niveau sont les suivants : • fatal : fatal uniquement. • error : fatal et error. • warn : fatal, error, and warn. • info : fatal, error, warn et info. • debug : fatal, error, warn, info et debug. **Conseil :** La valeur *chaîne* peut être en majuscules et/ou en minuscules.
MessageLog *chaîne*	-messagelog *chaîne*	Indique l'emplacement de consignation des messages. La valeur par défaut est stderr.
N/D	-propsfile*chaîne*	Indique le chemin d'accès au fichier de propriétés **nco_dbinit**. La valeur par défaut est $NCHOME/omnibus/etc/nco_dbinit.props.
ObjectServerPropsFile *chaîne*	-objservpropsfile *chaîne*	Indique le chemin d'accès au fichier de propriétés du serveur ObjectServer source. La valeur par défaut est $NCHOME/omnibus/etc/initial/NCOMS.props.
Props.CheckNames TRUE | FALSE	N/D	Si TRUE, **nco_dbinit** ne s'exécute pas si l'une des propriétés indiquées est non valide. La valeur par défaut est TRUE.

Tableau 52. Propriétés et options de ligne de commande de nco_dbinit (suite)

Propriété	Option de ligne de commande	Description
RestrictPasswords TRUE | FALSE	-restrictpasswords TRUE | FALSE	Si TRUE, les mots de passe doivent satisfaire aux restrictions suivantes : • Le mot de passe doit comprendre au moins huit caractères. • Le mot de passe doit comprendre au moins un caractère numérique. • Le mot de passe doit comprendre au moins un caractère alphabétique. La valeur par défaut est FALSE.
Sec.AuditLevel *chaîne*	-secauditlevel *chaîne*	Indique le niveau d'audit de sécurité. La valeur par défaut est warn.
Sec.AuditLog *chaîne*	-secauditlog *chaîne*	Indique l'emplacement de consignation de la trace d'audit de sécurité. La valeur par défaut est stdout.
SecurityFile *chaîne*	-securityfile *chaîne*	Indique le chemin d'accès au fichier de définition de sécurité, qui définit les rôles opérateur et administrateur. La valeur par défaut est $NCHOME/omnibus/etc/security.sql.
Server *chaîne*	-server *chaîne*	Indique le nom du serveur ObjectServer à initialiser. La valeur par défaut est NCOMS.
SystemFile *chaîne*	-systemfile *chaîne*	Indique la base de données de sécurité et les tables,les utilisateurs système, les groupes, les rôles et les droits. La valeur par défaut est $NCHOME/omnibus/etc/system.sql. **Avertissement :** Ne modifiez pas ce fichier.
N/A	Windows -utf8enabled TRUE | FALSE	Contrôle le codage des données communiquées ou gérées par cette application sous Windows. Définissez la valeur -utf8enabled sur TRUE pour exécuter l'application au codage UTF-8. La valeur par défaut est FALSE ; ce qui implique l'utilisation de la page de codes par défaut du système. **Important :** Bien qu'une propriété **UTF8Enabled** soit disponible, la définition de cette propriété sur TRUE en vue d'activer le codage UTF-8 n'a aucun effet. Pour une exécution sous Windows au codage UTF-8, vous devez toujours utiliser l'option de ligne de commande -utf8enabled.
N/D	-version	Affiche les informations de version de **nco_dbinit** et quitte.

Remarque : L'utilitaire **nco_dbinit** inclut des propriétés avancées qui doivent être utilisées uniquement sous la direction du service de support logiciel IBM. Ces propriétés ne sont pas documentées.

Après avoir créé un serveur ObjectServer

Après avoir créé un serveur ObjectServer, vous devez utiliser l'éditeur de serveurs pour ajouter des détails de communication pour le serveur ObjectServer sur la machine hôte et sur chaque machine qui doit se connecter au serveur ObjectServer.

Pour démarrer l'éditeur de serveurs, procédez comme suit :

- UNIX Linux Entrez `$NCHOME/omnibus/bin/nco_xigen` dans la ligne de commande.
- Windows Cliquez sur **Démarrer** > **Programmes** > **Netcool Suite** > **Utilitaires système** > **Editeur de serveurs**.

Après avoir ajouté les détails de communication à l'aide de l'éditeur de serveurs, vous pouvez démarrer le serveur ObjectServer.

De plus, vous pouvez effectuer les tâches suivantes :

- Modifier les objets et les données du serveur ObjectServer en utilisant Netcool/OMNIbus Administrator ou l'utilitaire **nco_sql**.
- Modifier les paramètres de propriété en utilisant Netcool/OMNIbus Administrator ou la commande SQL ALTER SYSTEM SET SQL.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Tâches associées:

«Démarrage d'un serveur ObjectServer»
Vous devez exécuter un serveur ObjectServer avant d'utiliser les composants de Tivoli Netcool/OMNIbus.

Démarrage d'un serveur ObjectServer

Vous devez exécuter un serveur ObjectServer avant d'utiliser les composants de Tivoli Netcool/OMNIbus.

Pourquoi et quand exécuter cette tâche

Vous pouvez démarrer un serveur ObjectServer :

Procédure

- automatiquement, à l'aide du contrôle de processus sous UNIX et Windows
- automatiquement, à l'aide des services sous Windows
- manuellement, à partir d'une ligne de commande

Démarrage d'un serveur ObjectServer à l'aide du contrôle de processus

Si le serveur ObjectServer est démarré par l'agent de processus, il redémarre automatiquement en cas de défaillance. En démarrant l'agent de processus au démarrage du système, le serveur ObjectServer démarre automatiquement sous UNIX ou Windows.

Pourquoi et quand exécuter cette tâche

Un serveur ObjectServer peut être démarré comme un processus, à l'aide d'un agent de processus. Le serveur ObjectServer doit être défini comme un processus ou une partie d'un service.

Vous pouvez démarrer le serveur ObjectServer à partir d'un ordinateur distant. Le nom que vous indiquez avec l'option `-server` est comparé aux noms d'agent de processus configurés dans l'éditeur de serveur. L'ordinateur hôte et le port sont identifiés et la commande envoyée à l'agent de processus correct.

Pour plus d'informations relatives au contrôle de processus et aux agents de processus, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Procédure

Pour démarrer un serveur ObjectServer comme un processus, entrez la commande suivante :

```
nco_pa_start -process ObjectServer
```

Dans cet exemple, le serveur ObjectServer a été défini comme un processus appelé `ObjectServer`.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Démarrage d'un serveur ObjectServer à l'aide des services (Windows)

Sous Windows, vous pouvez éventuellement installer et exécuter le serveur ObjectServer en tant que service Windows. Si le service est automatique, le serveur ObjectServer démarre en même temps que l'ordinateur.

Pourquoi et quand exécuter cette tâche

Si vous avez installé le serveur ObjectServer en tant que service Windows, vous pouvez démarrer le service dans la fenêtre Services du Panneau de configuration ou à partir de la ligne de commande.

Pour démarrer le serveur ObjectServer dans la fenêtre Services, procédez comme suit :

Procédure

1. Ouvrez le Panneau de configuration de Windows.
2. Cliquez deux fois sur **Outils d'administration** et sur l'icône **Services**.

3. Cliquez deux fois sur **Serveur d'objets Netcool/OMNIbus**. La fenêtre de propriétés de ce service s'ouvre.
4. Dans la zone **Paramètres de démarrage** de l'onglet **Général**, entrez les options de ligne de commande du serveur ObjectServer local. Par exemple, entrez :

   ```
   -name NCOMS
   ```

5. Vérifiez que la valeur `Automatique` est attribuée à la zone **Type de démarrage**.
6. Cliquez sur le bouton **Démarrer** pour lancer le serveur ObjectServer en tant que service Windows. Au démarrage du service, cliquez sur **OK** pour fermer la fenêtre de propriétés.

Exemple

Dans la ligne de commande, vous pouvez démarrer le service ObjectServer en exécutant la commande suivante :

```
net start nom_service
```

où *nom_service* est le nom de service du serveur ObjectServer, tel qu'il est défini dans la fenêtre Services (**NCOObjectServer**, par exemple) .

Tâches associées:

«Configuration des composants Tivoli Netcool/OMNIbus comme services Windows», à la page 100
Les composants serveur et sondes de Tivoli Netcool/OMNIbus peuvent être installés pour être exécutés en tant que services sur un hôte Windows. Les composants serveur que vous installez en tant que services incluent le serveur ObjectServer, l'agent de processus, le serveur proxy et les passerelles.

Démarrage manuel du serveur ObjectServer

Utilisez la commande **nco_objserv** pour démarrer manuellement le serveur ObjectServer.

Pourquoi et quand exécuter cette tâche

Pour démarrer un serveur ObjectServer, procédez comme suit :

Procédure

Dans la ligne de commande, entrez la commande appropriée pour votre système d'exploitation :

Système d'exploitation	Commande
UNIX	`$NCHOME/omnibus/bin/nco_objserv [ -name nom_serveur]`
Windows	`%NCHOME%\omnibus\bin\nco_objserv [ -name nom_serveur]`

Dans cette commande, *nom_serveur* est le nom du serveur ObjectServer. Si vous ne spécifiez pas l'option de ligne de commande `-name`, **nco_objserv** tente de démarrer le serveur ObjectServer NCOMS. Vous pouvez démarrer le serveur ObjectServer avec des options de ligne de commande supplémentaires. Pour plus de détails sur ces options de ligne de commande, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Remarque : Un serveur ObjectServer démarré à partir de la ligne de commande n'est pas sous le contrôle de processus et doit être démarré manuellement s'il est arrêté.
Au démarrage, le serveur ObjectServer tente d'ouvrir le fichier de propriétés

$NCHOME/omnibus/etc/*nom_serveur*.props, où *nom_serveur* est le nom du serveur ObjectServer spécifié.

Configuration d'un serveur ObjectServer en cours d'exécution

Lorsque le serveur ObjectServer est en cours d'exécution, vous pouvez utiliser les commandes ALTER SYSTEM et Netcool/OMNIbus Administrator pour modifier la configuration.

Pour plus de détails, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Arrêt d'un serveur ObjectServer

Vous pouvez arrêter un serveur ObjectServer à l'aide du contrôle de processus sous UNIX et Windows. Si le serveur ObjectServer est configuré comme un service Windows, vous pouvez l'arrêter à l'aide des services sous Windows. Vous pouvez également arrêter un serveur ObjectServer à partir de l'interface SQL interactive.

Pourquoi et quand exécuter cette tâche

Arrêt d'un serveur ObjectServer à l'aide du contrôle de processus

Sous UNIX et Windows, un serveur ObjectServer peut être arrêté (comme un processus) à l'aide d'un agent de processus. Le serveur ObjectServer doit être défini en tant que processus ou dans le cadre d'un service.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations relatives à l'utilisation de l'interface SQL interactive, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Procédure

- Pour arrêter un serveur ObjectServer en tant que processus, entrez la commande suivante :

  ```
  nco_pa_stop -process ObjectServer
  ```

  Dans cet exemple, le serveur ObjectServer est défini comme un processus appelé `ObjectServer`.
- Pour arrêter le serveur ObjectServer à partir d'un ordinateur distant, entrez la commande suivante :

  ```
  nco_pa_stop -server NAME_PA -process ObjectServer
  ```

  Dans cet exemple, la valeur *NOM*_PA que vous indiquez avec l'option `-server` est comparée aux noms d'agent de processus configurés dans l'éditeur de serveur. La machine hôte et le port sont identifiés, et la commande envoyée à l'agent de processus correct sur l'ordinateur distant.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Arrêt d'un serveur ObjectServer à l'aide de services (Windows)

Si vous avez configuré le serveur ObjectServer pour l'exécuter comme un service Windows, vous pouvez l'arrêter en arrêtant le service.

Pourquoi et quand exécuter cette tâche

Pour arrêter un serveur ObjectServer qui fonctionne comme un service Windows, procédez comme suit :

Procédure

1. Ouvrez le Panneau de configuration de Windows.
2. Cliquez deux fois sur **Outils d'administration** et sur l'icône **Services**.
3. Cliquez deux fois sur **Serveur d'objets Netcool/OMNIbus**. La fenêtre de propriétés de ce service s'ouvre.
4. Dans l'onglet **Général**, cliquez sur le bouton **Arrêter** pour arrêter le service ObjectServer.

Exemple

Dans la ligne de commande, vous pouvez arrêter le service ObjectServer en exécutant la commande suivante :

```
net stop nom_service
```

où *nom_service* est le nom de service du serveur ObjectServer, tel qu'il est défini dans la fenêtre Services (**NCOObjectServer**, par exemple) .

Tâches associées:

«Configuration des composants Tivoli Netcool/OMNIbus comme services Windows», à la page 100
Les composants serveur et sondes de Tivoli Netcool/OMNIbus peuvent être installés pour être exécutés en tant que services sur un hôte Windows. Les composants serveur que vous installez en tant que services incluent le serveur ObjectServer, l'agent de processus, le serveur proxy et les passerelles.

Arrêt d'un serveur ObjectServer à partir de l'interface SQL interactive

Si vous avez démarré manuellement un serveur ObjectServer à partir de la ligne de commande, vous devez l'arrêter manuellement à l'aide de l'interface SQL interactive. Vous devez détenir les droits correspondants d'arrêt du serveur ObjectServer.

Procédure

Pour arrêter un serveur ObjectServer qui a été démarré manuellement:

1. Connectez-vous à un serveur ObjectServer en exécutant la commande appropriée pour votre système d'exploitation :

Système d'exploitation	Commande
UNIX	`$NCHOME/omnibus/bin/nco_sql [ -server nom_serveur ] [ -user nom_utilisateur]`
Windows	`%NCHOME%\omnibus\bin\isql -S nom_serveur -U nom_utilisateur`

Dans ces commandes, *nom_serveur* est le nom d'un serveur ObjectServer local

ou éloigné et *nom_utilisateur* est un nom d'utilisateur valide.

UNIX Linux Si vous n'avez pas spécifié l'option de ligne de commande `-server`, l'interface SQL interactive se connecte au serveur ObjectServer NCOMS. Si vous ne précisez pas le nom d'utilisateur, la valeur par défaut est l'utilisateur qui exécute la commande.

Windows Vous devez préciser le nom du serveur ObjectServer et le nom d'utilisateur.

2. Indiquez le mot de passe demandé.
3. A l'invite SQL, entrez les commandes suivantes :

   ```
   1> alter system shutdown;
   2> go
   ```

   La commande **nco_sql** n'accepte pas les blancs avant le mot clé `go`. Un blanc engendre l'échec des instructions SQL.

Résultats

Si un serveur ObjectServer est démarré dans le cadre d'un contrôle de processus, l'agent de processus le redémarre automatiquement suite à un arrêt manuel. Dans ce cas, vous devez arrêter le serveur ObjectServer à l'aide du contrôle de processus.

Pour plus d'informations relatives à l'utilisation de l'interface SQL interactive, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Configuration des détails de communication du serveur dans l'éditeur de serveur

Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

L'éditeur de serveur vous permet de conserver des informations de communication pour les composants serveur suivants :

- Serveurs ObjectServer
- Passerelles
- Agents de processus
- Serveurs proxy

Création et conservation des entrées serveur après l'installation

Après l'installation, vous devez utiliser l'éditeur de serveur pour mettre à jour les informations de communication du serveur sur la machine hôte et sur chaque ordinateur qui doit se connecter au composant serveur.

Vous devez continuer de conserver les informations de communication du serveur sur l'ordinateur hôte et sur chaque ordinateur qui doit se connecter au composant serveur, à chaque fois que votre configuration système change.

Entrées par défaut de l'éditeur de serveur sous UNIX

Une entrée par défaut de l'éditeur de serveur est créée sur l'ordinateur hôte pour chaque serveur dans le cadre de l'installation de Tivoli Netcool/OMNIbus. Après l'installation, l'hôte est défini sur `omnihost` pour toutes les entrées serveur. Vous devez modifier ces paramètres `omnihost` et les définir sur le nom de l'ordinateur hôte du serveur.

En outre, vous devez créer une entrée client sur chaque ordinateur à partir duquel vous vous connectez au serveur avec des valeurs d'hôte et de port qui correspondent à celles de l'ordinateur hôte.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Entrées par défaut de l'éditeur de serveur sous Windows

Deux entrées par défaut de l'éditeur de serveur sont créées sur l'ordinateur hôte pour chaque serveur dans le cadre de l'installation de Tivoli Netcool/OMNIbus. Le programme d'écoute répond aux demandes du client. En outre, une entrée client est créée afin que les clients locaux puissent se connecter au serveur.

Remarque : Les connexions locales ne doivent pas être cryptées.

Vous devez créer une entrée client sur chaque ordinateur à partir duquel vous vous connectez au serveur avec des valeurs d'hôte et de port qui correspondent à celles de l'ordinateur hôte.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Entrée de définition de serveur de passerelle

Vous devez créer une entrée de définition de serveur de passerelle pour chaque passerelle s'exécutant sur l'hôte actuel.

Le nom par défaut pour le serveur de passerelle est NCO_GATE. Il utilise le fichier de propriétés `NCHOME/omnibus/etc/NCO_GATE.props`.

Chaque passerelle peut également être configurée pour s'exécuter avec son propre serveur de passerelle.

Pour de plus amples informations sur les passerelles, y compris comment les configurer et les exécuter, voir le manuel *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide* et les guides individuels des passerelles que vous exécutez.

Entrée de définition de serveur d'agent de processus

L'agent de processus vous permet d'utiliser des procédures externes dans le système d'automatisation. Cela signifie que vous pouvez émettre des commandes sur d'autres machines hôtes.

L'agent de processus doit posséder une entrée serveur et client dans l'éditeur de serveur. Ces entrées sont automatiquement créées lors de l'installation.

Le serveur d'agent de processus par défaut est appelé NCO_PA. Le numéro de port par défaut est 4200.

Pour de plus amples informations sur le contrôle de processus, y compris sur la configuration de ce dernier pour gérer des processus et exécuter des procédures externes dans des automatisations, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Tâches associées:

«Configuration des informations de communication du serveur»
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Configuration des informations de communication du serveur

Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Pourquoi et quand exécuter cette tâche

Pour configurer la communication du serveur à l'aide de l'éditeur de serveurs :

Procédure

1. Effectuez les actions appropriées pour votre système d'exploitation :

Tableau 53. Démarrage de l'éditeur de serveurs

Système d'exploitation	Action
UNIX	Effectuez une des actions suivantes : • Cliquez sur le bouton **Interfaces** du Conductor UNIX. • Entrez `$NCHOME/omnibus/bin/nco_xigen` sur la ligne de commande.
Windows	Effectuez une des actions suivantes : • Cliquez sur **Démarrer** > **Programmes** > **Netcool Suite** > **Utilitaires système** > **Editeur de serveurs**. • Ouvrez le menu **Conducteur** en cliquant avec le bouton droit de la souris sur l'icône bus sur le plateau du bureau puis sur **Servers** (Serveurs).

La fenêtre Server Editor (Editeur de serveur) s'ouvre, affichant une liste des serveurs existants sous les en-têtes **Serveur**, **Hôte**, **Port** et **SSL**. La fenêtre contient également un panneau **Serveur** et un panneau **Priorité**.

2. Complétez cette fenêtre comme suit :

Server list (Liste de serveurs)
La liste de serveurs affiche les composants serveur existant et leurs paramètres :

Serveur
Cette colonne affiche le nom de chaque serveur défini pour ce poste de travail. Les noms des serveurs par défaut sont les suivants :

- NCOMS : nom par défaut des serveurs ObjectServer
- NCO_PROXY : nom par défaut des serveurs proxy
- NCO_GATE : nom par défaut des passerelles
- NCO_PA : nom par défaut des agents de processus

Sous Windows, le poste de travail hôte du serveur doit avoir une entrée *listener* (programme d'écoute) et une entrée *client* ; cette dernière entrée est également requise sur tout poste de travail qui se connecte à ce serveur.

Les serveurs ObjectServer de secours apparaissent en dessous de l'éditeur de serveur. Pour masquer la liste des serveurs de secours, cliquez deux fois sur le nom ou l'icône du serveur ObjectServer principal. Les serveurs ObjectServer de secours sont masqués et la lettre *C* apparaît dans l'icône de serveur. Cliquez à nouveau deux fois pour afficher les serveurs ObjectServer de secours. L'icône de serveur revient à la normale.

Hostname (Nom d'hôte)
Cette colonne affiche le nom d'hôte ou l'adresse IP du poste de travail sur lequel le composant serveur est installé.

Port Cette colonne affiche le port sur lequel le serveur écoute les connexions non chiffrées.

SSL Sous UNIX, cette colonne affiche le port sur lequel le

composant serveur écoute les connexions chiffrées. Sous UNIX, un port standard, un port SSL, ou les deux peuvent être définis sur un composant serveur.

Sous Windows, cette colonne affiche le mot `oui` pour les connexions chiffrées. Sous Windows, le même numéro de port est utilisé pour les connexion chiffrées et non chiffrées.

Panneau du serveur

Les zones du panneau du serveur permettent d'entrer ou de modifier les détails de chaque composant serveur. Si vous modifiez les détails d'un composant serveur existant, vous devez d'abord sélectionner la ligne correspondante dans la liste de serveurs, pour que les détails s'affichent dans les zones du panneau du serveur.

Nom Entrez le nom du nouveau composant serveur ou renommez un composant existant. Sous Windows, vous pouvez également utiliser la liste de propriétés pour sélectionner la propriété à éditer. Pour nommer les composants, utilisez les suffixes suivants : _PROXY pour les serveurs proxy, _GATE pour les passerelles, et _PA pour les agents de processus.

Remarque : Le nom de l'entrée de serveur doit contenir au maximum 29 lettres en majuscule et ne doit pas commencer par un entier.

Hôte Entrez ou modifiez le nom d'hôte ou l'adresse IP du poste de travail sur lequel le serveur est installé. (Pour les nouveaux composants serveur sous UNIX, le nom est défini par défaut sur `omnihost`, et doit être modifié sur le nom d'hôte ou l'adresse IP actuel(le).)

Si vous entrez une adresse IP, vous pouvez spécifier une adresse IPv4 ou IPv6. Par exemple :

- `192.168.0.1`
- `2094:82a:2a6e:123:503:badd:fe43:f552`

Port Sous UNIX, si vous souhaitez que les clients utilisant les connexions non chiffrées puissent se connecter au serveur, entrez un numéro de port valide et non utilisé dans cette zone. Pour désactiver les connexions non chiffrées, n'indiquez pas de port.

Sous Windows, entrez un numéro de port valide et non utilisé.

SSL Sous UNIX, entrez un numéro de port valide et non utilisé si vous souhaitez que les clients utilisant les connexions chiffrées puissent se connecter au serveur. Pour désactiver les connexions chiffrées, ne définissez pas de port.

Sous Windows, cochez cette case pour indiquer que le port accepte les connexions chiffrées des clients utilisant SSL.

Remarque : Sous UNIX, un port standard, un port SSL ou les deux peuvent être définis sur le composant serveur. Sous Windows, le même numéro de port est utilisé pour les deux types de connexion.

Listener (Programme d'écoute) (Windows uniquement)
Cochez cette case s'il s'agit d'une entrée de programme d'écoute sur le poste de travail hôte du serveur. Décochez cette case s'il s'agit d'une entrée de client.

Ajouter
Cliquez sur ce bouton pour ajouter des détails de serveur nouveaux et spécifiques à la liste de serveurs.

Supprimer/Mettre à jour
Ce bouton est défini en fonction de l'action effectuée sur le composant serveur sélectionné, à savoir une éventuelle modification. Cliquez sur **Supprimer** si vous souhaitez supprimer le composant serveur sélectionné dans la liste de serveurs. Cliquez sur **Mettre à jour** pour actualiser la liste de serveurs avec les détails mis à jour du composant serveur existant.

Test Cliquez sur ce bouton pour tester la connexion au serveur sélectionné dans la liste de serveurs. L'éditeur de serveurs tenter de contacter le serveur sur le port et l'hôte spécifié. Les résultats de la commande de test sont affichés dans une fenêtre.

Panneau de priorité
Les zones de priorité de serveur vous permettent d'augmenter ou de baisser le niveau de priorité des composants serveur configurés comme systèmes de reprise en ligne. Par exemple, un serveur ObjectServer appelé NCOMS_PRI est configuré avec un serveur de sauvegarde appelé NCOMS_BAK. A l'aide des boutons **Raise** (Augmenter) ou **Lower** (Baisser), vous pouvez augmenter le niveau de priorité du serveur NCOMS_BAK afin de le définir comme ObjectServer principal, et définir NCOMS_PRI comme serveur de sauvegarde.

Raise(Augmenter)
Cliquez sur ce bouton pour augmenter la priorité du composant serveur sélectionné d'un niveau.

Lower (Baisser)
Cliquez sur ce bouton pour baisser la priorité du serveur sélectionné d'un niveau.

Generate All (Générer tous) (UNIX uniquement)
Cliquez sur ce bouton pour générer les fichiers d'interface pour tous les systèmes d'exploitation UNIX. Lorsque vous appliquez les modifications (à l'aide du bouton **Appliquer**), vous générez des fichiers d'interface appelés `$NCHOME/etc/interfaces.`*`arch`*, où *arch* représente les noms des plateformes UNIX individuelles ; par exemple, `interfaces.hpux11` et `interfaces.solaris2`.

Show Groups (Afficher les groupe) (Windows uniquement)
Sous Windows, cochez cette case pour regrouper chaque serveur par nom dans la liste de serveurs, avec les serveurs de sauvegarde et les programmes d'écoute identifiés en fonction de l'entrée de client.

Appliquer (UNIX uniquement)
Cliquez sur ce bouton pour appliquer les modifications au fichier d'interface. Tout composant serveur ajouté à la liste de serveurs, supprimé de cette liste ou modifié est sauvegardé dans ce fichier.

OK (Windows uniquement)
Cliquez sur ce bouton pour sauvegarder vos modifications et fermer la fenêtre.

Fermer (UNIX)/Annuler (Windows)
Cliquez sur ce bouton pour fermer la fenêtre après avoir sauvegardé les modifications avec le bouton **Appliquer**, ou pour fermer la fenêtre sans sauvegarder les modifications.

Importer (UNIX uniquement)
Cliquez sur ce bouton pour importer les détails de communication.

Résultats

Le serveur ObjectServer extrait sa propre définition de serveur pour identifier son nom d'hôte et son numéro de port. Il accepte ensuite les demandes de connexion vers cet emplacement. Les sondes, passerelles et clients de bureau ont des propriétés ou options de ligne de commande qui spécifient le serveur ObjectServer auquel se connecter. Vous pouvez également spécifier un serveur ObjectServer de sauvegarde à utiliser si le serveur ObjectServer principal n'est pas disponible.

Concepts associés:

Chapitre 15, «Configuration IPv6», à la page 413
Tivoli Netcool/OMNIbus offre la prise en charge des protocoles IPv4 et IPv6. Les composants peuvent à présent fonctionner et coexister sur un réseau prenant en charge une configuration IPv4 seulement, IPv6 seulement ou IPv4 et IPv6.

Tâches associées:

«Ajout d'un serveur ObjectServer de secours»
Vous pouvez spécifier un serveur ObjectServer de secours pour chaque ObjectServer défini dans l'éditeur de serveurs. Si une connexion au serveur ObjectServer principal échoue, le clients tentent de se connecter au serveur ObjectServer de secours.

Ajout d'un serveur ObjectServer de secours

Vous pouvez spécifier un serveur ObjectServer de secours pour chaque ObjectServer défini dans l'éditeur de serveurs. Si une connexion au serveur ObjectServer principal échoue, le clients tentent de se connecter au serveur ObjectServer de secours.

Pourquoi et quand exécuter cette tâche

Pour ajouter un serveur ObjectServer de secours, procédez comme suit :

Procédure

1. Créez le serveur ObjectServer de secours.
2. Créez les entrées de définition de serveur.
3. Créez l'entrée de client de secours.
4. Distribuez les fichiers d'interfaces (UNIX).

Etape 1 : création du serveur ObjectServer de secours

Créez le serveur ObjectServer qui servira de serveur de secours. Le serveur ObjectServer de secours doit avoir un nom et un numéro de port uniques et il est généralement installé sur un ordinateur hôte différent.

Pourquoi et quand exécuter cette tâche

Par exemple, si vous avez déjà un serveur ObjectServer principal appelé NCOMS, vous pouvez créer un serveur ObjectServer appelé NCOMS_BAK.

Remarque : Un serveur ObjectServer de secours installé sur un hôte différent du serveur ObjectServer principal doit être exécuté sous le contrôle des processus. Le cas échéant, vous devez également ajouter des définitions de serveur pour l'agent de processus sur les deux systèmes hôte.

Vous pouvez créer plusieurs serveurs ObjectServer de secours.

Tâches associées:

«Création d'un serveur ObjectServer», à la page 197
Vous créez un ou plusieurs serveurs ObjectServer sur un poste de travail hôte en exécutant l'utilitaire d'initialisation de base de données (**nco_dbinit**).

Etape 2 : création des entrées de définition de serveur

Dans l'éditeur de serveurs, créez une entrée de serveur pour chaque ObjectServer de secours.

Pourquoi et quand exécuter cette tâche

Sous UNIX, indiquez des valeurs dans les zones **Nom**, **Hôte**, **Port**, et **SSL**. Cliquez ensuite sur **Ajouter** pour ajouter le nouveau serveur puis sur **Appliquer** pour appliquer les modifications au fichier d'interfaces.

Sous Windows, indiquez des valeurs dans les zones **Nom**, **Hôte**, **Port**, **Listener** (Programme d'écoute) et **SSL**. Cliquez ensuite sur **Ajouter** pour ajouter le nouveau serveur.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Etape 3 : création de l'entrée du client de secours

Si les clients ne peuvent pas se connecter au serveur ObjectServer principal, recherchez une entrée de secours. Les sondes, passerelles et bureaux identifient le serveur ObjectServer de secours en recherchant un serveur ObjectServer qui correspond au nom du serveur ObjectServer principal.

Pourquoi et quand exécuter cette tâche

Pour créer cette entrée client dans l'éditeur de serveurs :

Procédure

1. Cliquez sur l'entrée du serveur ObjectServer principal, par exemple NCOMS.

   Remarque : Ne modifiez *pas* le nom du serveur ObjectServer.
2. Entrez le nom d'hôte du serveur ObjectServer de secours. Par exemple, si vous avez créé un serveur ObjectServer de secours appelé NCOMS_BAK, indiquez la machine hôte sur laquelle NCOMS_BAK est exécuté.
3. Entrez le numéro de port du serveur ObjectServer de secours. Par exemple, si vous avez créé un serveur ObjectServer de secours appelé NCOMS_BAK, indiquez le numéro de port pour NCOMS_BAK.
4. Cliquez sur le bouton **Ajouter**.
5. Sur les systèmes UNIX cliquez sur le bouton **Appliquer** pour appliquer les modifications au fichier d'interfaces.

Résultats

Le serveur ObjectServer de secours est affiché en retrait sous le serveur ObjectServer principal avec les détails concernant son hôte et son port.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Etape 4 : distribution du fichier d'interfaces (UNIX uniquement)

Le serveur ObjectServer de secours est généralement exécuté un hôte différent de celui du ObjectServer principal, bien que ce ne soit pas obligatoire. Vous devez avoir des entrées de serveur sur chaque hôte pour tous les serveurs de votre configuration.

Pourquoi et quand exécuter cette tâche

Pour distribuer le fichier d'interfaces, qui contient ces entrées, sur tous les ordinateurs hôtes de votre configuration, copiez le fichier d'interfaces spécifique à l'architecture correspondant dans le répertoire `$NCHOME/etc` sur chaque ordinateur hôte.

Par exemple, si vous avez trois installations Tivoli Netcool/OMNIbus sur des postes de travail Sun, copiez le fichier `$NCHOME/etc/interfaces.solaris2` sur le répertoire `$NCHOME/etc` de chaque poste de travail Sun.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Tâches associées:

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **`nco_igen`** pour générer le fichier d'interfaces.

Modification de la priorité des serveurs

Si vous avez un ou plusieurs serveurs de secours, vous pouvez décider de modifier leur priorité.

Pourquoi et quand exécuter cette tâche

Pour modifier la priorité des serveurs :

Procédure

1. Dans l'éditeur de serveurs, sélectionnez un serveur.
2. Cliquez sur le bouton **Augmenter** ou **Diminuer** pour augmenter ou diminuer la priorité du serveur.
3. Sur les systèmes UNIX, cliquez sur le bouton **Appliquer** pour appliquer les modifications au fichier d'interfaces.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Masquage des serveurs ObjectServer de secours dans l'éditeur de serveurs (UNIX uniquement)

Les serveurs ObjectServer de secours sont affichés sous le serveur ObjectServer de principal dans l'éditeur de serveurs.

Pourquoi et quand exécuter cette tâche

Pour masquer la liste des serveurs ObjectServer de secours :

Procédure

1. Dans l'éditeur de serveurs, cliquez deux fois sur le nom ou l'icône du serveur ObjectServer principal. Les serveurs ObjectServer de secours sont masqués et la lettre `C` est affichée dans l'icône du serveur.
2. Cliquez à nouveau deux fois pour afficher les serveurs ObjectServer de secours. L'icône du serveur redevient normale.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Test d'un serveur

Pour tester la disponibilité d'un serveur dans l'éditeur de serveurs, sélectionnez le nom d'un serveur en cours d'exécution dans la liste et cliquez sur le bouton **Test**.

Pourquoi et quand exécuter cette tâche

L'éditeur de serveurs tente de contacter le serveur sur l'hôte et le port spécifiés. Une boîte de dialogue affiche le résultat de la commande de test.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Edition manuelle du fichier de données de connexions

Le fichier de données de connexions permet de créer le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus. Dans certains cas, il peut être nécessaire d'éditer le fichier de connexions directement ; par exemple sur les systèmes UNIX qui ne disposent pas d'interface graphique.

Pourquoi et quand exécuter cette tâche

Remarque : Le cas échéant, vous devez utiliser l'éditeur de serveurs pour modifier les informations de connexion au lieu d'éditer directement le fichier de données de connexions.

Le fichier de données de connexions s'appelle :

```
$NCHOME/etc/omni.dat
```

Voici un exemple de fichier `omni.dat` :

```
[NCOMS]
{
Primary: sfo 4100
Backup: dfw 4100
Backup: lax 4100
}
[NCO_PA]
{
Primary: sfo 4200
}
[NCO_GATE]
{
Primary: sfo 4300
}
```

Si vous devez éditer manuellement le fichier `omni.dat`, utilisez ce format.

Remarque : Les numéros de port doivent être uniques pour chaque entrée de serveur.

Après avoir édité le fichier de données de connexions, vous devez générer le fichier d'interfaces. Si vous ne voulez pas utiliser l'éditeur de serveurs, vous

pouvez exécuter l'utilitaire de ligne de commande **nco_igen** pour générer le fichier d'interfaces.

Que faire ensuite

Si vous modifiez le nom d'hôte ou l'adresse IP de l'ordinateur sur lequel est installé un serveur ObjectServer, reconfigurez également le moteur de déploiement (DE) sur cet ordinateur.

Tâches associées:

«Génération du fichier d'interfaces pour plusieurs plateformes (UNIX uniquement)», à la page 219
Après avoir utilisé l'éditeur de serveurs pour configurer des communications entre composants, les informations de communication sont sauvegardées dans un *fichier d'interfaces*.

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Configuration d'installations réparties

Vous pouvez exécuter différents composants Tivoli Netcool/OMNIbus sur plusieurs systèmes de votre réseau. Vous pouvez par exemple exécuter un serveur ObjectServer sur un ordinateur, une passerelle sur un autre ordinateur et un serveur proxy sur un troisième ordinateur.

Pourquoi et quand exécuter cette tâche

Pour créer une installation distribuée, procédez comme suit :

Procédure

1. Installez les composants Tivoli Netcool/OMNIbus requis sur chaque ordinateur.
2. Configurez les communications des composants.
3. Distribuez les informations de communication sur chaque système Tivoli Netcool/OMNIbus (UNIX uniquement).

Etape 1 : Installation des composants Tivoli Netcool/OMNIbus

Installez les composants requis sur les ordinateurs désignés dans votre environnement.

Pourquoi et quand exécuter cette tâche

Conseil : Vous pouvez également créer des configurations du serveur ObjectServer en double à l'aide de l'utilitaire **nco_confpack**, utilisé pour importer et exporter des configurations du serveur ObjectServer.

Concepts associés:

Chapitre 11, «Importation et exportation de configurations du serveur ObjectServer», à la page 293
Tivoli Netcool/OMNIbus fournit deux utilitaires, nommés **nco_confpack** et **nco_osreport** ; vous pouvez les utiliser pour importer et exporter les configurations d'un serveur ObjectServer.

Etape 2 : Configuration des communications entre composants

Après avoir installé les composants Tivoli Netcool/OMNIbus sur chaque machine, vous devez vous assurer qu'ils peuvent communiquer entre eux.

Pourquoi et quand exécuter cette tâche

Pour ce faire :

Procédure

1. Configurez les communications serveur sur *un* poste de travail UNIX Tivoli Netcool/OMNIbus.
2. Configurez les communications serveur sur *tous* les postes de travail Windows.
3. Pour les systèmes UNIX uniquement, générez les informations de communications pour plusieurs systèmes d'exploitation si nécessaire.

Configuration des communications serveur sur les ordinateurs

Pour configurer les communications serveur, utilisez l'éditeur de serveurs.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Génération du fichier d'interfaces pour plusieurs plateformes (UNIX uniquement)

Après avoir utilisé l'éditeur de serveurs pour configurer des communications entre composants, les informations de communication sont sauvegardées dans un *fichier d'interfaces*.

Pourquoi et quand exécuter cette tâche

L'éditeur de serveurs génère par exemple le fichier d'interfaces suivant sur un poste de travail Solaris :

```
$NCHOME/etc/interfaces.solaris2
```

Si vous exécutez des composants Tivoli Netcool/OMNIbus sur plusieurs plateformes UNIX, vous devez générer des fichiers d'interfaces compatibles avant de les distribuer.

Vous pouvez utiliser l'éditeur de serveurs pour générer des fichiers d'interfaces pour chaque plateforme ou vous pouvez générer ces fichiers depuis la ligne de commande.

Pour générer des fichiers d'interfaces pour toutes les plateformes disponibles, dans l'éditeur de serveurs :

1. Cochez la case **Generate All** (Générer tout).
2. Cliquez sur **Appliquer**. Les fichiers d'interfaces `$NCHOME/etc/interfaces.`*arch* sont générés, où *arch* est le nom de la plateformeUNIX.

Pour générer un fichier d'interfaces pour une seule plateforme, entrez la commande suivante :

```
$NCHOME/bin/nco_igen -arch plateforme
```

Où *plateforme* peut être :

- solaris2
- hpux11
- aix5
- linux2x86
- linux2s390
- java
- hpux11hpia

Par exemple, pour générer un fichier d'interfaces pour un système AIX, entrez la commande suivante :

```
$NCHOME/bin/nco_igen -arch aix5
```

Le fichier suivant est créé :

$NCHOME/etc/interfaces.aix5

Pour générer des fichiers d'interfaces pour toutes les plateformes UNIX disponibles, entrez :

```
$NCHOME/bin/nco_igen -all
```

Un fichier d'interfaces `$NCHOME/etc/interfaces.`*arch* est généré pour chaque plateforme, où *arch* est le nom de la plateforme UNIX.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Tâches associées:

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **`nco_igen`** pour générer le fichier d'interfaces.

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Etape 3 : distribution des fichiers d'interfaces (UNIX uniquement)

Après avoir généré des fichiers d'interfaces pour chaque système d'exploitation UNIX dans votre système Tivoli Netcool/OMNIbus, vous pouvez les distribuer. Vous pouvez ainsi facilement dupliquer des paramètres de communication pour chaque ordinateur UNIX Tivoli Netcool/OMNIbus.

Pourquoi et quand exécuter cette tâche

Pour ce faire, copiez le fichier d'interfaces spécifique à l'architecture correspondant dans le répertoire `$NCHOME/etc` de chaque ordinateur hôte.

Par exemple, si vous avez trois installations Tivoli Netcool/OMNIbus sur des postes de travail Sun, copiez le fichier `$NCHOME/etc/interfaces.solaris2` sur le répertoire `$NCHOME/etc` de chaque poste de travail Sun.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Tâches associées:

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **`nco_igen`** pour générer le fichier d'interfaces.

Chapitre 8. Configuration et déploiement d'une architecture à plusieurs niveaux

Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

Tivoli Netcool/OMNIbus est fourni avec un ensemble de configurations qui offrent une configuration de référence pour des systèmes à un, deux ou trois niveaux. Ces configurations vous permettent de déployer rapidement une architecture à plusieurs niveaux, sans problème et d'une manière standardisée. L'ensemble de configurations est basé sur l'*architecture standard* de la structure ESF (Event Services Framework) précédemment éditée par IBM Tivoli Netcool Advanced Architecture Group. L'édition à configuration à plusieurs niveaux fournie avec Tivoli Netcool/OMNIbus contient uniquement les composants ESF qui ont trait au contrôle du flux d'événements, à l'intégrité des données et aux performances.

Important : Pour garantir un déploiement sans problème, lisez intégralement toutes les informations fournies ici pour vous familiariser avec les concepts avant de tenter de configurer et de déployer une architecture à plusieurs niveaux.

Avant de commencer

Avant d'installer et de déployer une architecture à plusieurs niveaux, lisez ces informations pour comprendre la méthode de configuration de l'architecture standard, les conventions de dénomination des composants de l'architecture, les considérations sur les ressources pour les composants, la gestion de la gravité et l'emplacement des fichiers de configuration.

Présentation d'une architecture standard à plusieurs niveaux

Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

La figure suivante présente l'architecture standard à plusieurs niveaux. Les composants de l'architecture se trouvent dans trois niveaux (ou couches) : le niveau de collecte, le niveau d'agrégation et le niveau d'affichage. Chaque couche présente les ordinateurs physiques sur lesquels les serveurs ObjectServer et les passerelles du serveur ObjectServer associées résident.

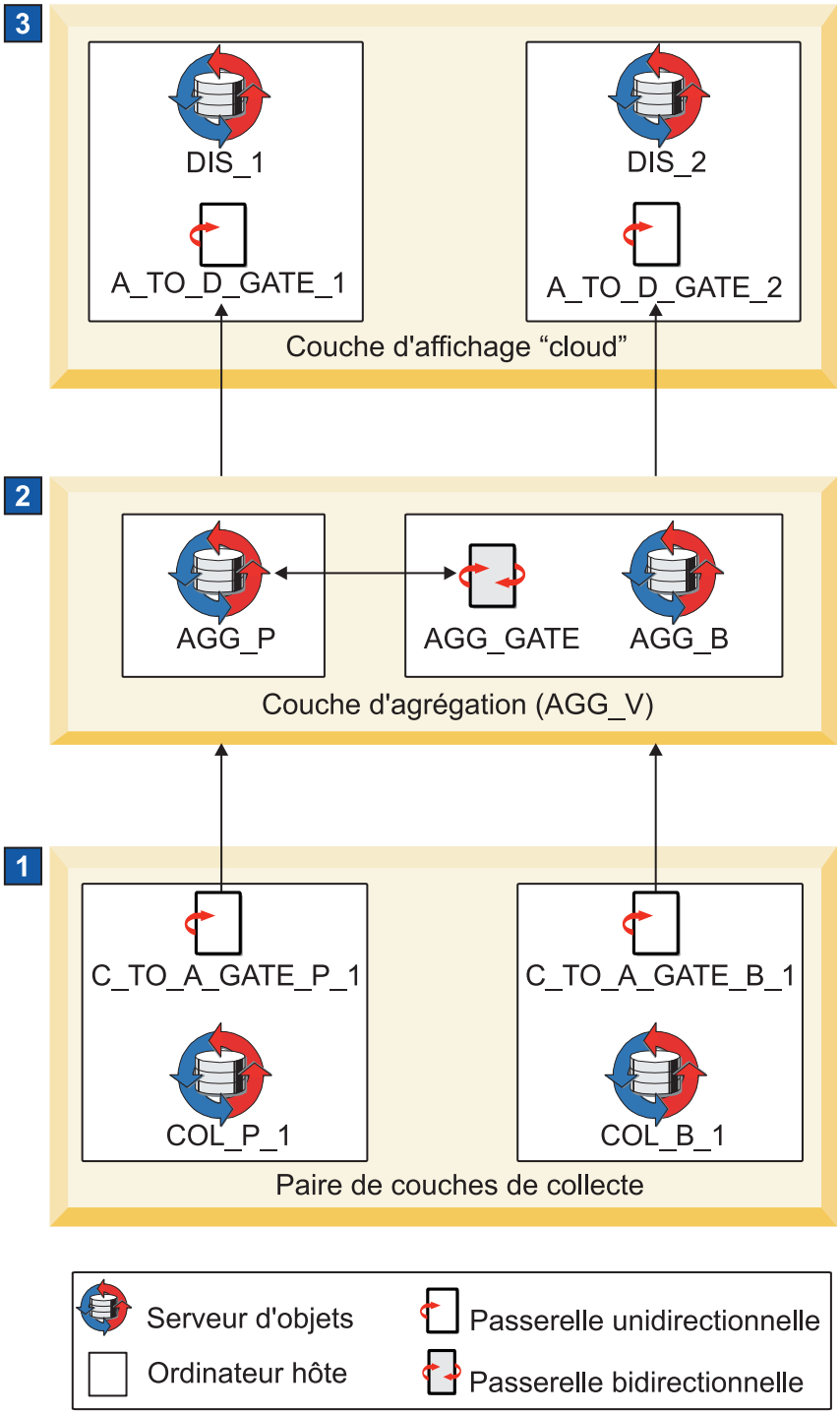

Figure 3. Architecture standard à plusieurs niveaux

Dans la figure, les passerelles unidirectionnelles transfèrent les données en direction de la flèche. L'extrémité de la passerelle qui se connecte au serveur ObjectServer source est connue sous le nom de programme de lecture car elle lit les données à partir de la source. L'extrémité de la passerelle qui se connecte à la cible est connue sous le nom de programme d'écriture car elle écrit les données dans la cible. La passerelle bidirectionnelle de la couche d'agrégation dispose d'un programme de lecture et d'un programme d'écriture à chaque extrémité car les données affluent dans les deux sens.

1 Couche de collecte

La couche de collecte inclut une paire de serveurs ObjectServer principal et de sauvegarde à laquelle les sondes se connectent. La configuration présente une paire de serveurs Objectserver de la couche de collecte, mais d'autres paires peuvent y être ajoutées si nécessaire. (Des détails relatifs à la configuration de paires supplémentaires de serveurs ObjectServer de collecte sont inclus en tant qu'extension de l'architecture standard à plusieurs niveaux. Pour de plus amples informations, voir les liens connexes à la fin de cette rubrique.)

Chaque ObjectServer de la couche de collecte possède sa propre passerelle unidirectionnelle du serveur ObjectServer dédiée qui relie le serveur ObjectServer à la couche d'agrégation. Chaque programme de lecture de passerelle de collecte se connecte, et est fixé, à son serveur Objectserver de collecte dédié, alors que chaque programme d'écriture de passerelle se connecte à la paire de serveurs Objectserver d'agrégation *virtuelle*. Par conséquent, même si les programmes d'écriture peuvent exécuter des opérations de *reprise en ligne* et de *reprise par restauration* entre les serveurs Objectserver principal et de sauvegarde de la couche d'agrégation, le programme de lecture reste connecté uniquement à son serveur Objectserver de collecte dédié.

2 Couche d'agrégation

La couche d'agrégation inclut une paire de serveurs ObjectServer qui est connectée par une passerelle bidirectionnelle du serveur ObjectServer pour que les serveurs restent synchronisés. Notez que la passerelle bidirectionnelle du serveur ObjectServer s'exécute sur l'hôte de sauvegarde.

Tous les programmes d'écriture de passerelle de collecte entrante et tous les programmes de lecture de passerelle d'affichage sortante se connectent à la paire d'agrégation virtuelle, appelée AGG_V, afin que les programmes d'écriture et de lecture puissent exécuter des opérations de reprise en ligne et de reprise par restauration si l'ordinateur ObjectServer d'agrégation principal est indisponible.

3 Couche d'affichage

La couche d'affichage inclut deux serveurs ObjectServer d'affichage autonomes auxquels les utilisateurs de la liste d'événements et les utilisateurs de l'Interface graphique Web se connectent. La configuration inclut deux serveurs ObjectServer de la couche d'affichage, mais des serveurs ObjectServer d'affichage peuvent être ajoutés si nécessaire. (Des détails relatifs à la configuration de paires supplémentaires de serveurs ObjectServer d'affichage sont inclus en tant qu'extension de l'architecture standard à plusieurs niveaux. Pour de plus amples informations, voir les liens connexes à la fin de cette rubrique.)

Chaque ObjectServer de la couche d'affichage possède sa propre passerelle unidirectionnelle du serveur ObjectServer dédiée qui relie le serveur ObjectServer à la couche d'agrégation. Chaque programme de lecture de passerelle d'affichage se connecte à la paire d'agrégation virtuelle alors que chaque programme d'écriture de passerelle se connecte, et est fixé, à son ObjectServer d'affichage dédié. Par conséquent, même si les programmes de lecture peuvent exécuter des opérations de reprise en ligne et de reprise par restauration entre les serveurs Objectserver principal et de sauvegarde de la couche d'agrégation, le programme d'écriture reste connecté uniquement à son serveur Objectserver d'affichage dédié. (Ces connexions de passerelle sont l'opposé des connexions de passerelle dans la couche de collecte.)

Concepts associés:

«Conventions de dénomination pour l'architecture à plusieurs niveaux»
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

«Ajout d'une seconde paire de serveurs ObjectServer de collecte», à la page 246
Si le chargement des serveurs ObjectServer de collecte démarre et atteint presque la limite de capacité, vous pouvez déployer des serveurs ObjectServer de collecte pour partager la charge. Vous pouvez surveiller les données de profilage enregistrées pour déterminer si le temps total utilisé par chaque ObjectServer atteint presque la période de granularité.

«Ajout d'un serveur ObjectServer d'affichage supplémentaire», à la page 251
Si le chargement des serveurs ObjectServer d'affichage démarre et atteint presque la limite de capacité, vous pouvez déployer des serveurs ObjectServer d'affichage pour partager la charge. Vous pouvez surveiller les données de profilage enregistrées pour déterminer si le temps total utilisé par chaque ObjectServer atteint presque la période de granularité. Vous pouvez également choisir de déployer des serveurs ObjectServer supplémentaires si les utilisateurs signalent des temps de réponse lents.

Tâches associées:

«Configuration de l'environnement à plusieurs niveaux standard», à la page 233
Les informations suivantes vous permettent de configurer l'environnement pour l'architecture à plusieurs niveaux standard.

Conventions de dénomination pour l'architecture à plusieurs niveaux

Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Important : Vérifiez que vous utilisez ces conventions de dénomination pour vos serveurs ObjectServer et vos passerelles du serveur ObjectServer. Les fichiers d'importation SQL et les fichiers de configuration de passerelle fournis pour la configuration de l'architecture dépendent de la conformité à ces conventions de dénomination. En particulier, vérifiez que les noms du serveur ObjectServer principal se terminent en _P* et que ceux des serveurs ObjectServer de sauvegarde se terminent en _B*.

Les conventions de dénomination utilisées pour l'architecture standard à plusieurs niveaux sont présentées dans le tableau suivant. Pour chaque composant présenté dans la première colonne, le tableau propose les détails suivants :

- Description : indique ce que le composant représente.
- Convention : indique la convention de dénomination de ce composant, où *n* représente un entier.
- Nom fourni : répertorie des exemples de nom de composant, comme indiqué dans l'architecture standard.
- Nom supplémentaire : fournit des noms suggérés (le cas échéant) pour les composants supplémentaires, lorsque vous en avez ajouté. Notez que les noms supplémentaires ne sont pas obligatoires pour les serveurs ObjectServer d'agrégation et la passerelle d'agrégation car il ne doit exister qu'une seule paire de serveurs ObjectServer d'agrégation et une seule passerelle d'agrégation dans un environnement à plusieurs niveaux.

Tableau 54. Conventions de dénomination pour l'architecture à plusieurs niveaux

Composant	Description	Convention	Nom fourni	Nom supplémentaire
Serveurs ObjectServer de collecte	Serveur Objectserver de collecte *principal n*	COL_P_*n*	COL_P_1	COL_P_2 COL_P_3 ...
	Serveur Objectserver de collecte *de sauvegarde n*	COL_B_*n*	COL_B_1	COL_B_2 COL_B_3 ...
	Paire *virtuelle* de collecte *n*	COL_V_*n*	COL_V_1	COL_V_2 COL_V_3 ...
Passerelles entre la couche de collecte et la couche d'agrégation	Passerelle du serveur Objectserver de collecte *principal n*	C_TO_A_GATE_P_*n*	C_TO_A_GATE_P_1	C_TO_A_GATE_P_2 C_TO_A_GATE_P_3 ...
	Passerelle du serveur Objectserver de collecte *de sauvegarde n*	C_TO_A_GATE_B_*n*	C_TO_A_GATE_B_1	C_TO_A_GATE_B_2 C_TO_A_GATE_B_3 ...
Serveurs Objectserver d'agrégation	Serveur Objectserver d'agrégation *principal*	AGG_P	AGG_P	Non applicable
	Serveur Objectserver d'agrégation *de sauvegarde*	AGG_B	AGG_B	Non applicable
	Paire d'agrégation *virtuelle*	AGG_V	AGG_V	Non applicable
Passerelle d'agrégation	Passerelle d'agrégation	AGG_GATE	AGG_GATE	Non applicable
Passerelles de la couche d'agrégation vers la couche d'affichage	Passerelle du serveur Objectserver d'affichage *n*	A_TO_D_GATE_*n*	A_TO_D_GATE_1 A_TO_D_GATE_2	A_TO_D_GATE_3 A_TO_D_GATE_4 ...
Serveurs Objectserver d'affichage	Serveur Objectserver d'affichage *n*	DIS_*n*	DIS_1 DIS_2	DIS_3 DIS_4 ...

Concepts associés:

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

«Emplacements des fichiers de configuration à plusieurs niveaux», à la page 232
Tous les fichiers de configuration fournis pour la génération de l'architecture à plusieurs niveaux se trouvent dans le répertoire `$NCHOME/omnibus/extensions/multitier`.

Ressources des composants : identification du nombre de serveurs ObjectServer nécessaires

L'architecture standard à plusieurs niveaux est basée sur la couche d'agrégation. Un environnement à un seul niveau, dans lequel un serveur ObjectServer principal et un serveur de sauvegarde sont connectés par une passerelle bidirectionnelle du serveur ObjectServer, est essentiellement une paire d'agrégation sans couche de collecte ou d'affichage connectée.

La conception modulaire de l'architecture standard à plusieurs niveaux signifie que tout système peut démarrer avec une seule paire de serveurs ObjectServer en tant que paire d'agrégation et se voir ajouter ultérieurement des composants de collecte ou d'affichage.

Une approche pragmatique de l'identification des ressources pour une architecture est de démarrer par une paire d'agrégation. Comme les exigences techniques sont implémentées sur le système (par exemple, les sondes déployées, les déclencheurs intégrés, la version de Netcool/Impact déployée, et les utilisateurs ajoutés), des composants supplémentaires peuvent être ajoutés en fonction des informations de profilage générées par les serveurs ObjectServer dans l'architecture.

Sur tous les serveurs ObjectServer de la configuration standard à plusieurs niveaux, le profilage est activé pour mesurer la durée d'exécution des requêtes SQL pour les connexions client. Les informations de profilage sont automatiquement enregistrées dans le fichier `$NCHOME/omnibus/log/`*`nom de serveur`*`_profiler_report.log`*`n`*, si la propriété **Profile** du serveur ObjectServer est définie sur `TRUE`. Par exemple, le journal de profilage du serveur ObjectServer principal (COL_P_1) de la couche de collecte est appelé `COL_P_1_profiler_report.log1`.

Par défaut, la granularité du serveur ObjectServer est de 60 secondes. Cela signifie que toutes les 60 secondes, le serveur ObjectServer enregistre une baisse de ses activités dans les 60 dernières secondes dans le journal de profilage. Voici des exemples de sortie :

```
Thu Nov 20 14:02:50 2008: Individual user profiles:
Thu Nov 20 14:02:50 2008: 'Administrator' (uid = 0) time on IBM-ADAF9B5BAFC: 0.020000s
Thu Nov 20 14:02:50 2008: 'PROBE' (uid = 0) time on devtest12.hursley.ibm.com: 0.000000s
Thu Nov 20 14:02:50 2008: 'isql' (uid = 0) time on devtest12.hursley.ibm.com: 0.000000s
Thu Nov 20 14:02:50 2008: 'GATEWAY' (uid = 0) time on devtest12.hursley.ibm.com: 0.000000s
Thu Nov 20 14:02:50 2008: Grouped user profiles:
Thu Nov 20 14:02:50 2008: Execution time for all connections whose application name is 'Administrator': 0.020000s
Thu Nov 20 14:02:50 2008: Execution time for all connections whose application name is 'PROBE': 0.000000s
Thu Nov 20 14:02:50 2008: Execution time for all connections whose application name is 'isql': 0.000000s
.Thu Nov 20 14:02:50 2008: Execution time for all connections whose application name is 'GATEWAY': 0.000000s
Thu Nov 20 14:02:50 2008: Total time in the report period (59.989325s): 0.020000s
```

Cet exemple de sortie indique qu'un faible volume d'activité se produit sur cet ObjectServer. La seule charge perceptible provient de Netcool/OMNIbus Administrator (0,02 secondes).

Par exemple, si le temps total consommé par les sondes (dans la section `Grouped user profiles` du fichier journal) augmente dans le temps et que la valeur `Total`

`time` approche la barre des 60 secondes, des serveurs ObjectServer de collecte supplémentaires peuvent être envisagés. Si la valeur `Total time` dépasse la période de granularité ou de rapport, il est possible que le serveur ObjectServer soit en retard sur le traitement de sa charge de travail. Si les valeurs `Total time` sont uniquement occasionnellement supérieures à 60 secondes, le serveur ObjectServer rattrape finalement son traitement. Cependant, si les valeurs `Total time` dépassent constamment les 60 secondes, il est possible que le serveur ObjectServer soit encore plus en retard.

Lors d'une exécution dans des conditions normales, il n'est pas prudent que le serveur ObjectServer soit constamment proche de la période de granularité car tous les systèmes doivent avoir un plan d'urgence pour les occurrences de rafales d'événements. Un système de gestion des incidents a une valeur limitée s'il est submergé en cas de crise réseau.

Remarque : Ce n'est pas uniquement l'application des accès logiciels qui protège des situations de rafales d'événements. D'autres aspects, notamment les ressources matérielles et la configuration du fichier de règles pour supprimer les alertes non essentielles, doivent également être pris en compte.

Des principes similaires s'appliquent à l'application des accès des serveurs ObjectServer de la couche d'affichage. Les données de profilage peuvent préciser quand le temps utilisé pour exécuter de manière collective des requêtes client, notamment des mises à jour de liste d'événements, fait s'approcher le temps total de la période de granularité. Ces informations peuvent indiquer lorsqu'il est adéquat de déployer des serveurs ObjectServer de la couche d'affichage.

si les utilisateurs signalent des temps de réponse lents, pensez à déployer des serveurs ObjectServer de la couche d'affichage. Le nombre d'utilisateurs pris en charge par un serveur ObjectServer dépend largement du nombre d'événements sur cet ObjectServer, des filtres en cours d'utilisation et du nombre d'alertes affichées. En règle générale, lorsque le nombre d'utilisateurs dépasse 10, pensez à déployer des serveurs ObjectServer d'affichage pour assurer des temps de réponse utilisateur corrects. Chaque serveur ObjectServer de la couche d'affichage peut prendre en charge jusqu'à 30 utilisateurs. Ce nombre dépend également de facteurs tels que le mode d'affichage des événements et le nombre d'événements.

Gestion de la gravité

Avant de déployer la configuration à plusieurs niveaux, tenez compte de la méthode de gestion de la zone Severity lors du dédoublonnage. Notez que cela s'applique uniquement au dédoublonnage au niveau de la couche d'agrégation.

Dans la configuration à plusieurs niveaux, le paramètre par défaut est de *toujours* mettre à jour la zone Severity lors du dédoublonnage. Cela signifie que toute récurrence entrante du même événement (en d'autres termes, un événement portant la même valeur Identifier) sera toujours mise à jour avec la valeur Severity entrante. Voici quelques implications de cela :

- L'effacement générique par dédoublonnage peut être utilisé pour des gains de performances significatifs.
- Toutes les mises à jour de la gravité sont appliquées à partir du nœud final.
- Toutes les modifications de gravité apportées à un événement par un utilisateur *peuvent être perdues* lors du dédoublonnage.

Le paramètre par défaut donne la priorité à la valeur Severity d'un événement par rapport à la valeur provenant du nœud final. En d'autres termes, l'événement doit

toujours adopter la valeur Severity provenant du nœud final s'il se reproduit. Ce paramètre a été sélectionné par défaut car il est largement utilisé et est nécessaire pour permettre à l'effacement générique par dédoublonnage de fonctionner.

Une approche alternative est le paramètre **Reawaken closed on deduplication**, qui était précédemment fourni dans Netcool/OMNIbus V3.x. Cette méthode accepte une valeur Severity entrante si la valeur actuelle est effacée (c'est-à-dire, définie sur zéro). Sinon, la gravité n'est pas mise à jour. Notez que cela signifie que l'effacement générique par dédoublonnage ne peut pas être utilisé. Cela signifie cependant que les modifications de gravité apportées à un événement à l'initiative de l'utilisateur ne sont pas perdues si l'événement est dédoublonné. Aucune approche n'est plus appropriée que l'autre car elle dépend des exigences du client.

Dans le déclencheur de dédoublonnage fourni dans le fichier `$NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql`, le fragment de code qui traite la zone Severity est contenu dans le déclencheur agg_deduplication et fonctionne de la manière suivante :

```
  ----------------------------------------
  -- GERER LA MISE A JOUR DE LA GRAVITE LORS DU DEDOUBLONNAGE
  ----------------------------------------
  -- VALEUR PAR DEFAUT - TOUJOURS METTRE A JOUR
  set old.Severity = new.Severity;
  ----------------------------------------
  -- REVEILLER UNIQUEMENT LES ZONES FERMEES - METTRE A JOUR UNIQUEMENT SI
LA GRAVITE EST EFFACEE
  -- if ((old.Severity = 0) and (new.Severity > 0)) then
  --
  -- set old.Severity = new.Severity;
  -- end if;
  ----------------------------------------
```

Notez que toutes les lignes sauf la gestion par défaut de la zone Severity sont commentées (c'est-à-dire, précédées de deux tirets). Pour utiliser le paramètre de gestion de la gravité **Reawaken closed on deduplication**, modifiez les lignes du fragment de code précédent de la manière suivante. Les modifications sont mises en évidence en gras. Vous devez commenter le code par défaut et supprimer la mise en commentaire du code **Reawaken closed on deduplication**.

```
  ----------------------------------------
  -- GERER LA MISE A JOUR DE LA GRAVITE LORS DU DEDOUBLONNAGE
  ----------------------------------------
  -- VALEUR PAR DEFAUT - TOUJOURS METTRE A JOUR
  -- set old.Severity = new.Severity;
  ----------------------------------------
  -- REVEILLER UNIQUEMENT LES ZONES FERMEES - METTRE A JOUR UNIQUEMENT SI
LA GRAVITE EST EFFACEE
  if ((old.Severity = 0) and (new.Severity > 0)) then

   set old.Severity = new.Severity;
  end if;
  ----------------------------------------
```

Remarque : Modifiez ce code *avant* d'appliquer le fichier `aggregation.sql` aux serveurs ObjectServer d'agrégation. Notez cependant que le déclencheur de dédoublonnage peut être modifié à tout moment après application de la configuration à plusieurs niveaux à l'aide de Netcool/OMNIbus Administrator (**nco_config**).

Dans certains cas, vos exigences peuvent nécessiter l'implémentation d'une méthode personnalisée de gestion de la gravité. Comme stipulé dans «Création de déclencheurs personnalisés», à la page 257, il est important de conserver le code

personnalisé dans un endroit séparé du code fourni par le fournisseur. L'une des raisons principales est que le code personnalisé n'est pas perdu lorsque de futures mises à jour du fournisseur sont appliquées au code existant.

Si un schéma personnalisé de gestion de la gravité doit être implémenté, commentez les options par défaut dans le code par défaut de la manière suivante et créez un fichier SQL distinct avec un déclencheur de réinsertion distinct :

```
  ----------------------------------------
  -- GERER LA MISE A JOUR DE LA GRAVITE LORS DU DEDOUBLONNAGE
  ----------------------------------------
  -- VALEUR PAR DEFAUT - TOUJOURS METTRE A JOUR
  -- set old.Severity = new.Severity;
  ----------------------------------------
  -- REVEILLER UNIQUEMENT LES ZONES FERMEES - METTRE A JOUR UNIQUEMENT SI
LA GRAVITE EST EFFACEE
  -- if ((old.Severity = 0) and (new.Severity > 0)) then
  --
  -- set old.Severity = new.Severity;
  -- end if;
  ----------------------------------------
```

Tous les fichiers SQL personnalisés doivent être appliqués après les fichiers SQL fournis dans la configuration à plusieurs niveaux à l'aide de l'utilitaire **nco_sql** ou **isql**, de la même manière que les fichiers de configuration à plusieurs niveaux sont appliqués.

Le code suivant présente un exemple de déclencheur de réinsertion personnalisé. Dans cet exemple, la zone Severity est mise à jour uniquement si la valeur entrante est plus élevée que la valeur existante. (Notez que cela ne permet pas à l'effacement générique par dédoublonnage de fonctionner.)

```
 -- CREEZ UN GROUPE DE DECLENCHEURS PERSONNALISE

 CREATE TRIGGER GROUP widgetcom_triggers;
 go

 -- CREEZ LE DECLENCHEUR DE REINSERTION PERSONNALISE

 CREATE OR REPLACE TRIGGER widgetcom_deduplication
 GROUP widgetcom_triggers
 PRIORITY 1
 COMMENT 'Widgetcom insère à nouveau un déclencheur (alerts.status) pour gérer la
zone Severity.'
 BEFORE REINSERT ON alerts.status
 FOR EACH ROW
 begin

  -- METTEZ A JOUR LA VALEUR SEVERITY UNIQUEMENT SI LA VALEUR ENTRANTE EST PLUS
ELEVEE QUE LA VALEUR EXISTANTE
  if (old.Severity < new.Severity) then

   set old.Severity = new.Severity;
  end if;
 end;
 go
```

Pour obtenir des références complètes sur le langage SQL du serveur ObjectServer, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Concepts associés:

«Emplacements des fichiers de configuration à plusieurs niveaux», à la page 232
Tous les fichiers de configuration fournis pour la génération de l'architecture à plusieurs niveaux se trouvent dans le répertoire $NCHOME/omnibus/extensions/

multitier.

Tâches associées:

«Configuration de l'environnement à plusieurs niveaux standard», à la page 233
Les informations suivantes vous permettent de configurer l'environnement pour l'architecture à plusieurs niveaux standard.

Référence associée:

«Création de déclencheurs personnalisés», à la page 257
La configuration d'architecture à plusieurs niveaux fonctionne en contrôlant minutieusement les opérations d'insertion, de réinsertion et de mise à jour des serveurs ObjectServer. Les déclencheurs ont été définis intentionnellement avec une priorité de 2 pour que toutes les opérations d'insertion, de réinsertion ou de mise à jour personnalisées requises puissent être implémentées dans des déclencheurs séparés ayant la priorité 1. Cette définition de priorité garantit que les déclencheurs personnalisés sont exécutés en premier.

Emplacements des fichiers de configuration à plusieurs niveaux

Tous les fichiers de configuration fournis pour la génération de l'architecture à plusieurs niveaux se trouvent dans le répertoire $NCHOME/omnibus/extensions/multitier.

Le sous-répertoire gateway contient les fichiers de définition de mappe personnalisés (.map) suivants, les fichiers de propriétés (.props) et les fichiers de définition de réplication de tables (.tblrep.def), qui peuvent être utilisés pour configurer les passerelles du serveur ObjectServer dans les couches de collecte, d'agrégation et d'affichage:

- A_TO_D_GATE.map
- A_TO_D_GATE.tblrep.def
- A_TO_D_GATE_1.props
- A_TO_D_GATE_2.props
- AGG_GATE.map
- AGG_GATE.props
- AGG_GATE.tblrep.def
- C_TO_A_GATE.map
- C_TO_A_GATE_B_1.props
- C_TO_A_GATE_B_1.tblrep.def
- C_TO_A_GATE_P_1.props
- C_TO_A_GATE_P_1.tblrep.def

Ces fichiers de passerelle sont préconfigurés avec les paramètres requis et doivent être utilisés tel quel. Ces fichiers de passerelle exigent une conformité aux conventions de dénomination pour les serveurs ObjectServer et les passerelles du serveur ObjectServer dans l'architecture à plusieurs niveaux.

Le sous-répertoire objectserver contient les fichiers d'importation SQL personnalisés (.sql) suivants que vous pouvez appliquer aux serveurs ObjectServer dans les couches de collecte, d'agrégation et d'affichage afin de mettre à jour le schéma de base de données avec la configuration à plusieurs niveaux requise :

- aggregation.sql
- aggregation_rollback.sql

- `collection.sql`
- `collection_rollback.sql`
- `display.sql`
- `display_rollback.sql`

Les fichiers SQL fournissent des automatisations qui requièrent une conformité aux conventions de dénomination et généralement :

- Ajoutent des colonnes pertinentes aux tables de base de données.
- Créent les automatisations qui contrôlent le comportement des serveurs ObjectServer, des passerelles du serveur ObjectServer et des clients, ainsi que du flot d'événements à travers ces composants.
- Activent et désactivent les déclencheurs, en fonction des besoins des serveurs ObjectServer.
- Attribuent des droits aux déclencheurs.
- Créent des conversions.
- Annulent les modifications apportées au schéma si nécessaire.

Tous les fichiers sont fournis dans un format en lecture seule. Lors de la configuration de votre environnement à plusieurs niveaux, vous devez exécuter des commandes qui désignent certains des fichiers ou effectuer des copies de certains des fichiers à des fins d'édition.

Utilisez ces fichiers comme indiqué dans les procédures pertinentes.

Concepts associés:

«Conventions de dénomination pour l'architecture à plusieurs niveaux», à la page 226
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Configuration de l'environnement à plusieurs niveaux standard

Les informations suivantes vous permettent de configurer l'environnement pour l'architecture à plusieurs niveaux standard.

Pourquoi et quand exécuter cette tâche

Si vous n'avez pas besoin de serveurs ObjectServer de couche collecte, les étapes de configuration des serveurs ObjectServer de couche collecte ainsi que leurs passerelles respectives peuvent être ignorées. De même, si des serveurs ObjectServer de couche affichage ne sont pas requis, ignorez les étapes de configuration des serveurs ObjectServer de couche affichage et de leurs passerelles respectives. Vous pouvez ajouter à tout moment des serveurs de collecte ou d'affichage ObjectServer à la solution, en fonction de vos besoins.

La procédure est la suivante :

1. Configurez le fichier d'interfaces.
2. Installez le serveur d'agrégation ObjectServer principal.
3. Installez le serveur d'agrégation ObjectServer de secours.
4. Configurez la passerelle d'agrégation ObjectServer bidirectionnelle
5. Installez le serveur de collecte ObjectServer principal.
6. Configurez la passerelle de collecte ObjectServer principale unidirectionnelle

7. Installez le serveur de collecte ObjectServer de secours.
8. Configurez la passerelle de collecte ObjectServer de secours unidirectionnelle
9. Installez le serveur d'affichage ObjectServer 1.
10. Configurez la passerelle d'affichage ObjectServer 1 unidirectionnelle
11. Installez le serveur d'affichage ObjectServer 2.
12. Configurez la passerelle d'affichage ObjectServer 2 unidirectionnelle

Concepts associés:

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

Configuration des informations de communication du serveur (architecture à plusieurs niveaux)

Chaque ordinateur hôte sur lesquel les composants s'exécutent doit être configuré avec des informations de communication de serveur qui permettent aux composants de l'architecture de s'exécuter et de communiquer entre eux.

Pourquoi et quand exécuter cette tâche

Sous UNIX ou Linux, mettez à jour les informations de communication pour tous les composants serveur de votre déploiement en modifiant manuellement le fichier de données de connexion `$NCHOME/etc/omni.dat`, utilisé pour créer le fichier d'interfaces. Nous vous conseillons d'ajouter tous les composants de l'ensemble du déploiement dans un fichier `omni.dat` unique, qui peut ensuite être distribué sur tous les ordinateurs du déploiement. Vous pouvez alors générer le fichier d'interfaces à partir de chaque ordinateur en exécutant la commande **`$NCHOME/bin/nco_igen`**, comme décrit dans des procédures ultérieures. (Les fichiers d'interfaces sont appelés `$NCHOME/etc/interfaces.`*`arch`*, *arch* désignant le système d'exploitation.) Les modèles de fichier `omni.dat` sont fournis pour décrire la configuration des serveurs dans la couche d'agrégation uniquement et dans l'architecture standard à trois niveaux.

Sous Windows, configurez les informations de communication de serveur sur chaque ordinateur à l'aide de l'éditeur de serveurs ; ce dernier est accessible via le menu **Démarrer** > **Tous les programmes** > **NETCOOL Suite** > **Utilitaires système** > **Editeur de serveurs**. Les informations sont sauvegardées dans le fichier de données de connexion `%NCHOME%\ini\sql.ini`.

Important : Vous devez continuer à gérer les informations de communication du serveur sur l'ordinateur hôte et sur chaque ordinateur qui doit se connecter au composant serveur à chaque modification de votre configuration du système.

Concepts associés:

«Conventions de dénomination pour l'architecture à plusieurs niveaux», à la page 226
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Tâches associées:

«Edition manuelle du fichier de données de connexions», à la page 217
Le fichier de données de connexions permet de créer le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus. Dans certains cas, il peut être nécessaire d'éditer le fichier de connexions directement ; par exemple sur les systèmes UNIX qui ne disposent pas d'interface graphique.

Référence associée:

«Modèles de fichier omni.dat», à la page 261
Deux modèles de fichier de données de connexion `$NCHOME/etc/omni.dat` sont fournis ici avec les détails de communication de tous les composants dans une configuration de reprise en ligne de base (couche d'agrégation uniquement), et dans l'architecture à plusieurs niveaux standard. Dans ces fichiers, les composants sont tous signalés comme installés sur le même hôte.

Installation du serveur d'agrégation ObjectServer principal

Pour installer le serveur d'agrégation ObjectServer principal AGG_P et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL d'agrégation fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```
4. Initialisez le serveur ObjectServer AGG_P et incluez le fichier SQL d'importation à appliquer à cet ObjectServer :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_P -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également.
5. Démarrez le serveur ObjectServer AGG_P :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name AGG_P &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur est déjà installé et en cours d'exécution, appliquez le fichier SQL d'agrégation sur le serveur ObjectServer AGG_P comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server AGG_P -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S AGG_P -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\aggregation.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `aggregation_rollback.sql` est fourni pour annuler les modifications apportées par le script `aggregation.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **`nco_sql`** ou **`isql`** avec la syntaxe indiquée pour l'application du script `aggregation.sql`.

Installation du serveur d'agrégation ObjectServer de secours

Pour installer le serveur d'agrégation ObjectServer de secours AGG_B et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL d'agrégation fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :
   ```
   $NCHOME/bin/nco_igen
   ```
4. Initialisez le serveur ObjectServer AGG_B et incluez le fichier SQL d'importation à appliquer à cet ObjectServer :
   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_B -customconfigfile $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```
   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également. Si le nom du serveur ObjectServer se termine par `_B` (conformément aux conventions de dénomination), la propriété **`BackupObjectServer`** est automatiquement définie sur `TRUE` et les automatisations correspondantes requises par le serveur ObjectServer de sauvegarde sont activées.
5. Démarrez le serveur ObjectServer AGG_B :

```
$NCHOME/omnibus/bin/nco_objserv -name AGG_B &
```

L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur est déjà installé et en cours d'exécution, appliquez le fichier SQL d'agrégation sur le serveur ObjectServer AGG_B, comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server AGG_B -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S AGG_B -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\aggregation.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `aggregation_rollback.sql` est fourni pour annuler les modifications apportées par le script `aggregation.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `aggregation.sql`.

Configuration de la passerelle d'agrégation ObjectServer bidirectionnelle

Pour configurer la passerelle d'agrégation ObjectServer bidirectionnelle AGG_GATE, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur d'agrégation ObjectServer de secours AGG_B.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/AGG_GATE.* $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `AGG_GATE.map`
   - `AGG_GATE.props`
   - `AGG_GATE.tblrep.def`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.

2. Démarrez la passerelle AGG_GATE :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_bi -propsfile $NCHOME/omnibus/etc/
   AGG_GATE.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation du serveur de collecte ObjectServer principal

Pour installer le serveur de collecte ObjectServer principal COL_P_1 et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL de collecte fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```

4. Initialisez le serveur ObjectServer COL_P_1 et insérez le fichier d'importation SQL à appliquer à cet ObjectServer :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server COL_P_1 -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également.
5. Démarrez le serveur ObjectServer COL_P_1 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name COL_P_1 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier de collecte SQL sur le serveur ObjectServer COL_P_1, comme suit :

UNIX `$NCHOME/omnibus/bin/nco_sql -server COL_P_1 -user root –password` *`mot_de_passe`* `< $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql`

Windows `"%NCHOME%\omnibus\bin\isql" -S COL_P_1 -U root -P` *`mot_de_passe`* `-i "%NCHOME%\omnibus\extensions\multitier\objectserver\collection.sql"`

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `collection_rollback.sql` est fourni pour annuler les modifications apportées par le script `collection.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `collection.sql`.

Configuration de la passerelle de collecte ObjectServer principale unidirectionnelle

Pour configurer la passerelle de collecte ObjectServer principale unidirectionnelle C_TO_A_GATE_P_1, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur de collecte ObjectServer principal COL_P_1.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE_P_1.*
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `C_TO_A_GATE.map`
   - `C_TO_A_GATE_P_1.props`
   - `C_TO_A_GATE_P_1.tblrep.def`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.

2. Démarrez la passerelle C_TO_A_GATE_P_1 :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
   C_TO_A_GATE_P_1.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation du serveur de collecte ObjectServer de secours

Pour installer le serveur de collecte ObjectServer de secours supplémentaire COL_B_1 et effectuer une personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL de collecte fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.

2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```
4. Initialisez le serveur ObjectServer COL_B_1 et insérez le fichier d'importation SQL à appliquer à cet ObjectServer :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server COL_B_1 -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également.
5. Démarrez le serveur ObjectServer COL_B_1 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name COL_B_1 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier de collecte SQL sur le serveur ObjectServer COL_B_1, comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server COL_B_1 -user root –password
mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/
collection.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S COL_B_1 -U root -P mot_de_passe -i
"%NCHOME%\omnibus\extensions\multitier\objectserver\collection.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `collection_rollback.sql` est fourni pour annuler les modifications apportées par le script `collection.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **`nco_sql`** ou **`isql`** avec la syntaxe indiquée pour l'application du script `collection.sql`.

Configuration de la passerelle de collecte ObjectServer de secours unidirectionnelle

Pour configurer la passerelle de collecte ObjectServer de secours unidirectionnelle C_TO_A_GATE_B_1, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur ObjectServer de collecte de secours COL_B_1.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE_B_1.*
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `C_TO_A_GATE.map`
   - `C_TO_A_GATE_B_1.props`
   - `C_TO_A_GATE_B_1.tblrep.def`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.

2. Démarrez la passerelle C_TO_A_GATE_B_1 :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
   C_TO_A_GATE_B_1.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation du serveur d'affichage ObjectServer 1

Pour installer le serveur d'affichage ObjectServer principal DIS_1 et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez appliquer la personnalisation SQL au serveur ObjectServer à l'aide du fichier SQL d'affichage fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```

4. Initialisez le serveur ObjectServer DIS_1 et incluez le fichier SQL d'importation à appliquer à cet ObjectServer . Les options de ligne de commande supplémentaires `-desktopserver`, `-dsddualwrite` et `-dsdprimary` sont requises pour l'initialisation des serveurs ObjectServer de couche affichage. Notez que l'option de ligne de commande `-dsdprimary` est définie pour indiquer le nom de la paire de serveurs ObjectServer virtuels dans la couche agrégation.

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server DIS_1 -desktopserver
   -dsddualwrite -dsdprimary AGG_V -customconfigfile $NCHOME/omnibus/
   extensions/multitier/objectserver/display.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. Le serveur ObjectServer est créé en tant que serveur ObjectServer de bureau avec le mode écriture double activé. La personnalisation SQL s'applique également.

5. Démarrez le serveur ObjectServer DIS_1 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name DIS_1 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Concepts associés:

Chapitre 12, «Configuration des serveurs ObjectServer de bureau», à la page 325
Vous pouvez configurer une architecture du serveur ObjectServer de bureau pour réduire la charge sur les serveurs ObjectServer qui reçoivent une grande quantité d'événements.

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Lors de la création du serveur ObjectServer, vous devez avoir exécuté la commande **nco_dbinit** avec les options de ligne de commande `-desktopserver`, `-dsddualwrite`, et `-dsdprimary`.

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier SQL d'affichage sur le serveur ObjectServer DIS_1 comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server DIS_1 -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/display.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S DIS_1 -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\display.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `display_rollback.sql` est fourni pour annuler les modifications apportées par le script `display.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `display.sql`.

Configuration de la passerelle d'affichage ObjectServer 1 unidirectionnelle

Pour configurer la passerelle ObjectServer unidirectionnelle A_TO_D_GATE_1 pour le serveur d'affichage ObjectServer DIS_1, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du premier serveur d'affichage ObjectServer DIS_1.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle d'affichage ObjectServer unidirectionnelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.tblrep.def
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE_1.props
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `A_TO_D_GATE.map`
   - `A_TO_D_GATE.tblrep.def`
   - `A_TO_D_GATE_1.props`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.
2. Démarrez la passerelle A_TO_D_GATE_1 :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
   A_TO_D_GATE_1.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation du serveur d'affichage ObjectServer 2

Pour installer le serveur d'affichage ObjectServer secondaire DIS_2 et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez appliquer la personnalisation SQL au serveur ObjectServer à l'aide du fichier SQL d'affichage fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

```
$NCHOME/bin/nco_igen
```

4. Initialisez le serveur ObjectServer DIS_2 et incluez le fichier SQL d'importation à appliquer à cet ObjectServer . Les options de ligne de commande supplémentaires `-desktopserver`, `-dsddualwrite` et `-dsdprimary` sont requises pour l'initialisation des serveurs ObjectServer de couche affichage. Notez que l'option de ligne de commande `-dsdprimary` est définie pour indiquer le nom de la paire de serveurs ObjectServer virtuels dans la couche agrégation.

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server DIS_2 -desktopserver
   -dsddualwrite -dsdprimary AGG_V -customconfigfile $NCHOME/omnibus/
   extensions/multitier/objectserver/display.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. Le serveur ObjectServer est créé en tant que serveur ObjectServer de bureau avec le mode écriture double activé. La personnalisation SQL s'applique également.

5. Démarrez le serveur ObjectServer DIS_2 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name DIS_2 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Concepts associés:

Chapitre 12, «Configuration des serveurs ObjectServer de bureau», à la page 325
Vous pouvez configurer une architecture du serveur ObjectServer de bureau pour réduire la charge sur les serveurs ObjectServer qui reçoivent une grande quantité d'événements.

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution

Pourquoi et quand exécuter cette tâche

Lors de la création du serveur ObjectServer, vous devez avoir exécuté la commande **nco_dbinit** avec les options de ligne de commande `-desktopserver`, `-dsddualwrite`, et `-dsdprimary`.

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier SQL d'affichage sur le serveur ObjectServer DIS_2 comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server DIS_2 -user root –password
mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/
display.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S DIS_2 -U root -P mot_de_passe -i
"%NCHOME%\omnibus\extensions\multitier\objectserver\display.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `display_rollback.sql` est fourni pour annuler les modifications apportées par le script `display.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **`nco_sql`** ou **`isql`** avec la syntaxe indiquée pour l'application du script `display.sql`.

Configuration de la passerelle d'affichage ObjectServer 2 unidirectionnelle

Pour configurer la passerelle ObjectServer unidirectionnelle A_TO_D_GATE_2 pour le serveur d'affichage ObjectServer DIS_2, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du deuxième serveur d'affichage ObjectServer DIS_2.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.tblrep.def
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE_2.props
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `A_TO_D_GATE.map`
   - `A_TO_D_GATE.tblrep.def`
   - `A_TO_D_GATE_2.props`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.

2. Démarrez la passerelle A_TO_D_GATE_2 :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
   A_TO_D_GATE_2.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation de serveurs ObjectServer supplémentaires

Vous pouvez ajouter des serveurs de collecte ou d'affichage ObjectServer à l'architecture à plusieurs niveaux standard. Analysez les besoins de votre environnement et envisagez l'ajout de serveurs de collecte ou d'affichage ObjectServer.

Pourquoi et quand exécuter cette tâche

Ajout d'une seconde paire de serveurs ObjectServer de collecte

Si le chargement des serveurs ObjectServer de collecte démarre et atteint presque la limite de capacité, vous pouvez déployer des serveurs ObjectServer de collecte pour partager la charge. Vous pouvez surveiller les données de profilage enregistrées pour déterminer si le temps total utilisé par chaque ObjectServer atteint presque la période de granularité.

La figure suivante montre une architecture à plusieurs niveaux avec une paire de serveurs de collecte supplémentaire et les passerelles du serveur ObjectServer associées. Notez que les serveurs ObjectServer et la passerelle respectent la convention de dénomination établie précédemment.

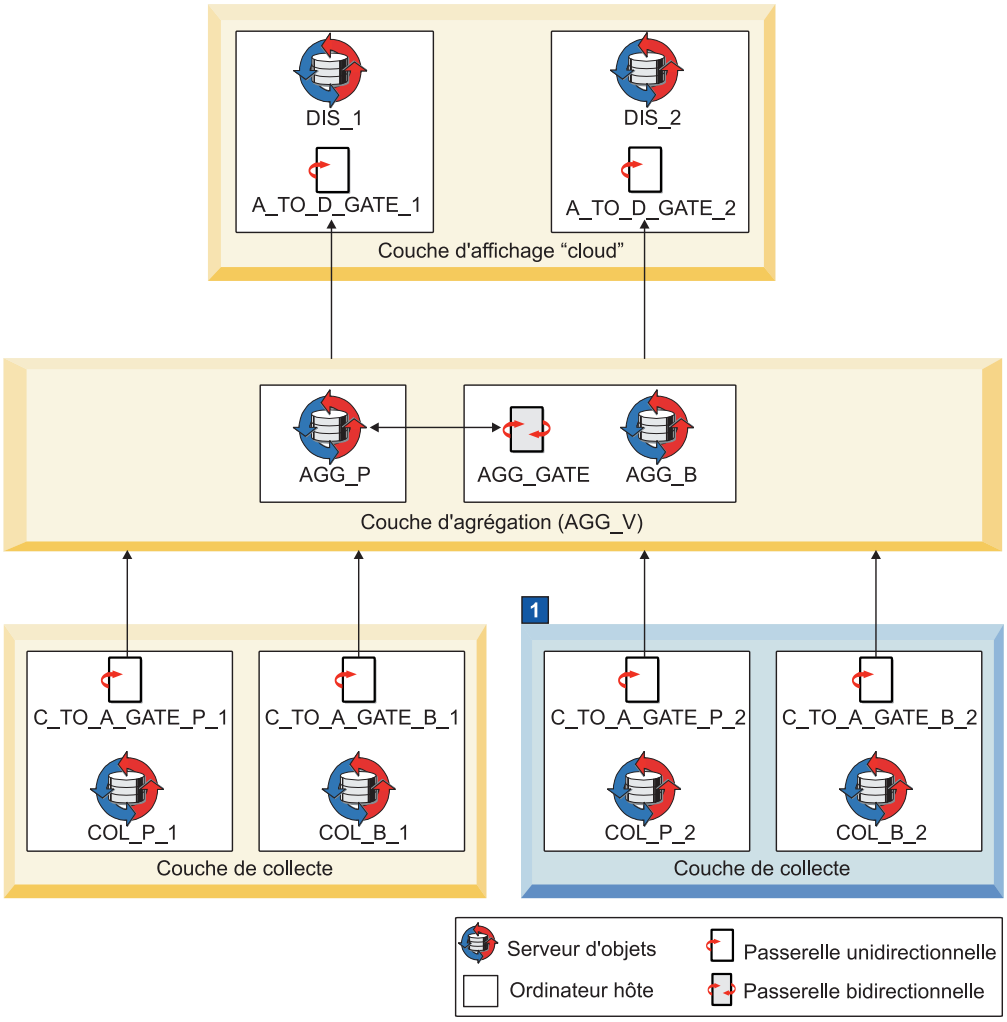

Figure 4. Deuxième paire de serveurs ObjectServer et de passerelles de collecte ajoutée à l'architecture standard à plusieurs niveaux

1 Deuxième paire de serveurs ObjectServer et passerelles unidirectionnelles du serveur ObjectServer dans la couche de collecte

Les serveurs ObjectServer sont présentés comme paire principale et de sauvegarde dans la couche de collecte dans la partie inférieure droite de la figure. Ce déploiement d'une deuxième paire de serveurs ObjectServer de collecte respecte un processus similaire à la paire d'origine dans

l'architecture standard. Chaque ObjectServer possède sa propre passerelle unidirectionnelle du serveur ObjectServer qui se connecte au serveur ObjectServer au niveau de la couche d'agrégation.

Vous pouvez déployer autant de paires de serveurs ObjectServer dans la couche de collecte que nécessaire pour répondre à vos exigences.

Concepts associés:

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

«Conventions de dénomination pour l'architecture à plusieurs niveaux», à la page 226
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Installation d'un serveur de collecte ObjectServer principal supplémentaire

Pour installer le serveur de collecte ObjectServer principal supplémentaire COL_P_2 et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL de collecte fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```
4. Initialisez le serveur ObjectServer COL_P_2 et insérez le fichier d'importation SQL à appliquer à cet ObjectServer :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server COL_P_2 -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également.
5. Démarrez le serveur ObjectServer COL_P_2 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name COL_P_2 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution :
Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier de collecte SQL sur le serveur ObjectServer COL_P_2, comme suit :

UNIX `$NCHOME/omnibus/bin/nco_sql -server COL_P_2 -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql`

Windows `"%NCHOME%\omnibus\bin\isql" -S COL_P_2 -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\collection.sql"`

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `collection_rollback.sql` est fourni pour annuler les modifications apportées par le script `collection.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `collection.sql`.

Configuration d'une passerelle de collecte ObjectServer principale unidirectionnelle supplémentaire

Pour configurer la passerelle de collecte ObjectServer principale unidirectionnelle supplémentaire C_TO_A_GATE_P_2, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur de collecte ObjectServer principal supplémentaire COL_P_2.

Pourquoi et quand exécuter cette tâche

Pour configurer une passerelle supplémentaire :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE_P_1.*
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `C_TO_A_GATE.map`
   - `C_TO_A_GATE_P_1.props`
   - `C_TO_A_GATE_P_1.tblrep.def`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.
2. Supprimez les droits de lecture seule de ces trois fichiers puis renommez les fichiers suivants :

```
cd $NCHOME/omnibus/etc
mv C_TO_A_GATE_P_1.props C_TO_A_GATE_P_2.props
mv C_TO_A_GATE_P_1.tblrep.def C_TO_A_GATE_P_2.tblrep.def
```

Les fichiers du répertoire `$NCHOME/omnibus/etc` doivent désormais s'appeler : `C_TO_A_GATE.map`, `C_TO_A_GATE_P_2.props`, et `C_TO_A_GATE_P_2.tblrep.def`.

3. Editez le fichier `C_TO_A_GATE_P_2.props` et modifiez uniquement les lignes suivantes :

```
MessageLog                          : '$OMNIHOME/log/C_TO_A_GATE_P_2.log'
Name                                : 'C_TO_A_GATE_P_2'
Gate.Reader.Server                  : 'COL_P_2'
Gate.Reader.TblReplicateDefFile     : '$OMNIHOME/etc/C_TO_A_GATE_P_2.tblrep.def'
Gate.Writer.SAFFile                 : '$OMNIHOME/var/objserv_uni/C_TO_A_GATE_P_2.store'
```

4. Editez le fichier `C_TO_A_GATE_P_2.tblrep.def` et modifiez uniquement la ligne suivante :

```
CACHE FILTER 'SourceServerName = \'COL_P_2\'';
```

5. Démarrez la passerelle C_TO_A_GATE_P_2 :

```
$NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
C_TO_A_GATE_P_2.props &
```

L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Installation d'un serveur de collecte ObjectServer de secours supplémentaire

Pour installer le serveur de collecte ObjectServer de secours supplémentaire COL_B_2 et effectuer une personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez lui appliquer la personnalisation SQL en utilisant le fichier SQL de collecte fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

```
$NCHOME/bin/nco_igen
```

4. Initialisez le serveur ObjectServer COL_B_2 et insérez le fichier SQL d'importation à appliquer à ce serveur :

```
$NCHOME/omnibus/bin/nco_dbinit -server COL_B_2 -customconfigfile
$NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
```

Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. La personnalisation SQL s'applique également.

5. Démarrez le serveur ObjectServer COL_B_2 :

```
$NCHOME/omnibus/bin/nco_objserv -name COL_B_2 &
```

L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution :
Pourquoi et quand exécuter cette tâche

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier SQL de collecte sur le serveur ObjectServer COL_B_2, comme suit :

UNIX `$NCHOME/omnibus/bin/nco_sql -server COL_B_2 -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/collection.sql`

Windows `"%NCHOME%\omnibus\bin\isql" -S COL_B_2 -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\collection.sql"`

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `collection_rollback.sql` est fourni pour annuler les modifications apportées par le script `collection.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `collection.sql`.

Configuration d'une passerelle de collecte ObjectServer de secours unidirectionnelle supplémentaire

Pour configurer la passerelle de collecte ObjectServer de secours unidirectionnelle supplémentaire C_TO_A_GATE_B_2, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur de collecte ObjectServer de secours supplémentaire COL_B_2.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle supplémentaire :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE.map
   $NCHOME/omnibus/etc/.
   ```

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/C_TO_A_GATE_B_1.*
   $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `C_TO_A_GATE.map`
   - `C_TO_A_GATE_B_1.props`
   - `C_TO_A_GATE_B_1.tblrep.def`

   Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis `%NCHOME%\omnibus\extensions\multitier\gateway` et les coller dans `%NCHOME%\omnibus\etc`.
2. Supprimez les droits de lecture seule de ces trois fichiers puis renommez les fichiers suivants :

```
cd $NCHOME/omnibus/etc
mv C_TO_A_GATE_B_1.props C_TO_A_GATE_B_2.props
mv C_TO_A_GATE_B_1.tblrep.def C_TO_A_GATE_B_2.tblrep.def
```

Les fichiers du répertoire $NCHOME/omnibus/etc doivent désormais s'appeler : C_TO_A_GATE.map, C_TO_A_GATE_B_2.props, et C_TO_A_GATE_B_2.tblrep.def.

3. Editez le fichier C_TO_A_GATE_B_2.props et modifiez uniquement les lignes suivantes :

```
MessageLog                          : '$OMNIHOME/log/C_TO_A_GATE_B_2.log'
Name                                : 'C_TO_A_GATE_B_2'
Gate.Reader.Server                  : 'COL_B_2'
Gate.Reader.TblReplicateDefFile     : '$OMNIHOME/etc/C_TO_A_GATE_B_2.tblrep.def'
Gate.Writer.SAFFile                 : '$OMNIHOME/var/objserv_uni/C_TO_A_GATE_B_2.store'
```

4. Editez le fichier C_TO_A_GATE_B_2.tblrep.def et modifiez uniquement la ligne suivante :

```
CACHE FILTER 'ServerName = \'COL_B_2\'';
```

5. Démarrez la passerelle C_TO_A_GATE_B_2 :

```
$NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
C_TO_A_GATE_B_2.props &
```

L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Ajout d'un serveur ObjectServer d'affichage supplémentaire

Si le chargement des serveurs ObjectServer d'affichage démarre et atteint presque la limite de capacité, vous pouvez déployer des serveurs ObjectServer d'affichage pour partager la charge. Vous pouvez surveiller les données de profilage enregistrées pour déterminer si le temps total utilisé par chaque ObjectServer atteint presque la période de granularité. Vous pouvez également choisir de déployer des serveurs ObjectServer supplémentaires si les utilisateurs signalent des temps de réponse lents.

La figure suivante montre une architecture à plusieurs niveaux avec un serveur ObjectServer d'affichage supplémentaire et la passerelle du serveur ObjectServer associée. Notez que le serveur ObjectServer et la passerelle respectent la convention de dénomination établie précédemment.

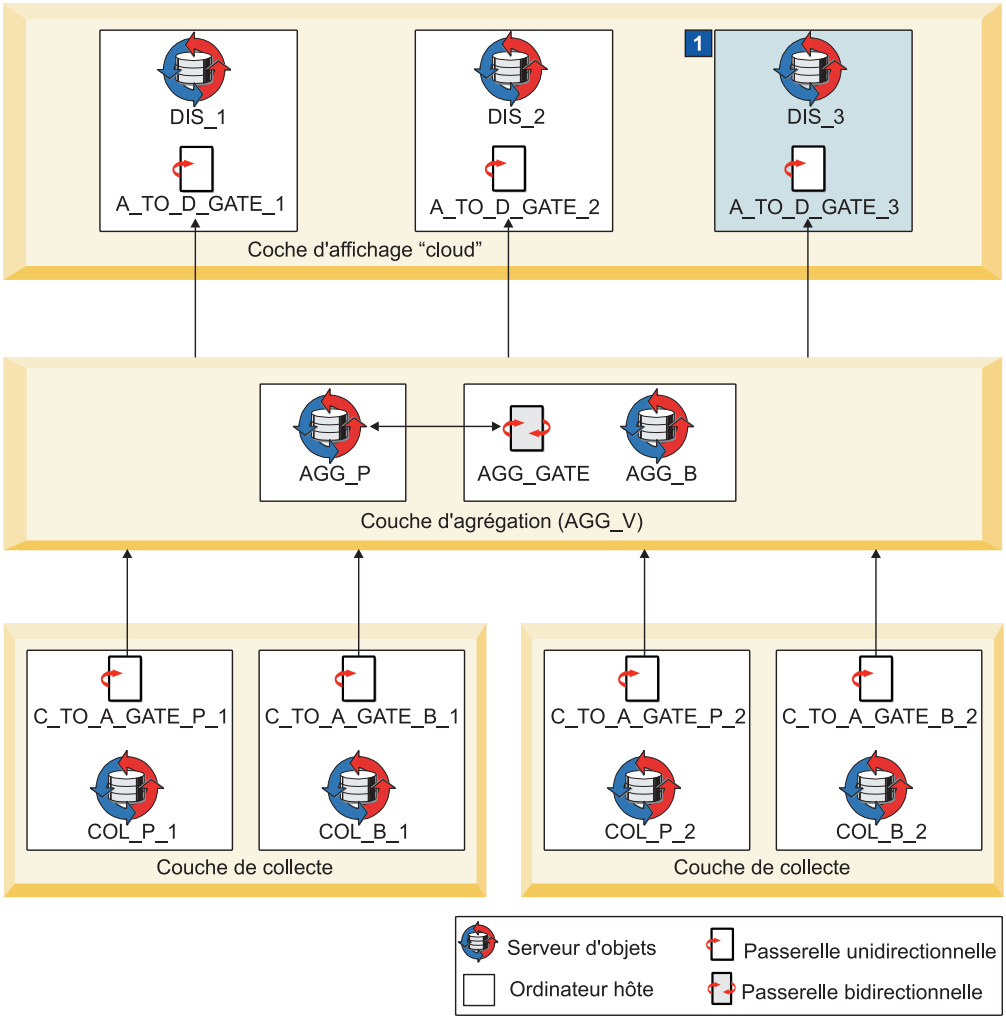

Figure 5. ObjectServer et passerelle d'affichage supplémentaires ajoutés à l'architecture à plusieurs niveaux

1 ObjectServer supplémentaire et passerelle unidirectionnelle du serveur ObjectServer dans la couche d'affichage

Le serveur ObjectServer est indiqué dans la couche d'affichage dans la partie supérieure droite de la figure. Ce déploiement d'un serveur ObjectServer d'affichage supplémentaire respecte un processus similaire aux processus initiaux dans l'architecture. Le serveur ObjectServer d'affichage dispose de sa propre passerelle unidirectionnelle du serveur ObjectServer dédiée qui se connecte au serveur ObjectServer au niveau de la couche d'agrégation.

Vous pouvez déployer autant de serveurs ObjectServer dans la couche d'affichage que nécessaire pour répondre à vos exigences.

Concepts associés:

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

«Conventions de dénomination pour l'architecture à plusieurs niveaux», à la page 226
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Installation d'un serveur d'affichage ObjectServer supplémentaire

Pour installer un serveur ObjectServer d'affichage supplémentaire DIS_3 et appliquer la personnalisation SQL, procédez comme suit. Si le serveur ObjectServer est déjà installé et en cours d'exécution, vous pouvez appliquer la personnalisation SQL au serveur ObjectServer à l'aide du fichier SQL d'affichage fourni.

Pourquoi et quand exécuter cette tâche

Pour installer et configurer le serveur ObjectServer :

Procédure

1. Installez Tivoli Netcool/OMNIbus et veillez à sélectionner tous les composants pour l'installation.
2. Assurez-vous que le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini` est configuré avec tous les détails des composants.
3. UNIX Générez le fichier d'interfaces comme suit :

   ```
   $NCHOME/bin/nco_igen
   ```
4. Initialisez le serveur ObjectServer DIS_3 et incluez le fichier SQL d'importation à appliquer à ce serveur. Les options de ligne de commande supplémentaires `-desktopserver`, `-dsddualwrite` et `-dsdprimary` sont requises pour l'initialisation des serveurs ObjectServer de couche affichage. Notez que l'option de ligne de commande `-dsdprimary` est définie pour indiquer le nom de la paire de serveurs ObjectServer virtuels dans la couche agrégation.

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server DIS_3 -desktopserver
   -dsddualwrite -dsdprimary AGG_V -customconfigfile $NCHOME/omnibus/
   extensions/multitier/objectserver/display.sql
   ```

   Le fichier de propriétés et les tables, données, utilisateurs, groupes et rôles de base de données par défaut sont créés pour le serveur ObjectServer. Le serveur ObjectServer est créé en tant que serveur ObjectServer de bureau avec le mode écriture double activé. La personnalisation SQL s'applique également.
5. Démarrez le serveur ObjectServer DIS_3 :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name DIS_3 &
   ```

   L'initialisation du serveur ObjectServer est confirmée et ce dernier entre à l'état RUN.

Concepts associés:

Chapitre 12, «Configuration des serveurs ObjectServer de bureau», à la page 325
Vous pouvez configurer une architecture du serveur ObjectServer de bureau pour réduire la charge sur les serveurs ObjectServer qui reçoivent une grande quantité d'événements.

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Application de la personnalisation SQL sur un serveur ObjectServer en cours d'exécution :
Pourquoi et quand exécuter cette tâche

Lors de la création du serveur ObjectServer, vous devez avoir exécuté la commande **nco_dbinit** avec les options de ligne de commande `-desktopserver`, `-dsddualwrite`, et `-dsdprimary`.

Pour appliquer la personnalisation SQL lorsque le serveur ObjectServer est déjà installé et en cours d'exécution, appliquez le fichier SQL d'affichage sur le serveur ObjectServer DIS_3, comme suit :

UNIX
```
$NCHOME/omnibus/bin/nco_sql -server DIS_3 -user root –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/display.sql
```

Windows
```
"%NCHOME%\omnibus\bin\isql" -S DIS_3 -U root -P mot_de_passe -i "%NCHOME%\omnibus\extensions\multitier\objectserver\display.sql"
```

Une connexion en tant qu'utilisateur root avec un mot de passe privilégié est supposée.

Conseil : Dans le répertoire `$NCHOME/omnibus/extensions/multitier/objectserver`, le script `display_rollback.sql` est fourni pour annuler les modifications apportées par le script `display.sql` au serveur ObjectServer, le cas échéant. Vous pouvez appliquer ce script d'annulation à l'aide de l'utilitaire **nco_sql** ou **isql** avec la syntaxe indiquée pour l'application du script `display.sql`.

Configuration d'une passerelle d'affichage ObjectServer unidirectionnelle supplémentaire

Pour configurer une passerelle ObjectServer unidirectionnelle supplémentaire A_TO_D_GATE_3 pour le serveur d'affichage ObjectServer DIS_3, procédez comme suit. Notez que l'installation de Tivoli Netcool/OMNIbus n'est pas nécessaire car la passerelle est configurée sur le même ordinateur hôte que celui du serveur d'affichage ObjectServer supplémentaire DIS_3.

Pourquoi et quand exécuter cette tâche

Pour configurer la passerelle d'affichage ObjectServer unidirectionnelle :

Procédure

1. UNIX Copiez les fichiers de propriétés à plusieurs niveaux pour la passerelle dans l'emplacement par défaut dans lequel sont conservés les fichiers de configuration et de propriétés :

   ```
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.map $NCHOME/omnibus/etc/.
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE.tblrep.def $NCHOME/omnibus/etc/.
   cp $NCHOME/omnibus/extensions/multitier/gateway/A_TO_D_GATE_1.props $NCHOME/omnibus/etc/.
   ```

   Les fichiers suivants sont copiés dans `$NCHOME/omnibus/etc` :

   - `A_TO_D_GATE.map`
   - `A_TO_D_GATE.tblrep.def`

- A_TO_D_GATE_1.props

Windows Vous pouvez utiliser Windows Explorer pour copier ces fichiers depuis %NCHOME%\omnibus\extensions\multitier\gateway et les coller dans %NCHOME%\omnibus\etc.

2. Supprimez les droits de lecture seule de ces trois fichiers puis renommez le fichier suivant :

   ```
   cd $NCHOME/omnibus/etc
   mv A_TO_D_GATE_1.props A_TO_D_GATE_3.props
   ```

   Les fichiers du répertoire $NCHOME/omnibus/etc doivent désormais s'appeler : A_TO_D_GATE.map, A_TO_D_GATE.tblrep.def et A_TO_D_GATE_3.props.

3. Editez le fichier A_TO_D_GATE_3.props et modifiez uniquement les lignes suivantes :

   ```
   MessageLog                          : '$OMNIHOME/log/A_TO_D_GATE_3.log'
   Name                                : 'A_TO_D_GATE_3'
   Gate.Writer.Server                  : 'DIS_3'
   Gate.Writer.SAFFile                 : '$OMNIHOME/var/objserv_uni/A_TO_D_GATE_3.store'
   ```

4. Démarrez la passerelle A_TO_D_GATE_3 :

   ```
   $NCHOME/omnibus/bin/nco_g_objserv_uni -propsfile $NCHOME/omnibus/etc/
   A_TO_D_GATE_3.props &
   ```

   L'initialisation de la passerelle est confirmée et cette dernière entre à l'état RUN.

Equilibrage automatique des charges des clients de liste d'événements

Les serveurs d'affichage serveurs ObjectServer peuvent être configurés pour équilibrer automatiquement les charges des listes d'événements qui s'y connectent. Une fois configurés, les utilisateurs font automatiquement l'objet d'un équilibrage de charge via les serveurs d'affichage ObjectServer disponibles, indépendamment du serveur d'affichage ObjectServer sélectionné au moment de la connexion de l'utilisateur.

L'équilibrage des charges est implémenté en renseignant la table master.servergroups des serveurs d'affichage ObjectServer. La table master.servergroups de chaque serveur d'affichage ObjectServer contient les mêmes informations : une ligne pour chaque serveur d'affichage ObjectServer dans la conception de l'architecture. Lorsque les utilisateurs se connectent, la liste d'événements interroge le contenu de la table, sélectionne un serveur d'affichage ObjectServer (en fonction d'un algorithme interne), puis se connecte à ce serveur. L'équilibrage de charges qui en résulte n'est pas réparti de manière entièrement équitable.

Remarque : Le contenu de la table master.servergroups est ignoré, à moins que la table master.national ne comporte une entrée. La table master.national est automatiquement renseignée pour les serveurs ObjectServer de couche affichage par le fichier de configuration $NCHOME/omnibus/extensions/multitier/display.sql.

Le fichier d'agrégation SQL $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql contient les lignes de code suivantes, destinées à renseigner la table master.servergroups avec les détails des deux serveurs d'affichage ObjectServer de l'architecture à plusieurs niveaux standard :

```
--------------------------------------------------------------------------------
-- INITIALISE LOAD-BALANCING FOR THE DISPLAY OBJECTSERVERS
-- NOT ENABLED BY DEFAULT
```

```
DELETE FROM master.servergroups;
go
-- INSERT INTO master.servergroups VALUES('DIS_1',1,1);
-- INSERT INTO master.servergroups VALUES('DIS_2',1,1);
-- go
```

Les données sont insérées au niveau de l'agrégation car la table master.servergroups est configurée pour effectuer automatiquement la réplication des serveurs d'agrégation ObjectServer vers les serveurs d'affichage ObjectServer. L'avantage est que les informations doivent uniquement être mises à jour à un endroit si des serveurs d'affichage ObjectServer supplémentaires sont ajoutés ultérieurement. De même, cette procédure garantit que tous les serveurs d'affichage ObjectServer contiennent les mêmes données, réduisant ainsi les risques d'erreurs.

Pour activer l'équilibrage automatique des charges pour les listes d'événements :

1. Copiez le fichier `$NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql` à un emplacement différent puis supprimez les droits de lecture seule.
2. Modifiez le fichier `aggregation.sql` en supprimant la mise en commentaire des deux instructions INSERT et du mot clé go, comme suit :

   ```
   ------------------------------------------------------------------------------
   -- INITIALISE LOAD-BALANCING FOR THE DISPLAY OBJECTSERVERS
   -- NOT ENABLED BY DEFAULT
   DELETE FROM master.servergroups;
   go
   INSERT INTO master.servergroups VALUES('DIS_1',1,1);
   INSERT INTO master.servergroups VALUES('DIS_2',1,1);
   go
   ```

   Dans chaque instruction INSERT, la première valeur (DIS_1 ou DIS_2) renseigne la colonne ServerName de la table. La deuxième valeur (1) renseigne la colonne GroupID et la troisième valeur (1) renseigne la colonne Weight. Si vous souhaitez que deux fois plus d'utilisateurs se connectent au serveur ObjectServer DIS_1 qu'au serveur DIS_2, par exemple, définissez la pondération de DIS_1 sur 2 et celle de DIS_2 sur 1.
3. Enregistrez et fermez le fichier.

   Vous devez à présent appliquer le fichier aux serveurs d'agrégation ObjectServer en utilisant la commande **nco_sql** (UNIX) ou **isql** (Windows).

Inclusion de serveurs d'affichage ObjectServer supplémentaires dans la configuration d'équilibrage des charges

Si des serveurs d'affichage ObjectServer supplémentaires sont ajoutés à la configuration, vous devez insérer des lignes supplémentaires dans le fichier `aggregation.sql` modifié afin d'inclure les serveurs d'affichage ObjectServer supplémentaires dans l'équilibrage des charges. Par exemple, si ObjectServer DIS_3 est ajouté à la couche affichage, ajoutez une troisième instruction INSERT comme suit :

```
------------------------------------------------------------------------------
-- INITIALISE LOAD-BALANCING FOR THE DISPLAY OBJECTSERVERS
-- NOT ENABLED BY DEFAULT
DELETE FROM master.servergroups;
go
INSERT INTO master.servergroups VALUES('DIS_1',1,1);
INSERT INTO master.servergroups VALUES('DIS_2',1,1);
INSERT INTO master.servergroups VALUES('DIS_3',1,1);
go
```

Vous pouvez appliquer le fichier `aggregation.sql` plusieurs fois aux serveurs d'agrégation ObjectServer :

- Vous pouvez ajouter des valeurs supplémentaires au fichier puis appliquer ce dernier au serveur d'agrégation ObjectServer principal.
- Vous pouvez modifier la table master.servergroups sur le serveur ObjectServer d'agrégation principal à l'aide de Netcool/OMNIbus Administrator (**`nco_config`**) ou de l'interface interactive SQL (**`nco_sql`** ou **`isql`**).

  Tout ajout ou modification est automatiquement diffusée au serveur d'agrégation ObjectServer de secours et à tous les serveurs d'affichage ObjectServer via les passerelles.

Remarque : Les applications ultérieures du fichier `aggregation.sql` peuvent générer des erreurs. Ces erreurs se produisent car l'instruction SQL tente de créer des zones qui existent déjà ou d'insérer des lignes existantes. Vous pouvez ignorer ces erreurs.

Concepts associés:

«Mode équilibrage de charges», à la page 333
Dans une configuration dans laquelle se trouve un groupe de serveurs ObjectServer de bureau, il est très probable que le nombre d'utilisateurs de liste d'événements connectés dans chaque ObjectServer de bureau ne soit pas pair. Dans certains cas, tous les utilisateurs peuvent être connectés à un serveur ObjectServer de bureau, laissant les serveurs ObjectServer de bureau restants en veille.

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

Création de déclencheurs personnalisés

La configuration d'architecture à plusieurs niveaux fonctionne en contrôlant minutieusement les opérations d'insertion, de réinsertion et de mise à jour des serveurs ObjectServer. Les déclencheurs ont été définis intentionnellement avec une priorité de 2 pour que toutes les opérations d'insertion, de réinsertion ou de mise à jour personnalisées requises puissent être implémentées dans des déclencheurs séparés ayant la priorité 1. Cette définition de priorité garantit que les déclencheurs personnalisés sont exécutés en premier.

Les instructions pour la création de déclencheurs personnalisés sont :

- Créez toujours un groupe de déclencheurs pour les déclencheurs personnalisés ; par exemple, déclencheurs_x_clients.
- Ne modifiez pas les déclencheurs par défaut ; créez-en de nouveaux et stockez-les à part.

  Conseil : La raison principale pour la création de groupes de déclencheurs et de déclencheurs distincts pour les fonctionnalités personnalisées est d'éliminer le risque d'écrasement de ces fonctionnalités. Si les déclencheurs par défaut n'ont pas été modifiés, ils peuvent être remplacés en toute sécurité par des versions mises à jour, si nécessaire pour les versions de produit futures.

Exemple 1

Vous souhaitez ajouter une nouvelle zone personnalisée qui doit être mise à jour lors du dédoublonnage. Les étapes typiques à effectuer sont les suivantes :

1. Ajouter des zones personnalisées à tous les serveurs ObjectServer.
2. Ajouter des zones personnalisées à tous les fichiers de mappage de passerelle.
3. Créer un nouveau groupe de déclencheurs sur les serveurs de collection et d'agrégation ObjectServer ; par exemple, déclencheurs_x.
4. Créer un nouveau déclencheur de réinsertion sur les serveurs de collection et d'agrégation ObjectServer. Définissez la priorité du déclencheur sur 1 et affectez-le au nouveau groupe de déclencheurs. Mettez à jour l'action de déclencheur pour inclure les lignes de code requises pour mettre à jour la zone. Par exemple :

```
set old.MyField = new.MyField;
```

Exemple 2

Vous souhaitez maintenant ajouter un déclencheur qui effectue des corrélations personnalisées. Les étapes typiques à effectuer sont les suivantes :

1. Créer un nouveau déclencheur temporel sur les serveurs d'agrégation ObjectServer principal et de secours.
2. Définir la priorité du déclencheur sur 1, sélectionner une durée de nombre premiers adaptée (par exemple, 61 secondes) et affecter le déclencheur au groupe de déclencheurs primaire_seul pour garantir que le déclencheur soit activé et désactivé correctement sur le serveur ObjectServer de secours.

Les déclencheurs qui effectuent une corrélation doivent uniquement être exécutés sur le serveur ObjectServer principal ou de secours. Par conséquent, le nouveau déclencheur temporel est affecté au groupe principal_seul car ce groupe est automatiquement activé ou désactivé si le serveur d'agrégation ObjectServer principal échoue ou démarre.

Remarque : Lors de la conception d'un déclencheur, déterminez s'il doit être exécuté simultanément sur les serveurs d'agrégation ObjectServer principal et de secours ou uniquement sur le serveur d'agrégation ObjectServer principal actif.

Déclencheurs de performances

Lorsque vous configurez un environnement à plusieurs niveaux, les scripts SQL fournis ajoutent des déclencheurs et des zones qui permettent aux utilisateurs de listes d'événements de voir le temps nécessaire pour que les alertes atteignent le serveur ObjectServer de la couche d'affichage auquel ils sont connectés. Ces données de performances fournissent un retour utile concernant la santé générale de votre système.

La figure suivante illustre une liste d'événements qui comprend l'une des nouvelles zones (TimeToDisplay) ajoutée aux serveurs ObjectServer de couche d'affichage. La zone TimeToDisplay affiche le nombre de secondes calculé à partir de l'heure de l'insertion initiale d'un événement sur un serveur ObjectServer, jusqu'à l'heure de son insertion sur le serveur ObjectServer actuel.

De plus, un événement synthétique est généré sur chaque serveur d'affichage ObjectServer pour informer les utilisateurs de la durée moyenne nécessaire pour afficher *tous* les événements actuellement sur le serveur d'affichage ObjectServer

auquel les utilisateurs sont connectés. (Sur la figure, l'événement synthétique est affiché en tant que première ligne de la liste d'événements.)

Remarque : La valeur TimeToDisplay moyenne est généralement comprise entre 20 et 40 secondes dans un environnement à trois niveaux.

Serveur source	Noeud	Récapitulatif	Dernière occurrence	Compte	Type	Délai d'affichage
DIS_1	DIS_1	Délai moyen pour l'affichage des événements...	29/12/2008	1	Informations	0
COL_P_1	Test2	Evénement de test 2	29/12/2008	1	Incident	27
COL_P_1	Test3	Evénement de test 3	29/12/2008	1	Incident	27
COL_P_1	Test4	Evénement de test 4	29/12/2008	1	Incident	27
COL_P_1	Test5	Evénement de test 5	29/12/2008	1	Incident	27
COL_P_1	myhost	Processus sur myhost connecté	29/12/2008	1	Incident	27
COL_P_1	myhost	Processus sur myhost déconnecté	29/12/2008	1	Résolution	27
COL_P_1	Test1	Evénement de test 1	29/12/2008	1	Incident	30
COL_P_1	Test2	Evénement de test 2	29/12/2008	1	Incident	30
COL_P_1	Test3	Evénement de test 3	29/12/2008	1	Incident	30
COL_P_1	Test4	Evénement de test 4	29/12/2008	1	Incident	30
COL_P_1	Test5	Evénement de test 5	29/12/2008	1	Incident	30

Figure 6. Liste d'événements présentant la zone TimeToDisplay et l'événement synthétique

Les données de performances peuvent occasionnellement être plus élevées, par exemple lors du redémarrage d'une passerelle d'affichage. Lorsque la passerelle est redémarrée, une resynchronisation complète est initiée et le serveur d'affichage ObjectServer correspondant est actualisé avec les données d'événement provenant de la couche d'agrégation. Etant donné que l'horodatage d'affichage est défini sur l'heure à laquelle l'événement a été inséré sur le serveur d'affichage ObjectServer, ces horodatages sont tous actualisés pour afficher l'heure actuelle.

Lorsque la métrique TimeToDisplay est calculée ultérieurement, la valeur est incorrecte (c'est-à-dire plus élevée) car le calcul compare l'heure actuelle à l'heure d'insertion de l'événement dans la couche d'agrégation. (L'insertion dans cette couche peut avoir été effectuée il y a longtemps). La figure suivante montrent des valeurs plus élevées dans les deux premières lignes d'une liste d'événements.

Serveur source	Noeud	Récapitulatif	Dernière toccurrence	Compte	Type	Délai d'affichage
AGG_P	myhost	Processus en cours sur la passerelle	29/12/2008	1	Résolution	15
AGG_P	myhost	Processus en cours sur la passerelle	29/12/2008	1	Incident	22
COL_P_1	Test3	Evénement de test 3	29/12/2008	1	Incident	1307
COL_P_1	Test4	Evénement de test 4	29/12/2008	1	Incident	1312
COL_P_1	Test5	Evénement de test 5	29/12/2008	1	Incident	1307
COL_P_1	Test6	Evénement de test 6	29/12/2008	1	Incident	1308
COL_P_1	Test7	Evénement de test 7	29/12/2008	1	Incident	1312
COL_P_1	Test1	Evénement de test 1	29/12/2008	1	Incident	1308
COL_P_1	Test2	Evénement de test 2	29/12/2008	1	Incident	1312
COL_P_1	Test3	Evénement de test 3	29/12/2008	1	Incident	1310
COL_P_1	Test4	Evénement de test 4	29/12/2008	1	Incident	1311
COL_P_1	Test5	Evénement de test 5	29/12/2008	1	Incident	1308

Figure 7. Liste d'événements présentant des valeurs de la zone TimeToDisplay non équilibrées après une reprise par restauration

Pour contrer cet effet, le déclencheur calculer_heure_à_afficher, qui calcule la valeur TimeToDisplay moyenne, inclut uniquement dans ses calculs les événements dont l'heure LastOccurence est postérieure à l'heure de la connexion de la passerelle aggregation-à-affichage. Cela est important car l'événement peut être assez ancien (c'est-à-dire que les horodatages CollectionFirst ou AggregationFirst peuvent avoir été effectués il y a un certain temps). Toutefois, la valeur DisplayFirst est toujours affichée comme l'heure d'insertion initiale sur le serveur d'affichage ObjectServer ; cette valeur sera nouvelle à chaque redémarrage ou reconnexion de la passerelle. (La zone DisplayFirst est définie lors de l'insertion initiale sur le serveur d'affichage ObjectServer par un déclencheur de base de données d'insertion et est par conséquent réinitialisée à chaque redémarrage ou nouvelle synchronisation de la passerelle au cours d'une reprise en ligne ou d'une reprise par restauration.)

Les événements qui se sont produits avant l'heure de connexion de la passerelle sont donc exclus du calcul de la moyenne et la zone TimeToDisplay de ces événements est définie sur N/A (Non applicable) pour permettre une identification aisée dans la liste des événements, comme indiqué dans la figure suivante.

Serveur source	Noeud	Récapitulatif	Dernière occurrence	Compte	Type	Délai d'affichage
DIS_1	DIS_1	Délai moyen pour l'affichage des événements : 52sec	09/01/2009	1	Information	0
COL_P_1	Test2	Evénement de test 2	08/01/2009	7	Incident	N/D
COL_P_1	Test3	Evénement de test 3	08/01/2009	7	Incident	N/D
COL_P_1	Test4	Evénement de test 4	08/01/2009	7	Incident	N/D
COL_P_1	Test5	Evénement de test 5	08/01/2009	7	Incident	N/D
COL_P_1	Test6	Evénement de test 6	08/01/2009	7	Incident	N/D
COL_P_1	Test7	Evénement de test 7	08/01/2009	7	Résolution	N/D
COL_P_1	Test1	Evénement de test 1	08/01/2009	7	Incident	N/D
COL_P_1	Test2	Evénement de test 2	08/01/2009	7	Incident	N/D
COL_P_1	Test3	Evénement de test 3	08/01/2009	7	Incident	N/D
COL_P_1	Test4	Evénement de test 4	08/01/2009	7	Incident	N/D
COL_P_1	Test5	Evénement de test 5	08/01/2009	7	Incident	N/D

Figure 8. Liste d'événements présentant des valeurs TimeToDisplay corrigées

Evénements synthétiques Resynchronisation terminée

Des déclencheurs sont disponibles sur les serveurs ObjectServer de couche agrégation pour créer des événements synthétiques indiquant la fin de la resynchronisation de la passerelle.

Ces événements sont affichés dans la liste des événements, comme le montre la figure ci-dessous.

Les événements Resynchronisation terminée ont un délai d'expiration de 86 400 secondes (ou 24 heures). De tels événements sont uniquement informatifs et ne doivent donc pas rester indéfiniment sur le serveur ObjectServer. Lorsque ces événements ont 24 heures, le déclencheur `expire` les efface en définissant la Severity sur 0. Les événements sont ensuite supprimés par le déclencheur supprimer_effacements.

Serveur source	Noeud	Récapitulatif	Dernière occurrence	Compte	Type	Délai d'affichage	Expiration
DIS_1	DIS_1	Délai moyen pour l'affichage : 24	09/01/2009	1	Informations	0	Non défini
AGG_P	AGG_P	Resynchronisation de la passerelle de reprise en ligne terminée	09/01/2009	1	Informations	40	86400
AGG_P	AGG_P	Resynchronisation de la passerelle d'affichage terminée	09/01/2009	1	Informations	22	86400
AGG_P	AGG_P	Resynchronisation de la passerelle d'affichage terminée	09/01/2009	1	Informations	20	86400
AGG_P	AGG_P	Resynchronisation de la passerelle de collecte terminée	09/01/2009	1	Informations	33	86400
AGG_P	AGG_P	Resynchronisation de la passerelle de collecte terminée	09/01/2009	1	Informations	47	86400

Figure 9. Liste d'événements présentant les événements synthétiques de resynchronisation terminée

Les événements Resynchronisation terminée représentent une manière utile d'indiquer que les passerelles se sont reconnectées et que le processus de resynchronisation a abouti après une opération de reprise en ligne ou de reprise par restauration, ou après une déconnexion et une reconnexion.

Etapes finales

Une fois que tous les composants sont installés et configurés dans l'environnement à plusieurs niveaux, procédez comme suit pour votre configuration.

- Effectuez un test de résistance au stress de l'environnement avec le nombre maximum d'événements que vous prévoyez d'envoyer vers les serveurs ObjectServers afin de vous assurer que votre environnement peut gérer la charge.
- Configurez les composants pour qu'ils s'exécutent sous contrôle de processus.
- Configurez l'équilibrage de charge sur les serveurs Interface graphique Web de votre environnement.
- Facultatif : si vous avez déployé des environnements distincts, par exemple pour répartir le charge entre les serveurs ObjectServers ou pour une répartition géographique, définissez ces serveurs ObjectServers sous forme de sources de données dans le fichier de définition de source de données Interface graphique Web.

Pour obtenir plus d'informations sur le contrôle de processus, voir le manuel *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Modèles de fichier omni.dat

Deux modèles de fichier de données de connexion `$NCHOME/etc/omni.dat` sont fournis ici avec les détails de communication de tous les composants dans une configuration de reprise en ligne de base (couche d'agrégation uniquement), et dans l'architecture à plusieurs niveaux standard. Dans ces fichiers, les composants sont tous signalés comme installés sur le même hôte.

Fichier omni.dat pour une configuration de reprise en ligne

```
#
# omni.dat file as prototype for interfaces file
#
# Ident: $Id: omni.dat 1.5 1999/07/13 09:34:20 chris Development $
#

[AGG_P]
{
        Primary: myhost_name.ibm.com 4100
}
```

```
[AGG_B]
{
        Primary: myhost_name.ibm.com 4150
}

[AGG_V]
{
        Primary: myhost_name.ibm.com 4100
        Backup: myhost_name.ibm.com 4150
}

[AGG_GATE]
{
        Primary: myhost_name.ibm.com 4105
}
```

Fichier omni.dat pour une architecture à plusieurs niveaux standard

```
#
# omni.dat file as prototype for interfaces file
#
# Ident: $Id: omni.dat 1.5 1999/07/13 09:34:20 chris Development $
#

[AGG_P]
{
        Primary: myhost_name.ibm.com 4100
}

[AGG_B]
{
        Primary: myhost_name.ibm.com 4150
}

[AGG_V]
{
        Primary: myhost_name.ibm.com 4100
        Backup: myhost_name.ibm.com 4150
}

[COL_P_1]
{
        Primary: myhost_name.ibm.com 4101
}

[COL_B_1]
{
        Primary: myhost_name.ibm.com 4151
}

[DIS_1]
{
        Primary: myhost_name.ibm.com 4102
}

[DIS_2]
{
        Primary: myhost_name.ibm.com 4152
}

[C_TO_A_GATE_P_1]
{
        Primary: myhost_name.ibm.com 4103
}

[C_TO_A_GATE_B_1]
```

```
{
        Primary: myhost_name.ibm.com 4153
}

[A_TO_D_GATE_1]
{
        Primary: myhost_name.ibm.com 4104
}

[A_TO_D_GATE_2]
{
        Primary: myhost_name.ibm.com 4154
}

[AGG_GATE]
{
        Primary: myhost_name.ibm.com 4105
}
```

Déclencheurs utilisateur dans les environnements à plusieurs niveaux

Dans une configuration ObjectServer à plusieurs niveaux, le déclencheur disable_inactive_users peut verrouiller des serveurs ObjectServer.

La table alerts.login_failures stocke les détails concernant l'heure de la dernière connexion des utilisateurs au serveur d'objets local, ainsi que les échecs de connexion. Par défaut, le déclencheur disable_inactive_users est inactif et fait partie du groupe de déclencheurs security_watch.

Lorsque le déclencheur disable_inactive_users est actif et qu'un utilisateur se connecte à l'ObjectServer de sauvegarde et ne se reconnecte pas pour la période mandatée par le déclencheur, l'utilisateur est désactivé.

Lorsque des utilisateurs effectuent un basculement sur le serveur ObjectServer de sauvegarde puis procèdent à une reprise par restauration sur le serveur ObjectServer principal, ils peuvent être désactivés si le déclencheur disable_inactive_users est actif sur le serveur ObjectServer de sauvegarde. La désactivation peut ensuite être propagée dans le système, via le serveur ObjectServer bidirectionnel, au serveur ObjectServer principal et sur les serveurs ObjectServer d'affichage.

Le déclencheur disable_inactive_users par défaut peut avoir une incidence sur tous les utilisateurs, ce qui les empêche de se connecter au système.

Si le déclencheur disable_inactive_users est nécessaire dans un environnement à plusieurs niveaux, il est conseillé de déplacer le déclencheur vers le groupe de déclencheurs primary_only dans la couche d'agrégation.

Pour empêcher tous les utilisateurs d'être désactivés, dans n'importe quelle situation, modifiez le déclencheur disable_inactive_users afin d'exclure les utilisateurs administrateurs.

Mise à niveau d'une architecture à plusieurs niveaux

La procédure décrite ici vous montre comment mettre à niveau un déploiement à plusieurs niveaux existant. Si vous installez une nouvelle configuration multiniveau Tivoli Netcool/OMNIbus version 8.1, n'utilisez pas cette procédure.

Avant de commencer

Pour éviter de perdre toute personnalisation de votre configuration, réalisez des copies de sauvegarde de tous les fichiers qui sont écrasés dans le cadre de cette procédure.

Pourquoi et quand exécuter cette tâche

Si vous mettez à niveau à partir d'une architecture multiniveau version 7.3 ou version 7.3.1 existante, exécutez d'abord les étapes 1 à 10, et ensuite les étapes 11 à 14. Si vous mettez à niveau à partir d'une architecture multiniveau version 7.4 existante, ignorez les étapes 1 à 10 et exécutez uniquement les étapes 11 à 14.

Procédure

Mise à niveau depuis la version 7.3 ou 7.3.1 vers la version 7.4

1. Ajoutez la propriété **Gate.Reader.IgnoreStatusFilter** à chaque fichier de propriétés de passerelle Collection-to-Aggregation (C_TO_A_GATE) et définissez-la sur TRUE.

   Par exemple : `Gate.Reader.IgnoreStatusFilter : TRUE`
2. Selon le nombre de passerelles définies dans votre architecture, copiez et renommez les fichiers de définition de réplication de table Collection-to-Aggregation de *NCHOME*/omnibus/extensions/multitier/gateway/ en *NCHOME*/omnibus/etc/.

   Par exemple, `C_TO_A_GATE_P_2.tblrep.def` et `C_TO_A_GATE_B_2.tblrep.def`.

   Remarque : Si vous répliquez des tables personnalisées, ajoutez-les aux fichiers de définition de réplication copiés.
3. Utilisez les commandes suivantes avec l'interface interactive SQL pour réactiver le déclencheur de changement d'état par défaut sur tous les ObjectServers.
   - Pour les ObjectServers de la couche Collection et de la couche Agrégation :

     ```
     1> ALTER TRIGGER state_change SET ENABLED TRUE;
     2> go
     ```
   - Pour les ObjectServers de la couche Affichage :

     ```
     1> ALTER TRIGGER dsd_state_change SET ENABLED TRUE;
     2> go
     ```
4. Utilisez les commandes suivantes avec l'interface interactive SQL pour permettre aux déclencheurs de nettoyage sur les ObjectServers de la couche Affichage de nettoyer les journaux et les détails orphelins.

   ```
   1> ALTER TRIGGER clean_journal_table SET GROUP dsd_triggers;
   2> ALTER TRIGGER clean_details_table SET GROUP dsd_triggers;
   3> go
   ```
5. Supprimez les déclencheurs suivants de chaque type d'ObjectServer :
   - A partir des ObjectServers de la couche Collection : `col_state_change`
   - A partir des ObjectServers de la couche Agrégation : `agg_state_change`
   - A partir des ObjectServers de la couche Affichage : `dsd_state_change_2`

L'exemple suivant utilise l'interface interactive SQL pour supprimer le déclencheur `col_state_change` :

```
1> DROP TRIGGER col_state_change;
2> go
```

6. Supprimez les lignes suivantes dans tous les fichiers de définition de mappe :

```
'SourceStateChange' = '@SourceStateChange' ON INSERT ONLY,
'SourceServerName' = '@SourceServerName' ON INSERT ONLY,
'SourceServerSerial' = '@SourceServerSerial' ON INSERT ONLY,
```

7. Redémarrez toutes les passerelles pour lesquelles vous avez modifié les fichiers de configuration.
8. Utilisez l'interface interactive SQL pour importer les nouveaux fichiers ObjectServer SQL dans vos ObjectServers en cours d'exécution.

UNIX Linux

- Exemple d'ObjectServer de la couche Collection :

```
$NCHOME/omnibus/bin/nco_sql -server COL_P_1 -user root <
$NCHOME/omnibus/extensions/multitier/objectserver/collection.sql
```

- Exemple d'ObjectServer de la couche Agrégation :

```
$NCHOME/omnibus/bin/nco_sql -server AGG_P -user root <
$NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
```

- Exemple d'ObjectServer de la couche Affichage :

```
$NCHOME/omnibus/bin/nco_sql -server DIS_1 -user root <
$NCHOME/omnibus/extensions/multitier/objectserver/display.sql
```

Windows

- Exemple d'ObjectServer de la couche Collection :

```
%NCHOME%\omnibus\bin\isql -S COL_P_1 -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\collection.sql
```

- Exemple d'ObjectServer de la couche Agrégation :

```
%NCHOME%\omnibus\bin\isql -S AGG_P -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\aggregation.sql
```

- Exemple d'ObjectServer de la couche Affichage :

```
%NCHOME%\omnibus\bin\isql -S DIS_1 -U root < %NCHOME%\omnibus\
extensions\multitier\objectserver\display.sql
```

Remarque : L'application de ces scripts SQL provoque des erreurs lorsque l'interface tente de créer des zones qui sont déjà présentes. Vous pouvez ignore ces erreurs en toute sécurité. Le but de réimporter le SQL est de mettre à jour les déclencheurs.

9. Facultatif : Supprimez des zones de configuration multiniveau redondantes en supprimant les colonnes suivantes de tous les ObjectServers :
   - `SourceStateChange`
   - `SourceServerName`
   - `SourceServerSerial`

   L'exemple suivant utilise l'interface interactive SQL pour supprimer la colonne `SourceStateChange` :

```
1> ALTER TABLE alerts.status DROP COLUMN SourceStateChange;
2> go
```

Remarque : Avant de supprimer ces colonnes, vérifiez qu'aucune fonction personnalisée dans votre environnement ne dépend de ces colonnes.

10. Appliquez le script SQL suivant à tous les serveurs ObjectServer inclus dans votre configuration multiniveau :

    NCHOME/omnibus/etc/update731to74.sql

Mise à niveau depuis la version 7.4 vers la version 8.1

11. Appliquez les scripts SQL suivants, dans l'ordre indiqué, à tous les serveurs ObjectServer inclus dans votre configuration multiniveau.
    a. *NCHOME*/omnibus/etc/update74to74fp3.sql
    b. *NCHOME*/omnibus/etc/update74fp3to81.sql
12. Ajoutez la section suivante à tous les fichiers de définition de mappe ObjectServer Gateway.

```
###############################################################################
# Mappe de registre de sonde
#
# NOTE:
# 'ConnectionID'   Only set on the original ObjectServer that probes are
#   connected to. Elsewhere it defaults to '0'.
###############################################################################
CREATE MAPPING ProbeMap
(
 'Name'  = '@Name'  ON INSERT ONLY,
 'Hostname' = '@Hostname' ON INSERT ONLY,
 'ProbeType' = '@ProbeType',
 'HTTP_port' = '@HTTP_port',
 'HTTPS_port' = '@HTTPS_port',
 'RulesChecksum' = '@RulesChecksum',
 'PID'  = '@PID',
 'Status' = '@Status',
 'StartTime' = '@StartTime',
 'LastUpdate' = '@LastUpdate',
 'ApiReleaseID' = '@ApiReleaseID',
 'ApiVersion' = '@ApiVersion'
);
```

13. Ajoutez la commande REPLICATE suivante au fichier de définition de réplication de table AGG_GATE.tblrep.def.

```
REPLICATE ALL FROM TABLE 'registry.probes'
 USING map 'ProbeMap'
 WITH NORESYNC;
```

14. Ajoutez la commande REPLICATE suivante à tous les fichiers de définition de réplication de table de passerelles unidirectionnelles (exemple : A_TO_D_GATE.tblrep.def, C_TO_A_GATE_B_1.tblrep.def et C_TO_A_GATE_P_1.tblrep.def).

```
REPLICATE ALL FROM TABLE 'registry.probes'
 USING map 'ProbeMap';
```

Résultats

Votre architecture multiniveau est mise à niveau pour utiliser la fonction de registre de la sonde.

Chapitre 9. Configuration de la haute disponibilité

Lorsque Tivoli Netcool/OMNIbus est configuré pour la haute disponibilité, la perte d'événements est réduite, l'intégrité des données, optimisée et les performances sont accrues.

L'architecture à plusieurs niveaux offre la toile de fond de la configuration à haute disponibilité dans laquelle les serveurs ObjectServer sont déployés dans une configuration à un, deux ou trois niveaux. L'architecture à plusieurs niveaux vous permet de démarrer votre déploiement dans la couche ou le niveau d'agrégation et d'ajouter des ressources du serveur ObjectServer aux couches de collecte et d'affichage, en fonction de vos besoins. La configuration à un, deux ou trois niveaux est un prérequis pour configurer la haute disponibilité. Votre système doit au minimum être configuré pour la reprise en ligne et la reprise par restauration dans la couche d'agrégation.

Votre installation de Tivoli Netcool/OMNIbus inclut un ensemble de personnalisations que vous pouvez appliquer à vos serveurs ObjectServer et à vos passerelles ObjectServer pour configurer chaque couche. Ces personnalisations sont fournies dans les répertoires `$NCHOME/omnibus/extensions/multitier` et `$NCHOME/omnibus/extensions/control_shutdown`.

Concepts associés:

Chapitre 8, «Configuration et déploiement d'une architecture à plusieurs niveaux», à la page 223
Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

Configuration de reprise en ligne

La configuration de reprise en ligne est une condition de la haute disponibilité, et est basée sur la couche d'agrégation de l'architecture à plusieurs niveaux standard. Dans sa configuration la plus simple, la configuration de reprise en ligne consiste en un serveur ObjectServer principal et de sauvegarde connectés par une passerelle ObjectServer bidirectionnelle dans la couche d'agrégation, sans qu'une couche de collecte ou d'affichage ne soit connectée.

La figure suivante montre un exemple de configuration de reprise en ligne.

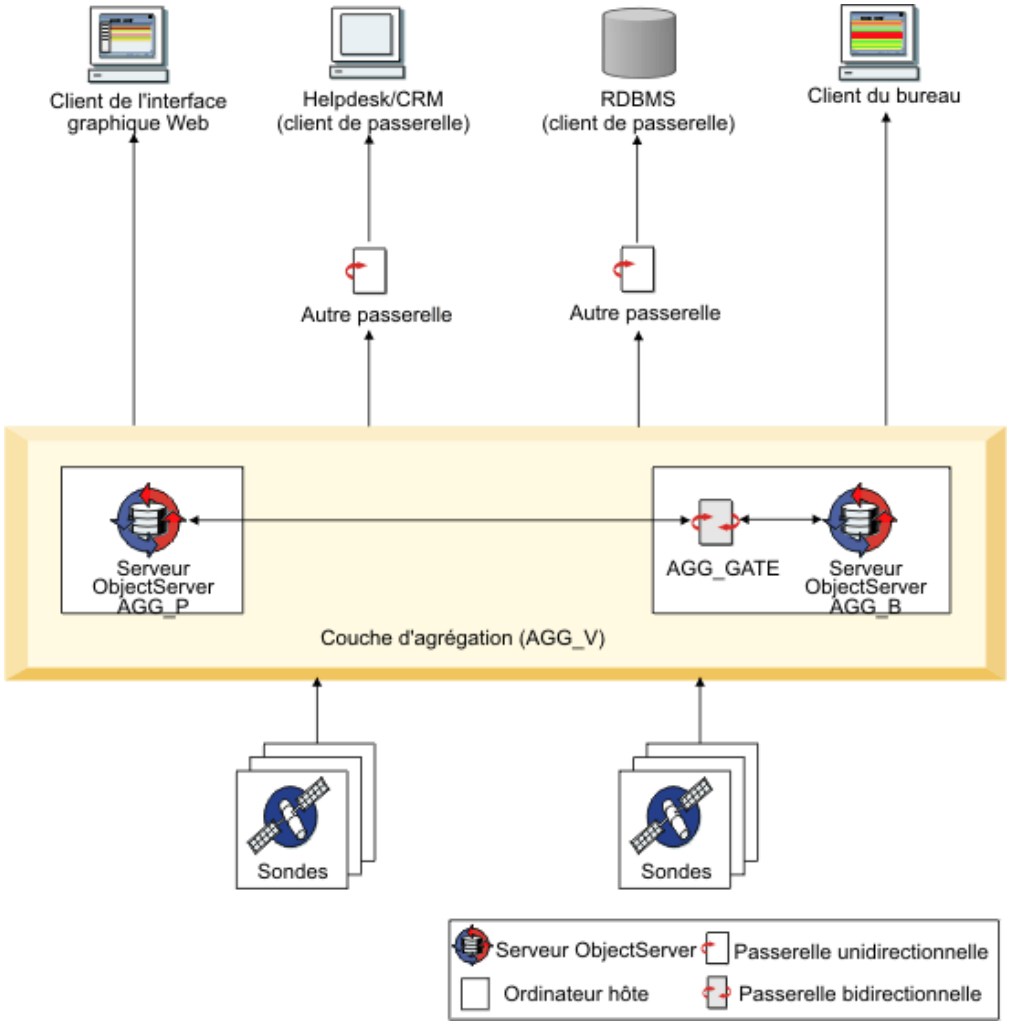

Figure 10. Configuration de base de la reprise en ligne

Dans la figure, la paire de serveurs ObjectServer d'agrégation est connectée par une passerelle ObjectServer bidirectionnelle afin que les serveurs restent synchronisés ; la passerelle bidirectionnelle s'exécute sur l'hôte de sauvegarde. Les sondes se connectent directement à la paire d'agrégation virtuelle (AGG_V) afin de faciliter la reprise en ligne et la reprise par restauration si le serveur ObjectServer d'agrégation principal est indisponible. Les autres cibles auxquelles les alertes peuvent être envoyées depuis la couche d'agrégation apparaissent également :

- Une passerelle ObjectServer unidirectionnelle dédiée pour un serveur ObjectServer de couche d'affichage peut se connecter à la paire d'agrégation virtuelle, et les alertes peuvent être transmises aux clients du bureau ou de l'Interface graphique Web.
- Les autres passerelles peuvent se connecter à la paire d'agrégation virtuelle et transmettre les alertes aux clients tels que le centre d'assistance ou un système de gestion de la relation client (CRM) et un système de gestion de base de données relationnelle (RDBMS).
- Les alertes peuvent être transmises directement aux clients du bureau ou de l'Interface graphique Web.

Si vous souhaitez effectuer la configuration de reprise en ligne présentée dans la couche d'agrégation de la figure précédente, seules certaines étapes de la

configuration d'architecture à plusieurs niveaux standard sont nécessaires. Les étapes requise pour la configuration de reprise en ligne dans la couche d'agrégation sont les suivantes :

1. «Configuration des informations de communication du serveur (architecture à plusieurs niveaux)», à la page 234
2. «Installation du serveur d'agrégation ObjectServer principal», à la page 235
3. «Installation du serveur d'agrégation ObjectServer de secours», à la page 236
4. «Configuration de la passerelle d'agrégation ObjectServer bidirectionnelle», à la page 237

Concepts associés:

«Présentation d'une architecture standard à plusieurs niveaux», à la page 223
Pour réduire l'impact d'un échec de l'ordinateur, il est recommandé d'utiliser plusieurs ordinateurs dans l'architecture standard à plusieurs niveaux. Tous les composants peuvent, cependant, être installés et exécutés sur n'importe quel ordinateur et peuvent même être configurés pour s'exécuter sur un seul ordinateur.

Configuration de la reprise par restauration contrôlée des clients

Pour réduire le risque de perte de données, ce qui peut arriver si le client est repris par restauration sur un serveur ObjectServer principal avant que la synchronisation soit effectuée, le comportement de reprise par restauration doit être géré par une paire de serveurs ObjectServer de reprise en ligne et non pas par les clients eux-mêmes. La configuration de la reprise par restauration contrôlée est basée sur la couche d'agrégation de l'architecture à plusieurs niveaux.

Avant de commencer

Configuration à plusieurs niveaux : L'architecture à plusieurs niveaux est préconfigurée par défaut avec les valeurs requises pour les reprises par restauration des passerelles nord ; autrement dit, les passerelles unidirectionnelles qui connectent la couche de collecte à la couche d'agrégation, et la couche d'agrégation à la couche d'affichage, sont configurées pour une reprise par restauration contrôlée.

Autre configuration de paire de reprise en ligne : Si vous avez défini la paire de reprise en ligne dans la couche d'agrégation comme indiqué, les automatisations requises pour la reprise par restauration contrôlée sont en place :

- Les déclencheurs backup_startup, backup_counterpart_down, et backup_counterpart_up sont activés pour se connecter au serveur ObjectServer de secours.
- Le déclencheur disconnect_all_clients est également activé dans le serveur ObjectServer de secours.

Pourquoi et quand exécuter cette tâche

Pour configurer la reprise par restauration contrôlée pour les clients qui se connectent à la paire de reprise en ligne, effectuez les étapes suivantes pour les types de client :

Procédure

- **Sondes se connectant à la paire de reprise en ligne de collection :** Ces sondes doivent utiliser les paramètres de propriété de reprise en ligne et de reprise par

restauration standard et la valeur **PollServer** doit être supérieure à la valeur **NetworkTimeout**. Dans le fichier de propriétés de sonde :

- Paramétrez **Server** sur COL_V_1 (nom virtuel)
- Paramétrez **NetworkTimeout** sur 30
- Paramétrez **PollServer** sur 120

Ou

- Paramétrez **Server** sur COL_P_1
- Paramétrez **ServerBackup** sur COL_B_1
- Paramétrez **NetworkTimeout** sur 30
- Paramétrez **PollServer** sur 120

- **Sondes se connectant à la paire d'agrégation de reprise en ligne :** Ces sondes doivent utiliser les paramètres de propriétés de reprise en ligne et de reprise par restauration standard, avec la propriété **PollServer** paramétrée sur 0 de sorte que la reprise par restauration fonctionne correctement. Dans le fichier de propriétés de sonde :
  - Paramétrez **Server** sur AGG_V
  - Paramétrez **NetworkTimeout** sur 30
  - Paramétrez **PollServer** sur 0

  Ou
  - Paramétrez **Server** sur AGG_P
  - Paramétrez **ServerBackup** sur AGG_B
  - Paramétrez **NetworkTimeout** sur 30
  - Paramétrez **PollServer** sur 0
- **Passerelles ObjectServer unidirectionnelles :**
  - Si les passerelles unidirectionnelles sont configurées pour se connecter de la paire de collecte à la paire d'agrégation (virtuelle), désactivez la reprise par restauration dans les passerelles unidirectionnelles de couche de collecte (C_TO_A_GATE_P_1 et C_TO_A_GATE_B_1). Dans chaque fichier de propriétés de passerelle ObjectServer :
    - Définissez **Gate.Writer.Server** sur AGG_V.
    - Définissez **Gate.Writer.FailbackEnabled** sur FALSE.
  - Si les passerelles unidirectionnelles sont configurées pour se connecter à la paire d'agrégation (virtuelle) aux serveurs ObjectServer d'affichage, désactivez la reprise par restauration dans les passerelles unidirectionnelles d'affichage (A_TO_D_GATE_P_1 et A_TO_D_GATE_B_1). Dans chaque fichier de propriétés de passerelle ObjectServer :
    - Définissez **Gate.Reader.Server** sur AGG_V.
    - Définissez **Gate.Reader.FailbackEnabled** sur FALSE.
- **Passerelles ObjectServer bidirectionnelles :** Elles ne figurent pas dans la configuration à plusieurs niveaux proposée ; toutefois, si ces passerelles ObjectServer bidirectionnelles sont utilisées entre la couche de collecte et la couche d'agrégation, désactivez leur fonction de reprise par restauration en utilisant les propriétés suivantes :
  - Définissez **Gate.ObjectServerB.Server** sur AGG_V.
  - Définissez **Gate.ObjectServerB.FailbackEnabled** sur FALSE.
- **Listes d'événements :** Si les listes d'événements se connectent à la paire d'agrégation de reprise en ligne, désactivez la reprise par restauration pour les

listes d'événements en définissant l'option de ligne de commande `-failbackpolltime` sur `0` lors de l'exécution de **nco_event** sous UNIX et Linux, ou **NCOEvent.exe** sous Windows.

Si les listes d'événements sont configurées pour se connecter aux serveurs ObjectServer de la couche d'affichage, et que les listes d'événements effectuent une connexion double écriture sur la paire d'agrégation de reprise en ligne, lancez les listes d'événements avec l'option de ligne de commande `-failbackpolltime` définie sur `0` pour qu'elles affichent le comportement de reprise par restauration contrôlée.

Résultats

Lorsque la reprise par restauration est désactivée pour les clients, ces derniers restent connectés au serveur ObjectServer de secours jusqu'à ce que le serveur force la déconnexion à la fin de la resynchronisation.

Pour signaler que la resynchronisation est terminée, la passerelle du serveur ObjectServer envoie un signal gw_resync_finish aux serveurs ObjectServer principal et de secours. A réception de ce signal, le serveur ObjectServer de secours déconnecte les clients pour que ces derniers puissent se connecter au serveur ObjectServer principal resynchronisé.

Concepts associés:

Chapitre 8, «Configuration et déploiement d'une architecture à plusieurs niveaux», à la page 223
Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

«Conventions de dénomination pour l'architecture à plusieurs niveaux», à la page 226
Une convention de dénomination est conçue pour vous aider à identifier les composants connexes dans chaque couche d'une architecture à plusieurs niveaux et le flot de données dans et à travers les couches.

Configuration des sondes pour la haute disponibilité

Pour les sondes dans votre environnement, vous pouvez configurer la haute disponibilité en définissant les sondes pour s'exécuter en mode stockage et retransmission circulaire. Vous pouvez également, si la sonde a la fonctionnalité de reprise en ligne d'égal à égal, exécuter deux instances de la sonde dans une configuration maître-esclave.

Pour déterminer si une sonde prend en charge la reprise en ligne d'égal à égal, voir la documentation de la sonde individuelle.

Configuration des sondes pour une exécution en mode stocker-et-transmettre circulaire

Vous pouvez exécuter les sondes en mode stocker-et-transmettre circulaire afin de réduire la perte d'événements lors de la reprise en ligne et la reprise par restauration. Avec ce mode, la sonde stocke toutes les alertes qu'elle génère lorsqu'elle est connectée au serveur ObjectServer.

Pourquoi et quand exécuter cette tâche

Ces alertes sont stockées dans des fichiers stocker-et-transmettre tournants après un intervalle défini par la propriété **RollSAFInterval**. Définissez la propriété **RollSAFInterval** sur une valeur supérieure ou égale à la granularité du serveur ObjectServer.

Les fichiers stocker-et-transmettre circulaires sont appelés `SAFFileName.nom_serveur` et `SAFFileName.nom_serveur_1`.

Pour plus d'informations sur le mode stocker-et-transmettre, consultez *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*.

Procédure

Pour configurer la sonde pour l'exécution en mode stocker-et-transmettre circulaire :

1. Dans le fichier de propriétés de sonde, définissez les propriétés comme indiqué dans l'exemple suivant. Dans cet exemple, définissez le paramètre **StoreAndForward** sur 2 pour activer le mode stocker-et-transmettre circulaire. Les autres propriétés affichent les valeurs par défaut qui peuvent être modifiées.

   ```
   StoreAndForward:2
   SAFFileName:'$OMNIHOME/var/SAF'
   MaxSAFFileSize:1024
   SAFPoolSize:3
   RollSAFInterval:90
   ```

2. La propriété **Server** doit être définie sur le nom du serveur ObjectServer principal et la propriété **ServerBackup** doit être définie sur le nom du serveur ObjectServer de sauvegarde, s'il existe un serveur de sauvegarde. N'utilisez pas les définitions des pairs ObjectServer virtuelles pour ces propriétés.

Résultats

Lorsque la sonde est déconnectée du serveur ObjectServer, elle enregistre l'horodatage du dernier événement ayant abouti ainsi que le nom de serveur ObjectServer dans un fichier nommé selon le format **SAFFilename.**`DisconnectionTime`. Ce fichier est stocké dans le même répertoire que les fichiers stocker-et-transmettre. Si un serveur ObjectServer de secours est disponible pour la reprise en ligne, la sonde se reconnecte à ce serveur et rejoue les événements à partir du fichier stocker-et-transmettre envoyé préalablement au serveur ObjectServer principal lors de la période de temps correspondant à l'intervalle **RollSAFInterval** avant la déconnexion. Par conséquent, il est possible que la sonde renvoie des événements déjà envoyés au serveur ObjectServer principal, mais qui n'ont pas été répliqués sur le serveur ObjectServer de sauvegarde avant l'échec du serveur principal.

Si la sonde ne peut pas se connecter à un serveur ObjectServer, sa fonction de gestion des fichiers stocker-et-transmettre tournants est automatiquement remplacée par la fonction stocker-et-transmettre héritée. La sonde commence à stocker tous les événements dans un pool de fichiers stocker-et-transmettre ; la taille du pool est définie par la propriété **SAFPoolSize**, et la taille maximale de fichier est définie par la propriété **MaxSAFFileSize**. Dans le même temps, la propriété **RollSAFInterval** n'est pas utilisée pour faire tourner les fichiers stocker-et-transmettre. Le roulement des fichiers s'effectue lorsqu'un fichier attend la taille maximale définie par la propriété **MaxSAFFileSize**.

Configuration du mode de reprise en ligne d'égal à égal

Deux instances d'une sonde peuvent être exécutées simultanément dans une relation de reprise en ligne d'égal à égal. Une instance est désignée comme maître. L'autre agit comme esclave et est en mode secours automatique. En cas d'échec de l'instance maître, l'instance esclave est activée.

Remarque : Le mode reprise en ligne d'égal à égal n'est pas pris en charge pour toutes les sondes. Les sondes qui répertorient les propriétés **Mode**, **PeerHost** et **PeerPort** lorsque vous exécutez la commande `$OMNIHOME/probes/nco_p_`*`nom_sonde`* `-dumpprops` prennent en charge le mode reprise en ligne d'égal à égal.

Pour configurer une relation de reprise en ligne d'égal à égal :

- Pour l'instance maître, définissez la propriété **Mode** sur `master` et la propriété **PeerHost** sur le nom de l'élément réseau de l'esclave.
- Pour l'instance esclave, définissez la propriété **Mode** sur `slave` et la propriété **PeerHost** sur le nom de l'élément réseau du maître.
- Pour les deux instances, définissez la propriété **PeerPort** sur le port via lequel le maître et l'esclave communiquent.

L'instance maître envoie un signal de présence à l'instance esclave à chaque intervalle défini par la propriété **BeatInterval**. L'instance esclave met en cache toutes les données d'alerte qu'elle reçoit et supprime ces données d'alerte à chaque fois qu'elle reçoit un signal de l'instance maître. Si l'instance esclave ne reçoit pas de signal dans le délai défini par la somme des valeurs des propriétés **BeatInterval** et **BeatThreshold** (**BeatInterval** + **BeatThreshold**), l'instance esclave suppose que l'instance maître n'est plus active, et transmet les alertes de la mémoire cache au serveur ObjectServer. L'instance esclave continue à transmettre toutes les alertes jusqu'à ce qu'elle reçoive un signal de présencede l'instance maître. Le délai de dépassement d'attente du signal de présence est de 1 seconde. Le délai d'attente maximal est de (**BeatInterval** + **BeatThreshold** + 1) secondes avant que l'instance esclave transmette les alertes de sa mémoire cache. Toutes les alertes de la mémoire cache sont envoyées.

Le paramètre **BeatInterval** défini pour l'instance maître prévaut ; le paramètre local **BeatInterval** de l'instance esclave est ignoré.

Pour désactiver la relation de reprise en ligne d'égal à égal, exécutez une seule instance de la sonde avec la propriété **Mode** définie sur `standard`. Il s'agit du paramétrage par défaut.

Le mode de reprise en ligne des sondes exécutées en relation de reprise en ligne d'égal à égal est défini dans le fichier de propriétés.

Vous pouvez également commuter le mode d'une sonde entre maître et esclave dans le fichier de règles. Un délai d'environ une seconde s'écoule avant que la

modification de mode entre en vigueur. Cela peut engendrer des événements en double si deux instances de sonde sont commutées du mode `standard` en `master` ou `slave` ; toutefois, aucune donnée n'est perdue.

Lorsque deux instances exécutées en mode stocker-et-transmettre sont connectées à une paire de reprise en ligne de serveurs ObjectServer, l'instance maître envoie des alertes au serveur ObjectServer principal. Si le serveur ObjectServer principal échoue, l'instance maître de la sonde effectue une reprise en ligne et commence à envoyer les alertes de son fichier stocker-et-transmettre au serveur ObjectServer de secours. Si l'instance maître de la sonde échoue, l'instance esclave prend le relais. Si l'instance esclave ne parvient pas à se connecter au serveur ObjectServer, l'esclave crée un fichier stocker-et-transmettre pour stocker les données d'alerte. Si l'instance maître est réactivée, tous les fichier stocker-et-transmettre de l'instance maître sont supprimés pour éviter que les anciennes alertes soient renvoyées.

Exemple : configuration du mode de reprise en ligne d'égal à égal dans le fichier de propriétés

Les exemples de valeurs de fichier de propriété pour le maître sont les suivants :

```
PeerPort: 9999
PeerHost: "slavehost"
Mode: "master"
```

Les exemples de valeurs de fichier de propriété pour l'esclave sont les suivants :

```
PeerPort: 9999
PeerHost: "masterhost"
Mode: "slave"
```

Exemple : configuration du mode de reprise en ligne d'égal à égal dans le fichier de règles

Pour faire passer une instance en maître, utilisez la syntaxe de fichier de règles suivante :

```
%Mode = "master"
```

Réduction de la perte d'événements suite à un échec du serveur ObjectServer lors de la resynchronisation

Pour limiter la perte d'événements lors de l'échec d'un serveur ObjectServer lors de la resynchronisation, la propriété ObjectServer **`ActingPrimary`** permet de déterminer quel était le serveur ObjectServer principal lors de l'échec de la dernière resynchronisation. La passerelle ObjectServer bidirectionnelle détermine la direction de la resynchronisation à l'aide de la propriété **`ActingPrimary`** du serveur ObjectServer. Ce paramètre de propriété est mis à jour par les automatisations, et ne requiert aucune intervention de l'utilisateur.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la façon dont la passerelle ObjectServer détermine le serveur ObjectServer responsable de la resynchronisation, voir *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*. Allez sur le centre de documentation *IBM Tivoli Network Management* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp. Recherchez le nœud *IBM Tivoli Netcool/OMNIbus* dans le panneau de navigation de gauche et accédez au nœud des passerelles *Tivoli Netcool/OMNIbus*.

Réduction du délai de resynchronisation

Pour réduire le temps nécessaire pour resynchroniser les contenus d'un serveur ObjectServer sur un autre (suite à la récupération d'un serveur ObjectServer principal ou de secours ou d'une passerelle ObjectServer bidirectionnelle), vous pouvez configurer la passerelle de façon à resynchroniser uniquement les événements qui ont changé depuis l'échec.

Pourquoi et quand exécuter cette tâche

Utilisez la propriété **Gate.Resync.Type** pour indiquer le type de resynchronisation requis. Définissez **Gate.Resync.Type** sur `Minimal` pour que la passerelle resynchronise uniquement les événements insérés ou mis à jour dans le serveur ObjectServer source après l'échec de l'autre ObjectServer ou de la passerelle.

Pour obtenir plus d'informations sur la méthode de resynchronisation de la passerelle ObjectServer, voir *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*. Allez sur le centre de documentation *IBM Tivoli Network Management* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp. Recherchez le nœud *IBM Tivoli Netcool/OMNIbus* dans le panneau de navigation de gauche et accédez au nœud des passerelles *Tivoli Netcool/OMNIbus*.

Les détails sur le dernier transfert de modifications IDUC à un client IDUC avant un échec sont stockés dans la table iduc_system.iduc_stats.

Configuration de l'arrêt contrôlé d'un serveur ObjectServer

Vous pouvez configurer l'arrêt contrôlé de tout ObjectServer de façon à ce que les modifications en cours soient transmises aux clients IDUC avant l'arrêt du serveur ObjectServer. Cela réduit la possibilité de perte de données lors de l'arrêt.

Pourquoi et quand exécuter cette tâche

Pour activer l'arrêt contrôlé, le schéma ObjectServer doit être mis à jour avec un ensemble de déclencheurs et de procédures fournis dans un fichier SQL d'importation `control_shutdown.sql`, stocké dans le répertoire `$NCHOME/omnibus/extensions/control_shutdown`. Le serveur ObjectServer doit également être configuré pour s'exécuter sous contrôle de processus car l'utilitaire **nco_pa_stop** doit être appelé par une procédure externe pour arrêter le serveur ObjectServer.

Les déclencheurs et procédures fournis dans le fichier `control_shutdown.sql` gèrent l'arrêt contrôlé. Le serveur ObjectServer est d'abord mis à l'état restreint. Les connexions identifiées des clients non-IDUC (tels que **nco_sql** et **nco_config**) sont interrompues, et la commande IDUC FLUSH est lancée pour envoyer les modifications en attente à tous les clients IDUC identifiés (tels que les passerelles et les listes d'événements). Toute demande de nouvelle connexion au serveur ObjectServer est bloquée. Si la fonction stocker et transmettre est activée pour les sondes, toutes les nouvelles alertes sont stockées dans un fichier stocker-et-transmettre jusqu'à ce que la sonde se reconnecte à un serveur ObjectServer. Lorsque la récupération de données est terminée pour les clients IDUC, l'utilitaire **nco_pa_stop** est utilisé pour arrêter le processus du serveur ObjectServer qui s'exécute sous contrôle de processus. Pour plus d'informations sur la fonction stocker et transmettre, voir le manuel *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*. Pour plus d'informations sur la configuration du

serveur ObjectServer pour une exécution sous contrôle de processus, voir le manuel *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Les sections du fichier `control_shutdown.sql` doivent être modifiées pour indiquer les informations requises lors la configuration.

Pour configurer et effectuer un arrêt contrôlé pour un serveur ObjectServer :

Procédure

1. Accédez au répertoire `$NCHOME/omnibus/extensions/control_shutdown` et copiez le fichier `control_shutdown.sql` dans le répertoire `$NCHOME/omnibus/etc` ou dans un autre emplacement privilégié.
2. Supprimez les droits d'accès en lecture seule par défaut du fichier `control_shutdown.sql` et lisez le fichier pour vous familiarisez avec son contenu. Puis, modifiez le fichier comme suit :
   - Recherchez la section de code suivante pour la procédure ext_shutdown :

     ```
     ------------------------------------------------------------------------
     -- Procédure externe pour arrêter le système d'exploitation à l'aide de nco_pa_stop
     ...
     ------------------------------------------------------------------------

     create or replace procedure ext_shutdown (in process_name Char(255),
       in username Char(255), in pass Char(255), in paserver Char(255))
     executable '$OMNIHOME/bin/nco_pa_stop'
     host  'nchost1'
     user user1 group grp1
     arguments ' -process ' + process_name +  ' -user ' + username + ' -password ' + pass
       + ' -server ' + paserver
     go
     ```

     Les exemples de valeur sont formatés en texte **gras**. Remplacez la marque de réservation **nchost1** par le nom de l'hôte sur lequel vous souhaitez exécuter l'utilitaire **nco_pa_stop** pour arrêter le serveur ObjectServer. Remplacez **user1** par l'ID utilisateur adéquat et remplacez **grp1** par l'ID de groupe sur lequel vous voulez exécuter **nco_pa_stop**. La procédure ext_shutdown est appelée à partir de la procédure control_shutdown et du déclencheur d'arrêt final du fichier `control_shutdown.sql` ; ces sections de code doivent également être modifiées.
   - Recherchez la section de code suivante pour la procédure control_shutdown :

     ```
     ------------------------------------------------------------------------
     -- Procédure d'arrêt et de suppression des connexions pour l'arrêt contrôlé
     ------------------------------------------------------------------------

     create or replace procedure control_shutdown()
     declare
       iduc_clients int;
     ...
     ...
     ...
      if ( iduc_clients = 0 )
       then
      -- ne rien faire, simplement arrêter
      -- appeler la procédure externe pour arrêter le système d'exploitation à l'aide de nco_pa_stop
      -- remplacer 'MasterObjectServer' par le nom du processus ObjectServer dans le fichier de
     configuration de l'agent de processus
      -- remplacer 'user1' avec le nom d'utilisateur pour exécuter nco_pa_stop.
      -- remplacer 'pass1' avec le mot de passe pour exécuter nco_pa_stop.
      -- remplacer 'AGG_PA' avec le nom de serveur d'agent de processus pour se connecter.
       execute procedure ext_shutdown ( 'MasterObjectServer', 'user1', 'pass1', 'AGG_PA' );
       else
      -- activer le déclencheur pour vérifier si GET IDUC a terminé sur tous les clients.
       execute procedure enable_control_shutdown;
      end if;
     ```

     Les exemples de valeur sont formatés en texte **gras**. Dans la ligne `execute procedure ext_shutdown` remplacer les marques de réservation **MasterObjectServer**, **user1**, **pass1**, et **AGG_PA** par le nom de processus ObjectServer défini dans le fichier de configuration d'agent de processus, les

données d'identification de l'utilisateur pour l'exécution de **nco_pa_stop** et le nom de l'agent de processus utilisé par le serveur ObjectServer pour exécuter l'automatisation externe.

- Recherchez la section de code suivante du déclencheur final_shutdown :

```
------------------------------------------------------------------------------
-- Déclencheur pour redéfinir l'indicateur Pending (En attente) sur GET IDUC
   à partir de tous les clients
------------------------------------------------------------------------------

create or replace trigger final_shutdown
group control_shutdown_triggers
...
...
...
 if( pending_cnt = 0 ) then
 -- désactiver ce groupe de déclencheurs et arrêter le serveur ObjectServer.
  execute procedure disable_control_shutdown;
 -- appeler la procédure externe pour arrêter le système d'exploitation à l'aide de nco_pa_stop
 -- remplacer 'MasterObjectServer' par le nom du processus ObjectServer dans le fichier
de configuration de l'agent de processus
 -- remplacer 'user1' avec le nom d'utilisateur pour exécuter nco_pa_stop.
 -- remplacer 'pass1' avec le mot de passe pour exécuter nco_pa_stop.
 -- remplacer 'AGG_PA' avec le nom de serveur d'agent de processus pour se connecter.
  execute procedure ext_shutdown ( 'MasterObjectServer', 'user1', 'pass1', 'AGG_PA' );
 end if;
```

Les exemples de valeur sont formatés en texte **gras**. Dans la ligne `execute procedure ext_shutdown` remplacer les marques de réservation **MasterObjectServer**, **user1**, **pass1**, et **AGG_PA** par le nom de processus ObjectServer défini dans le fichier de configuration d'agent de processus, les données d'identification de l'utilisateur pour l'exécution de **nco_pa_stop** et le nom de l'agent de processus utilisé par le serveur ObjectServer pour exécuter l'automatisation externe.

3. Appliquez la personnalisation d'arrêt contrôlé sur un serveur ObjectServer nouveau ou existant, comme suit :
   - Lors de la création du serveur ObjectServer à l'aide de la commande **nco_dbinit**, appliquez la personnalisation à la base de données ObjectServer :

     ```
     $NCHOME/omnibus/bin/nco_dbinit -server nom_serveur -customconfigfile
     $NCHOME/omnibus/extensions/control_shutdown/control_shutdown.sql
     ```

   - Si le serveur ObjectServer existe déjà, appliquez la personnalisation comme suit :

     UNIX Linux
     ```
     $NCHOME/omnibus/bin/nco_sql -server nom_serveur
     -user nom_utilisateur –password mot_de_passe < $NCHOME/omnibus/
     extensions/control_shutdown/control_shutdown.sql
     ```

     Windows
     ```
     "%NCHOME%\omnibus\bin\isql" -S nom_serveur -U
     nom_utilisateur -P mot_de_passe -i "%NCHOME%\omnibus\extensions\
     control_shutdown\control_shutdown.sql"
     ```

   Dans ces commandes, *nom_serveur* est le nom du serveur ObjectServer, *nom_utilisateur* est un nom d'utilisateur valide utilisé pour se connecter au serveur ObjectServer, et *mot_de_passe* est le mot de passe correspondant.
4. Configurez le serveur ObjectServer pour qu'il s'exécute sous contrôle de processus. Dans le fichier de propriétés du serveur ObjectServer, définissez les propriétés suivantes pour le contrôle de processus :
   - Définissez **PA.Name** pour le nom de l'agent de processus utilisé par le serveur ObjectServer pour exécuter des automatisations externes.
   - Définissez **PA.Username** et **PA.Password** comme combinaison de nom d'utilisateur et de mot de passe valide afin de vous connecter à un agent de processus pour exécuter la procédure ext_shutdown.

Pour plus d'informations sur la configuration du serveur ObjectServer pour qu'il s'exécute sous contrôle de processus, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

5. Démarrez l'agent de processus qui exécute le serveur ObjectServer sous contrôle de processus.
6. En supposant que des clients (IDUC et non-IDUC) ont été démarrés dans votre environnement, vous pouvez effectuer un arrêt contrôlé à tout moment en exécutant les commandes SQL suivantes à partir de l'interface SQL interactive :

   ```
   execute procedure control_shutdown;
   go
   ```

   Remarque : Après avoir supprimé tous les clients IDUC, le serveur ObjectServer attend une réponse GET IDUC de la part des clients notifiés. Si l'un des clients IDUC ne répond pas, le serveur ObjectServer reste à l'état restreint. Dans cet état, seul l'utilitaire d'interface SQL interactive (**nco_sql**) est autorisé à se connecter. Vous pouvez demander au serveur ObjectServer d'identifier le client qui ne répond pas en exécutant la commande **nco_sql**. Si le client ne répond pas dans le délai prévu, vous pouvez forcer la déconnexion du client et tenter d'exécuter à nouveau la procédure control_shutdown. Par exemple :

   ```
   select ConnectionId, AppName, AppDesc from iduc_system.temp_connections where Pending =1 ;
   alter system drop connection 'connectionid';
   execute procedure control_shutdown;
   go
   ```

   Pour plus d'informations sur l'interface SQL interactive, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Exemple de fichier de configuration d'agent de processus : AGG_PA.conf

Voici des exemples de valeurs d'un fichier de configuration d'agent de processus appelé `AGG_PA.conf`, mappé aux valeurs de marque de réservation à compléter dans le fichier `control_shutdown.sql` (cf. étapes précédentes).

Le code contient des exemples de valeurs du fichier `AGG_PA.conf`, pour l'agent de processus appelé AGG_PA. Dans le fichier, un processus ObjectServer appelé **MasterObjectServer** a été configuré pour exécuter le serveur ObjectServeur **AGG_P** sous contrôle de processus. Les données d'identification **user1** et **pass1** seront utilisées pour vous connecter à AGG_PA afin d'exécuter la procédure externe ext_shutdown et arrêter le serveur ObjectServer, qui est en cours d'exécution sur l'hôte **nchost1**.

```
===================================
Example Process agent config file  AGG_PA.conf
===================================
#
# Fichier de configuration de démon d'agent de processus version 1.1
#
#
# Liste des processus.
#
nco_process 'MasterObjectServer'
{
        Command '$OMNIHOME/bin/nco_objserv -name AGG_P -pa AGG_PA -pausername user1 -papassword pass1 run as 0
        Host            =       'nchost1'
        Managed         =       True
        RestartMsg  =  '${NAME} running as ${EUID} has been restored on ${HOST}.'
        AlertMsg = '${NAME} running as ${EUID} has died on ${HOST}.'
        RetryCount      =       0
        ProcessType     =       PaPA_AWARE
}

#
```

```
# Liste de services.
#
nco_service 'Core'
{
        ServiceType     =       Master
        ServiceStart    =       Auto
        process 'MasterObjectServer' NONE
}

nco_service 'InactiveProcesses'
{
        ServiceType     =       Non-Master
        ServiceStart    =       Non-Auto
}


#
# Entrées de table de routage.
#
# 'user' - (facultatif) uniquement requis pour l'assembleur désassembleur de paquets en mode sécurisé sur
un hôte cible
#                  'user' doit être membre du groupe UNIX 'ncoadmin'
# 'password' - (facultatif) uniquement obligatoire pour l'assembleur désassembleur de paquets en mode sécurisé
sur l'hôte cible
#                  utiliser nco_pa_crypt pour chiffrer.
nco_routing
{
        host 'nchost1' 'AGG_PA' 'user1' 'pass1'
}
```

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Configuration des serveurs proxy pour la reprise en ligne

La configuration de reprise en ligne du serveur proxy requiert l'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus, ainsi que les composants supplémentaires suivants : un serveur proxy principal et un serveur proxy de secours.

Pourquoi et quand exécuter cette tâche

La figure suivante décrit la configuration de la reprise en ligne du serveur proxy.

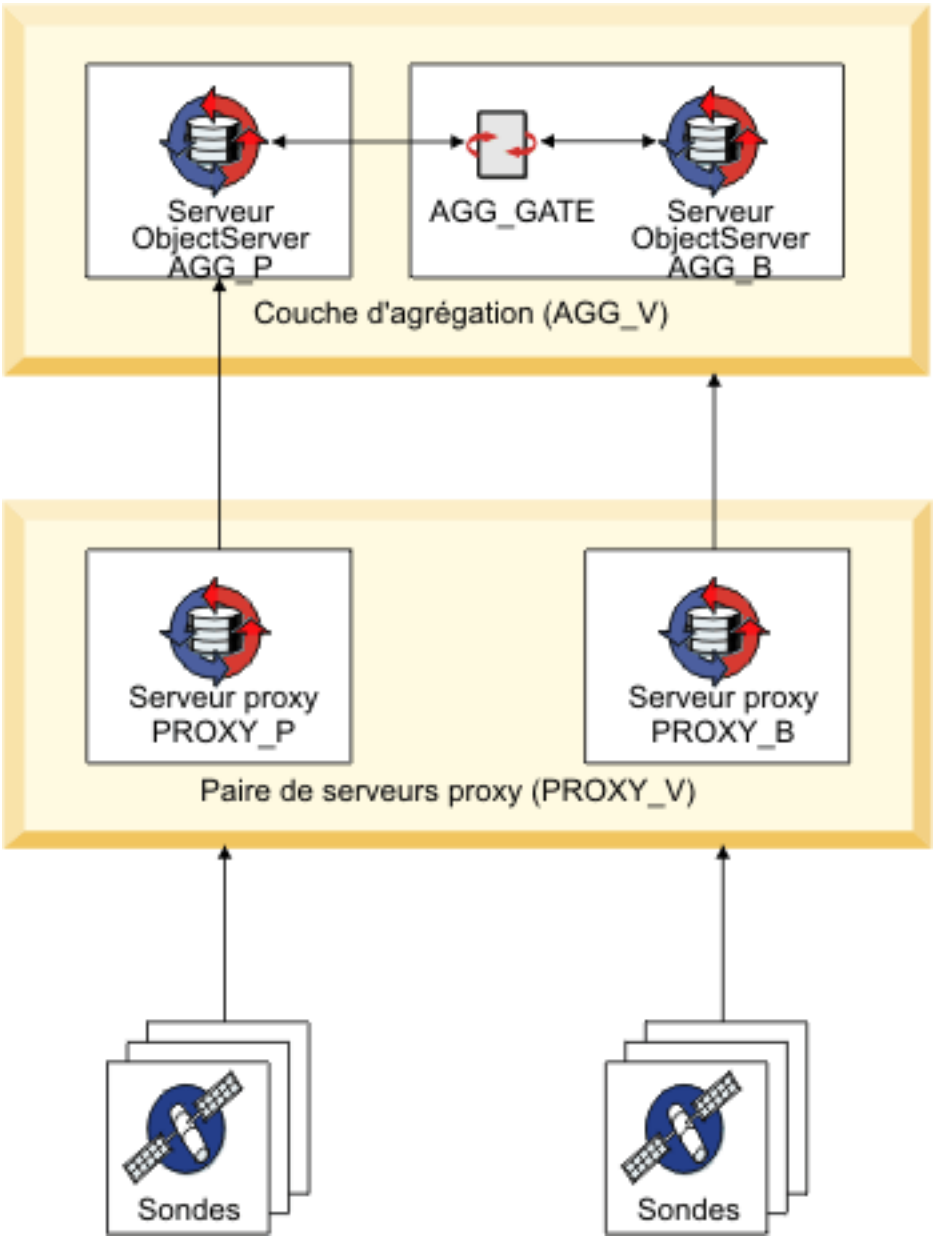

Figure 11. Configuration de la reprise en ligne du serveur proxy

Dans la configuration de reprise en ligne de base, les données d'alerte du serveur ObjectServer d'agrégation principal sont répliquées dans le serveur ObjectServer d'agrégation de secours via une passerelle ObjectServer bidirectionnelle. Si la connexion au serveur ObjectServer d'agrégation principal échoue, les clients tentent de se connecter au serveur ObjectServer d'agrégation de secours. Comme indiqué dans la figure, vous devez configurer une paire de serveurs proxy virtuels auxquels les sondes peuvent se connecter. Configurez le serveur proxy principal PROXY_P pour définir une connexion unique sur le serveur ObjectServer d'agrégation principal AGG_P. Configurez le serveur proxy de secours PROXY_B pour la reprise en ligne de telle façon qu'il se connecte à la paire virtuelle de serveurs ObjectServer AGG_V.

Si vous utilisez un agent de processus pour contrôler le serveur proxy principal dans cette configuration et que le serveur ObjectServer principal échoue, l'agent de

processus peut redémarrer PROXY_P et empêcher le basculement sur PROXY_B. Les sondes se connectant via PROXY_P passent ensuite en mode stockage et retransmission car le serveur ObjectServer principal n'est pas en cours d'exécution et PROXY_P n'a pas basculé sur PROXY_B. Dans un tel cas, vous pouvez faire pointer le serveur proxy principal vers la paire virtuelle ObjectServer AGG_V. Lorsque le serveur ObjectServer principal échoue, les événements routés via PROXY_P sont ensuite envoyés au serveur ObjectServer de secours.

Procédure

A l'aide de l'architecture indiquée dans la figure précédente, configurez les serveurs proxy pour la reprise en ligne, comme suit :

1. Définissez les détails de communication du serveur dans le fichier de données de connexions (`$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini`).

   Utilisez la configuration modèle suivante comme recommandation :

```
[AGG_P]
{
        Primary:        nchost1 10000
}
[AGG_B]
{
        Primary:        nchost2 10001
}
[AGG_GATE]
{
        Primary:        nchost2 10002
}
[AGG_V]
{
        Primary:        nchost1 10000
        Backup:         nchost2 10001

}
[PROXY_P]
{
        Primary:        nchost1 10003
}
[PROXY_B]
{
        Primary:        nchost2 10004
}
[PROXY_V]
{
        Primary:        nchost1 10003
        Backup:         nchost2 10004
}
```

2. Configurez les sondes pour qu'elles se connectent aux serveurs proxy. Dans le fichier de propriétés de sonde :
   - Définissez **Server** sur `PROXY_V`.
   - Définissez **ServerBackup** sur `""`.
3. Dans le fichier de propriétés du serveur proxy principal (PROXY_P), définissez la propriété **RemoteServer**. La valeur que vous définissez varie selon que vous exécutez le serveur proxy sous le contrôle de processus ou non.
   - Si vous n'exécutez pas le serveur de processus principal sous contrôle de processus, définissez **RemoteServer** sur `AGG_P`, comme illustré dans la configuration exemple ci-dessus.
   - Si vous exécutez le serveur de processus principal sous contrôle de processus, définissez **RemoteServer** sur `AGG_V`.

4. Dans le fichier de propriétés du serveur proxy de secours (PROXY_B), définissez **RemoteServer** sur AGG_V.

Résultats

Avec la configuration exemple illustrée ci-dessus, lorsque AGG_P échoue, PROXY_P échoue également, mais les sondes sont automatiquement connectées à PROXY_B, qui lui se connectera à AGG_B. Si seul PROXY_P échoue, les sondes se connecteront automatiquement à PROXY_B, et les événements seront envoyés à AGG_P, qui est toujours en cours d'exécution comme ObjectServer principal.

Si vous exécutez PROXY_P sous contrôle de processus et que vous avez défini sa propriété **RemoteServer** sur AGG_V, les sondes vont continuer à envoyer des événements via le proxy PROXY_P redémarré lequel les enverra ensuite au serveur ObjectServer de secours.

Pour plus d'informations sur l'utilisation du contrôle de processus pour gérer des processus, voir *Tivoli Netcool/OMNIbus Administration Guide*.

Chapitre 10. Configuration de la prise en charge de FIPS 140–2 pour les composants serveur

Vous pouvez exécuter les composants serveur suivants en mode FIPS 140–2 : les serveurs ObjectServer, les agents de processus, les serveurs proxy et les passerelles du serveur ObjectServer. Dans ce mode, les fonctions cryptographiques de Tivoli Netcool/OMNIbus utilisent les modules cryptographiques approuvés par la norme FIPS 140–2.

Pour faire fonctionner Tivoli Netcool/OMNIbus en mode FIPS 140–2, vous devez créer un fichier FIPS dans votre installation et configurer les composants serveur pour le mode FIPS 140–2.

Si vous souhaitez utiliser SSL pour les communications client et serveur, vous devez aussi activer le mode FIPS 140–2 pour les communications SSL.

Référence associée:

«Basculement de votre installation vers le mode FIPS 140-2», à la page 289
Si vous souhaitez changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2, suivez les étapes décrites dans la liste de contrôle de la configuration de FIPS 140-2.

Création du fichier de configuration FIPS

Un fichier de configuration FIPS est requis pour l'initialisation de FIPS. Ce fichier est appelé `fips.conf` et il est obligatoire sur chaque ordinateur sur lequel un composant serveur est installé.

Pourquoi et quand exécuter cette tâche

Avant d'exécuter les composants serveur en mode FIPS 140–2, créez le fichier de configuration FIPS en procédant comme suit :

Procédure

1. Créez un fichier texte vide, appelé `fips.conf`.
2. Sauvegardez ce fichier dans le répertoire correspondant à votre système d'exploitation :
   - UNIX : `$NCHOME/etc/security`
   - Windows : `%NCHOME%\ini\security`

Que faire ensuite

Vous devez à présent configurer les composants serveurs pour le mode FIPS 140–2.

Configuration des composants serveur pour le mode FIPS 140–2

Si les composants serveur sont configurés avec les paramètres obligatoires du mode FIPS 140–2, tous les clients se connectant doivent se connecter avec des mots de passe en texte en clair pour satisfaire aux exigences du mode FIPS 140–2. Si un client utilise le chiffrement des valeurs de propriété, l'algorithme de chiffrement pertinent pour le mode FIPS 140–2 doit également être utilisé.

Lorsque vous exécutez des composants serveur configurés pour le mode FIPS 140–2, ils vérifient l'existence du fichier `fips.conf` ainsi que si leurs propriétés pertinentes sont définies sur les valeurs obligatoires pour le mode FIPS 140–2. Les messages d'erreur sont consignés dans les fichiers journaux du serveur si des propriétés définies sur des paramètres non-FIPS 140–2 sont détectées. En mode de consignation de débogage, la confirmation du mode FIPS 140–2 est également consignée.

Lors de l'exécution d'un composant serveur dans les modes FIPS 140–2 et sécurisé, les mots de passe d'authentification des applications client sont généralement stockés de la manière suivante :

- Les serveurs proxy et les sondes stockent les mots de passe d'authentification à l'aide de la propriété **AuthPassword** dans les fichiers de propriétés du serveur proxy et de la sonde.
- Les passerelles unidirectionnelles du serveur ObjectServer stockent des mots de passe d'authentification à l'aide des propriétés **Gate.Writer.Password** et **Gate.Reader.Password** du fichier de propriétés.
- Les passerelles bidirectionnelles du serveur ObjectServer stockent des mots de passe d'authentification à l'aide des propriétés **Gate.ObjectServerA.Password** et **Gate.ObjectServerB.Password** du fichier de propriétés.
- Le fichier de configuration de l'agent de processus peut également stocker des mots de passe pour les connexions sécurisées.

En mode FIPS 140–2, vous pouvez indiquer des mots de passe en texte en clair dans ces fichiers ou indiquer des mots de passe chiffrés en exécutant l'utilitaire **$NCHOME/omnibus/bin/nco_aes_crypt** avec un fichier de clés et un algorithme cryptographique spécifique. Si vous utilisez des mots de passe chiffrés, vous devez également définir des propriétés qui indiquent le fichier de clés et l'algorithme dans les fichiers de propriétés du serveur proxy, de la sonde et de la passerelle. Ces valeurs sont nécessaires pour déchiffrer les mots de passe lors de l'exécution afin qu'ils puissent être envoyés au serveur en tant que texte en clair. Dans le cas de l'agent de processus, qui n'utilise pas de propriétés, vous devez indiquer des options de ligne de commande pour déchiffrer les mots de passe du fichier de configuration lorsque vous exécutez **$NCHOME/omnibus/bin/nco_pad**.

Remarque : N'utilisez pas les utilitaires **nco_g_crypt**, **nco_pa_crypt** et **nco_sql_crypt** pour chiffrer des mots de passe lors de l'exécution en mode FIPS 140-2.

Configuration du serveur ObjectServer en mode FIPS 140–2

Pour exécuter un serveur ObjectServer en mode FIPS 140–2, la configuration suivante est requise :

- Définissez la propriété **PasswordEncryption** du serveur ObjectServer sur le paramètre `AES`.

- Si vous souhaitez exécuter le serveur ObjectServer en mode sécurisé et chiffrer les mots de passe dans les fichiers de propriétés du serveur proxy, de la sonde ou de la passerelle, chiffrez les mots de passe en exécutant l'utilitaire **nco_aes_crypt** et utilisez l'option de ligne de commande `-c` pour indiquer AES_FIPS en tant qu'algorithme de chiffrement.

Configuration de l'agent de processus pour le mode FIPS 140–2

Pour exécuter un agent de processus en mode FIPS 140–2, la configuration suivante est requise :

- Sous UNIX, seuls les modules PAM sont pris en charge pour l'authentification externe en mode FIPS 140–2. Lors de l'exécution de l'agent de processus avec la commande **nco_pad**, définissez l'option de ligne de commande `-authenticate` sur le paramètre `PAM` si vous souhaitez vérifier les droits d'accès d'un utilisateur ou d'un démon d'agent de processus distant.

  Sous Windows, les connexions d'agent de processus sont authentifiées par rapport aux comptes utilisateur Windows. Aucune configuration supplémentaire n'est requise en mode FIPS 140–2.
- Si vous souhaitez exécuter les utilitaires de contrôle de processus (notamment **$NCHOME/omnibus/bin/nco_pa_status**) avec les options de ligne de commande `-user` et `-password` (droits d'accès de connexion), indiquez les mots de passe en texte en clair.
- Si vous souhaitez exécuter l'agent de processus en mode sécurisé, vous devez généralement indiquer les droits d'accès de connexion suivants dans la section de définition de routage du fichier de configuration de l'agent de processus (`$NCHOME/omnibus/etc/nco_pa.conf`) :
  - Les données d'identification de nom d'utilisateur et de mot de passe de chaque hôte se connectant à l'agent de processus
  - Les données d'identification de nom d'utilisateur et de mot de passe pour se connecter à un agent de processus distant (le cas échéant)

  Si vous souhaitez chiffrer les mots de passe dans le fichier de configuration, exécutez l'utilitaire **nco_aes_crypt** et utilisez l'option de ligne de commande `-c` pour indiquer AES_FIPS en tant qu'algorithme de chiffrement.

Configuration du serveur proxy en mode FIPS 140–2

Pour exécuter un server proxy en mode FIPS 140–2, la configuration suivante est requise :

- Si vous souhaitez exécuter le serveur proxy en mode sécurisé et chiffrer les mots de passe dans les fichiers de propriétés de la sonde, chiffrez les mots de passe en exécutant l'utilitaire **nco_aes_crypt** et utilisez l'option de ligne de commande `-c` pour indiquer AES_FIPS en tant qu'algorithme de chiffrement.
- En outre, si le serveur proxy se connecte à un serveur ObjectServer qui s'exécute en mode sécurisé et que vous souhaitez chiffrer les mots de passe dans les fichiers de propriétés du serveur proxy, chiffrez les mots de passe en exécutant l'utilitaire **nco_aes_crypt** et utilisez l'option de ligne de commande `-c` pour indiquer AES_FIPS en tant qu'algorithme de chiffrement.

Configuration de la passerelle en mode FIPS 140–2

Pour exécuter des passerelles en mode FIPS 140–2, la configuration suivante est requise :

- Sous UNIX, seuls les modules PAM sont pris en charge pour l'authentification externe en mode FIPS 140–2. Lors de l'exécution d'une passerelle, définissez la propriété **Gate.UsePamAuth** de la passerelle sur TRUE pour utiliser l'authentification PAM.
- Si une passerelle se connecte à un serveur ObjectServer qui s'exécute en mode sécurisé et que vous souhaitez chiffrer le mot de passe dans le fichier de propriétés de la passerelle, chiffrez le mot de passe en exécutant l'utilitaire **nco_aes_crypt** et utilisez l'option de ligne de commande -c pour indiquer AES_FIPS en tant qu'algorithme de chiffrement.

Remarque sur les options d'algorithme de chiffrement

Lorsque le mode FIPS 140–2 est activé, vous devez utiliser l'algorithme AES_FIPS lors du chiffrement des mots de passe à l'aide de l'utilitaire **nco_aes_crypt**. Vous pouvez indiquer l'algorithme AES_FIPS ou utiliser son synonyme, AES_CBC, qui permet d'obtenir le même résultat. Dans un souci de simplicité, seul AES_FIPS est indiqué dans la documentation.

En mode FIPS 140–2 désactivé, vous pouvez indiquer un algorithme supplémentaire, AES ou AES_CFB1. Ces deux algorithmes sont synonymes et permettent d'obtenir le même résultat. Dans un souci de simplicité, seuls AES et AES_FIPS sont indiqués dans la documentation. L'option AES permet principalement d'assurer la compatibilité avec le chiffrement de propriétés AES qui est disponible dans Tivoli Netcool/OMNIbus version 7.2. L'utilisation de l'algorithme AES_FIPS est privilégiée.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

Configuration des composants serveur pour le chiffrement étendu SP800-131

Vous pouvez configurer le chiffrement étendu SP800-131 dans le fichier de configuration FIPS pour appliquer le chiffrement TLS 1.2 aux composants serveur prenant en charge le mode FIPS 140-2.

Avant de commencer

Vous devez configurer le mode FIPS 140-2 avant de pouvoir configurer le chiffrement étendu SP800-131. Si vous utilisez des composants Java, vous devez aussi configurer l'environnement d'exécution Java pour le mode FIPS 140-2.

Procédure

1. Ouvrez le fichier de configuration FIPS à éditer. Le fichier de configuration FIPS se trouve dans le répertoire suivant :
   - UNIX Linux `$NCHOME/etc/security/fips.conf`
   - Windows `%NCHOME%\ini\security\fips.conf`
2. Ajoutez les paramètres suivants au fichier `fips.conf` :
   - `SP800_131MODE=TRUE`

Ce paramètre active TLS 1.2.

Pour les composants Java, ce paramètre active également le support JSSE2 SP800-131 (chiffrement SP800-131 «transition»). Lorsque les deux paramètres SP800_131MODE et STRICT_CERTIFICATE_CHECK sont définis sur TRUE, le chiffrement SP800-131 «strict» est activé pour Java.

- TLS12_ONLY=TRUE

  Ce paramètre désactive tous les protocoles sauf TLS 1.2. Utilisez cette valeur lorsque le paramètre SP800_131MODE est défini sur TRUE.

- SHA2_CERTIFICATES_ONLY=TRUE

  Ce paramètre active les restrictions de signature et d'algorithme de hachage de TLS 1.2. Seuls les certificats serveur satisfaisant aux restrictions sont acceptés. Ce paramètre n'a pas d'effet sur les composants Java sauf si le paramètre STRICT_CERTIFICATE_CHECK est également défini sur TRUE.

- STRICT_CERTIFICATE_CHECK=TRUE

  Ce paramètre applique les restrictions de signature et d'algorithme de hachage de TLS 1.2 sur tous les certificats de la chaîne. Utilisez cette valeur uniquement lorsque les paramètres SP800_131MODE et SHA2_CERTIFICATES_ONLY sont également définis sur TRUE.

  Pour les composants Java, utilisez cette valeur uniquement lorsque les paramètresSP800_131MODE, TLS12_ONLY et SHA2_CERTIFICATES_ONLY sont également définis sur TRUE.

Exemple

L'exemple suivant montre comment les paramètres sont répertoriés dans le fichier de configuration FIPS. Vous pouvez omettre les paramètres qui ne sont pas obligatoires pour votre environnement d'exploitation.

```
SP800_131MODE=TRUE
TLS12_ONLY=TRUE
SHA2_CERTIFICATES_ONLY=TRUE
STRICT_CERTIFICATE_CHECK=TRUE
```

Que faire ensuite

Si vous définissez le paramètre SHA2_CERTIFICATES_ONLY ou STRICT_CERTIFICATE_CHECK ou les deux sur TRUE, vous devez utiliser une taille de clé et un algorithme de signature autorisé par NIST SP800-131 lorsque vous générez ou signez des certificats avec l'utilitaire de gestion des certificats et des clés **nc_gskcmd**.

Par exemple, si vous exécutez **nc_gskcmd** avec les options de ligne de commande -cert -create ou -certreq -create, utilisez l'option -size pour spécifier la taille de clé 2048 et l'option -sig_alg pour spécifier l'algorithme de signature SHA512_WITH_RSA.

Si vous exécutez **nc_gskcmd** avec l'option de ligne de commande -cert -sign, utilisez l'option -sig_alg pour spécifier l'algorithme de signature SHA512_WITH_RSA.

Tâches associées:

«Configuration de l'environnement d'exécution Java pour FIPS 140–2», à la page 97
Pour configurer l'environnement d'exécution Java (JRE) fourni avec Tivoli Netcool/OMNIbus pour utiliser le chiffrement FIPS 140-2, modifiez la configuration du fichier java.security. Vous pouvez également télécharger et ajouter des fichiers de règles pour utiliser des algorithmes de chiffrement étendus.

Référence associée:

«Options de ligne de commande nc_gskcmd», à la page 406
L'utilitaire de ligne de commande **nc_gskcmd** fournit davantage de fonctionnalités que l'interface graphique iKeyman.

Configuration requise pour la connexion de clients version 7.2 ou inférieure aux serveurs version 7.2.1 ou supérieure en mode FIPS 140–2

Tivoli Netcool/OMNIbus version 7.2.1, ou supérieure reste compatible en amont avec les applications client existantes lors de l'exécution en mode non-FIPS 140–2. Pour fonctionner en mode FIPS 140–2, une configuration est requise pour les clients version 7.2 ou inférieure qui doivent se connecter aux serveurs s'exécutant en mode sécurisé.

Le tableau suivant décrit la compatibilité entre les clients version 7.2 ou inférieure et les serveurs version 7.2.1 ou supérieure s'exécutant en mode sécurisé, ainsi que les modifications de configuration requises pour le mode FIPS 140–2.

Tableau 55. Compatibilité entre les clients version 7.2 ou inférieure et les serveurs FIPS 140-2 version 7.2.1 ou supérieure en mode sécurisé

Client version 7.2 ou inférieure	**Compatible**	**Modifications de configuration pour la connexion en mode FIPS 140–2**
Passerelles unidirectionnelles et bidirectionnelles	Oui	Les passerelles peuvent s'authentifier et se connecter sur un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé, sans aucune modification.
Client de contrôle de processus (**nco_pad**) et utilitaires de contrôle de processus (**nco_pa_shutdown**, **nco_pa_start**, **nco_pa_status** et **nco_pa_stop**)	Oui	Les clients peuvent se connecter à un agent de processus version 7.2.1 ou supérieure s'exécutant en mode sécurisé si l'application client est démarrée avec l'option `-nosecure` et un mot de passe en texte en clair.
Conductor (**nco**) et listes d'événements (**nco_event** et **nco_elct**)	Non	Les clients ne peuvent pas se connecter à un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé.
Sondes	Oui	Les sondes peuvent se connecter à un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé si elles sont démarrées avec l'option **-nosecurelogin** et un mot de passe en texte en clair. En outre, le paramètre de propriété **AuthPassword** du fichier de propriétés de la sonde ne doit pas être chiffré avec l'utilitaire **nco_crypt** ou **nco_g_crypt**.
Interface interactive SQL (**nco_sql**)	Oui	Les clients peuvent se connecter à un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé s'ils sont démarrés avec l'option `-nosecure`. L'authentification échoue si l'option `-nosecure` n'est pas indiquée.

Tableau 55. Compatibilité entre les clients version 7.2 ou inférieure et les serveurs FIPS 140-2 version 7.2.1 ou supérieure en mode sécurisé (suite)

Client version 7.2 ou inférieure	Compatible	Modifications de configuration pour la connexion en mode FIPS 140–2
Client de serveur proxy (**nco_proxyserv**)	Oui	Les serveurs proxy peuvent se connecter à un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé sans aucune modification.
Client d'agent de processus (**nco_pad**)	Oui	Les agents de processus peuvent se connecter à un serveur ObjectServer version 7.2.1 ou supérieure s'exécutant en mode sécurisé sans aucune modification.
Autres clients	-	Lorsque le serveur ObjectServer est en mode FIPS 140–2, les clients fournissant des mots de passe chiffrés ne peuvent pas se connecter au serveur ObjectServer.

Basculement de votre installation vers le mode FIPS 140-2

Si vous souhaitez changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2, suivez les étapes décrites dans la liste de contrôle de la configuration de FIPS 140-2.

Remarque : Changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2 modifie automatiquement le schéma utilisé pour chiffrer les mots de passe depuis la norme `DES` vers la norme AES (Advanced Encryption Standard).

Si les mots de passe utilisateur de votre système sont chiffrés avec un algorithme DES, ou si vous utilisez un chiffrement de valeurs de propriétés pour chiffrer les valeurs de chaînes dans les fichiers de propriétés, les étapes de configuration pour le mode FIPS 140-2 sont décrites ci-dessous.

Modification du schéma de chiffrement pour les mots de passe utilisateurs chiffrés avec DES

Lorsque le mode FIPS 140–2 est activé, l'algorithme AES (Advanced Encryption Standard) doit être utilisé pour coder les mots de passe utilisateur stockés dans le serveur ObjectServer. Si les mots de passe sont chiffrés avec DES dans votre installation existante, vous devez remplacer ce schéma de chiffrement par AES.

Pour savoir si vos mots de passe sont chiffrés avec DES, vérifiez la valeur de la propriété **`PasswordEncryption`** du serveur ObjectServer pour voir si elle est définie sur DES ou AES.

Pour définir le schéma de chiffrement sur AES :

1. Modifiez la propriété **`PasswordEncryption`** du serveur ObjectServer en la définissant sur `AES`.
2. Vérifiez que tous les mots de passe utilisateur sont modifiés ou redéfinis. Les mots de passe sont maintenant chiffrés via AES. (Voir les informations ci-dessous pour obtenir des instructions sur la modification ou la redéfinition de mots de passe.)
3. Configurez Tivoli Netcool/OMNIbus pour opérer en mode FIPS 140–2.
4. Redémarrez le serveur ObjectServer.

Instructions pour la modification ou la redéfinition des mots de passe

Vous pouvez utiliser l'interface SQL interactive (**nco_sql**) pour modifier ou redéfinir les mots de passe.

Si vous demandez aux utilisateurs de modifier leurs mots de passe, vous devez vérifier que les modifications ont été effectuées et vous devrez probablement envoyer des rappels. Pour vérifier si tous les mots de passe ont été modifiés ou pour identifier ceux devant encore être modifiés, effectuez l'une des actions suivantes :

- Démarrez l'interface interactive SQL et entrez la commande suivante :

  ```
  select UserName,Passwd from security.users;
  ```

  Vérifiez la longueur des mots de passe codés renvoyés. Les mots de passe encore chiffrés avec l'algorithme DES contiennent 11 caractères alors que ceux chiffrés avec l'algorithme AES contiennent 24 caractères.

  Pour obtenir des informations sur le démarrage de l'interface SQL interactive, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.
- A partir de Netcool/OMNIbus Administrator :
  1. Connectez-vous au serveur ObjectServer adéquat. Cliquez ensuite sur le bouton du menu **System (Système)** et cliquez sur **Databases (Bases de données)** pour ouvrir le panneau Databases, Tables and Columns (Bases de données, tables et colonnes).
  2. Sélectionnez la base de données **sécurité** et la table **utilisateurs**, puis cliquez sur l'onglet **Data View** (Vue des données) dans le panneau Databases, Tables and Columns (Bases de données, tables et colonnes) pour visualiser les données utilisateur.

     Dans la colonne **Passwd** (Mot de passe), les mots de passe qui sont toujours chiffrés via DES contiennent 11 caractères, alors que les mots de passe qui sont chiffrés via AES en contiennent 24.

Un administrateur système peut réinitialiser les mots de passe utilisateur à partir de l'interface SQL interactive de la manière suivante :

```
alter user 'nom d'utilisateur' set password 'mot de passe';
```

Où *nom d'utilisateur* correspond au nom de l'utilisateur et *mot de passe* aux nouveaux mots de passe.

Modification du chiffrement de valeur de propriété

Lorsque le mode FIPS 140–2 est activé, le chiffrement des valeurs de propriété doit être exécuté à l'aide d'un algorithme et d'un mode d'opération définis comme AES_FIPS. Le chiffrement des valeurs de propriété est utilisé pour chiffrer des valeurs de chaîne dans un fichier de propriétés ou dans un fichier de configuration de sorte que les chaînes ne puissent pas être lues sans clé.

Si votre installation existante utilise le chiffrement de valeur de propriété avec l'algorithme AES, ou utilise les utilitaires **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe, ces valeurs chiffrées ne répondent pas aux critères permettant le fonctionnement du mode FIPS 140–2. Pour exécuter votre système en mode FIPS 140–2, vous devez déchiffrer ces valeurs puis les chiffrer à nouveau à l'aide de l'algorithme AES_FIPS. Vous devez exécuter cette tâche pour chaque ObjectServer,

serveur proxy, agent de processus, sonde et passerelle utilisant des valeurs de propriété chiffrées, dont des mots de passe.

Pour modifier le chiffrement de la valeur de la propriété (et du mot de passe) en mode FIPS 140–2, procédez comme suit :

1. Dans votre installation existante, identifiez toutes les clés générées à l'aide du générateur de clés de la ligne de commande **nco_keygen**.

   Conseil : L'utilitaire **nco_keygen** stocke des clés dans des fichiers de clés. Vous devez pouvoir identifier tous les fichiers de clés utilisés en vérifiant les paramètres de la propriété **ConfigKeyFile** de votre fichiers de propriétés.
2. A l'aide des clés de votre installation existante, déchiffrez toutes les propriétés et tous les mots de passe chiffrés de vos fichiers de propriétés et de configuration en exécutant l'utilitaire **nco_aes_crypt** avec l'option de la ligne de commande `-d`.
3. Configurez Tivoli Netcool/OMNIbus pour opérer en mode FIPS 140–2.
4. Chiffrez de nouveau les valeurs à l'aide de l'utilitaire **nco_keygen** afin de générer une ou plusieurs nouvelles clés, puis à l'aide de l'utilitaire **nco_aes_crypt** avec le paramètre de fichier de clés approprié.

Concepts associés:

Chapitre 10, «Configuration de la prise en charge de FIPS 140–2 pour les composants serveur», à la page 283
Vous pouvez exécuter les composants serveur suivants en mode FIPS 140–2 : les serveurs ObjectServer, les agents de processus, les serveurs proxy et les passerelles du serveur ObjectServer. Dans ce mode, les fonctions cryptographiques de Tivoli Netcool/OMNIbus utilisent les modules cryptographiques approuvés par la norme FIPS 140–2.

Tâches associées:

«Configuration de l'environnement d'exécution Java pour FIPS 140–2», à la page 97
Pour configurer l'environnement d'exécution Java (JRE) fourni avec Tivoli Netcool/OMNIbus pour utiliser le chiffrement FIPS 140-2, modifiez la configuration du fichier `java.security`. Vous pouvez également télécharger et ajouter des fichiers de règles pour utiliser des algorithmes de chiffrement étendus.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

«Options de ligne de commande nco_aes_crypt», à la page 370
Vous pouvez utiliser l'utilitaire **nco_aes_crypt** pour chiffrer et déchiffrer les valeurs de chaîne ou les données contenues dans un fichier.

Chapitre 11. Importation et exportation de configurations du serveur ObjectServer

Tivoli Netcool/OMNIbus fournit deux utilitaires, nommés **nco_confpack** et **nco_osreport** ; vous pouvez les utiliser pour importer et exporter les configurations d'un serveur ObjectServer.

Les utilitaires **nco_confpack** et **nco_osreport** exigent que la version appropriée de Java Runtime Environment (JRE) soit installée sur votre système. Les dispositifs permettant d'installer ces utilitaires utilisent JRE, qui est fourni avec Tivoli Netcool/OMNIbus.

nco_osreport

L'utilitaire **nco_osreport** permet d'effectuer les tâches suivantes :

- Exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peuvent être entrés dans un nouvel ObjectServer créé à l'aide de la commande **nco_dbinit**.

  En exportant les contenus d'un serveur ObjectServer vers des fichiers SQL, vous pouvez créer une copie du serveur ObjectServer sur des systèmes d'exploitation autres que le serveur ObjectServer source. Vous pouvez afficher et modifier les fichiers SQL avant de les utiliser pour créer un nouvel ObjectServer ; vous pouvez également utiliser ces fichiers pour archiver les contenus du serveur ObjectServer sous une forme qui soit indépendante des considérations de systèmes d'exploitation. De plus, vous pouvez utiliser les fichiers SQL exportés pour soumettre les contenus du serveur ObjectServer à une équipe d'assistance technique de sorte qu'ils soient lisible à l'oeil.
- Exporter les contenus des tables du serveur ObjectServer vers un fichier HTML afin de capturer une image instantanée d'une configuration du serveur ObjectServer qui servirait, par exemple, à soumettre cette configuration à une équipe d'assistance technique.
- Exporter les contenus des tables du serveur ObjectServer vers un fichier XML qui pourrait être utilisé lors de la programmation, par exemple.

nco_confpack

L'utilitaire **nco_confpack** permet d'extraire un sous-ensemble d'objets de configuration (par exemple, les menus, les outils, les déclencheurs et les procédures de listes d'événements ainsi que les numéros de classe) à partir de serveurs ObjectServer et d'importer ces objets vers d'autres serveurs ObjectServer existants. L'utilitaire **nco_confpack** n'est pas adapté à l'importation de configurations complètes de serveurs ObjectServer. Pour extraire une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer à partir duquel vous souhaitez extraire la configuration. Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Les serveurs ObjectServer source et cible peuvent se trouver sur différentes installations de Tivoli Netcool/OMNIbus. Vous pouvez exporter la configuration à partir d'une installation, l'envoyer à une installation sur un autre serveur et importer la configuration vers un serveur ObjectServer sur cette installation.

Remarque : Lorsque **nco_confpack** tente d'importer un objet de configuration, il vérifie si l'objet existe déjà dans le serveur ObjectServer cible. Si l'objet existe déjà, **nco_confpack** modifie l'objet cible pour qu'il corresponde à l'objet en cours d'importation. Si l'objet n'existe pas dans le serveur ObjectServer cible, **nco_confpack** le crée dans cet emplacement. **nco_confpack** ne supprime pas un objet qui existe déjà dans le serveur ObjectServer cible.

Ce comportement rend **nco_confpack** inadapté pour la réplication ou le clonage de la totalité des serveurs ObjectServer. Il n'est destiné qu'à l'exportation et l'importation des données de configuration partielles entre les serveurs ObjectServer. Utilisez **nco_osreport** pour répliquer ou cloner des serveurs ObjectServer entiers.

Concepts associés:

«Exigences de l'environnement d'exécution Java (JRE)», à la page 49
L'interface graphique de Netcool/OMNIbus Administrator, l'utilitaire Confpack (**nco_confpack**) et un composant de notification d'événement accéléré exigent que l'environnement d'exécution Java (JRE) soit installé sur votre système.

«A propos de l'utilitaire nco_osreport»
L'utilitaire **nco_osreport** exporte le contenu des tables d'un serveur ObjectServer vers un fichier HTML ou XML. Il peut également servir à exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peut être utilisée pour créer les contenus initiaux d'un nouvel ObjectServer.

Exportation et importation de configurations ObjectServer à l'aide de l'utilitaire nco_osreport

L'utilitaire **nco_osreport** permet d'extraire le contenu des tables d'un serveur ObjectServer vers des fichiers HTML, XML ou SQL. Vous pouvez utilisez les fichiers SQL extraits pour cloner les serveurs ObjectServer.

A propos de l'utilitaire nco_osreport

L'utilitaire **nco_osreport** exporte le contenu des tables d'un serveur ObjectServer vers un fichier HTML ou XML. Il peut également servir à exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peut être utilisée pour créer les contenus initiaux d'un nouvel ObjectServer.

Après avoir exécuté l'utilitaire à l'aide de l'option de ligne de commande `-dbinit`, vous pouvez utiliser la commande **nco_dbinit** pour créer un nouvel ObjectServer à partir des contenus du serveur ObjectServer exporté.

Le chemin d'accès complet vers l'utilitaire **nco_osreport** est `$NCOME/omnibus/bin/nco_osreport`.

Fichiers SQL créés par l'utilitaire nco_osreport

Après que vous avez exécuté l'utilitaire **nco_osreport** à l'aide de l'option de ligne de commande `-dbinit`, les fichiers suivants sont générés :

- `system.sql` : ce fichier indique la base de données et les tables de sécurité, les utilisateurs système, les groupes, les rôles ainsi que les autorisations. Vous ne devez pas l'éditer.
- `application.sql` : Ce fichier crée les tables initiales pour les bases de données `alerts` et `tools`.

- `alertsdata.sql` : Les contenus des tables extérieures au système sont exportés vers ce fichier.

  Si vous utilisez l'utilitaire **nco_dbinit** pour importer les fichiers SQL vers un nouvel ObjectServer, ce fichier sera utilisé à la place d'`application.sql` pour créer les tables par défaut des bases de données `alerts` et `tools`. Si vous ne voulez pas importer toutes les données de ce fichier vers un nouvel ObjectServer, vous pouvez éditer ce fichier. Indiquez les *deux* arguments de *alertsdata.sql*, `-alertsdata` *et* `-alertsdatafile`. Si vous n'incluez pas ces deux arguments, beaucoup de tables resteront vides. Les fichiers générés par l'utilitaire **nco_osreport** incluent *alertsdata.sql* de manière à conserver les références de table croisées. Les références de table croisées sont généralement basées sur les colonnes de type INCR. L'utilitaire **nco_dbinit** réaffecte généralement des valeurs aux colonnes INCR car il remplit les tables ; cette opération est suspendue lors de la lecture de `alertsdata.sql`.
- `desktop.sql` : ce fichier indique les valeurs initiales des tables de bureau, y compris les couleurs, les conversions, les outils et les menus par défaut. Ce fichier est vide mais il est fournit dans un souci de complétude, car il est demandé par l'utilitaire **nco_dbinit**.
- `automation.sql` : Ce fichier crée les groupes de déclencheurs initiaux, les déclencheurs et les procédures.

  Dans ce fichier, les déclencheurs et les procédures internes sont définis deux fois : une fois avec un corps vide, une fois avec la valeur définie dans la configuration du serveur ObjectServer exporté. Ces doublons garantissent que lorsqu'une référence est importée d'une automatisation à l'autre, l'automatisation référencée est reconnue par le serveur ObjectServer cible (c'est-à-dire, le serveur ObjectServer que l'utilitaire **nco_dbinit** est sur le point de créer).
- `security.sql` : ce fichier indique les rôles opérateur et administrateur supplémentaires. Les propriétaires des entités du serveur ObjectServer source n'ont accès qu'aux entités qu'ils détiennent dans le serveur ObjectServer exporté ; les droits de propriétés sont transmis à l'utilisateur root.

Exemples

Pour générer un fichier HTML contenant le contenu des tables d'un serveur ObjectServer qui n'est pas défini dans le fichier d'interfaces et exporter le fichier vers un répertoire spécifique, exécutez l'utilitaire **nco_osreport** de la façon suivante :

```
$NCHOME/omnibus/bin/nco_osreport -html -server NCOMS -user root
-password ' ' -directory /home/output/html
```

Tâches associées:

«Exportation de configurations ObjectServer et clonage de serveurs ObjectServer», à la page 296
Les options de ligne de commande de l'utilitaire **nco_osreport** permettent de sélectionner le format dans lequel l'utilitaire exporte les contenus d'un serveur ObjectServer. Les contenus exportés vers des fichiers SQL peuvent être utilisés pour créer un nouvel ObjectServer à l'aide de la commande **nco_dbinit**.

Référence associée:

«Options de ligne de commande pour la commande nco_osreport», à la page 297
Utilisez les options de ligne de commande de l'utilitaire **nco_osreport** pour indiquer le type de sortie demandé et le serveur ObjectServer que vous souhaitez exporter.

Exportation de configurations ObjectServer et clonage de serveurs ObjectServer

Les options de ligne de commande de l'utilitaire **nco_osreport** permettent de sélectionner le format dans lequel l'utilitaire exporte les contenus d'un serveur ObjectServer. Les contenus exportés vers des fichiers SQL peuvent être utilisés pour créer un nouvel ObjectServer à l'aide de la commande **nco_dbinit**.

Pourquoi et quand exécuter cette tâche

Pour exporter des configurations ObjectServer ou utiliser les fichiers exportés pour créer de nouveaux serveurs ObjectServer :

Procédure

- Pour exporter les tables d'un serveur ObjectServer vers un fichier HTML unique, exécutez l'utilitaire **nco_osreport** à l'aide de l'option `-html`.
- Pour exporter les tables d'un serveur ObjectServer vers un fichier XML unique file, exécutez l'utilitaire **nco_osreport** à l'aide de l'option `-xml`.
- Pour exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL et utiliser ces fichiers pour créer un nouvel ObjectServer :
  1. Exécutez l'utilitaire **nco_osreport** à l'aide de l'option `-dbinit`.
  2. Accédez au répertoire vers lequel les fichiers SQL ont été exportés.
  3. Pour créer un nouvel ObjectServer basé sur la configuration du serveur ObjectServer exporté, exécutez l'utilitaire **nco_dbinit** comme suit :

     ```
     $NCHOME/omnibus/bin/nco_dbinit -server NOM DE SERVEUR
     -systemfile system.sql -applicationfile application.sql
     -alertsdata -alertsdatafile alertsdata.sql
     -desktopfile desktop.sql -automationfile automation.sql
     -securityfile security.sql
     ```

     Dans cette commande, *NOM DE SERVEUR* est le nom du nouvel ObjectServer que vous voulez créer, et les arguments *.sql* sont les noms et chemins de fichiers devant être lus par l'utilitaire **nco_dbinit**.

     Important :
  4. Ajoutez les caractéristiques des communications du serveur ObjectServer nouvellement créé en exécutant l'utilitaire **nco_xigen** sous UNIX ou l'éditeur de serveurs sous Windows.
  5. Démarrez le nouvel ObjectServer.

Que faire ensuite

Si vous avez créé un nouvel ObjectServer, utilisez l'utilitaire **nco_config**, **nco_sql**, **nco_event** ou l'Interface graphique Web pour vérifier certaines des données de cet ObjectServer. S'il apparaît qu'aucune donnée n'a été incluse, vous avez peut-être oublié d'utiliser les deux arguments`-alertsdata` et `-alertsdatafile` de *alertsdata.sql* pour l'utilitaire **nco_dbinit**.

Concepts associés:

«A propos de l'utilitaire nco_osreport», à la page 294
L'utilitaire **nco_osreport** exporte le contenu des tables d'un serveur ObjectServer vers un fichier HTML ou XML. Il peut également servir à exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peut être utilisée pour créer les contenus initiaux d'un nouvel ObjectServer.

Tâches associées:

«Après avoir créé un serveur ObjectServer», à la page 202
Après avoir créé un serveur ObjectServer, vous devez utiliser l'éditeur de serveurs pour ajouter des détails de communication pour le serveur ObjectServer sur la machine hôte et sur chaque machine qui doit se connecter au serveur ObjectServer.

«Démarrage d'un serveur ObjectServer», à la page 202
Vous devez exécuter un serveur ObjectServer avant d'utiliser les composants de Tivoli Netcool/OMNIbus.

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Référence associée:

«Options de ligne de commande pour la commande nco_osreport»
Utilisez les options de ligne de commande de l'utilitaire **nco_osreport** pour indiquer le type de sortie demandé et le serveur ObjectServer que vous souhaitez exporter.

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Options de ligne de commande pour la commande nco_osreport

Utilisez les options de ligne de commande de l'utilitaire **nco_osreport** pour indiquer le type de sortie demandé et le serveur ObjectServer que vous souhaitez exporter.

Le tableau suivant décrit les options de ligne de commande de la commande **nco_osreport**. Les options de ligne de commande `-dbinit`, `-xml` et `-html` sont mutuellement exclusives.

Tableau 56. Options de ligne de commande de la commande **nco_osreport**

Option de ligne de commande	Description
`-directory` *chaîne*	Indique un répertoire dans lequel la sortie de l'utilitaire est stockée. Si vous n'utilisez pas cette option pour indiquer un répertoire, le ou les fichiers sont exportés vers le répertoire de travail en cours
`-dbinit`	Par défaut : Extrait la configuration du serveur ObjectServer indiqué et la stocke dans une série de fichiers SQL. L'utilitaire **nco_dbinit** peut utiliser ces fichiers SQL pour importer la configuration du serveur ObjectServer indiqué vers un nouvel ObjectServer.
`-help`	Affiche des informations d'aide sur les options de ligne de commande.

Tableau 56. Options de ligne de commande de la commande **nco_osreport** *(suite)*

Option de ligne de commande	Description
`-host` *chaîne*	Si le serveur ObjectServer requis n'est pas défini dans le fichier d'interfaces, utilisez cette option de ligne de commande avec l'option `-port` pour indiquer le nom qualifié complet du serveur sur lequel le serveur ObjectServer est installé.
`-html`	Extrait les contenus des tables du serveur ObjectServer indiqué vers un fichier HTML unique. Par défaut, le fichier de sortie est nommé `osreport.html`.
`-password` *chaîne*	Le mot de passe de l'utilisateur spécifié.
`-port` *chaîne*	Le numéro de port sur lequel le serveur ObjectServer est installé sur le serveur indiqué par l'option `-hostname` est en mode écoute des événements.
`-server` *chaîne*	Nom du serveur ObjectServer, tel qu'il est indiqué dans le fichier d'interfaces, à partir duquel extraire la configuration ou les tables. **Remarque :** Spécifie soit l'option de ligne de commande `-server`, soit la combinaison des options de ligne de commande `-host` et `-port`.
`-user` *chaîne*	Le nom d'utilisateur pour se connecter au serveur ObjectServer indiqué par l'option de ligne de commande `-server`.
`-timeout` *chaîne*	Indique le délai, en millisecondes, qu'attend l'utilitaire pour obtenir une réponse du serveur ObjectServer, où *chaîne* représente le délai. Le délai par défaut est 6000 millisecondes (une minute).
`-version`	Affiche les informations de version de logiciel et quitte.
`-xml`	Extrait les contenus des tables du serveur ObjectServer indiqué vers un fichier XML unique. Par défaut, le fichier de sortie est nommé `osreport.xml`.
`-ignoreerrors`	Ignore les erreurs et les corruptions d'ObjectServer.

Concepts associés:

«A propos de l'utilitaire nco_osreport», à la page 294
L'utilitaire **nco_osreport** exporte le contenu des tables d'un serveur ObjectServer vers un fichier HTML ou XML. Il peut également servir à exporter la configuration d'un serveur ObjectServer vers une série de fichiers SQL qui peut être utilisée pour créer les contenus initiaux d'un nouvel ObjectServer.

Tâches associées:

«Exportation de configurations ObjectServer et clonage de serveurs ObjectServer», à la page 296
Les options de ligne de commande de l'utilitaire **nco_osreport** permettent de sélectionner le format dans lequel l'utilitaire exporte les contenus d'un serveur ObjectServer. Les contenus exportés vers des fichiers SQL peuvent être utilisés pour créer un nouvel ObjectServer à l'aide de la commande **nco_dbinit**.

Exportation et importation de données de configuration à l'aide de l'utilitaire nco_confpack

L'utilitaire **nco_confpack** vous permet d'exporter et d'importer des données de configuration entre des serveurs ObjectServer.

Terminologie de l'importation et de l'exportation

Un certain nombre de termes sont utilisés dans les instructions pour importer et exporter des configurations du serveur ObjectServer.

Ces termes sont les suivants :

- Serveurs ObjectServer *source* et *cible* : exportez des objets de configuration à partir du serveur ObjectServer source et importez des objets dans le serveur ObjectServer cible.
- *Fichiers de liste de configuration* : il s'agit de fichiers qui détaillent les objets que vous pouvez exporter à partir d'un serveur ObjectServer. Vous pouvez ensuite sélectionner les objets à exporter depuis ou à importer dans un serveur ObjectServer.
- *Package de configuration* : lorsque vous exportez des objets de configuration à partir d'un serveur ObjectServer, les objets sont sauvegardés dans un package de configuration. Utilisez le package de configuration pour importer des objets dans un serveur ObjectServer cible. Les packages de configuration sont sauvegardés en tant que fichiers archive Java (`.jar`).

Objets importables et exportables

L'utilitaire **nco_confpack** vous permet d'importer et d'exporter un certain nombre d'objets du serveur ObjectServer.

Parmi ces objets figurent :

- Déclencheurs
- Groupes de déclencheurs
- Procédures
- Signaux définis par l'utilisateur
- Menus
- Outils
- Invites
- Classes
- Conversions
- Visuels de colonne
- Couleurs
- Utilisateurs
- Groupes
- Rôles

- Tables
- Index
- Vues
- Filtres de restriction
- Définitions de fichier du serveur ObjectServer

Remarque : L'utilitaire **nco_confpack** n'importe ou n'exporte pas les permissions accordées des tables considérées comme étant des objets système.

Les tables considérées comme étant des objets système pour les rôles créés dans le serveur source ObjectServer ne contiennent pas leurs autorisations accordées dans le serveur cible ObjectServer lorsqu'elles sont importées ou exportées à l'aide de l'utilitaire **nco_confpack**. Les tables standard suivantes sont considérées comme étant des objets système :

- Toutes les tables standard de la base de données de catalogue
- Toutes les tables standard de la base de données de conservation
- Toutes les tables standard de la base de données de sécurité
- Toutes les tables standard de la base de données de transfert

Les tables non considérées comme étant des objets système dans le serveur source ObjectServer contiennent encore leurs autorisations accordées dans le serveur cible ObjectServer lorsqu'elles sont importées ou exportées à l'aide de l'utilitaire **nco_confpack** . Les tables standard suivantes ne sont pas considérées comme étant des objets système :

- Toutes les tables standard de la base de données d'alertes
- Toutes les tables standard de la base de données iduc_system
- Toutes les tables standard de la base de données maître
- Toutes les tables standard de la base de données de précision
- Toutes les tables standard de la base de données de service
- Toutes les tables standard de la base de données d'outils

Remarque :

- Les tables standard sont créées lorsque le serveur ObjectServer est initialisé.
- Les groupes de déclencheurs et les invites sont exportés de manière indirecte, en fonction de leur association avec les déclencheurs et les outils. Lors de l'exportation des déclencheurs, les groupes de déclencheurs sont automatiquement exportés. De la même manière, lorsque des outils sont exportés, les invites sont automatiquement exportées.
- Les objets système, qui incluent les utilisateurs système, les groupes de systèmes, les rôles système et les signaux système, ne peuvent pas être exportés ou importés.
- La propriété de l'objet dans le serveur ObjectServer source n'est pas importée dans le serveur ObjectServer cible. L'utilisateur important l'objet devient le propriétaire de celui-ci dans le serveur ObjectServer cible.

Propriétés et options de ligne de commande pour nco_confpack

L'utilitaire **nco_confpack** inclut un certain nombre de propriétés et d'options de ligne de commande. Vous devez indiquer des *sous-commandes* supplémentaires pour la plupart des options de ligne de commande.

Le tableau suivant répertorie les propriétés et les options de ligne de commande pour **nco_confpack**.

Tableau 57. Options de ligne de commande et propriétés pour nco_confpack

Option de ligne de commande	Propriété	Description
`-contents` *paramètre -sous-commande, ...*	N/D	Répertorie le contenu d'un package de configuration.
`-dumpprops`	N/D	Affiche les propriétés système et de **nco_confpack**.
`-export` *paramètre -sous-commande, ...*	N/D	Exporte les objets de configuration sélectionnés à partir d'un serveur ObjectServer source dans un package de configuration.
`-help`	N/D	Affiche l'aide pour **nco_confpack** et quitte.
`-import` *paramètre -sous-commande, ...*	N/D	Extrait des objets d'un package de configuration et les importe dans un serveur ObjectServer cible.
`-list` *paramètre -sous-commande, ...*	N/D	Crée une liste des objets de configuration exportables dans un serveur ObjectServer source.
N/D	**nc.home** *chaîne*	Chemin d'accès complet à l'emplacement de base de Netcool. Cette propriété prend la valeur de NCHOME. La valeur peut être ignorée, mais ce n'est pas recommandé. La valeur par défaut est `/opt/netcool`.
N/D	**omni.home** *chaîne*	Chemin d'accès complet vers l'installation de Tivoli Netcool/OMNIbus. Cette propriété prend la valeur de `NCHOME/omnibus`. La valeur peut être ignorée, mais ce n'est pas recommandé. La valeur par défaut est `/opt/netcool/omnibus`.
`-version`	N/D	Affiche la version du programme et quitte.

La valeur par défaut du fichier de propriétés de **nco_confpack** est `$NCHOME/omnibus/etc/nco_confpack.props`. Vous pouvez utiliser le fichier de propriétés avec les options de ligne de commande `-list`, `-export`, `-contents` et `-import`.

Conseil : Vous pouvez utiliser le fichier de propriétés en tant qu'alternative à la saisie de sous-commandes dans la ligne de commande. C'est utile, par exemple, si vous avez besoin d'exporter fréquemment la même configuration du serveur ObjectServer.

Dans un fichier de propriétés non édité, toutes les propriétés sont répertoriées avec leurs valeurs par défaut, commentées par un symbole dièse (#) au début de la ligne. Une propriété et sa valeur correspondante sont séparées par deux points (:). Les valeurs de chaîne sont encadrées par des guillemets simples, droits.

Vous pouvez utiliser le fichier de propriétés en tant que modèle et le modifier à différentes fins. Par exemple, vous pouvez posséder un fichier de propriétés pour créer un fichier de liste, un pour exporter des configurations et un pour importer des configurations. Vous pouvez éditer les valeurs de propriété à l'aide d'un éditeur de texte. Pour ignorer la valeur par défaut, modifiez un paramètre dans le fichier de propriétés et supprimez le symbole dièse.

Remarque : Commencez les commentaires sur une nouvelle ligne. Sinon, les valeurs de propriété ne sont pas lues correctement.

Si vous indiquez un paramètre dans la ligne de commande, il écrase la valeur par défaut et le paramètre du fichier de propriétés.

Exemple : utilisation des options de ligne de commande pour répertorier, exporter et importer des objets de configuration

Cet exemple présente comment utiliser l'utilitaire **nco_confpack**.

La commande suivante permet de créer le fichier de liste de configuration `confpack.list`, qui détaille les objets du serveur ObjectServer appelé MASTER.

```
nco_confpack -list -file confpack.list -server MASTER -user root
```

Editez le fichier de liste de configuration pour supprimer les objets que vous ne souhaitez pas exporter. Par exemple, si vous souhaitez uniquement exporter les menus et outils, supprimez tous les objets sauf les menus et les outils.

Ensuite, créez un package de configuration. La commande suivante permet d'exporter les objets détaillés dans le fichier de liste de configuration `confpack.list` et de produire un package de configuration appelé `menutools.jar`.

```
nco_confpack -export -file confpack.list -package menutools.jar -user root
```

Vous n'avez pas besoin d'indiquer le nom du serveur ObjectServer dans la commande précédente car le nom est indiqué dans le fichier de liste.

La commande suivante permet d'importer les objets du package `menutools.jar` dans le serveur ObjectServer TEST.

```
nco_confpack -import -package menutools.jar -user root -server TEST -nowarn
```

Référence associée:

«Exemple : fichier de liste de configuration», à la page 309
L'exemple suivant de fichier de liste de configuration partiel est créé à partir d'une installation de Tivoli Netcool/OMNIbus comprenant deux serveurs ObjectServer (NCOMS1 et NCOMS2) s'exécutant sur le même hôte.

Création et édition des fichiers de liste de configuration

Les fichiers de liste de configuration vous permettent d'afficher les objets exportables dans un serveur ObjectServer et de sélectionner les objets à exporter de ou à importer dans un serveur ObjectServer.

Lors de l'exportation d'une configuration, le fichier de liste détermine les objets exportables à inclure dans le package de configuration. Pour sélectionner les objets à exporter dans un package de configuration, vous devez éditer le fichier de liste.

Tâches associées:

«Edition des fichiers de liste de configuration», à la page 308
Vous pouvez modifier les fichiers de liste de configuration pour spécifier les objets à exporter d'un serveur ObjectServer source ou à importer dans un serveur ObjectServer cible.

Création des fichiers de liste de configuration

Pour créer un fichier de liste de configuration pour un serveur ObjectServer, entrez la commande suivante :

```
$NCHOME/omnibus/bin/nco_confpack -list [ paramètre -sous-commande, ... ]
```

Dans cette commande, la variable *paramètre -sous-commande* peut être n'importe quelle sous-commande du tableau suivant.

Tableau 58. Sous-commandes et propriétés correspondantes pour l'option -list de nco_confpack

Sous-commande	Propriété	Description
`-file` *chaîne*	**`confpack.list.name`** *chaîne*	Nom de chemin et de fichier de la liste de configuration de sortie. La valeur par défaut est `stdout`.

Tableau 58. Sous-commandes et propriétés correspondantes pour l'option -list de nco_confpack (suite)

Sous-commande	Propriété	Description

`-memstoredatadirectory` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.***nom-serveurOS* **.memstoredatadirectory** *chaîne*	Indique un répertoire de base de données alternatif pour chaque ObjectServer, où :
		• *nom-serveurOS* représente le nom du serveur ObjectServer.
		• *chaîne* représente le chemin contenant les fichiers base de données du serveur ObjectServer. La valeur par défaut est `$NCHOME/omnibus/db`.
		• *nom-serveurOS* peut être remplacé par un astérisque (*) pour indiquer un chemin d'accès général pour tous les serveurs ObjectServer pour lesquels aucun chemin d'accès explicite n'est indiqué.
		• Si le chemin d'accès est identique pour tous les serveurs ObjectServer, la variable *nom-serveurOS* peut être omise. Par exemple : `-memstoredatadirectory` *chaîne*
		
		Vous pouvez avoir plusieurs entrées dans le même fichier de propriétés pour différents serveurs ObjectServer. Exemple :
		`objectserver.NCOMSA.`
		`  memstoredatadirectory : path1`
		`objectserver.NCOMSB.`
		`  memstoredatadirectory : path2`
		
		Remarque : Sous Windows, si vous souhaitez indique un chemin d'accès qui inclut un identificateur d'unité, n'omettez *pas* la valeur *nom-serveurOS* car l'identificateur d'unité est interprété comme un nom du serveur ObjectServer. Par exemple, si vous indiquez `-memstoredatadirectory C:\MyDir`, la lettre C est interprétée comme le nom du serveur ObjectServer.

Tableau 58. Sous-commandes et propriétés correspondantes pour l'option -list de nco_confpack (suite)

Sous-commande	Propriété	Description

`-password` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.***nom-serveurOS***.password** *chaîne*	Mot de passe de connexion des serveurs ObjectServer, où :
		• *nom-serveurOS* est le nom du serveur ObjectServer
		• *chaîne* est le mot de passe de connexion
		• Si le mot de passe est identique pour tous les serveurs ObjectServer, *nom-serveurOS* peut être omis
		• *nom-serveurOS* peut être remplacé par un astérisque (*) suivi d'un mot de passe à utiliser pour tous les serveurs ObjectServer pour lesquels un mot de passe n'est pas fourni
		• Si un nom d'utilisateur et un mot de passe sont définis, mais pas pour tous les serveurs ObjectServer, les serveurs ObjectServer restants sont définis par défaut sur l'utilisateur système actuel sans mot de passe
		La valeur *nom-serveurOS* par défaut est tous les serveurs ObjectServer s'exécutant sur la machine locale.
		Le mot de passe par défaut est `''`.
		Vous pouvez avoir plusieurs entrées dans le fichier de propriétés pour vous connecter à différents serveurs ObjectServer. Par exemple :
		`objectserver.NCOMSA.password : mdp1`
		`objectserver.NCOMSB.password : mdp2`

`-propsfile` *chaîne*	N/D	Indique le fichier de propriétés de **nco_confpack**. Vous pouvez utiliser le fichier de propriétés au lieu d'entrer des sous-commandes individuelles dans la ligne de commande. Le fichier de propriétés par défaut est `$NCHOME/omnibus/etc/nco_confpack.props`.
`-server` *nom-serveurOS1, nom-serveurOS2, ...*	**confpack.omnibus.servers** *nom-serveurOS, nom-serveurOS, ...*	Les serveurs ObjectServer à partir desquels extraire les informations de configuration. Vous pouvez uniquement extraire des informations à partir des serveurs ObjectServer qui s'exécutent sur la machine locale. La valeur par défaut est tous les serveurs ObjectServer s'exécutant sur la machine locale.

Tableau 58. Sous-commandes et propriétés correspondantes pour l'option -list de nco_confpack (suite)

Sous-commande	Propriété	Description
`-timeout`*nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.**_nom-serveurOS_**.timeout** *chaîne*	Indique le délai, en millisecondes, qu'attend l'utilitaire pour obtenir une réponse du serveur ObjectServer, où *nom-serveurOS* correspond au nom du serveur ObjectServer, et *chaîne* au délai. Le délai par défaut est `6000` millisecondes (une minute).

`-user` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.**_nom-serveurOS_**.user** *chaîne*	Nom d'utilisateur de connexion pour les serveurs ObjectServer, où :
		• *nom-serveurOS* est le nom du serveur ObjectServer
		• *chaîne* est le nom d'utilisateur de connexion
		• Si le nom d'utilisateur est identique pour tous les serveurs ObjectServer, *nom-serveurOS* peut être omis
		• *nom-serveurOS* peut être remplacé par un astérisque (*) pour indiquer un nom d'utilisateur général pour tous les serveurs ObjectServer pour lesquels un nom d'utilisateur explicite n'est pas indiqué
		• Si un nom d'utilisateur et un mot de passe sont définis, mais pas pour tous les serveurs ObjectServer, les serveurs ObjectServer restants sont définis par défaut sur l'utilisateur système actuel sans mot de passe
		
		La valeur *nom-serveurOS* par défaut est tous les serveurs ObjectServer s'exécutant sur la machine locale.
		
		Le nom d'utilisateur par défaut est l'utilisateur du système d'exploitation actuel.
		
		Vous pouvez avoir plusieurs entrées dans le fichier de propriétés pour vous connecter à différents serveurs ObjectServer. Par exemple :
		`objectserver.NCOMSA.user : fred`
		`objectserver.NCOMSB.user : rob`

Exemple : création de fichiers de liste de configuration :

Cet exemple décrit différentes méthodes de création de fichiers de liste de configuration.

La commande suivante permet de se connecter au serveur ObjectServer NCOMS en tant qu'utilisateur système actuel sans mot de passe et de créer le fichier de liste de configuration `/tmp/NCOMS_conf.txt`.

```
nco_confpack -list -server NCOMS -file /tmp/NCOMS_conf.txt
```

La commande suivante permet de se connecter à tous les serveurs ObjectServer en cours d'exécution en tant qu'utilisateur fred avec le mot de passe secret et de créer le fichier de liste de configuration /tmp/NCOMS_conf.txt.

```
nco_confpack -list -user fred -password secret -file /tmp/NCOMS_conf.txt
```

La commande suivante permet de se connecter aux serveurs ObjectServer NCOMS et NYC en tant qu'utilisateur système actuel sans mot de passe. Le fichier de liste de configuration s'affiche à l'écran (sortie standard).

```
nco_confpack -list -server NCOMS,NYC
```

Pour les exemples suivants, supposons qu'il y ait trois serveurs ObjectServer actifs : NCOMS1, NCOMS2 et NCOMS3.

La commande suivante permet de se connecter au serveur ObjectServer NCOMS1 avec le nom d'utilisateur user1 et le mot de passe pass1, au serveur ObjectServer NCOMS2 avec le nom d'utilisateur user2 et le mot de passe pass2, et au serveur ObjectServer NCOMS3 en tant qu'utilisateur système actuel sans mot de passe.

```
nco_confpack -list -user NCOMS1:user1,NCOMS2:user2 -password NCOMS1:pass1,NCOMS2:pass2
```

La commande suivante permet de se connecter au serveur ObjectServer NCOMS1 avec le nom d'utilisateur user1 et le mot de passe pass1, au serveur ObjectServer NCOMS2 avec le nom d'utilisateur seth et le mot de passe secret, et au serveur ObjectServer NCOMS3 avec le nom d'utilisateur seth et le mot de passe muse.

```
nco_confpack -list -user "NCOMS1:user1,*:seth" -password NCOMS1:pass1,NCOMS2:secret,NCOMS3:muse
```

La commande suivante permet de se connecter au serveur ObjectServer NCOMS1 avec le nom d'utilisateur user1 sans mot de passe, au serveur ObjectServer NCOMS2 en tant qu'utilisateur système actuel sans mot de pass, et au serveur NCOMS3 en tant qu'utilisateur système sans mot de passe.

```
nco_confpack -list -user NCOMS1:user1
```

La commande suivante permet de se connecter à tous les serveurs ObjectServer en tant qu'utilisateur système actuel avec le mot de passe sesame.

```
nco_confpack -list -password sesame
```

Conseil : Même si le mot de passe est indiqué dans la ligne de commande, il n'apparaît pas dans la sortie de la commande ps.

Exemple : fichier de propriétés pour créer un fichier de liste de configuration :

L'exemple suivante de fichier de propriétés crée un fichier de liste de configuration appelé NCOMS_NY_export_list.txt pour le serveur ObjectServer NCOMS_NY.

```
nc.home                         :  '/opt/netcool'
omni.home                       :  '/opt/netcool/omnibus'
license.file                    :  '27000@licenseA_NY&27000@licenseB_NY'
objectserver.NCOMS_NY.user      :  'joe_ny'
objectserver.NCOMS_NY.password  :  'jOE_4_NY'
confpack.list.name              :  'NCOMS_NY_export_list.txt'
confpack.package.name           :  ''
confpack.omnibus.servers        :  'NCOMS_NY'
```

Edition des fichiers de liste de configuration

Vous pouvez modifier les fichiers de liste de configuration pour spécifier les objets à exporter d'un serveur ObjectServer source ou à importer dans un serveur ObjectServer cible.

Pourquoi et quand exécuter cette tâche

Pour éditer un fichier de liste de configuration :

Procédure

1. Créez le fichier de liste de configuration à l'aide de l'option de ligne de commande `-list` avec la commande **nco_confpack**.
2. Modifiez le fichier pour supprimer les objets que vous ne souhaitez par inclure dans le package de configuration. Vous pouvez par exemple supprimer tous les objets `Menu` si vous ne souhaitez pas exporter de menu du serveur ObjectServer source.
3. Sauvegardez le fichier.

Résultats

Vous pouvez utiliser le fichier de liste de configuration modifié avec la sous-commande `-file` pour l'option de ligne de commande `-export` ou la sous-commande `-select` pour l'option de ligne de commande `-import`.

Référence associée:

«Création des fichiers de liste de configuration», à la page 303

«Exemple : fichier de liste de configuration», à la page 309
L'exemple suivant de fichier de liste de configuration partiel est créé à partir d'une installation de Tivoli Netcool/OMNIbus comprenant deux serveurs ObjectServer (NCOMS1 et NCOMS2) s'exécutant sur le même hôte.

«Exportation des configurations», à la page 309
Pour extraire une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer à partir duquel vous souhaitez extraire la configuration. Une configuration exportée est sauvegardée dans un package de configuration.

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Exemple : fichier de liste de configuration :

L'exemple suivant de fichier de liste de configuration partiel est créé à partir d'une installation de Tivoli Netcool/OMNIbus comprenant deux serveurs ObjectServer (NCOMS1 et NCOMS2) s'exécutant sur le même hôte.

```
ObjectServer    NCOMS1    Menu    AlertsMenu
ObjectServer    NCOMS1    Menu    AlertsMenu->&Ownership
ObjectServer    NCOMS1    Menu    AlertsMenu->&Prioritize
ObjectServer    NCOMS1    Menu    AlertsMenu->&Resolve
ObjectServer    NCOMS1    Menu    AlertsMenu->&Tools
ObjectServer    NCOMS1    Menu    AlertsMenu->Related E&vents
ObjectServer    NCOMS1    Menu    AlertsMenu->Related E&vents->&Far-End Events
ObjectServer    NCOMS1    Menu    AlertsMenu->Related E&vents->&Near-End Events
ObjectServer    NCOMS1    Menu    AlertsMenu->Task &List
ObjectServer    NCOMS1    Menu    ConductorMenu
ObjectServer    NCOMS1    Menu    MainEventListMenu
ObjectServer    NCOMS1    Menu    SubEventListMenu
ObjectServer    NCOMS1    Menu    SymbolToolsMenu
ObjectServer    NCOMS2    Tool    Acknowledged Action
ObjectServer    NCOMS2    Tool    Add to Task List
ObjectServer    NCOMS2    Tool    Assign Action
ObjectServer    NCOMS2    Tool    Change Severity
ObjectServer    NCOMS2    Tool    Deacknowledged Action
ObjectServer    NCOMS2    Tool    Delete Action
ObjectServer    NCOMS2    Tool    Group Action
ObjectServer    NCOMS2    Tool    Ping Tool
ObjectServer    NCOMS2    Tool    Prompted Ping Tool
ObjectServer    NCOMS2    Tool    Prompted Telnet Tool
ObjectServer    NCOMS2    Tool    Remove from Task List
ObjectServer    NCOMS2    Tool    Sample Tool
ObjectServer    NCOMS2    Tool    Show Related FE Node
ObjectServer    NCOMS2    Tool    Show Related FE Object
ObjectServer    NCOMS2    Tool    Show Related NE Node
ObjectServer    NCOMS2    Tool    Show Related NE Object
ObjectServer    NCOMS2    Tool    Suppress/Escalate
ObjectServer    NCOMS2    Tool    Takeownership Action
ObjectServer    NCOMS2    Tool    Telnet Tool
```

Exportation des configurations

Pour extraire une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer à partir duquel vous souhaitez extraire la configuration. Une configuration exportée est sauvegardée dans un package de configuration.

Les serveurs ObjectServer source et cible peuvent se trouver sur différentes installations de Tivoli Netcool/OMNIbus. Vous pouvez exporter la configuration à partir d'une installation, l'envoyer à une installation sur un autre serveur et importer la configuration vers un serveur ObjectServer sur cette installation.

Pour créer un package de configuration, exécutez la commande suivante :

```
$NCHOME/omnibus/bin/nco_confpack -export paramètre -sous-commande, ...
```

Dans cette commande, *paramètre -sous-commande* peut être n'importe quelle sous-commande du tableau suivant.

Tableau 59. Sous-commandes et propriétés correspondantes pour l'option -export de nco_confpack

Sous-commande	Propriété	Description
`-file` *chaîne*	**`confpack.list.name`** *chaîne*	Nom du fichier de liste de configuration qui détaille les objets à exporter. Si vous utilisez cette sous-commande, vous ne pouvez pas utiliser la sous-commande `-server` ou la propriété **`confpack.omnibus.servers`**. La valeur par défaut est de lire l'entrée depuis l'entrée standard (`stdin`) si vous n'utilisez pas la sous-commande `-file` ou `-server` avec `nco_confpack -export`.

`-memstoredatadirectory` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**`objectserver.`***nom-serveurOS* **`.memstoredatadirectory`** *chaîne*	Indique un répertoire de base de données alternatif pour chaque ObjectServer, où :
		• *nom-serveurOS* représente le nom du serveur ObjectServer.
		• *chaîne* représente le chemin contenant les fichiers base de données du serveur ObjectServer. La valeur par défaut est `$NCHOME/omnibus/db`.
		• *nom-serveurOS* peut être remplacé par un astérisque (*) pour indiquer un chemin d'accès général pour tous les serveurs ObjectServer pour lesquels aucun chemin d'accès explicite n'est indiqué.
		• Si le chemin d'accès est identique pour tous les serveurs ObjectServer, la variable *nom-serveurOS* peut être omise. Par exemple : `-memstoredatadirectory` *chaîne*
		
		Vous pouvez avoir plusieurs entrées dans le même fichier de propriétés pour différents serveurs ObjectServer. Exemple :
		`objectserver.NCOMSA.`
		`  memstoredatadirectory : path1`
		`objectserver.NCOMSB.`
		`  memstoredatadirectory : path2`
		
		Remarque : Sous Windows, si vous souhaitez indique un chemin d'accès qui inclut un identificateur d'unité, n'omettez *pas* la valeur *nom-serveurOS* car l'identificateur d'unité est interprété comme un nom du serveur ObjectServer. Par exemple, si vous indiquez `-memstoredatadirectory C:\MyDir`, la lettre C est interprétée comme le nom du serveur ObjectServer.

`-package` *chaîne*	**`confpack.package.name`** *chaîne*	Chemin et nom de fichier vers lequel le package de configuration doit être exporté. La valeur par défaut est `stdout`.

Tableau 59. Sous-commandes et propriétés correspondantes pour l'option -export de nco_confpack (suite)

Sous-commande	Propriété	Description

`-password` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.***nom-serveurOS***.password** *chaîne*	Mot de passe de connexion des serveurs ObjectServer, où :
		• *nom-serveurOS* est le nom du serveur ObjectServer.
		• *chaîne* est le mot de passe de connexion.
		• Si le mot de passe est identique pour tous les serveurs ObjectServer, *nom-serveurOS* peut être omis.
		• *nom-serveurOS* peut être remplacée par un astérisque (*) pour indiquer un mot de passe général pour tous les serveurs ObjectServer pour lesquels un mot de passe explicite n'est pas indiqué.
		• Si un nom d'utilisateur et un mot de passe sont définis, mais pas pour tous les serveurs ObjectServer, les serveurs ObjectServer restants sont définis par défaut sur l'utilisateur système actuel sans mot de passe.
		La valeur *nom-serveurOS* par défaut est tous les serveurs ObjectServer s'exécutant sur l'ordinateur local.
		Le mot de passe par défaut est `''`.
		Vous pouvez avoir plusieurs entrées dans le fichier de propriétés pour vous connecter à différents serveurs ObjectServer. Par exemple :
		`objectserver.NCOMSA.password : mdp1`
		`objectserver.NCOMSB.password : mdp2`

`-propsfile` *chaîne*	N/D	Indique le fichier de propriétés de **nco_confpack**. Vous pouvez utiliser le fichier de propriétés au lieu d'entrer des sous-commandes individuelles dans la ligne de commande. Le fichier de propriétés par défaut est `$NCHOME/omnibus/etc/nco_confpack.props`.
`-rename` *nom-serveurOS:package-serveurOS, nom-serveurOS2:package-serveurOS,...*	**confpack.export.rename** *nom-serveurOS:package-serveurOS, nom-serveurOS2:package-serveurOS2, ...*	Renomme les serveurs ObjectServer source dans le package de configuration. • *nom-serveurOS* est le nom du serveur ObjectServer source. • *package-serveurOS* est le nom du serveur ObjectServer correspondant dans le package de configuration. Par exemple, vous pouvez renommer les serveurs ObjectServer source NCOMS1 et NCOMS2 en PRIMARY et SECONDARY dans le package de configuration.

Tableau 59. Sous-commandes et propriétés correspondantes pour l'option -export de nco_confpack (suite)

Sous-commande	Propriété	Description
`-server` *nom-serveurOS1, nom-serveurOS2, ...*	**`confpack.omnibus.servers`** *nom-serveurOS, nom-serveurOS, ...*	Serveurs ObjectServer à partir desquels exporter les objets de configuration. Si vous utilisez cette sous-commande, vous ne pouvez pas utiliser la sous-commande `-file` (ou la propriété **`config.list.name`**). Vous pouvez uniquement exporter des données à partir de serveurs ObjectServer en cours d'exécution sur la machine locale. Cette sous-commande permet d'exporter tous les objets à partir des serveurs ObjectServer sélectionnés.
`-timeout`*nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**`objectserver.`***nom-serveurOS*`.timeout`** *chaîne*	Indique le délai, en millisecondes, qu'attend l'utilitaire pour obtenir une réponse du serveur ObjectServer, où *nom-serveurOS* correspond au nom du serveur ObjectServer, et *chaîne* au délai. Le délai par défaut est `6000` millisecondes (une minute).

`-user` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**`objectserver.`***nom-serveurOS*`.user`** *chaîne*	Nom d'utilisateur de connexion pour les serveurs ObjectServer, où :
		• *nom-serveurOS* est le nom du serveur ObjectServer.
		• *chaîne* est le nom d'utilisateur de connexion.
		• Si le nom d'utilisateur est identique pour tous les serveurs ObjectServer, la variable *nom-serveurOS* peut être omise.
		• La variable *nom-serveurOS* peut être remplacée par un astérisque (*) pour indiquer un nom d'utilisateur général pour tous les serveurs ObjectServer pour lesquels un nom d'utilisateur explicite n'est pas indiqué.
		• Si un nom d'utilisateur et un mot de passe sont définis, mais pas pour tous les serveurs ObjectServer, les serveurs ObjectServer restants sont définis par défaut sur l'utilisateur système actuel sans mot de passe.
		
		La valeur *nom-serveurOS* par défaut est tous les serveurs ObjectServer s'exécutant sur l'ordinateur local.
		
		Le nom d'utilisateur par défaut est l'utilisateur du système d'exploitation actuel.
		
		Vous pouvez avoir plusieurs entrées dans le fichier de propriétés pour vous connecter à différents serveurs ObjectServer. Par exemple :
		`objectserver.NCOMSA.user : fred`
		`objectserver.NCOMSB.user : rob`

Concepts associés:

«Création et édition des fichiers de liste de configuration», à la page 303
Les fichiers de liste de configuration vous permettent d'afficher les objets exportables dans un serveur ObjectServer et de sélectionner les objets à exporter de ou à importer dans un serveur ObjectServer.

Remarques pour l'exportation

Lors de l'exportation d'un package de configuration, notez un certain nombre de considérations.

Ces considérations sont les suivantes :

- N'utilisez pas l'association de caractères `->` dans les noms de menus.
- L'ordre dans lequel les noms de sous-menus s'affichent dans le fichier de liste de configuration détermine l'ordre dans lequel les noms s'affichent dans la liste d'événements. Pour modifier l'ordre, vous pouvez éditer le fichier de liste.
- Vous devez inclure tous les sous-menus d'un menu dans un fichier de liste de configuration. Sinon, une erreur se produit lorsque vous tentez d'importer le menu.
- Vous ne pouvez pas exporter les objets système, qui incluent les utilisateurs système, les groupes de systèmes, les rôles système et les signaux système.
- Tous les outils qui désignent des invites ne disposant pas d'entrée dans la table tools.prompt_defs sont exclus de l'exportation. Cela est dû au fait que l'importation d'outils avec des invites inexistantes dans un serveur ObjectServer cible provoque l'échec du bureau.

A propos du fichier d'exclusions

Certains objets du serveur ObjectServer, notamment les outils, les déclencheurs et les procédures, peuvent contenir des références à des fichiers externes qui font partie d'une installation standard de Tivoli Netcool/OMNIbus ou d'une installation de système d'exploitation. Ces fichiers n'ont pas besoin d'être exportés et peuvent être exclus des packages de configuration.

Le fichier d'exclusions contient une liste des fichiers et répertoires à exclure lors de l'exportation d'un package de configuration. Le nom du fichier d'exclusions est `$NCHOME/omnibus/etc/exclusions.xml`.

Le fichier d'exclusions par défaut contient des entrées empêchant l'inclusion de certains fichiers et répertoires aux packages de configuration. Cependant, vous pouvez éditer ce fichier afin d'y ajouter des entrées.

Le fichier `exlusions.xml` contient un élément pour les fichiers et répertoires de `$NCHOME/omnibus` (`OmniHome`) et un élément pour chaque système d'exploitation pris en charge (`Platform`).

Une barre oblique (`/`) est utilisée en tant que séparateur de chemin générique. La barre oblique est remplacée par le séparateur spécifique au système d'exploitation lors du traitement. Pour les entrées de l'élément `OmniHome`, les chemins doivent être relatifs à `$NCHOME/omnibus`. Pour les éléments `Platform`, les chemins doivent être relatifs à la racine système.

Pour les systèmes Windows, vous devez inclure l'identificateur d'unité, par exemple `C:` ou `D:`. L'unité `C:` est la valeur par défaut.

Exemple : fichier d'exclusions :

Cet exemple présente le contenu d'un fichier `exlusions.xml`.

```
<exclusions>
<OmniHome>
     <File Name="/utils/nco_functions"/>
     <File Name="/utils/nco_mail"/>
     <File Name="/desktop/default.elv"/>
     <File Name="/desktop/default.elc"/>
     <File Name="/desktop/minimal.elc"/>
     <File Name="/ini/default.elc"/>
     <File Name="/ini/default.elv"/>
     <File Name="/ini/tool.elf"/>
     <File Name="/ini/minimal.elc"/>
     <File Name="/desktop/NCOelct.exe"/>
     <Dir Name="/bin"/>
     <Dir Name="/db"/>
     <Dir Name="/etc"/>
     <Dir Name="/install"/>
     <Dir Name="/log"/>
     <Dir Name="/platform"/>
     <Dir Name="/patches"/>
</OmniHome>


<Platform Name="SunOS" Type="UNIX">
     <Dir Name="/bin"/>
     <Dir Name="/etc"/>
     <Dir Name="/lib"/>
     <Dir Name="/sbin"/>
     <Dir Name="/usr"/>
</Platform>

<Platform Name="AIX" Type="UNIX">
     <Dir Name="/bin"/>
     <Dir Name="/etc"/>
     <Dir Name="/lib"/>
     <Dir Name="/lpp"/>
     <Dir Name="/sbin"/>
     <Dir Name="/usr"/>
</Platform>

<Platform Name="HP-UX" Type="UNIX">
     <Dir Name="/bin"/>
     <Dir Name="/etc"/>
     <Dir Name="/lib"/>
     <Dir Name="/sbin"/>
     <DIR Name="/usr"/>
</Platform>

<Platform Name="Linux" Type="UNIX">
     <Dir Name="/bin"/>
     <Dir Name="/etc"/>
     <Dir Name="/lib"/>
     <Dir Name="/sbin"/>
     <Dir Name="/usr"/>
</Platform>

<Platform Name="Windows 2000" Type="WIN">
     <Dir Name="C:/WINDOWS"/>
     <Dir Name="C:/WINNT"/>
</Platform>

<Platform Name="Windows 2003" Type="WIN">
     <Dir Name="C:/WINDOWS"/>
     <Dir Name="C:/WINNT"/>
```

```
</Platform>

<Platform Name="Windows XP" Type="WIN">
     <Dir Name="C:/WINDOWS"/>
     <Dir Name="C:/WINNT"/>
</Platform>
</exclusions>
```

Création d'une configuration de sauvegarde

Vous pouvez utiliser **nco_confpack** pour exporter un package de configuration de sauvegarde pour pouvoir l'importer en cas de problème avec votre installation Netcool/OMNIbus afin de restaurer a configuration du serveur ObjectServer.

Pourquoi et quand exécuter cette tâche

Remarque : Cette opération ne sauvegarde pas les données d'alertes du serveur ObjectServer.

Référence associée:

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Exemple : exportation des packages de configuration

Cet exemple présente les différentes méthodes d'utilisation de l'utilitaire **nco_confpack** pour exporter des packages de configuration à partir des serveurs ObjectServer.

La commande suivante permet d'exporter tous les objets de configuration du serveur ObjectServer NCOMS vers le package de configuration /tmp/NCOMS_package. Elle permet de se connecter au serveur ObjectServer en tant qu'utilisateur système actuel sans mot de passe.

```
nco_confpack -export -server NCOMS -package /tmp/NCOMS_package
```

La commande suivante permet de se connecter au serveur ObjectServer indiqué dans le fichier de liste en tant qu'utilisateur système actuel sans mot de passe. Elle permet ensuite d'exporter les objets indiqués dans le fichier de liste /tmp/listfile1.txt en tant que package de configuration /tmp/NCOMS_package.

```
nco_confpack -export -file /tmp/listfile1.txt -package /tmp/NCOMS_package
```

La commande suivante permet de se connecter aux serveurs ObjectServer NCOMS et NCOMS2 en tant qu'utilisateur système actuel sans mot de passe. Elle permet ensuite d'exporter tous les objets de configuration des serveurs ObjectServer vers le package de configuration /tmp/NCOMS_package.

```
nco_confpack -export -server NCOMS,NCOMS2 -package /tmp/NCOMS_package
```

La commande suivante permet de se connecter au serveur NCOMS1 en tant qu'utilisateur user1 avec le mot de passe pass1 et au serveur NCOMS2 en tant qu'utilisateur user2 avec le mot de passe pass2. Elle permet d'exporter tous les objets de configuration des serveurs ObjectServer vers le package de configuration /tmp/NCOMS_package.

```
nco_confpack -export -server NCOMS,NCOMS2 -user NCOMS:user1,NCOMS2:user2 -password
NCOMS:pass1,NCOMS2:pass2 -package /tmp/NCOMS_package
```

La commande suivante permet de se connecter au serveur ObjectServer NCOMS en tant qu'utilisateur système actuel sans mot de passe. Elle crée un package de configuration dans /tmp/NCOMS_package. Dans ce package de configuration, le nom du serveur ObjectServer source (NCOMS) est remplacé par MYSERVER.

```
nco_confpack -export -server NCOMS -rename NCOMS:MYSERVER -package /tmp/NCOMS_package
```

Exemple : fichier de propriétés pour exporter un fichier de package :

Cet exemple de fichier de propriétés permet d'exporter un package de configuration à partir du serveur ObjectServer NCOMS_NY à l'aide du fichier de liste de configuration NCOMS_NY_export_list.txt pour identifier les objets à exporter.

```
nc.home                          :  '/opt/netcool'
omni.home                        :  '/opt/netcool/omnibus'
license.file                     :  '27000@licenseA_NY&27000@licenseB_NY'
objectserver.NCOMS_NY.user       :  'joe_ny'
objectserver.NCOMS_NY.password   :  'jOE_4_NY'
confpack.list.name               :  'NCOMS_NY_export_list.txt'
confpack.package.name            :  'NCOMS_NY_export.pak.jar'
confpack.omnibus.servers         :  'NCOMS_NY'
confpack.export.rename           :  ''
```

Affichage du contenu du package de configuration

Vous pouvez utiliser **nco_confpack** pour afficher le contenu d'un package de configuration exporté ou pour sauvegarder le contenu du package dans un fichier texte. Ceci est utile pour vérifier les objets que vous pouvez importer depuis le package dans un serveur ObjectServer.

Pour afficher le contenu d'un package de configuration ou pour sauvegarder le contenu du package dans un fichier texte, entrez la commande suivante :

```
$NCHOME/omnibus/bin/nco_confpack -contents paramètre -sous-commande, ...
```

Dans cette commande, la variable *paramètre -sous-commande* peut être n'importe quelle sous-commande du tableau suivant.

Tableau 60. Sous-commandes et propriétés correspondantes pour l'option -contents de nco_confpack

Sous-commande	Propriété	Description
-file *chaîne*	**confpack.list.name** *chaîne*	Chemin et nom du fichier texte de sortie. La valeur par défaut est stdout.
-package *chaîne*	**confpack.package.name** *chaîne*	Chemin d'accès et nom de fichier du package de configuration. La valeur par défaut est stdin. **Remarque :** Si vous n'utilisez pas la sous-commande -package pour indiquer un nom de fichier, l'utilitaire **nco_confpack** attend indéfiniment des informations de l'entrée standard.

Concepts associés:

«Création et édition des fichiers de liste de configuration», à la page 303
Les fichiers de liste de configuration vous permettent d'afficher les objets exportables dans un serveur ObjectServer et de sélectionner les objets à exporter de ou à importer dans un serveur ObjectServer.

Exemple : affichage du contenu du package de configuration

Cet exemple explique comment utiliser l'utilitaire **nco_confpack** pour écrire le contenu d'un package de configuration dans la sortie standard ou dans un fichier texte.

La commande suivante permet d'écrire le contenu du package de configuration /tmp/NCOMS_package dans la sortie standard.

```
nco_confpack -contents -package /tmp/NCOMS_package
```

La commande suivante permet d'écrire le contenu du package de configuration /tmp/NCOMS_package dans le fichier texte /jsmith/package1.txt.

```
nco_confpack -contents -package /tmp/NCOMS_package -file /jsmith/package1.txt
```

Importation des configurations

Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Les serveurs ObjectServer source et cible peuvent se trouver sur différentes installations de Tivoli Netcool/OMNIbus. Vous pouvez exporter la configuration à partir d'une installation, l'envoyer à une installation sur un autre serveur et importer la configuration vers un serveur ObjectServer sur cette installation.

Remarque : Si un objet du package de configuration a le même nom qu'un objet du même type sur le serveur ObjectServer cible, l'objet existant est remplacé par l'objet du package de configuration. Par exemple, un outil appelé sample dans le package de configuration écrase un outil existant appelé sample sur le serveur ObjectServer cible. Pour éviter toute perte de données, assurez-vous de sauvegarder votre ObjectServer avant d'importer un package de configuration.

Pour importer un package de configuration, exécutez la commande suivante :

```
$NCHOME/omnibus/bin/nco_confpack -import paramètre
-sous-commande, ...
```

Dans cette commande, *paramètre -sous-commande* peut être n'importe quelle sous-commande du tableau suivant.

Tableau 61. Sous-commandes et propriétés correspondantes pour l'option -import de nco_confpack

Sous-commande	Propriété	Description
`-force TRUE | FALSE`	**`confpack.import.force`** `TRUE | FALSE`	Par défaut, lors de l'importation d'un outil ou d'une procédure mémorisée qui désigne un fichier externe (notamment un script), le fichier est inclus lors de l'importation. Si un fichier identique existe déjà, le fichier existant n'est *pas* écrasé. Vous pouvez utiliser l'option `-force` pour forcer un écrasement même si le fichier désigné existe déjà. **Avertissement :** Utilisez la sous-commande `-force` avec prudence. Assurez-vous que votre système de fichiers est sauvegardé avant d'importer le package de configuration. La valeur par défaut est `FALSE`.
`-from` *chaîne*	**`confpack.import.from`** *chaîne*	Le nom du serveur ObjectServer source, comme indiqué dans le package de configuration à partir duquel vous importez les objets de configuration. **Remarque :** Si le package de configuration contient des informations pour un seul ObjectServer, vous n'avez pas besoin d'utiliser cette sous-commande. Si le package de configuration contient des informations pour plusieurs serveurs ObjectServer, cette sous-commande est obligatoire. La valeur par défaut est `''`.

Tableau 61. Sous-commandes et propriétés correspondantes pour l'option -import de nco_confpack (suite)

Sous-commande	Propriété	Description

`-memstoredatadirectory` *nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**objectserver.***nom-serveurOS* **.memstoredatadirectory** *chaîne*	Indique un répertoire de base de données alternatif pour chaque ObjectServer, où :
		• *nom-serveurOS* représente le nom du serveur ObjectServer.
		• *chaîne* représente le chemin contenant les fichiers base de données du serveur ObjectServer. La valeur par défaut est `$NCHOME/omnibus/db`.
		• *nom-serveurOS* peut être remplacé par un astérisque (*) pour indiquer un chemin d'accès général pour tous les serveurs ObjectServer pour lesquels aucun chemin d'accès explicite n'est indiqué.
		• Si le chemin d'accès est identique pour tous les serveurs ObjectServer, la variable *nom-serveurOS* peut être omise. Par exemple : `-memstoredatadirectory` *chaîne*
		
		Vous pouvez avoir plusieurs entrées dans le même fichier de propriétés pour différents serveurs ObjectServer. Exemple :
		`objectserver.NCOMSA.`
		`memstoredatadirectory : path1`
		`objectserver.NCOMSB.`
		`memstoredatadirectory : path2`
		
		Remarque : Sous Windows, si vous souhaitez indique un chemin d'accès qui inclut un identificateur d'unité, n'omettez *pas* la valeur *nom-serveurOS* car l'identificateur d'unité est interprété comme un nom du serveur ObjectServer. Par exemple, si vous indiquez `-memstoredatadirectory C:\MyDir`, la lettre C est interprétée comme le nom du serveur ObjectServer.

`-nowarn TRUE | FALSE`	**confpack.import.nowarn** `TRUE | FALSE`	Supprime les messages d'avertissement. **Remarque :** Si vous utilisez l'entrée standard pour importer le package de configuration, vous devez activer cette option. La valeur par défaut est `FALSE`.
`-package` *chaîne*	**confpack.package.name** *chaîne*	Nom du package de configuration. La valeur par défaut est `stdin`.
`-password` *chaîne*	**objectserver.***nom-serveurOS***.password** *chaîne*	Mot de passe de connexion pour le serveur ObjectServer. Le mot de passe par défaut est `''`.

Tableau 61. Sous-commandes et propriétés correspondantes pour l'option -import de nco_confpack (suite)

Sous-commande	Propriété	Description
`-propsfile` *chaîne*	N/D	Indique le fichier de propriétés de **`nco_confpack`**. Vous pouvez utiliser le fichier de propriétés au lieu d'entrer des sous-commandes individuelles dans la ligne de commande. Le fichier de propriétés par défaut est `$NCHOME/omnibus/etc/nco_confpack.props`.
`-select` *chaîne*	**`confpack.import.select`** *chaîne*	Indique un fichier contenant un sous-ensemble d'objets à récupérer du package et à importer dans le serveur ObjectServer. Créez le fichier à l'aide de l'option de ligne de commande `-list`. Editez le fichier pour supprimer toutes les entrées sauf celles que vous souhaitez importer dans le serveur ObjectServer. La valeur par défaut est `''`.
`-server` *nom-serveurOS*	**`confpack.omnibus.servers`** *nom-serveurOS*	ObjectServer dans lequel vous importez les objets de configuration. Vous pouvez uniquement importer des données dans un serveur ObjectServer qui s'exécute sur la machine locale. Le serveur ObjectServer par défaut est `NCOMS`.
`-timeout`*nom-serveurOS:chaîne, nom-serveurOS2:chaîne, ...*	**`objectserver.`***nom-serveurOS***`.timeout`** *chaîne*	Indique le délai, en millisecondes, qu'attend l'utilitaire pour obtenir une réponse du serveur ObjectServer, où *nom-serveurOS* correspond au nom du serveur ObjectServer, et *chaîne* au délai. Le délai par défaut est `6000` millisecondes (une minute).
`-user` *chaîne*	**`objectserver.`***nom-serveurOS***`.user`** *chaîne*	Nom d'utilisateur de connexion pour le serveur ObjectServer. Le nom d'utilisateur par défaut est l'utilisateur du système d'exploitation actuel.

Concepts associés:

«Création et édition des fichiers de liste de configuration», à la page 303
Les fichiers de liste de configuration vous permettent d'afficher les objets exportables dans un serveur ObjectServer et de sélectionner les objets à exporter de ou à importer dans un serveur ObjectServer.

Référence associée:

«Affichage du contenu du package de configuration», à la page 316
Vous pouvez utiliser **`nco_confpack`** pour afficher le contenu d'un package de configuration exporté ou pour sauvegarder le contenu du package dans un fichier texte. Ceci est utile pour vérifier les objets que vous pouvez importer depuis le package dans un serveur ObjectServer.

Remarques sur l'importation

Lors de l'importation d'un package de configuration, notez un certain nombre de considérations et d'instructions.

Sauvegardez votre installation cible de Tivoli Netcool/OMNIbus avant d'importer un package de configuration.

Remarque : Lorsque **nco_confpack** tente d'importer un objet de configuration, il vérifie si l'objet existe déjà dans le serveur ObjectServer cible. Si l'objet existe déjà, **nco_confpack** modifie l'objet cible pour le mettre en conformité avec l'objet en cours d'importation. Si l'objet n'existe pas dans le serveur ObjectServer cible, **nco_confpack** le crée dans cet emplacement. **nco_confpack** ne supprime pas un objet qui existe déjà dans le serveur ObjectServer cible.

Ce comportement rend **nco_confpack** inadapté pour la réplication ou le clonage de la totalité des serveurs ObjectServer. Il n'est destiné qu'à l'exportation et l'importation des données de configuration partielles entre les serveurs ObjectServer. Utilisez **nco_osreport** pour répliquer ou cloner des serveurs ObjectServer entiers.

Les considérations et instructions suivantes s'appliquent aux importations :

- Lorsque vous utilisez stdin pour importer le package de configuration, vous devez utiliser la sous-commande `-nowarn`. Cela est dû au fait que **nco_confpack** ne peut pas lire le package de configuration et inviter l'utilisateur en même temps.
- Lors de l'importation des informations sur les utilisateurs, les groupes et les rôles, **nco_confpack** tente d'utiliser l'ID utilisateur, groupe ou rôle du serveur ObjectServer source. Si un ID est déjà en cours d'utilisation sur le serveur ObjectServer cible, le prochain ID disponible est utilisé. Les ID du serveur ObjectServer ne doivent pas correspondre aux ID utilisateur du système d'exploitation.
- Si vous tentez d'importer un utilisateur qui appartient à un groupe qui n'existe pas dans le package de configuration ou sur le système cible, une erreur se produit et l'utilisateur n'est pas importé.
- Si vous importez un utilisateur qui existe déjà sur le serveur ObjectServer cible, mais dans un groupe différent, cet utilisateur appartiendra aux deux groupes et obtiendra les autorisations attribuées au groupe possédant le niveau d'autorisation le plus élevé. Pour assurer que l'utilisateur dispose des autorisations correctes, il se peut que vous deviez supprimer l'utilisateur de l'un des groupes.
- Vous devez être le propriétaire de tout objet que vous importez dans un serveur ObjectServer. La propriété de l'objet dans le serveur ObjectServer source n'est pas importée dans le serveur ObjectServer cible.
- Les autorisations associées à un objet du serveur ObjectServer sont implicitement importées avec l'objet. Par exemple, la capacité d'un utilisateur d'exécuter des commandes SQL.
- Vous ne pouvez pas importer une classe à partir du serveur ObjectServer source si le serveur ObjectServer cible contient une classe définie avec le même ID, mais un nom différent.
- Vous ne pouvez pas importer un signal défini par l'utilisateur si un signal du même nom, mais dont les paramètres diffèrent, existe dans le serveur ObjectServer cible.

- Si vous importez un déclencheur qui référence un objet, assurez-vous que l'objet existe sur le système cible ou est inclus dans le package de configuration. Si ce n'est pas le cas, une erreur se produit lors du processus d'importation.
- Lors de l'importation de menus et d'éléments de menu, les règles suivantes sont appliquées :
  - Les menus du module d'importation qui n'existent pas dans le serveur ObjectServer cible sont créés dans ce dernier. Tous les éléments de menu du module sont ajoutés dans le même ordre dans lequel ils apparaissent dans le module (qui correspond à l'ordre dans lequel ils apparaissaient sur le serveur ObjectServer source).
  - Les menus du module d'importation qui existent déjà dans le serveur ObjectServer cible sont fusionnés dans le menu cible. Les éléments de menu du module qui n'existent pas dans le serveur ObjectServer cible sont ajoutés à la fin du menu cible, dans le même ordre dans lequel ils apparaissent dans le module. Les éléments de menu du module qui existent déjà dans le serveur ObjectServer cible sont conservés dans le même ordre dans le menu cible, mais leurs définitions sont mises à jour de sorte qu'ils correspondent au contenu du module.
- Le module de configuration stocke des chaînes de texte au format Unicode. Par conséquent, si le serveur ObjectServer cible utilise un codage de caractères différent de celui du serveur ObjectServer source, le texte sera converti du codage source pour en codage cible. Dans ce cas, vous devez vérifier la configuration importée car les caractères qui ne peuvent pas être représentés dans le codage cible sont remplacés par des points d'interrogation (?).

Tâches associées:

«Création d'une configuration de sauvegarde», à la page 315
Vous pouvez utiliser **nco_confpack** pour exporter un package de configuration de sauvegarde pour pouvoir l'importer en cas de problème avec votre installation Netcool/OMNIbus afin de restaurer a configuration du serveur ObjectServer.

Exemples d'importation de packages de configuration

Ces exemples présentent comment utiliser l'utilitaire **nco_confpack** pour importer des packages de configuration dans des serveurs ObjectServer.

Exemple : importation de packages de configuration complets :

Cet exemple présente les différentes méthodes d'importation d'un package de configuration.

La commande suivante permet d'importer le package de configuration `/tmp/NCOMS_package` dans le serveur ObjectServer NCOMS. Elle permet de se connecter au serveur ObjectServer en tant qu'utilisateur système actuel sans mot de passe.

```
nco_confpack -import -package /tmp/NCOMS_package -server NCOMS
```

La commande suivante permet d'importer le package de configuration `/tmp/NCOMS_package` dans le serveur ObjectServer NCOMS avec le nom d'utilisateur fred et le mot de passe `secret`.

```
nco_confpack -import -package /tmp/NCOMS_package -server NCOMS
-user fred -password secret
```

La commande suivante permet d'importer le package de configuration `/tmp/NCOMS_package` dans le serveur ObjectServer MYSERVER. Seuls les objets de configuration du serveur ObjectServer NCOMS sont importés.

```
nco_confpack -import -package /tmp/NCOMS_package -server MYSERVER -from NCOMS
```

Exemple : importation d'une partie d'un package de configuration :

La série suivante de commandes crée un fichier de liste de configuration et importe une partie du package de configuration dans un deuxième ObjectServer. Editez le fichier de liste de configuration dans un éditeur de texte pour indiquer les composants à importer dans le deuxième ObjectServer.

1. La commande suivante permet d'écrire le contenu du package de configuration `/tmp/NCOMS_package` dans le fichier de liste de configuration `/jsmith/package1.txt`.

   ```
   nco_confpack -contents -package /tmp/NCOMS_package -file /jsmith/package1.txt
   ```

2. Editez le fichier pour garder uniquement les lignes correspondant aux entrées devant être importées dans le deuxième ObjectServer. Dans cet exemple, les lignes suivantes sont conservées ; elles correspondent aux menus d'outils personnalisés :

   ```
   ObjectServer    NCOMS1    Menu    AlertsMenu->&Custom Tools
   ObjectServer    NCOMS1    Menu    AlertsMenu->&Custom Tools->&Far-End Events
   ObjectServer    NCOMS1    Menu    AlertsMenu->&Custom Tools->&Near-End Events
   ```

3. La commande suivante permet d'importer des objets indiqués dans le fichier de liste de configuration `/jsmith/package1.txt` à partir du package de configuration `/tmp/NCOMS_package` dans le serveur ObjectServer MYSERVER.

   ```
   nco_confpack -import -package /tmp/NCOMS_package -server MYSERVER
   -select /jsmith/package1.txt
   ```

Tâches associées:

«Edition des fichiers de liste de configuration», à la page 308
Vous pouvez modifier les fichiers de liste de configuration pour spécifier les objets à exporter d'un serveur ObjectServer source ou à importer dans un serveur ObjectServer cible.

Exemple : fichier de propriétés pour importer un fichier de package :

Cet exemple de fichier de propriétés importe le package de configuration `NCOMS_NY_export.pak.jar` dans le serveur ObjectServer NCOMS_LON.

```
nc.home                          :  '/opt/netcool'
omni.home                        :  '/opt/netcool/omnibus'
license.file                     :  '27000@licenseA_NY&27000@licenseB_NY'
objectserver.NCOMS_LON.user      :  'joe_lon'
objectserver.NCOMS_LON.password  :  'jOE789'
confpack.list.name               :  ''
confpack.package.name            :  'NCOMS_NY_export.pak.jar'
confpack.omnibus.servers         :  'NCOMS_LON'
confpack.import.nowarn           :  TRUE
confpack.import.force            :  FALSE
confpack.import.from             :  ''
confpack.import.select           :  ''
```

Chapitre 12. Configuration des serveurs ObjectServer de bureau

Vous pouvez configurer une architecture du serveur ObjectServer de bureau pour réduire la charge sur les serveurs ObjectServer qui reçoivent une grande quantité d'événements.

Par exemple, cela peut se produire lorsque plusieurs serveurs ObjectServer régionaux envoient des événements à un serveur ObjectServer central via des passerelles unidirectionnelles du serveur ObjectServer et que plusieurs bureaux se connectent directement au serveur ObjectServer central. Si le serveur ObjectServer devient surchargé, les passerelles unidirectionnelles du serveur ObjectServer ne peuvent pas insérer tous les événements dans le serveur ObjectServer. Les bureaux connectés directement au serveur ObjectServer augmentent encore la charge, en particulier si un grand nombre de bureaux se connectent simultanément.

Architecture du serveur ObjectServer de bureau

L'architecture du serveur ObjectServer de bureau peut améliorer les performances d'un serveur ObjectServer fréquemment soumis à de lourdes charges.

L'architecture du serveur ObjectServer de bureau :

- Réduit la charge de travail du serveur ObjectServer central en déplaçant la charge sur les serveurs ObjectServer de bureau spécialisés
- Améliore la réactivité du bureau. En d'autres termes, le temps de réponse entre une action de l'opérateur du bureau et sa réflexion dans l'interface graphique du bureau
- Réduit la probabilité de gel de l'interface graphique du bureau
- Améliore les délais de latence de bout en bout dans les configurations du serveur ObjectServer standard soumises à de très lourdes charges
- Maintient une intégrité et une cohérence des données élevées en mettant simultanément à jour le serveur ObjectServer maître

L'architecture du serveur ObjectServer de bureau consiste en un serveur ObjectServer maître et un ou plusieurs serveurs ObjectServer de bureau qui partagent les tâches normalement exécutées par un seul ObjectServer. L'architecture DSD se connecte à un seul ObjectServer maître lors de l'écriture des données, mais lit et affiche les données d'alerte provenant des serveurs ObjectServer de bureau. La fonctionnalité principale de l'architecture DSD est identique à celle d'un bureau standard. Pour les opérateurs, l'architecture DSD se comporte de la même manière qu'un bureau standard.

L'architecture du serveur ObjectServer de bureau est présentée dans la figure suivante.

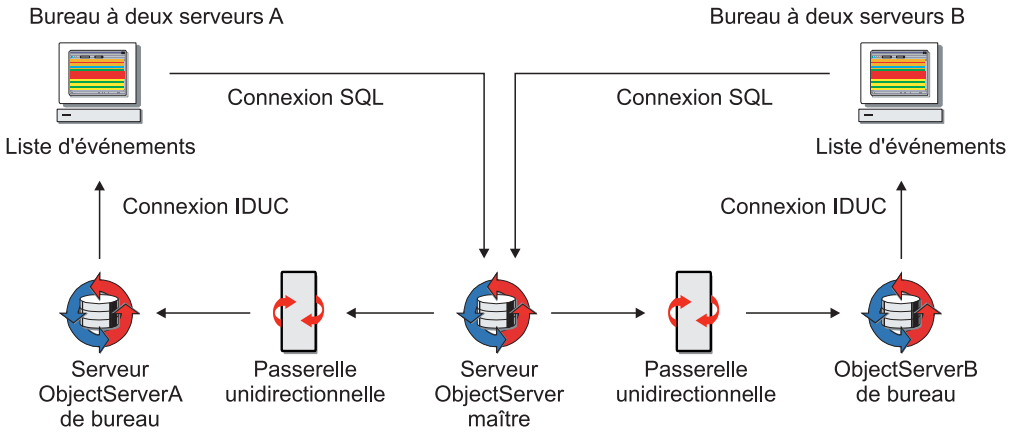

Figure 12. Exemple d'architecture du bureau à deux serveurs

L'architecture DSD se connecte simultanément au serveur ObjectServer de bureau et au serveur ObjectServer maître. Toutes les actions de l'opérateur (par exemple, les outils ou les actions de journal) exécutées dans l'architecture DSD sont directement envoyées au serveur ObjectServer maître via une connexion SQL unidirectionnelle.

Les alertes du serveur ObjectServer maître sont envoyées à l'architecture DSD via le serveur ObjectServer de bureau. Pour ce faire, le système utilise une passerelle unidirectionnelle du serveur ObjectServer reliant le serveur ObjectServer maître et le serveur ObjectServer de bureau, et une connexion IDUC reliant le serveur ObjectServer de bureau à l'architecture DSD.

Si le mode d'écriture double est activé, les mises à jour sont également envoyées au serveur ObjectServer de bureau via une autre connexion SQL unidirectionnelle, comme indiqué dans la figure suivante.

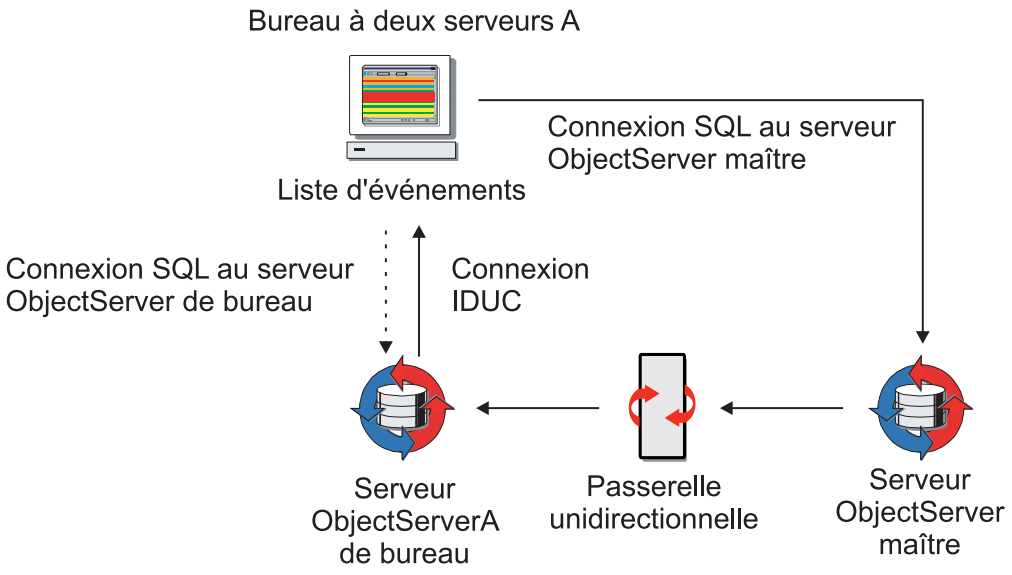

Figure 13. Exemple d'architecture de bureau à deux serveurs en mode écriture double

Référence associée:

«Affichage des résultats des actions d'outils à l'aide du mode écriture double», à la page 331
Le mode écriture double permet aux opérateurs d'afficher rapidement les résultats des actions d'outils (par exemple, les accusés réception et les définitions de priorité) à partir d'un bureau à deux serveurs (DSD). Lorsque ce mode est activé, toutes les actions d'outils sont envoyées au serveur ObjectServer de bureau et au serveur ObjectServer maître.

Remarques relatives à l'installation d'une architecture du serveur ObjectServer de bureau

Lors de la configuration d'une architecture du serveur ObjectServer de bureau, un ensemble d'instructions se trouve à votre disposition.

Il s'agit des instructions suivantes :

- Un serveur ObjectServer doit être désigné comme ObjectServer maître.
- Un ou plusieurs serveurs ObjectServer peuvent être désignés comme ObjectServer de bureau.
- Une passerelle du serveur ObjectServer unidirectionnelle doit connecter le serveur ObjectServer maître à chaque ObjectServer de bureau.
- Si vous utilisez la passerelle du serveur ObjectServer pour répliquer les données de sécurité (y compris les utilisateurs, les groupes, les rôles et les filtres de restriction) entre le serveur ObjectServer maître et les serveurs ObjectServer de bureau, vous devez conserver les données de sécurité sur le serveur ObjectServer maître. N'ajoutez pas d'objets du serveur ObjectServer directement aux serveurs ObjectServer de bureau car tous les droits se trouvant sur les serveurs ObjectServer de bureau pour des objets conservés par le serveur ObjectServer maître sont perdus lors de la resynchronisation. Les autorisations perdues peuvent inclure des autorisations accordées à des rôles ou des rôles accordés à des groupes.

  Avertissement : Si vous souhaitez resynchroniser les données de sécurité lorsque vos serveurs ObjectServer s'exécutent en mode sécurisé, exécutez la passerelle en tant qu'utilisateur root. Si vous n'y parvenez pas, la passerelle s'arrête lorsque vous lancez la resynchronisation et le serveur ObjectServer de destination ne possédera aucune donnée de sécurité. Cela est dû au fait que la passerelle supprime les autorisations de destination et ne peut pas insérer de lignes copiées depuis la table source. Si vous exécutez la passerelle en tant qu'utilisateur root, ignorez ce problème car vous n'avez pas besoin que les autorisations soient définies explicitement.

Configuration d'une architecture ObjectServer de bureau

Pour configurer une architecture ObjectServer de bureau, vous devez créer et configurer un nouveau serveur ObjectServer de bureau puis configurer une passerelle ObjectServer unidirectionnelle pour envoyer les données pertinentes au serveur ObjectServer de bureau.

Création et configuration d'un serveur ObjectServer de bureau

Vous devez exécuter l'utilitaire d'initialisation de la base de données avec les options de ligne de commande appropriées pour créer un serveur ObjectServer du bureau.

Pourquoi et quand exécuter cette tâche

Pour créer et configurer un serveur ObjectServer de bureau :

Procédure

1. Pour créer le serveur ObjectServer du bureau, entrez la commande appropriée à votre système d'exploitation :

Tableau 62. Création d'un serveur ObjectServer de bureau

Option	Description
UNIX	`$NCHOME/omnibus/bin/nco_dbinit -server` *`nom_serveur`* `-desktopserver -dsdprimary` *`nom_serveur_maître`* `-dsddualwrite`
Windows	`%NCHOME%\omnibus\bin\nco_dbinit -server` *`nom_serveur`* `-desktopserver -dsdprimary` *`nom_serveur_maître`* `-dsddualwrite`

   Dans les commandes ci-dessus, *nom_serveur* est le nom du nouveau serveur ObjectServer de bureau et *nom_serveur_maître* est le nom du serveur ObjectServer maître.

   Le fichier SQL par défaut utilisé pour créer les serveurs ObjectServer de bureau est `$NCHOME/omnibus/etc/desktopserver.sql`. Vous pouvez utiliser facultativement l'option de ligne de commande `-desktopserverfile` pour spécifier un autre fichier SQL, auquel cas le serveur ObjectServer de bureau est créé à l'aide des commande du fichier SQL que vous spécifiez.

   Lorsque vous initialisez le serveur ObjectServer de bureau, la table de base de données master.national est créée. Cette table identifie le serveur ObjectServer maître et le mode écriture double.
2. Après la création d'un serveur ObjectServer de bureau, assurez-vous de l'ajouter au fichier de définition de serveur sur tout hôte qui exécute un bureau à deux serveurs.
3. Démarrez le serveur ObjectServer de bureau.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Tâches associées:

«Démarrage d'un serveur ObjectServer», à la page 202
Vous devez exécuter un serveur ObjectServer avant d'utiliser les composants de Tivoli Netcool/OMNIbus.

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Configuration de la passerelle ObjectServer unidirectionnelle

Vous devez configurer la passerelle ObjectServer unidirectionnelle (**nco_g_objserv_uni**) pour garantir que toutes les données pertinentes sont envoyées depuis le serveur ObjectServer maître au serveur ObjectServer du bureau. Pour ce faire, vous devez apporter des modifications aux fichiers de configuration de la passerelle ObjectServer.

Pourquoi et quand exécuter cette tâche

Remarque : Pour obtenir des informations complètes sur la configuration de la passerelle ObjectServer unidirectionelle, voir *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*SC11-7240.

Pour configurer la passerelle ObjectServer unidirectionnelle :

Procédure

1. Créez un répertoire pour les fichiers de la passerelle, par exemple `$NCHOME/omnibus/gates/DSD_GATE`.

   Conseil : Cette tâche utilise un exemple de nom de répertoire `$NCHOME/omnibus/gates/DSD_GATE`. Dès qu'il est référencé, remplacez ce nom par le nom de votre répertoire de fichiers de passerelle réel.
2. Copiez tous les fichiers du répertoire `$NCHOME/omnibus/gates/objserv_uni` dans `$NCHOME/omnibus/gates/DSD_GATE`.
3. Renommez le fichier `$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.props` en `$NCHOME/omnibus/gates/DSD_GATE/DSD_GATE.props`.
4. Dans le fichier `$NCHOME/omnibus/gates/DSD_GATE/DSD_GATE.props`, modifiez les propriétés répertoriées dans le tableau suivant.

Tableau 63. Configuration des propriétés de passerelle ObjectServer unidirectionnelle pour le bureau à deux serveurs

Propriété	Description
Gate.MapFile	Emplacement du fichier de définition de mappe de passerelle. Définissez ce paramètre sur `$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.map`.
Gate.Reader.Server	Nom du serveur ObjectServer à partir duquel la passerelle lit les alertes ; c'est-à-dire le serveur ObjectServer maître.
Gate.Reader.Tbl.ReplicateDefFile	Chemin d'accès au fichier de définition de réplication de table de passerelle. Définissez ce paramètre sur `$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.reader.tblrep.def`.
Gate.StartupCmdFile	Chemin d'accès au fichier de commande de démarrage de la passerelle. Définissez ce paramètre sur `$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.startup.cmd`.
Gate.Writer.Server	Nom de la passerelle dans laquelle le serveur ObjectServer écrit les alertes ; c'est-à-dire le serveur ObjectServer du bureau.

Par exemple :

```
# Common Netcool/OMNIbus Properties.
MessageLog                 : '$NCHOME/omnibus/log/DSD_GATE.log'

# Common Gateway Properties.
Gate.MapFile               : '$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.map'
```

```
Gate.StartupCmdFile         : '$NCHOME/omnibus/gates/DSD_GATE/objserv_uni.startup.cmd'

# Unidirectional ObjectServer Gateway Properties.
Gate.Reader.Server          : 'NETCOOLPRI'
Gate.Reader.Username        : 'root'
Gate.Reader.Password        : ''
Gate.Reader.Tbl.ReplicateDefFile:
                    $NCHOME/omnibus/gates/DSD_GATE/objserv_uni.reader.tblrep.def
Gate.Writer.Server          : 'DESKOS'
Gate.Writer.Username        : 'root'
Gate.Writer.Password        : ''
```

5. Copiez le fichier de propriétés $NCHOME/omnibus/gates/DSD_GATE/DSD_GATE.props dans $NCHOME/omnibus/etc. La passerelle recherche son fichier de propriétés à cet emplacement.
6. Dans le fichier $NCHOME/omnibus/gates/DSD_GATE/objserv_uni.map, ajoutez une entrée MasterSerial à la fin de la section de mappage StatusMap. Par exemple :

```
'URL'               = '@URL'                        ON INSERT ONLY,
'ServerName'        = '@ServerName'                 ON INSERT ONLY,
'ServerSerial'      = '@ServerSerial'               ON INSERT ONLY,
'MasterSerial'      = '@Serial'                     ON INSERT ONLY
);
```

   Cette entrée fournit une identification unique des événements dans le serveur ObjectServer maître.

   Remarque : Les étapes précédentes vous permettent d'obtenir une passerelle ObjectServer unidirectionelle à utiliser dans une architecture de bureau à deux serveurs. Toutefois, si vous vous arrêtez ici, toutes les modifications de configuration apportées au serveur ObjectServer maître ou à tout ObjectServer du bureau doivent être effectuées manuellement sur les autres serveurs ObjectServer du système. Par exemple, si vous ajoutez un utilisateur au serveur ObjectServer maître, vous devez l'ajouter manuellement aux serveurs ObjectServer du bureau pour vous assurer qu'il puisse se connecter au bureau à deux serveurs. De même, toutes les modifications apportées aux configurations du serveur ObjectServer du bureau, telles que les outils et les conversions, ne seront pas transmises correctement par la passerelle. Si vous prévoyez d'apporter des modifications ultérieures à l'un des serveurs ObjectServer de l'environnement de bureau à deux serveurs, vous devez effectuer les étapes restantes.
7. Editez le fichier $NCHOME/omnibus/gates/DSD_GATE/objserv_uni.reader.tblrep.def pour spécifier les tables du serveur ObjectServer maître qui sont répliquées dans le serveur ObjectServer du bureau. Le fichier contient des entrées de réplication de table mises en commentaire ; par exemple :

```
# REPLICATE ALL FROM TABLE 'security.users'
#    USING MAP 'SecurityUsersMap'
#    INTO 'transfer.users';
```

   Supprimez la mise en commentaire des entrées de réplication de table appropriées dans les sections alertes, sécurité et outils du fichier. Pour répliquer toutes les données d'alertes, de sécurité et d'outils de la table, supprimez la mise en commentaire de toutes les entrées.

   Vous devez également mettre à jour le fichier objserv_uni.reader.tblrep.def pour protéger les droits de la table master.national, présente sur le serveur ObjectServer du bureau, mais pas sur le serveur ObjectServer maître. Mettez à jour la section sécurité du fichier comme suit, pour vous assurer que les droits ne soient pas supprimés lors de la resynchronisation :

```
REPLICATE ALL FROM TABLE 'security.role_grants'
        USING MAP 'SecurityRoleGrantsMap'
    INTO 'transfer.role_grants'
```

```
        RESYNC DELETES FILTER 'RoleID not in (3)';

REPLICATE ALL FROM TABLE 'security.permissions'
        USING MAP 'SecurityPermissionsMap'
    INTO 'transfer.permissions'
        RESYNC DELETES FILTER 'Object not in (\'master.national\')';
```

8. Editez le fichier $NCHOME/omnibus/gates/DSD_GATE/objserv_uni.map pour définir comment mapper les données répliquées du serveur ObjectServer maître sur le serveur ObjectServer du bureau. Le fichier contient des entrées de mappage mises en commentaire ; par exemple :

```
# CREATE MAPPING SecurityUsersMap
# (
#       'UserID'         =       '@UserID'           ON INSERT ONLY,
#       'UserName'       =       '@UserName',
#       'SystemUser'     =       '@SystemUser',
#       'FullName'       =       '@FullName',
#       'Passwd'         =       '@Passwd',
#       'UsePAM'         =       '@UsePAM',
#       'Enabled'        =       '@Enabled'
# );
```

   Supprimez la mise en commentaire de toutes les entrées de mappage dans le fichier pour qu'elles correspondent aux données de la table que vous souhaitez répliquer.

9. Ajoutez une entrée pour la passerelle vers l'éditeur de serveurs.

   La passerelle ObjectServer unidirectionnelle est maintenant configuré pour l'utilisation avec l'architecture de bureau à deux serveurs.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Affichage des résultats des actions d'outils à l'aide du mode écriture double

Le mode écriture double permet aux opérateurs d'afficher rapidement les résultats des actions d'outils (par exemple, les accusés réception et les définitions de priorité) à partir d'un bureau à deux serveurs (DSD). Lorsque ce mode est activé, toutes les actions d'outils sont envoyées au serveur ObjectServer de bureau et au serveur ObjectServer maître.

Lorsque vous initialisez le serveur ObjectServer de bureau, vous pouvez activer ou désactiver le mode écriture double à l'aide de l'option de ligne de commande `-dsddualwrite` de l'utilitaire **nco_dbinit**.

Vous pouvez activer ou désactiver le mode écriture double en modifiant le paramètre de colonne DualWrite de la table master.national du serveur ObjectServer de bureau. Pour activer le mode écriture double, définissez la colonne DualWrite sur 1. Pour désactiver le mode écriture double, définissez la colonne DualWrite sur `0`. Voici un exemple de commande `update` pour activer le mode écriture double :

```
update master.national set DualWrite = 1;
```

Vous pouvez également remplacer le paramètre de mode écriture double actuel à l'aide de l'option de ligne de commande `-dualwrite` de la liste d'événements.

Remarque : Si vous activez le mode écriture double, il est possible que les informations d'alerte ne soient pas mises à jour sur tous les bureaux à deux serveurs simultanément. Par exemple, cela peut être dû à un trafic réseau important. Si vous souhaitez que tous les bureaux à deux serveurs affichent toujours des informations identiques, désactivez le mode écriture double.

Affichage des entrées du journal opérateur à partir d'un bureau à deux serveurs (DSD)

Les entrées du journal d'alerte effectuées par un opérateur à partir d'une alerte DSD sont généralement envoyées uniquement au serveur ObjectServer maître. Cependant, si une alerte sélectionnée est exclusive pour le serveur ObjectServer de bureau (auquel cas, elle porte la valeur MasterSerial de `0`), ses entrées de journal manuelles sont envoyées uniquement au serveur ObjectServer de bureau.

Une alerte est exclusive pour le serveur ObjectServer de bureau si elle est insérée dans le serveur ObjectServer de bureau par tout autre moyen que via la passerelle unidirectionnelle du serveur ObjectServer (à partir du serveur ObjectServer maître dans le serveur ObjectServer de bureau).

Authentification du serveur ObjectServer de bureau

Pourquoi et quand exécuter cette tâche

Tivoli Netcool/OMNIbus effectue les étapes suivantes pour authentifier un serveur ObjectServer de bureau :

Procédure

1. Tivoli Netcool/OMNIbus vérifie la présence de la définition de colonne MasterSerial dans la table alerts.status du serveur ObjectServer. Si MasterSerial n'existe pas, le bureau entre en mode standard et se connecte uniquement au serveur ObjectServer du bureau.
2. Lorsqu'un opérateur se connecte au bureau, ce dernier vérifie l'existence de la table master.national sur le serveur ObjectServer sélectionné.
3. Si la table master.national existe et contient une entrée valide dans la colonne MasterServer, le bureau entre en mode bureau à deux serveurs (DSD). Le DSD traite le serveur ObjectServer sélectionné comme ObjectServer du bureau et le serveur ObjectServer indiqué dans la colonne MasterServer comme ObjectServer maître.

   Remarque : L'option de ligne de commande `-masterserver` pour la liste d'événements se substitue à la colonne MasterServer.

   Si le bureau ne détecte pas la table master.national sur le serveur ObjectServer sélectionné, il entre en mode ObjectServer standard.
4. Le DSD tente de s'authentifier auprès du serveur ObjectServer maître en utilisant le nom d'utilisateur et le mot de passe entrés lors de la connexion de l'opérateur (étape 2).

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **`nco_dbinit`** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

Mode équilibrage de charges

Dans une configuration dans laquelle se trouve un groupe de serveurs ObjectServer de bureau, il est très probable que le nombre d'utilisateurs de liste d'événements connectés dans chaque ObjectServer de bureau ne soit pas pair. Dans certains cas, tous les utilisateurs peuvent être connectés à un serveur ObjectServer de bureau, laissant les serveurs ObjectServer de bureau restants en veille.

Le mode équilibrage de charges distribue automatiquement les données de connexion des utilisateurs à la liste d'événements à un groupe de serveurs ObjectServer de bureau indiqué, conformément à une pondération indiquée par l'administrateur. Ce processus est transparent pour l'utilisateur de la liste d'événements.

Configuration du mode équilibrage de charges

Pourquoi et quand exécuter cette tâche

Le mode équilibrage de charge est configuré comme suit :

Procédure

1. Déterminez un groupe de serveurs ObjectServer de bureau entre lesquels les connexions de la liste d'événements doivent être distribuées. Ces serveurs ObjectServer de bureau doivent tous être connectés au même ObjectServer maître via une passerelle ObjectServer unidirectionelle.
2. Définissez chaque ObjectServer du groupe comme serveur `Primary` en utilisant l'éditeur de serveurs ou en éditant le fichier de données de connexion `$NCHOME/etc/omni.dat`.
3. Créez des entrées dans la table master.servergroups pour tous les serveurs ObjectServer de bureau. Le tableau suivant décrit les entrées de colonnes requises pour chaque ObjectServer de bureau dans la table master.servergroups. Vous pouvez utiliser Netcool/OMNIbus Administrator ainsi que la commande INSERT pour insérer une ligne pour chaque ObjectServer de bureau.

Tableau 64. Table master.servergroups

Colonne	Type de données	Description
ServerName	varchar(64)	Nom du serveur ObjectServer de bureau. Il s'agit de la clé principale.
GroupID	entier	Groupe auquel appartient chaque ObjectServer de bureau. Les informations de connexion des utilisateurs de la liste d'événements sont uniquement distribués entre les serveurs ObjectServer de bureau ayant le même GroupID.
Weight	entier	Priorité de chaque ObjectServer de bureau. Des valeurs plus élevées attirent proportionnellement plus de connexions. Par exemple, un serveur ObjectServer avec une valeur Weight de `2` attire deux fois plus de connexions qu'un serveur ayant une valeur Weight de `1`. Les connexions avec équilibrage de charge ne sont pas redirigées vers les serveurs ObjectServer ayant une valeur Weight de `0`.

Conseil : Vous pouvez configurer la passerelle ObjectServer unidirectionnelle pour que les tables master.servergroups du serveur ObjectServer de bureau

soient synchronisées avec la table master.servergroups du serveur ObjectServer maître. Pour plus d'informations sur la configuration de la passerelle ObjectServer unidirectionelle, voir *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*SC11-7240.

Résultats

Une fois cette configuration effectuée, les connexions de la liste d'événements des serveurs ObjectServer de bureau seront basées sur un algorithme qui garantit une distribution homogène des connexions sur les serveurs ObjectServer de bureau, conformément aux spécifications de pondération.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Tâches associées:

«Création et configuration d'un serveur ObjectServer de bureau», à la page 328
Vous devez exécuter l'utilitaire d'initialisation de la base de données avec les options de ligne de commande appropriées pour créer un serveur ObjectServer du bureau.

«Configuration de la passerelle ObjectServer unidirectionnelle», à la page 329
Vous devez configurer la passerelle ObjectServer unidirectionnelle (**nco_g_objserv_uni**) pour garantir que toutes les données pertinentes sont envoyées depuis le serveur ObjectServer maître au serveur ObjectServer du bureau. Pour ce faire, vous devez apporter des modifications aux fichiers de configuration de la passerelle ObjectServer.

«Edition manuelle du fichier de données de connexions», à la page 217
Le fichier de données de connexions permet de créer le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus. Dans certains cas, il peut être nécessaire d'éditer le fichier de connexions directement ; par exemple sur les systèmes UNIX qui ne disposent pas d'interface graphique.

Exemple : pondération

Un système est configuré avec quatre serveurs ObjectServer de bureau, DISP_A, DISP_B, DISP_C et DISP_D, où :

- DISP_A peut prendre en charge 1/6 des connexions.
- DISP_B peut prendre en charge 1/3 des connexions.
- DISP_C peut prendre en charge 1/2 des connexions.
- DISP_D n'est pas disponible pour les connexions à charges équilibrées.

DISP_A, qui prend en charge le nombre le plus faible de connexions, se voit attribuer une pondération de 1. DISP_B, qui prend en charge deux fois plus de connexions que DISP_A, se voit attribuer une pondération de 2. DISP_C, qui prend en charge trois fois plus de connexions que DISP_A, se voit attribuer une pondération de 3. DISP_D n'accepte pas les connexions à charges équilibrées et se voit donc attribuer une pondération de 0.

Tous les serveurs ObjectServer obtiennent la même valeur GroupID afin que les connexions puissent être réacheminées entre eux.

Les commandes `insert` permettant de configurer la table master.servergroups pour ce système sont les suivantes :

```
insert into master.servergroups values ('DISP_A', 1, 1);
insert into master.servergroups values ('DISP_B', 1, 2);
insert into master.servergroups values ('DISP_C', 1, 3);
insert into master.servergroups values ('DISP_D', 1, 0);go
```

Exemple : groupes à charges équilibrées

Le système décrit dans la rubrique «Exemple : pondération», à la page 334 est maintenant étendu pour permettre l'utilisation de deux serveurs ObjectServer de bureau supplémentaires : DISP_E et DISP_F.

Ces serveurs ObjectServer de bureau peuvent prendre en charge le même nombre de connexions entre eux, mais ne partagent pas des connexions à charges équilibrées avec les serveurs ObjectServer existants. DISP_E et DISP_F se voient attribuer une valeur GroupID de 2 et tous deux ont une pondération de 1.

Les commandes `insert` permettant de configurer la table master.servergroups pour les serveurs ObjectServer de bureau supplémentaires sont les suivantes :

```
insert into master.servergroups values ('DISP_E', 2, 1);
insert into master.servergroups values ('DISP_B', 2, 1);go
```

Référence associée:

«Exemple : pondération», à la page 334

Chapitre 13. Sécurité des accès utilisateur dans Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus offre des mécanismes de *sécurité des accès utilisateur* pour protéger votre système Tivoli Netcool/OMNIbus de dommages accidentels ou délibérés causés par les utilisateurs ou des utilisateurs potentiels de votre système.

Les techniques de *sécurité des communications* protègent les connexions entre différents composants de votre système Tivoli Netcool/OMNIbus. Tivoli Netcool/OMNIbus utilise le protocole de sécurité SSL pour fournit une confidentialité, une authenticité et une intégrité des informations entre les composants.

Concepts associés:

Chapitre 14, «Utilisation du protocole SSL pour les communications serveur et client», à la page 371
Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

Mécanismes de sécurité des accès utilisateur

Tivoli Netcool/OMNIbus est un système réparti qui peut être utilisé simultanément par différents types d'utilisateurs. Dans un déploiement classique, les opérateurs utilisent des outils de bureau pour surveiller les incidents dans une zone particulière du réseau. En même temps, les administrateurs utilisent l'interface interactive SQL, Netcool/OMNIbus Administrator, et le contrôle de processus pour assurer l'exécution normale et efficace de Tivoli Netcool/OMNIbus.

Dans un déploiement large, il est fréquent de posséder différentes équipes d'utilisateurs pour différentes régions de déploiement. Par exemple, un centre d'opérations de réseaux (NOC) situé à New York peut être responsable de l'exécution et de l'utilisation du déploiement de Tivoli Netcool/OMNIbus en Amérique, alors qu'un autre NOC situé à Londres peut être responsable du déploiement en Europe.

Pour plusieurs utilisateurs et types d'utilisateurs dans plusieurs régions, il est important de contrôler les droits dont dispose chaque utilisateur pour afficher et modifier le système Tivoli Netcool/OMNIbus et les informations qu'il contient. Pour protéger votre système, vous devez considérer les zones d'accès utilisateur suivantes :

- Authentification
- Autorisation

Authentification

L'*authentification* est la vérification de l'identité d'une personne. Par exemple, si une personne tente de se connecter en tant qu'administrateur à votre centre d'opérations de réseaux de Londres, il est important de vérifier tout d'abord que cette personne est bien celle qu'elle prétend être et non un imposteur.

Tous les utilisateurs de Tivoli Netcool/OMNIbus possèdent un nom d'utilisateur et un mot de passe associé. En fonction de l'application client, vous pouvez indiquer le nom d'utilisateur et le mot de passe à l'aide du fichier de propriétés ou d'options de ligne de commande, ou en répondant à une invite de l'application. L'association du nom d'utilisateur et du mot de passe est authentifiée avant établissement d'une connexion avec le serveur ObjectServer. Ce contrôle d'accès atteste que l'utilisateur possède un nom d'utilisateur valide et que le mot de passe correct correspondant a été saisi. Le chiffrement du mot de passe offre une sécurité supplémentaire.

Les utilisateurs peuvent être authentifiés sur le serveur ObjectServer ou de manière externe. Sur les systèmes UNIX et Linux, les utilisateurs du serveur ObjectServer peuvent être authentifiés de façon externe à l'aide des modules PAM ou d'un système LDAP. Le mécanisme par défaut est le module PAM. Sur les systèmes Windows, les utilisateurs peuvent être authentifiés de manière externe à l'aide du protocole LDAP.

Après s'être connecté à une application, un utilisateur est autorisé à exécuter ses tâches, en fonction des groupes auxquels il appartient et des rôles attribués à ces groupes.

Concepts associés:

«Authentification PAM (sous UNIX et Linux)», à la page 354
Le module PAM est une infrastructure préfabriquée de connexion intégrée sous UNIX. Il est utilisé par les composants d'entrée du système, notamment le gestionnaire d'affichage **dtlogin** de l'environnement CDE, pour authentifier les connexions des utilisateurs dans un système UNIX.

«Authentification en mode sécurisé», à la page 339
Les composants Tivoli Netcool/OMNIbus exécutent des vérifications d'authentification pour offrir un environnement sécurisé.

Tâches associées:

«Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe», à la page 343
Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

Autorisation

L'*autorisation* est la vérification des droits pour afficher et modifier des informations.

Par exemple, vous pouvez être autorisé à créer une automatisation sur le serveur ObjectServer du centre d'opérations de réseaux de Londres, mais pas pour le serveur ObjectServer du centre d'opérations de réseaux de New York.

Chaque objet du serveur ObjectServer est associé à des actions. Le serveur ObjectServer stocke des informations sur les actions que chaque utilisateur est, ou non, autorisé à exécuter sur le système et pour chaque objet.

Les administrateurs peuvent autoriser et refuser des actions sur le système et pour des objets individuels en attribuant des droits à des rôles, et en accordant des rôles aux groupes d'utilisateurs adéquats ou en les révoquant.

Les administrateurs peuvent également créer des filtres de restriction pour limiter les données tabulaires qu'un utilisateur ou un groupe peut afficher.

Concepts associés:

«Implémentation d'une autorisation à l'aide de groupes et de rôles», à la page 359
Les droits contrôlent l'accès aux objets et aux données dans le serveur ObjectServer. En regroupant un ou plusieurs droits en *rôles*, vous pouvez gérer les accès rapidement et efficacement.

«Utilisation de filtres de restriction pour filtrer les informations de table», à la page 365
Un filtre de restriction est une façon de limiter les lignes qui s'affichent lorsqu'un utilisateur consulte des données tabulaires. Lorsque le filtre est attribué à un utilisateur ou à un groupe, le filtre contrôle les données qui s'affichent et qui sont modifiées à partir d'applications client et modifiées dans des commandes SQL.

Authentification en mode sécurisé

Les composants Tivoli Netcool/OMNIbus exécutent des vérifications d'authentification pour offrir un environnement sécurisé.

L'authentification d'utilisateur est mise en place des manières suivantes :

- Vous pouvez exécuter le serveur ObjectServer, le serveur proxy et l'agent de processus en mode sécurisé. Dans ce mode, les connexions de sonde et de passerelle à un serveur ObjectServer ou à un serveur proxy sont authentifiées par un nom d'utilisateur et un mot de passe. Lorsque l'agent de processus est exécuté en mode sécurisé, les connexions sont authentifiées avant l'exécution des procédures externes. *Les autres demandes de connexion client sont toujours authentifiées.*
- Vous pouvez coder les mots de passe stockés dans les fichiers de configuration et de propriétés.

  Lorsque le mode FIPS 140–2 est activé, le mot de passe peut être spécifié en texte normal ou chiffré à l'aide de l'utilitaire **nco_aes_crypt**. Si vous chiffrez des mots de passe à l'aide de l'utilitaire **nco_aes_crypt** en mode FIPS 140–2, vous devez spécifier `AES_FIPS` comme algorithme de chiffrement.

  Lorsque le mode FIPS 140–2 est désactivé, le mot de passe peut être chiffré à l'aide des utilitaires **nco_g_crypt** ou **nco_aes_crypt**. Si vous chiffrez des mots de passe à l'aide de l'utilitaire **nco_aes_crypt** en mode FIPS 140–2 désactivé, vous pouvez spécifier `AES_FIPS` ou `AES` comme algorithme de chiffrement. Utilisez uniquement `AES` si vous devez conserver une compatibilité avec des mots de passe codés à l'aide des outils fournis dans des versions antérieures à Tivoli Netcool/OMNIbus V7.2.1.

Remarque : Pour éviter que des utilisateurs non autorisés ne puissent y avoir accès, la sécurité du système d'exploitation doit être définie de manière appropriée pour les fichiers comme les fichiers de configuration et de propriétés qui peuvent contenir des noms d'utilisateur et des mots de passe.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

Mode sécurisé du serveur ObjectServer

Vous pouvez exécuter le serveur ObjectServer en mode sécurisé. Lorsque vous indiquez l'option de ligne de commande `-secure`, le serveur ObjectServer authentifie les connexions de sonde, de passerelle et de serveur proxy en demandant un nom d'utilisateur et un mot de passe.

Lorsqu'une demande de connexion est envoyée, le serveur ObjectServer émet un message d'authentification. La sonde, la passerelle ou le serveur proxy doit répondre par l'association nom d'utilisateur/mot de passe correcte.

Si le serveur ObjectServer ne s'exécute pas en mode sécurisé, les demandes de connexion de sonde, de passerelle et de serveur proxy ne sont pas authentifiées.

Les connexions d'autres clients, notamment la liste d'événements et l'interface interactive SQL, sont toujours authentifiées.

Mode sécurisé du serveur proxy

Vous pouvez exécuter le serveur proxy en mode sécurisé. Lorsque vous indiquez l'option de ligne de commande `-secure`, le serveur proxy authentifie les connexions de sonde en demandant un nom d'utilisateur et un mot de passe.

Lorsqu'une demande de connexion est envoyée, le serveur proxy émet un message d'authentification. La sonde doit répondre par le nom d'utilisateur et le mot de passe corrects.

Si le serveur proxy ne s'exécute pas en mode sécurisé, les demandes de connexion de sonde ne sont pas authentifiées.

Connexion sécurisée à partir de sondes et de passerelles

Lorsque le serveur ObjectServer ou le serveur proxy s'exécute en mode sécurisé, les connexions de sonde et de passerelle au serveur ObjectServer ou au serveur proxy sont authentifiées par un nom d'utilisateur et un mot de passe.

En outre, vous pouvez coder les mots de passe de connexion en texte en clair, stockés dans le fichier de propriétés de la passerelle. Les mots de passe sont décodés par la passerelle cible et utilisés pour se connecter au système cible.

Sécurité du contrôle de processus

Vous pouvez exécuter l'agent de processus en mode sécurisé. L'option `-secure` contrôle l'authentification de demandes de connexion lors de l'exécution de procédures externes en vérifiant un nom d'utilisateur et un mot de passe sur l'hôte local.

Les options de ligne de commande du serveur ObjectServer, `-pa`, `-pausername` et `-papassword`, et les propriétés correspondantes, **`PA.Name`**, **`PA.Username`** et

PA.Password, vous permettent d'indiquer l'agent de processus auquel se connecter et le nom d'utilisateur ainsi que le mot de passe à authentifier lors de l'exécution de procédures externes.

Vous pouvez également indiquer que seuls certains hôtes peuvent se connecter aux agents de processus en ajoutant une définition de sécurité au fichier de configuration de l'agent de processus. Pour chaque définition d'hôte, vous devez également indiquer les données d'identification de nom d'utilisateur et de mot de passe pour se connecter à l'agent de processus en mode sécurisé. Sinon, vous pouvez indiquer en option des données d'identification pour se connecter à un agent de processus distant.

En outre, vous pouvez utiliser l'utilitaire **nco_pa_crypt** ou **nco_aes_crypt** pour coder les mots de passe de connexion en texte en clair stockés dans le fichier de configuration de l'agent de processus.

Remarque : Si l'agent de processus est exécuté en tant qu'utilisateur disposant de certains privilèges ou en tant que superutilisateur sur la machine hôte, il est possible pour un administrateur Netcool/OMNIbus de configurer les actions externes qui sont ensuite exécutées sur le système hôte en tant qu'utilisateur disposant de certains privilèges. Pour éviter ce risque de sécurité potentiel, vous devez exécuter l'agent de processus comme un utilisateur non privilégié.

Si l'agent de processus est exécuté en tant qu'utilisateur disposant de certains privilèges ou en tant que superutilisateur sur la machine hôte, et qu'un serveur ObjectServer est configuré pour exécuter des actions externes via cet agent de processus, un administrateur ObjectServer Netcool/OMNIbus peut configurer des actions externes qui sont ensuite exécutées sur le système hôte en tant qu'utilisateur disposant de certains privilèges. Ceci est dû au fait que les actions sont exécutées de la part du serveur ObjectServer par l'agent de processus comme l'utilisateur sous la forme duquel l'agent de processus est exécuté. Pour éviter ce risque de sécurité potentiel, vous devez configurer les serveurs ObjectServers pour exécuter les actions externes utilisant un agent de processus exécuté comme un utilisateur non privilégié. Pour plus d'informations, voir Considérations concernant le sécurité de agent de processus.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

Protection par mot de passe de l'interface interactive SQL dans des scripts

Par défaut, l'interface interactive SQL (**nco_sql**) chiffre les informations de connexion lors de la connexion à un serveur ObjectServer en mode sécurisé.

En outre, vous pouvez utiliser l'utilitaire **nco_sql_crypt** (en mode FIPS 140-2) pour coder les mots de passe de connexion en texte en clair qui ne sont pas exposés dans des scripts exécutant **nco_sql**.

Configuration du serveur ObjectServer pour l'authentification d'utilisateurs

Si les utilisateurs sont authentifiés dans le serveur ObjectServer, vous pouvez contrôler le mécanisme d'authentification d'utilisateurs en définissant les propriétés du serveur ObjectServer. Vous pouvez changer l'algorithme de chiffrement des mots de passe ou restreindre les mots de passe à un format spécifique, ou les deux.

Procédure

- Pour modifier l'algorithme de chiffrement pour les mots de passe, définissez la propriété **PasswordEncryption** sur la valeur requise. Cette propriété définit le schéma de chiffrement utilisé pour coder les mots de passe utilisateur stockés dans le serveur ObjectServer. Les valeurs possibles sont les suivantes :
  - `DES` : chiffrement Data Encryption Standard (DES). Seuls les huit premiers caractères d'un mot de passe DES sont lus. Les autres caractères sont ignorés.
  - `AES` : chiffrement Advanced Encryption Standard (AES128). Seuls les 16 premiers caractères d'un mot de passe AES128 sont lus. Les autres caractères sont ignorés. En mode FIPS 140–2, l'option `AES` est mandatée par le système.

  Pour les installations non FIPS 140-2, la valeur par défaut est `DES`. En mode FIPS 140-2, la valeur par défaut est `AES`.
- Pour limiter le format des mots de passe, définissez la propriété **RestrictPasswords** sur `TRUE`.
- Pour spécifier le format auquel les mots de passe sont limités, définissez la propriété **PasswordFormat** sur la valeur requise. La propriété définit le format des mots de passe utilisateur. Elle ne fonctionne que quand la propriété **RestrictPasswords** est paramétrée sur `TRUE`. Indiquez la valeur de cette propriété sous la forme d'un ensemble de valeurs de type entier séparées par des signes deux-points. Chaque valeur définit une exigence de mot de passe. Le format est le suivant : *long_min*:*nbre_alpha*:*nbre_num*:*nbre_ponct* où :
  - *lon_min* est la longueur du mot de passe.
  - *nbre_alpha* est le nombre minimum de caractères alphabétiques.
  - *nbre_num* est le nombre minimum de caractères numériques.
  - *nbre_ponct* est le nombre minimum de caractères de ponctuation.

  Les exigences de caractère alphabétique, numérique et de ponctuation doivent être satisfaites au sein du nombre de caractères spécifié par la longueur minimale du mot de passe. La valeur par défaut de `8:1:1:0` doit comporter au moins un caractère alphabétique et un caractère numérique dans les 8 premiers caractères de la chaîne de mot de passe. Par exemple, si la propriété a pour valeur `8:1:1:0` et qu'un utilisateur indique le mot de passe abcdefgh590675, ce dernier est rejeté car les 8 premiers caractères ne contiennent aucun caractère numérique. Une fois cette propriété définie, l'ObjectServer valide tous les mots de passe nouveaux ou modifiés par rapport à cette exigence et les mots de passe ne remplissant pas cette exigence sont rejetés. Les mots de passe existants ne sont pas validés.

Exemple

Pour vous aider à comprendre les effets des propriétés **RestrictPasswords**, **PasswordFormat** et **PasswordEncryption**, examinez l'exemple suivant :

- **RestrictPasswords** est définie sur `TRUE`.
- **PasswordFormat** est définie sur sa valeur par défaut, `8:1:1:0`.

- **PasswordEncryption** est définie sur sa valeur par défaut, DES.

Si un utilisateur crée le mot de passe 1234abcdxyz, ce mot de passe est accepté parce que il répond à l'exigence indiquée par la propriété **PasswordFormat** : un minimum de 8 caractères, un minimum de 1 caractère alphabétique et un minimum de 1 caractère numérique. Etant donné que le chiffrement DES est défini, seuls les 8 premiers caractères, 1234abcd, sont lus. Les caractères xyz sont ignorés. Par conséquent, le même utilisateur peut se connecter avec le mot de passe 1234abcdxxx. Etant donné que seuls les 8 premiers caractères sont importants pour le chiffrement et que les exigences de format de mot de passe sont respectées, le mot de passe incorrect est accepté.

Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe

Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

Avant de commencer

Obtenez les données de configuration LDAP suivantes auprès de votre administrateur LDAP :

- Si tous les utilisateurs qui nécessitent un accès à Tivoli Netcool/OMNIbus appartiennent à la même unité organisationnelle, demandez à votre administrateur LDAP le modèle de nom distinctif pour cette unité organisationnelle. Le modèle fournit la valeur de la propriété **DistinguishedName** dans le fichier de propriétés LDAP Tivoli Netcool/OMNIbus.

  Par exemple, dans le modèle `cn=%s,ou=Development,o=ABCcorp`, le nom distinctif de base auquel appartiennent tous les utilisateurs est `ou=Development,o=ABCcorp` et la zone `cn` se mappe sur un nom d'utilisateur dans le référentiel d'utilisateurs ObjectServer. Lorsqu'un utilisateur se connecte à l'ObjectServer, ce dernier remplace la variable `%s` par le nom d'utilisateur et soumet la totalité de la chaîne au serveur LDAP pour authentification.
- Si les utilisateurs appartiennent à plusieurs unités organisationnelles, vous devez configurer l'ObjectServer pour effectuer une recherche LDAP pour le nom distinctif de chaque utilisateur. Demandez les informations suivantes à votre administrateur LDAP :
  - Nom distinctif de l'unité organisationnelle racine pour tous les utilisateurs ou une liste des unités organisationnelles auxquels appartient chaque utilisateur.

    Le nom distinctif ou la liste des unités organisationnelles fournit la valeur de la propriété **LDAPSearchBase** dans le fichier de propriétés LDAP Tivoli Netcool/OMNIbus.
  - Modèle permettant de générer un filtre de recherche LDAP pour chaque utilisateur Tivoli Netcool/OMNIbus.

    Le modèle (par exemple : `(cn=%s)`) fournit la valeur de la propriété **LDAPSearchFilter** dans le fichier de propriétés LDAP Tivoli Netcool/OMNIbus.
- Confirmez si un nom distinctif de liaison est requis pour les opérations d'écriture afin d'obtenir des informations d'utilisateur et de groupe ou pour effectuer des recherches.

- Si un nom distinctif de liaison est requis, vous devez indiquer des valeurs pour les propriétés **LDAPBindDn** et **LDAPBindPassword** dans le fichier de propriétés LDAP Tivoli Netcool/OMNIbus. L'ObjectServer utilise ces valeurs pour établir une connexion permanente au serveur LDAP et pour émettre des requêtes et des recherches de liaisons d'authentification.
- Si un nom distinctif de liaison n'est pas requis, supprimez ou mettez en commentaire les propriétés **LDAPBindDn** et **LDAPBindPassword** dans le fichier de propriétés LDAP Tivoli Netcool/OMNIbus. L'ObjectServer se connecte ensuite à LDAP anonymement.

- Examinez les paramètres du fichier de propriétés LDAP Tivoli Netcool/OMNIbus et demandez toute autre information nécessaire, telle que le nom d'hôte du serveur LDAP et le numéro de port.
- Utilisez l'utilitaire **ldapsearch** pour tester votre configuration avant de l'implémenter dans l'ObjectServer.

Remarque : Lorsque l'ObjectServer se connecte à un serveur LDAP sur une connexion SSL, il agit comme un client lorsqu'il lance la connexion SSL. Si vous configurez une connexion SSL, l'ObjectServer doit vérifier la signature sur le certificat présenté par le serveur LDAP. Pour ce faire, il a besoin de la clé publique de l'autorité de certification émettrice. Consultez votre administrateur LDAP pour obtenir le certificat racine autosigné émis par l'autorité de certification. Vous devez ajouter ce certificat à la base de données de clés ObjectServer.

Si vous avez configuré Tivoli Netcool/OMNIbus afin qu'il fonctionne en mode FIPS 140-2 avec le protocole SSL, l'interface LDAP doit également être configurée pour le fonctionnement en mode FIPS 140-2. Consultez votre administrateur LDAP pour vérifier que le support de chiffrement requis est en place pour le fonctionnement en mode FIPS 140-2.

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le serveur ObjectServer pour agir en tant que client LDAP, afin que les mots de passe des utilisateurs se connectant au serveur ObjectServer soient authentifiés dans un serveur LDAP. Vous pouvez utiliser un serveur LDAP unique pour authentifier tous les utilisateurs Tivoli Netcool/OMNIbus, y compris les utilisateurs qui accèdent aux composants de bureau.

Les détails de l'utilisateur sont stockés dans le référentiel d'utilisateurs ObjectServer et les entrées d'utilisateur sont configurées pour s'authentifier en externe. Les mots de passe d'utilisateur ne sont pas stockés dans l'ObjectServer. Lorsqu'un utilisateur se connecte à l'ObjectServer, ce dernier localise l'entrée d'utilisateur dans son référentiel et se connecte au référentiel LDAP pour authentifier l'utilisateur.

Remarque : Le comportement par défaut de l'ObjectServer lorsqu'il authentifie un utilisateur consiste à assumer qu'un mot de passe en texte en clair est utilisé. Si une connexion échoue avec un mot de passe en texte en clair, l'ObjectServer prend en compte un mot de passe chiffré et tente de le déchiffrer et d'authentifier à nouveau l'utilisateur. Un mot de passe non valide peut entraîner deux échecs de tentative de connexion. Pour éviter une deuxième tentative de connexion à LDAP lorsque la première tentative échoue, modifiez la propriété **WTPasswordCheck** de l'ObjectServer pour l'adapter à votre configuration.

Restriction :

- Tivoli Netcool/OMNIbus n'est pas conçu pour être utilisé pour gérer les comptes utilisateur dans LDAP, et n'offre par conséquent pas la capacité de modifier les mots de passe dans un serveur LDAP.
- Le module LDAP utilisé par le serveur ObjectServer se connecte à une seule instance de serveur LDAP. Le composant de l'Interface graphique Web qui est déployé dans Tivoli Integrated Portal peut se connecter à plusieurs référentiels LDAP.

Procédure

Pour configurer l'authentification LDAP, suivez les instructions figurant dans le tableau ci-dessous. Pour chaque étape, les liens sont fournis vers les tâches requises qui expliquent comment exécuter chaque étape ou aux rubriques contenant des informations supplémentaires.

Tableau 65. Etapes permettant de configurer le produit permettant d'utiliser un protocole LDAP

Action	Informations complémentaires
1. Configurez le fichier de propriétés LDAP Tivoli Netcool/OMNIbus (`$NCHOME/omnibus/etc/ldap.props`) avec les paramètres que vous avez obtenus auprès de votre administrateur LDAP. Si les performances d'autorisation sont importantes et que tous les utilisateurs requis appartiennent à une seule unité organisationnelle, utilisez la propriété **`DistinguishedName`** pour créer une liaison directe à LDAP. Si tel n'est pas le cas, utilisez les propriétés **`LDAPSearchBase`** et **`LDAPSearchFilter`** pour effectuer une recherche de noms distinctifs.	«Propriétés LDAP», à la page 348
2. Configurez le serveur ObjectServer pour utiliser l'authentification LDAP en définissant la propriété **`Sec.ExternalAuthentication`** sur `LDAP`. Celle-ci est gérée dans le serveur ObjectServer.	Propriétés et options de ligne de commande du serveur ObjectServer
3. SSL uniquement : si aucune base de données de clés n'existe sur l'hôte de l'ObjectServer, créez-en une.	«A propos des fichiers de la base de données de clés», à la page 379 «Création d'une base de données de clés», à la page 381
4. SSL uniquement : ajoutez le certificat racine auto-signé de l'autorité de certification émettrice du certificat de serveur LDAP à la base de données de clés.	«Ajout de certificats d'autorités de certification», à la page 399

Tableau 65. Etapes permettant de configurer le produit permettant d'utiliser un protocole LDAP (suite)

Action	Informations complémentaires
5. SSL uniquement : vérifiez que les propriétés SSL suivantes sont définies dans le fichier `ldap.props` : **`SLLEnabled`** Paramétrez cette propriété sur `TRUE`. **`SSLport`** Indiquez un numéro de port sur lequel le serveur LDAP écoute les connexions LDAP. **`SSLKeyStoreLabel`** Indiquez l'étiquette du certificat que le serveur ObjectServer présente au serveur LDAP.	«Propriétés LDAP», à la page 348
6. Configurez chaque utilisateur Tivoli Netcool/OMNIbus externe pour une authentification externe. Utilisez l'administrateur Netcool/OMNIbus (**`nco_config`**) pour cette tâche ou, dans l'interface interactive SQL, utilisez la commande CREATE USER ou la commande ALTER USER. Si vous utilisez l'administrateur Netcool/OMNIbus, indiquez les informations suivantes dans la sous-fenêtre User Details (Informations utilisateur) : **Nom d'utilisateur** Entrez un nom d'utilisateur identique au nom stocké dans le référentiel d'authentification externe. **Password** Laissez cette zone vide. Les mots de passe sont stockés dans le référentiel externe. **Verify (Confirmer)** Laissez cette zone vide **External Authentication (Authentification externe)** Cochez cette case. Si vous utilisez l'interface interactive SQL, vérifiez que le nom d'utilisateur est identique au nom stocké dans le référentiel d'authentification externe, qu'aucun mot de passe n'est spécifié et que le mot clé PAM est paramétré sur TRUE.	Création et édition d'utilisateurs Commande CREATE USER Commande ALTER USER

Tableau 65. Etapes permettant de configurer le produit permettant d'utiliser un protocole LDAP (suite)

Action	Informations complémentaires
7. Facultatif : faites appel à l'utilitaire **nco_keygen**, puis à l'utilitaire **nco_aes_crypt** pour chiffrer le mot de passe LDAP. Une fois que vous avez chiffré le mot de passe, rééditez le fichier `ldap.props` en définissant les propriétés suivantes : • **ConfigCryptoAlg** : paramétrez cette propriété sur `AES`. • **Hostname** • **ConfigKeyFile** • **LDAPBindPassword** • **LDAPBindDN**	«Chiffrement des valeurs de propriété», à la page 366 «Propriétés LDAP», à la page 348
8. Si des comptes utilisateur de l'Interface graphique Web sont créés dans le serveur ObjectServer par le processus de synchronisation à l'aide du serveur LDAP et que ces utilisateurs doivent accéder aux outils du bureau (tels que le conducteur et la liste d'événements), exécutez les tâches suivantes : • Activez les utilisateurs dans le serveur ObjectServer. • Ajoutez les utilisateurs au groupe Normal pour vous assurer qu'ils disposent des droits suffisants pour afficher et manipuler les alertes dans la liste d'événements, créer des filtres et des vues, et exécuter des outils standard sur des alertes. Pour éditer les informations utilisateur dans l'administrateur Netcool/OMNIbus, ouvrez la fenêtre User Details (Informations utilisateur), cochez la case **User Enabled** (utilisateur activé) sous l'onglet **Settings** (Paramètres), puis utilisez l'onglet **Groups** (Groupes) pour affecter l'utilisateur au groupe Normal. Sinon, dans l'interface interactive SQL, exécutez la commande ALTER USER avec la propriété ENABLED définie sur TRUE, puis exécutez la commande ALTER GROUP avec le paramètre ASSIGN MEMBERS.	Création et édition d'utilisateurs Commande ALTER USER
9. Facultatif : testez la connexion entre le serveur LDAP et le serveur ObjectServer en faisant appel à un utilitaire **ldapsearch**.	La note technique suivante décrit les options permettant d'utiliser **ldapsearch** : http://www-01.ibm.com/support/docview.wss?uid=swg21579907

Tâches associées:

«Synchronisation des utilisateurs LDAP avec le serveur ObjectServer», à la page 510
Une fois que vous avez défini l'annuaire LDAP et affecté des rôles de l'Interface graphique Web aux utilisateurs LDAP, activez la fonction de synchronisation des utilisateurs. Cette fonction crée les utilisateurs LDAP dans le serveur ObjectServer, afin qu'ils puissent utiliser toutes les fonctions qui permettent d'écrire sur le serveur ObjectServer. Ces fonctions incluent la Liste d'événements actifs (AEL) et les outils de l'Interface graphique Web.

«Configuration de l'authentification des utilisateurs», à la page 501
Les utilisateurs peuvent s'authentifier auprès d'un ObjectServer, un référentiel externe, tel qu'un annuaire LDAP, ou le référentiel de fichiers par défaut. Un ObjectServer ou le référentiel de fichiers peut être sélectionné pendant l'installation. Si l'option que vous avez sélectionnée pendant l'installation est la source d'authentification que vous souhaitez utiliser, aucune configuration supplémentaire n'est nécessaire. Si vous souhaitez utiliser LDAP ou modifier la sélection que vous avez effectuée, les étapes sont décrites ici.

Référence associée:

«Exemples LDAP», à la page 352
Le modèle de fichier de propriétés LDAP fourni avec l'Tivoli Netcool/OMNIbus contient des exemples de requête. Vérifiez avec votre administrateur LDAP que les requêtes sont adaptées à votre environnement.

«Erreurs d'authentification LDAP communes», à la page 660
Erreurs d'authentification LDAP communes

Propriétés LDAP

Le fichier de propriétés `$NCHOME/omnibus/etc/ldap.props` vous permet de définir des paramètres de configuration pour se connecter à un référentiel LDAP.

Les propriétés LDAP sont décrites dans le tableau suivant. Vous devez vérifier la valeur de toutes ces propriétés avec l'administrateur LDAP, à l'exception des propriétés **ConfigCryptoAlg**, **ConfigKeyFile** et **SSLKeyStoreLabel**.

Conseil : Vous pouvez chiffrer les valeurs de chaîne dans un fichier de propriétés en utilisant le chiffrement de valeur de propriété.

Tableau 66. Propriétés LDAP

Propriété	Description
ConfigCryptoAlg *chaîne*	Indique l'algorithme de cryptographie à utiliser pour le déchiffrement des valeurs de chaîne (dont les mots de passe) chiffrées à l'aide de l'utilitaire **nco_aes_crypt** et stockées ensuite dans le fichier de propriétés. Définissez la valeur *chaîne* comme suit : • En mode FIPS 140–2, utilisez `AES_FIPS`. • En mode FIPS 140–2 désactivé, vous pouvez utiliser `AES_FIPS` ou `AES`. Utilisez uniquement `AES` si vous devez conserver une compatibilité avec des mots de passe chiffrés à l'aide des outils fournis dans des versions antérieures à Tivoli Netcool/OMNIbus version 7.2.1. La valeur que vous indiquez doit être identique à celle utilisée lors de l'exécution de **nco_aes_crypt** avec le paramètre `-c` pour chiffrer les valeurs de chaîne. Utilisez cette propriété avec la propriété **ConfigKeyFile**.

Tableau 66. Propriétés LDAP (suite)

Propriété	Description
ConfigKeyFile *chaîne*	Indique le chemin et le nom du fichier de clés contenant la clé utilisée pour déchiffrer les valeurs de chaîne chiffrées (dont les mots de passe) dans le fichier de propriétés. La clé est utilisée au moment de l'exécution pour déchiffrer les valeurs de chaîne chiffrées à l'aide de l'utilitaire **nco_aes_crypt**. Le fichier de clés que vous avez spécifié doit être identique au fichier utilisé pour chiffrer les valeurs de chaîne lors de l'exécution de **nco_aes_crypt** avec le paramètre `-k`. Utilisez cette propriété avec la propriété **ConfigCryptoAlg**.

DistinguishedName *chaîne*	Indique le nom distinctif qui identifie l'utilisateur authentifié sur le serveur LDAP cible. Voici un exemple de format présentant certaines des paires type d'attribut/valeur dans le nom distinctif :
	
	`cn=%s,o=`*`chaîne1`*`,ou=`*`chaîne2`*`,dc=`*`chaîne3`*`,l=`*`chaîne4`*`,st=`*`chaîne5`*`,c=`*`chaîne6`*
	
	Où :
	• `cn` est la valeur de nom usuel qui doit être entrée au format `cn=%s`. La variable `%s` est remplacée par le nom d'utilisateur de l'ObjectServer.
	• `o` indique le nom de votre organisation ou de votre société.
	• `ou` indique le nom d'unité organisationnelle ou de service.
	• `dc` indique le composant de domaine.
	• `l` indique la localité ou la ville de votre organisation.
	• `st` spécifie votre état ou votre province.
	• `c` indique le code ISO à deux lettres de votre pays.
	
	Exemples de nom distinctif :
	
	`cn=%s,ou=Development,o=ABCcorp`
	
	`cn=%s,ou=NOC,dc=ABCcorp,dc=com`
	
	`cn=%s,ou=Operators,ou=NOC,l=london,o=ABCcorp`
	
	La valeur par défaut est `cn=%s`.
	
	Les attributs peuvent être en majuscules ou en minuscules, par exemple : `CN` ou `cn`. Au minimum, vous devez indiquer le paramètre de nom usuel (sous la forme `cn=%s`).

Tableau 66. Propriétés LDAP (suite)

Propriété	Description

Hostname *chaîne*	Identifie le nom de l'hôte sur lequel le serveur LDAP s'exécute, et auquel le serveur ObjectServer se connecte. Les valeurs acceptables sont les suivantes :
	• Un seul nom d'hôte.
	• Une liste de noms d'hôtes séparés par des blancs et, facultativement, des numéros de port au format suivant :
	`hôte1[:port1] hôte2[:port2] ...`
	Ce format peut vous être utile pour indiquer une configuration de reprise en ligne. Les tentatives de connexion ont lieu dans l'ordre indiqué pour les noms d'hôte et les numéros de port. Lorsque le serveur ObjectServer parvient à établir une connexion à un serveur LDAP, il reste connecté à ce serveur jusqu'à ce que la connexion ne soit plus nécessaire ou échoue. Si un numéro de port n'est pas indiqué, le numéro de port défini pour la propriété **Port** est utilisé.
	Voici des exemples d'entrées :
	`Hostname: 'serveur1'`
	`Hostname: 'serveur2:1200'`
	`Hostname: 'serveur1:800 serveur2:2000 serveur3'`
	La valeur par défaut est `localhost`.

LDAPBindDn *chaîne*	Indique le nom distinctif du compte utilisateur LDAP utilisé pour l'authentification de la liaison. Cette valeur est utilisée pour établir une connexion permanente au serveur LDAP et pour les opérations d'authentification ultérieures. Si vous n'indiquez aucune valeur pour cette propriété, l'ObjectServer utilise une liaison anonyme avec LDAP. La valeur par défaut est `''`. Utilisez cette propriété avec la propriété **LDAPBindPassword**.
LDAPBindPassword *chaîne*	Indique le mot de passe pour l'authentification de liaison LDAP. La valeur par défaut est `''`. Utilisez cette propriété avec la propriété **LDAPBindDn**.

LDAPSearchBase *chaîne*	Spécifie le nom distinctif de base à partir duquel une recherche LDAP démarre. Par exemple :
	`LDAPSearchBase: "ou=Tivoli,ou=SWG,o=ibm"`
	Pour spécifier que plusieurs noms distinctifs sont recherchés, séparez chaque nom distinctif par deux point-virgule (;;). Par exemple :
	`LDAPSearchBase: "ou=WebGUI,ou=Tivoli,ou=SWG,o=ibm;;ou=OMNIbus,ou=Tivoli, ou=SWG,o=ibm;;ou=ITNM,ou=Tivoli,ou=SWG,o=ibm"`
	Remarque : Si la chaîne de nom distinctif contient des guillemets ("), utilisez un caractère de barre oblique inversée (\) pour les isoler, par exemple `\"`.
	La valeur par défaut est `''`.

Tableau 66. Propriétés LDAP (suite)

Propriété	Description
LDAPSearchFilter *chaîne*	Spécifie un filtre pour une recherche LDAP. Par exemple : `LDAPSearchFilter: "(cn=%s)"` Les conditions suivantes de caractère spécial s'appliquent aux chaînes de filtrage : • Le caractère de pourcentage (%) peut être utilisé une seule fois dans la chaîne de filtrage et uniquement pour spécifier le nom d'utilisateur de Tivoli Netcool/OMNIbus (`%s`). • Utilisez le caractère de barre oblique inversée (\) pour isoler les guillemets (") dans la chaîne de filtrage. Par exemple, \" est envoyé au serveur LDAP sous la forme ". • Utilisez le caractère de barre oblique inversée (\) pour isoler les caractères de barre oblique inversée dans la chaîne de filtrage. Par exemple, \\ est envoyé au serveur LDAP sous la forme \. **Remarque :** Toutes les séquences d'échappement définies dans cette propriété sont appliquées dans Tivoli Netcool/OMNIbus avant que les valeurs ne sont transmises à LDAP. Elles sont séparées des séquences d'échappement qui sont définies dans la spécification de filtre de chaîne LDAP. La valeur par défaut est `cn=%s`.
LDAPTimeout *entier*	Spécifie un délai d'expiration (en secondes) pour des demandes vers le serveur LDAP. Si une demande dépasse la durée spécifiée, une erreur est consignée. La valeur par défaut est `60`.
LDAPVersion *entier*	Indique la version de LDAP exécutée par le serveur. Les valeurs valides sont `2` et `3`. La valeur par défaut est `3`.
Port *entier*	Indique le port d'écoute du serveur LDAP. La valeur par défaut est `389`.
SSLEnabled `TRUE | FALSE`	Détermine si le protocole SSL peut être utilisé pour les connexions au serveur LDAP. La valeur par défaut est `FALSE`. Sous Windows uniquement, si SSL est activé pour les connexions au serveur LDAP, la variable d'environnement suivante doit être définie pour que le serveur ObjectServer démarre avec succès : `GSKIT_LOCAL_INSTALL_MODE=true`
SSLKeyStoreLabel *chaîne*	Indique l'intitulé du certificat serveur du serveur ObjectServer. Ce certificat est conservé dans la base de données de clés de Tivoli Netcool/OMNIbus et peut être présenté au serveur LDAP lorsque l'authentification du client est nécessaire. Si cette propriété n'est pas définie et que le protocole SSL est activé, l'authentification du serveur est utilisée. Cette propriété est uniquement applicable lorsque la propriété **SSLEnabled** est définie sur `TRUE`. La valeur par défaut est `''`.
SSLPort *entier*	Indique le port sur lequel le serveur LDAP écoute les connexions SSL. Cette propriété est uniquement applicable lorsque la propriété **SSLEnabled** est définie sur `TRUE`. La valeur par défaut est `636`.

Pour des informations sur la vérification d'une version et des informations sur les groupes de correctifs pour votre installation de l'Tivoli Netcool/OMNIbus, voir *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.

Tâches associées:

«Gestion des certificats numériques», à la page 401
Exécutez ces tâches dans le cadre de la gestion d'un réseau protégé SSL.

Référence associée:

«Chiffrement des valeurs de propriété», à la page 366
Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

«Exemples LDAP»
Le modèle de fichier de propriétés LDAP fourni avec l'Tivoli Netcool/OMNIbus contient des exemples de requête. Vérifiez avec votre administrateur LDAP que les requêtes sont adaptées à votre environnement.

«Erreurs d'authentification LDAP communes», à la page 660
Erreurs d'authentification LDAP communes

Exemples LDAP

Le modèle de fichier de propriétés LDAP fourni avec l'Tivoli Netcool/OMNIbus contient des exemples de requête. Vérifiez avec votre administrateur LDAP que les requêtes sont adaptées à votre environnement.

Exemple de fichier de propriétés LDAP

Voici un exemple de fichier `ldap.props` configuré pour l'authentification de liaison directe avec la sécurité de liaison et SSL :

```
Hostname: 'testserver.tivlab.austin.ibm.com'
Port: 389
DistinguishedName: 'cn=%s;ou=Webgui,ou=Tivoli,ou=SWG,o=ibm'
LDAPBindDN: 'cn=Authorised User,ou=Webgui,ou=Tivoli,ou=SWG,o=ibm'
LDAPBindPassword: '@67:HYTR8gfROP9uixQaygh5mBT7sJUHYTffYPNX+HuMQ=B'
SSLEnabled: TRUE
SSLPort: 636
SSLKeyStoreLabel: 'LDAP-C'
ConfigCryptoAlg: "AES"
ConfigKeyFile: "/opt/omnibus/netcool/etc/security/keys/key.out"
```

Le groupe de correctifs 2 fournit un exemple de fichier `ldap.props` contenant des exemple mis en commentaire des nouvelles propriétés de recherche LDAP. Si votre fichier de propriétés original (`$NCHOME/omnibus/etc/ldap.props`) n'a pas changé depuis l'installation, il est remplacé par le nouveau fichier de propriétés lorsque vous appliquez le groupe de correctifs.

Si vous avez modifié le fichier de propriétés original depuis l'installation, il n'est pas remplacé par le groupe de correctifs. Dans ce cas, le nouvel exemple de fichier de propriétés est disponible dans le répertoire `$OMNIHOME/etc/default`. Pour utiliser les exemples de configuration, copiez le nouveau fichier de propriétés dans le répertoire `$NCHOME/omnibus/etc/` et éditez-le selon vos besoins.

Authentification sur MS Active Directory sAMAccountName

L'exemple de requête suivant recherche le nom de compte Microsoft Active Directory SAM sur lequel s'authentifier :

```
LDAPSearchFilter: '(
&(objectCategory=person)(objectClass=user)(sAMAccountName=%s))'
```

Cette requête renvoie des résultats où la catégorie d'objet est `person`,la classe d'objets est `user` et l'attribut `sAMAccountName` correspond au nom d'utilisateur de l'ObjectServer.

Restriction de l'accès aux membres des groupes MS Active Directory

Vous pouvez limiter l'accès aux membres d'un groupe Microsoft Active Directory. Par exemple, pour limiter l'accès aux utilisateurs qui sont membres du groupe «OMNIbus Operators» :

1. Exécutez l'utilitaire `dsquery` sur le serveur Windows pour recherchez le nom distinctif du groupe auquel vous souhaitez limiter l'accès. Par exemple :

   ```
   dsquery group -samid "OMNIbus Operators" "CN=OMNIbus
   operators,CN=Users,DC=OMNI3,DC=COM"
   ```

2. Ajoutez la clause suivante au filtre de recherche :

   ```
   (memberOf=CN=OMNIbus Operators,CN=Users,DC=OMNI)
   ```

   Par exemple :

   ```
   LDAPSearchFilter: '(
   &(objectCategory=person)(objectClass=user)(sAMAccountName=
   %s)(memberOf=CN=OMNIbus Operators,CN=Users,DC=OMNI))'
   ```

Pour des informations sur la vérification d'une version et des informations sur les groupes de correctifs pour votre installation de l'Tivoli Netcool/OMNIbus, voir *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.

Tâches associées:

«Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe», à la page 343
Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

Référence associée:

«Propriétés LDAP», à la page 348
Le fichier de propriétés `$NCHOME/omnibus/etc/ldap.props` vous permet de définir des paramètres de configuration pour se connecter à un référentiel LDAP.

Authentification PAM (sous UNIX et Linux)

Le module PAM est une infrastructure préfabriquée de connexion intégrée sous UNIX. Il est utilisé par les composants d'entrée du système, notamment le gestionnaire d'affichage **dtlogin** de l'environnement CDE, pour authentifier les connexions des utilisateurs dans un système UNIX.

Le module PAM peut également être utilisé par les applications le prenant en charge à des fins d'authentification. Parmi ces applications figurent le serveur ObjectServer, l'agent de processus et les passerelles.

Vous pouvez définir une authentification PAM à l'aide de sources d'authentification externes, notamment NIS et LDAP, ou à l'aide d'un seul ObjectServer central.

Restriction : Le module PAM fourni dans l'installation de Tivoli Netcool/OMNIbus *ne prend pas en charge* l'authentification externe auprès d'un système d'authentification tiers. Ce module PAM est uniquement conçu pour être utilisé lors de la configuration d'un seul ObjectServer central en tant que source d'authentification.

Configuration de Tivoli Netcool/OMNIbus pour utiliser PAM pour l'authentification externe

Sous UNIX et Linux, vous pouvez configurer des serveurs ObjectServer, des agents de processus et des passerelles afin d'utiliser une infrastructure PAM avec des modules d'authentification externes, tels que NIS et LDAP.

Avant de commencer

Le module PAM doit être installé, comme décrit dans la documentation du module utilisé.

Important : Différentes versions d'UNIX et de Linux utilisent différentes méthodes pour configurer le module PAM. Il est donc important de vous référer à la documentation de votre système d'exploitation lorsque vous installez et configurez le module PAM en externe.

Pourquoi et quand exécuter cette tâche

Dans votre système d'exploitation, vous devez définir des valeurs de configuration pour les composants (ou services) de Tivoli Netcool/OMNIbus qui requièrent une authentification. Sous UNIX, un seul fichier (`/etc/pam.conf`) est utilisé pour la configuration du module PAM. Sous Linux, chaque règle PAM se trouve généralement dans un fichier de configuration distinct, qui porte le nom du service du composant associé et est stocké dans le répertoire `/etc/pam.d/`. Vous devez créer un fichier de configuration pour chaque service Tivoli Netcool/OMNIbus dans ce répertoire. Si le répertoire `/etc/pam.d/` n'existe pas dans votre système Linux, vous pouvez utiliser le fichier `/etc/pam.conf` à la place.

Pour activer l'authentification externe entre Tivoli Netcool/OMNIbus et le module PAM :

Procédure

1. Linux En supposant que le répertoire `pam.d` existe sur votre système Linux, créez les fichiers de configuration suivants pour les services Tivoli Netcool/OMNIbus. Vous pouvez créer chaque fichier de configuration en copiant `/etc/pam.d/system-auth`.
   - `/etc/pam.d/nco_objserv` : obligatoire pour le serveur ObjectServer.
   - `/etc/pam.d/netcool` : obligatoire pour l'agent de processus.
   - `/etc/pam.d/`*`nom_passerelle`* : obligatoire pour la passerelle, où *nom_passerelle* représente le nom binaire de la passerelle ; par exemple `nco_g_objserv_uni` ou `nco_g_objserv_bi`.
2. Mettez à jour le fichier de configuration du module PAM (`/etc/pam.conf` ou `/etc/pam.d/`*`nom_service`*) avec les entrées suivantes pour Tivoli Netcool/OMNIbus. Si vous utilisez des fichiers de configuration distincts sous Linux, le nom du service est omis dans le fichier de configuration du module PAM.

	Nom du service	**Type de module**
Obligatoire pour le serveur ObjectServer	`nco_objserv`	`auth, account, password`
Obligatoire pour l'agent de processus	`netcool`	`auth`
Obligatoire pour la passerelle	*`nom_passerelle`* (où *nom_passerelle* est le nom binaire)	`auth, account`

   Consultez la documentation du module PAM pour connaître les informations de configuration supplémentaires requises, telles que les indicateurs de contrôle, les chemins d'accès aux modules et les options. Voici un exemple de configuration :

```
service      module_type  control_flag  module_path         options
nco_objserv  auth         required      pam_nom_fichier
```

3. Configurez le serveur ObjectServer pour utiliser l'authentification PAM en définissant la propriété **`Sec.ExternalAuthentication`** du serveur ObjectServer sur `PAM`. Sous UNIX et Linux, la valeur par défaut est `PAM`.

   Lorsque **`Sec.ExternalAuthentication`** est paramétré sur `PAM`, le serveur ObjectServer peut utiliser la méthode d'authentification externe spécifiée dans le fichier de configuration PAM du système pour la gestion de l'authentification et des mots de passe. Toutefois, il n'utilise pas PAM pour l'autorisation. Celle-ci est gérée dans le serveur ObjectServer.
4. Configurez l'agent de processus pour utiliser l'authentification PAM. Lorsque vous exécutez la commande `$NCHOME/omnibus/bin/nco_pad`, définissez l'option de ligne de commande `-authenticate` sur PAM.

   Remarque : Lorsque vous exécutez le démon agent de contrôle de processus (nco_pad) à l'aide de l'authentification du module PAM sous SUSE Linux, la valeur par défaut de la taille de la pile nco_pad doit être augmentée. Pour augmenter la taille de la pile Nco_pad et permettre ainsi de prendre en compte l'authentification du module PAM, exécutez la commande `$NCHOME/omnibus/bin/nco_pad` en indiquant une des options de ligne de commande suivantes :
   - `-stacksize 139248` (sous SUSE Linux version 9.0)
   - `-stacksize 278496` (sous SUSE Linux version 10.0).

5. Configurez la passerelle pour utiliser l'authentification PAM. Pour les passerelles ObjectServer ou d'autres passerelles qui prennent en charge l'authentification PAM, définissez la propriété **Gate.UsePamAuth** sur TRUE.

   Consultez les publications relatives aux passerelles individuelles afin de déterminer les passerelles qui prennent en charge l'authentification PAM. Pour afficher les publications, allez sur le centre de documentation IBM Tivoli Network Management à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp. Développez ensuite le nœud *IBM Tivoli Netcool/OMNIbus* dans le panneau de navigation à gauche et accédez au nœud *Tivoli Netcool/OMNIbus gateways*.
6. Configurez chaque utilisateur Tivoli Netcool/OMNIbus pour l'authentification externe en utilisant une des méthodes suivantes :
   - Dans Netcool/OMNIbus Administrator, créez ou modifiez l'utilisateur en veillant à renseigner les détails suivants dans le panneau User Details (Détails utilisateur) :
     - **Nom d'utilisateur** : entrez un nom d'utilisateur identique à celui stocké dans le référentiel d'authentification externe.
     - **Mot de passe** et **Verify** (Vérifier) : laissez ces zones vides. (Les mots de passe sont stockés dans le référentiel externe.)
     - **External Authentication** (Authentification externe) : cochez cette case.
   - Dans l'interface SQL interactive, utilisez la commande CREATE USER pour créer l'utilisateur ou la commande ALTER USER pour le modifier. Assurez-vous que :
     - Le nom d'utilisateur entré est identique au nom stocké dans le référentiel d'authentification externe.
     - Aucun mot de passe n'est spécifié.
     - Le mot clé PAM est paramétré sur TRUE.

Concepts associés:

«Implémentation d'une autorisation à l'aide de groupes et de rôles», à la page 359
Les droits contrôlent l'accès aux objets et aux données dans le serveur ObjectServer. En regroupant un ou plusieurs droits en *rôles*, vous pouvez gérer les accès rapidement et efficacement.

Référence associée:

«Echec d'authentification d'utilisateur avec les modules PAM», à la page 658
L'authentification auprès d'un système d'authentification PAM externe peut échouer si le serveur ObjectServer, l'agent de processus ou le processus de passerelle ne s'exécute pas en tant que root.

Configuration d'un serveur ObjectServer comme source d'authentification PAM

Pour configurer un serveur ObjectServer afin de contrôler l'authentification PAM, vous devez configurer vos serveurs ObjectServer pour transférer la gestion de l'authentification et des mots de passe à un seul ObjectServer central puis activer l'authentification externe pour chaque ObjectServer et utilisateur de votre système.

Pourquoi et quand exécuter cette tâche

Les modules PAM implémentent l'authentification en utilisant, par exemple, LDAP, NIS ou kerberos. Dans les rares cas où une telle authentification est indisponible ou non requise, il est possible d'utiliser un serveur ObjectServer comme méthode d'authentification des utilisateurs.

Dans cette situation, les agents de processus et le serveur ObjectServer utilisent un autre ObjectServer comme méthode d'authentification des utilisateurs. Les agents de processus ou le premier ObjectServer utilise PAM, configuré pour utiliser le module PAM du serveur ObjectServer, qui se connecte à son tour à l'autre ObjectServer.

Une fois que ces tâches ont été effectuées, le serveur ObjectServer peut être utilisé pour effectuer l'authentification PAM.

Configuration d'un serveur ObjectServer comme source d'authentification centrale

Pour reconnaître un serveur ObjectServer central comme source d'authentification, un module PAM ObjectServer doit être installé sur chaque machine sur laquelle un serveur ObjectServer client est exécuté. Le serveur ObjectServer central doit également être défini dans le fichier de configuration PAM du système ou dans un fichier de configuration PAM ObjectServer.

Pourquoi et quand exécuter cette tâche

Pour installer le module PAM ObjectServer sur chaque ObjectServer client et configurer un serveur ObjectServer central pour l'authentification, procédez comme suit :

Procédure

1. Connectez-vous au système en tant qu'utilisateur `root`.
2. Exécutez le script `$NCHOME/omnibus/bin/nco_install_ospam`.
3. Lorsque vous y êtes invité, entrez le nom du serveur ObjectServer à utiliser comme source d'authentification. Le script **`nco_install_ospam`** :
   a. Installe le module PAM ObjectServer.
   b. Met à jour votre fichier de configuration PAM du système avec les entrées `auth`, `account` et `password` pour l'application **`nco_objserv`**. Ces entrées configurent le serveur ObjectServer pour qu'il utilise le module PAM ObjectServer pour la gestion de l'authentification et des mots de passe. Sur la majorité des plateformes UNIX, le nom du fichier de configuration PAM du système est `/etc/pam.conf`.

      Conseil : Sur les plateformes Linux, chaque règle PAM est conservée dans un fichier de configuration distinct qui porte le nom du service de l'application associée. Par conséquent, le script **`nco_install_ospam`** crée un nouveau fichier, `/etc/pam.d/nco_objserv`, avec les entrées `auth`, `account` et `password`.

      Vous pouvez facultativement ajouter les entrées du serveur ObjectServer dans le fichier de configuration PAM du système.
   c. Crée un fichier de configuration PAM ObjectServer appelé `$NCHOME/omnibus/etc/pam_omnibus_os.conf`. Le serveur ObjectServer spécifié est défini dans ce fichier. Vous pouvez modifier le serveur ObjectServer à utiliser comme source d'authentification à l'aide de ce fichier ou en ajoutant les entrées du serveur ObjectServer dans le fichier de configuration PAM du système.

Modification de vos paramètres du serveur ObjectServer dans le fichier de configuration PAM du système :

Vous pouvez ajouter des arguments aux entrées du module PAM du serveur ObjectServer dans le fichier de configuration PAM du système. Cela inclut la détermination du serveur ObjectServer central à utiliser pour la gestion de l'authentification et des mots de passe.

Remarque : Le fichier de configuration PAM du système doit être modifié par l'utilisateur `root`.

Le tableau suivant répertorie les arguments pouvant être ajoutés aux entrées du module PAM du serveur ObjectServer dans ce fichier.

Tableau 67. Arguments du module PAM du serveur ObjectServer

Argument	Description
`debug`	Si indiqué, les informations de débogage sont écrites dans syslog.
`log_to_stderr`	Si indiqué, les informations sont consignées dans l'erreur standard et non dans syslog.
`no_warn`	Si indiqué, les informations sur le niveau d'avertissement ne sont pas envoyées à l'application demandant la gestion de l'authentification ou des mots de passe.
`server=`*`chaîne`*	Indique le serveur ObjectServer central à utiliser pour la gestion de l'authentification et des mots de passe. Si cet argument n'est pas indiqué, le serveur ObjectServer indiqué dans le fichier de configuration PAM du serveur ObjectServer est utilisé.
`try_first_pass`	Si indiqué, le module PAM du serveur ObjectServer ne demande pas de mot de passe. Il obtient un mot de passe déjà saisi lors de l'empilage des modules PAM. Cet argument peut uniquement être indiqué dans les entrées `auth` et `password`.
`use_first_pass`	Si indiqué, le module PAM du serveur ObjectServer ne demande pas de mot de passe. Il obtient un mot de passe déjà saisi lors de l'empilage des modules PAM. Cet argument peut uniquement être indiqué dans les entrées `auth`.

Remarque : Les arguments indiqués pour le module PAM du serveur ObjectServer dans le fichier de configuration PAM du système écrasent les paramètres du fichier de configuration PAM du serveur ObjectServer.

Référence associée:

«Modification de vos paramètres du serveur ObjectServer dans le fichier de configuration PAM du serveur ObjectServer», à la page 359
Le fichier de configuration PAM du serveur ObjectServer est créé lors de l'installation du module PAM du serveur ObjectServer à l'aide du script **`nco_install_ospam`**.

Modification de vos paramètres du serveur ObjectServer dans le fichier de configuration PAM du serveur ObjectServer :

Le fichier de configuration PAM du serveur ObjectServer est créé lors de l'installation du module PAM du serveur ObjectServer à l'aide du script **nco_install_ospam**.

Le fichier de configuration PAM du serveur ObjectServer a pour nom $NCHOME/omnibus/etc/pam_omnibus_os.conf. Ce fichier définit le serveur ObjectServer central qui est configuré pour gérer l'authentification PAM.

Le tableau suivant décrit les paramètres que vous pouvez modifier dans le fichier pam_omnibus_os.conf.

Tableau 68. Propriétés du fichier de configuration PAM de l'ObjectServer

Propriété	Description
Debug TRUE | FALSE	Si TRUE, les informations de débogage sont écrites dans syslog. La valeur par défaut est FALSE.
LogToStderr TRUE | FALSE	Si TRUE, les informations sont consignées dans l'erreur standard et non dans syslog. La valeur par défaut est FALSE.
Server *chaîne*	Indique le serveur ObjectServer à utiliser pour l'authentification. Cette propriété est à l'origine définie sur le serveur ObjectServer que vous avez indiqué lors de l'exécution du script **nco_install_ospam** pour installer le module PAM du serveur ObjectServer.

Remarque : Les arguments indiqués pour le module PAM du serveur ObjectServer dans le fichier de configuration PAM du système écrasent les paramètres du fichier pam_omnibus_os.conf.

Référence associée:

«Modification de vos paramètres du serveur ObjectServer dans le fichier de configuration PAM du système», à la page 358
Vous pouvez ajouter des arguments aux entrées du module PAM du serveur ObjectServer dans le fichier de configuration PAM du système. Cela inclut la détermination du serveur ObjectServer central à utiliser pour la gestion de l'authentification et des mots de passe.

Implémentation d'une autorisation à l'aide de groupes et de rôles

Les droits contrôlent l'accès aux objets et aux données dans le serveur ObjectServer. En regroupant un ou plusieurs droits en *rôles*, vous pouvez gérer les accès rapidement et efficacement.

Chaque utilisateur est affecté à un ou plusieurs *groupes*. Vous pouvez attribuer des droits à chaque groupe pour exécuter des actions sur les objets de base de données en accordant un ou plusieurs rôles au groupe. Vous pouvez créer des regroupements logiques, notamment les utilisateurs root ou les administrateurs système, des regroupements physiques, notamment les centres d'opérations de réseaux (NOC) de Londres ou de New York, ou tout autre regroupement pour simplifier votre configuration de sécurité.

Par exemple, la création d'automatisations exige de posséder des connaissances sur le fonctionnement de Tivoli Netcool/OMNIbus et la manière dont un serveur

ObjectServer spécifique est configuré. Vous ne souhaitez généralement pas que tous vos utilisateurs puissent créer ou modifier des automatisations. Une solution est de créer un rôle appelé AutoAdmin, disposant de droits pour créer et modifier des groupes de déclencheurs, des fichiers , des procédures SQL et externes, ainsi que des signaux. Vous pouvez ensuite accorder ce rôle à un groupe d'administrateurs qui créera et mettra à jour les automatisations.

Le script `security.sql` contient les groupes et les rôles par défaut de différentes classes d'utilisateurs, notamment des opérateurs et des administrateurs. Vous pouvez également utiliser ce script en tant que modèles pour créer vos propres groupes et rôles.

Les utilisateurs, groupes et rôles peuvent être configurés à l'aide de Netcool/OMNIbus Administrator ou d'instructions SQL pour le serveur ObjectServer. Pour de plus amples informations, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Droits système et objet

Les droits déterminent les types d'actions pouvant être exécutés par les utilisateurs sur le serveur ObjectServer.

Vous attribuez des droits aux rôles à l'aide de la commande GRANT. Il existe deux types de droits :

- Les *droits système*, qui contrôlent les commandes pouvant être exécutées sur le serveur ObjectServer
- Les *droits objet*, qui contrôlent l'accès à des objets individuels comme les tables.

Les droits système incluent la capacité d'utiliser l'interface interactive SQL, de créer une base de données ou de mettre le serveur ObjectServer hors tension. Par exemple :

- Le droit ISQL est obligatoire pour se connecter au serveur ObjectServer à l'aide de l'interface interactive SQL.
- Le droit ISQLWrite est obligatoire pour modifier les données du serveur ObjectServer à l'aide de l'interface interactive SQL.

Les droits objet indiquent les actions que chaque rôle est autorisé à exécuter sur un objet spécifique. Chaque objet est associé à un ensemble d'actions. Par exemple, les actions que vous pouvez exécuter sur une base de données du serveur ObjectServer sont les suivantes :

- DROP
- CREATE TABLE
- CREATE VIEW

Rôles de Tivoli Netcool/OMNIbus par défaut

Lorsque vous exécutez l'utilitaire d'initialisation de la base de données (**nco_dbinit**) pour créer un serveur ObjectServer, un ensemble de rôles par défaut est créé.

Le tableau suivant décrit les rôles par défaut, qui sont définis dans le script `security.sql`.

Tableau 69. Rôles par défaut

Nom du rôle	Description
CatalogUser	Ce rôle comprend des droits d'accès permettant de visualiser des informations sur le système, les outils, la sécurité et les tableaux de la base de données du bureau. Ce rôle offre une base pour les droits d'accès de Tivoli Netcool/OMNIbus. Ce rôle ne fournit pas de droits d'accès suffisants pour utiliser des applications Tivoli Netcool/OMNIbus. Attribuez ce rôle à tous les groupes.
AlertsUser	Ce rôle comprend les droits d'accès suivants : • Afficher, mettre à jour et supprimer des entrées dans la table alerts.status • Afficher, insérer et supprimer des entrées dans la table alerts.journal • Afficher et supprimer des entrées dans la table alerts.details Utilisez ce rôle avec le rôle CatalogUser afin d'afficher et de manipuler des alertes, de créer des filtres et des vues et d'exécuter des outils standard dans la liste d'événements.
AlertsProbe	Ce rôle comprend les droits d'accès permettant d'insérer et de mettre à jour des entrées dans la table alerts.status ainsi que d'insérer des entrées dans la table alerts.details. En association avec le rôle CatalogUser, il fournit les droits d'accès nécessaires à une sonde pour générer des alertes sur le serveur ObjectServer. Accordez ces droits d'accès à tout utilisateur exécutant une application de sonde.

Tableau 69. Rôles par défaut (suite)

Nom du rôle	Description
AlertsGateway	Ce rôle comprend des droits d'accès permettant d'insérer, de mettre à jour et de supprimer des entrées dans les tables alerts.status, alerts.details, alerts.journal, alerts.conversions, alerts.col_visuals, alerts.colors ainsi que dans la table des `outils` du bureau et les tables de la base de données de `transfert`. La base de données de `transfert` est utilisée en interne par la passerelle bidirectionnelle du serveur ObjectServer pour synchroniser les informations de sécurité entre les serveurs ObjectServer. Ce rôle inclut également des droits pour sélectionner, insérer, mettre à jour et supprimer des entrées de la table master.servergroups et des droits pour déclencher les signaux : gw_counterpart_down, gw_counterpart_up, gw_resync_start et gw_resync_finish. Ce rôle, en association avec le rôle CatalogUser, fournit les droits d'accès nécessaires à une passerelle pour générer des alertes sur le serveur ObjectServer. Accordez ces droits d'accès à tout utilisateur exécutant une application passerelle.
DatabaseAdmin	Ce rôle comprend des droits d'accès permettant de créer des bases de données et des fichiers ainsi que des tables dans les bases de données `d'alertes`, `d'outils` et `de service`. Il comprend également des droits d'accès permettant de modifier ou de supprimer les tables alerts.status, alerts.details et alerts.journal ainsi que des droits d'accès permettant de créer et de supprimer des index dans les tables alerts.status, alerts.details et alerts.journal. En association avec le rôle CatalogUser, il fournit les droits d'accès permettant de créer des structures de données relationnelles sur le serveur ObjectServer.
AutoAdmin	Ce rôle comprend les droits d'accès permettant de créer des groupes de déclencheurs, des fichiers, des procédures SQL, des procédures externes et des signaux utilisateur. Il comprend également des droits d'accès permettant de créer, de modifier et de supprimer des déclencheurs dans les groupes de déclencheurs par défaut ainsi que de modifier ou de supprimer les groupes de déclencheurs par défaut. En association avec le rôle CatalogUser, il fournit des droits d'accès permettant de créer des automatisations sur le serveur ObjectServer.
ToolsAdmin	Ce rôle comprend des droits d'accès permettant de supprimer, d'insérer et de mettre à jour toutes les tables d'outils. En association avec le rôle CatalogUser, il fournit des droits d'accès permettant de créer et de modifier les outils pouvant être exécutés depuis le bureau et Netcool/OMNIbus Administrator.

Tableau 69. Rôles par défaut (suite)

Nom du rôle	Description
DesktopAdmin	Ce rôle comprend des droits d'accès permettant de mettre à jour tous les catalogues du bureau afin d'insérer, de mettre à jour et de supprimer des couleurs, des vues, des menus, des classes, des résolutions et des conversions. En association avec le rôle CatalogUser, il fournit des droits d'accès permettant de personnaliser le bureau.
SecurityAdmin	En association avec le rôle CatalogUser, ce rôle comprend des droits d'accès permettant de manipuler des utilisateurs, des groupes et des rôles à l'aide de Netcool/OMNIbus Administrator ou de l'interface interactive SQL. Ce rôle comprend également des droits d'accès permettant de définir et de supprimer des connexions utilisateur.
ISQL	En association avec le rôle CatalogUser, ce rôle comprend des droits d'accès permettant de visualiser les données du serveur ObjectServer à l'aide de l'interface interactive SQL.
ISQLWrite	En association avec le rôle CatalogUser, ce rôle comprend des droits d'accès permettant de visualiser et de modifier les données du serveur ObjectServer à l'aide de l'interface interactive SQL.
SuperUser	Ce rôle dispose de tous les droits d'accès disponibles. Vous ne pouvez pas modifier le rôle SuperUser.
Public	Ce rôle est affecté à tous les utilisateurs. Par défaut, aucun droit d'accès n'est affecté au rôle Public. Vous pouvez le modifier mais pas le supprimer.
ChannelAdmin	Ce rôle comprend des droits d'accès permettant de définir des canaux pour une notification d'événement accéléré.
ChannelUser	Ce rôle comprend des droits d'accès permettant de recevoir des notifications d'événements accélérés et d'agir sur celles qui sont diffusées via les canaux.
RegisterProbe	Ce rôle inclut des droits d'accès permettant d'ajouter et de mettre à jour des entrées dans la table registry.probes. Il doit être attribué à tous les comptes utilisateur de sonde.
RegistryReader	Ce rôle inclut des droits d'accès permettant de visualiser des données dans la table registry.probes. Ce rôle n'inclut pas de droit pour modifier des données dans la table registry.probes.
RegistryAdmin	Ce rôle inclut des droits d'accès pour visualiser, modifier, ajouter et supprimer des données dans la table registry.probes. Ce rôle s'adresse uniquement aux administrateurs système et leur permet de résoudre des problèmes inattendus liés à l'enregistrement des sondes.

Groupes de Tivoli Netcool/OMNIbus par défaut

Lorsque vous exécutez l'utilitaire d'initialisation de la base de données (**nco_dbinit**) pour créer un serveur ObjectServer, un ensemble de groupes par défaut est créé.

Le tableau suivant décrit les groupes par défaut pour les opérateurs et administrateurs de Network Management, qui sont définis dans le script `security.sql`.

Tableau 70. Groupes par défaut

Nom du groupe	Description
Sonde	Les rôles CatalogUser, AlertsUser, AlertsProbe et RegisterProbe sont affectés à ce groupe.
Passerelle	Les rôles CatalogUser, AlertsUser, AlertsGateway et RegistryAdmin sont affectés à ce groupe.
ISQL	Le rôle ISQL est affecté à ce groupe.
ISQLWrite	Le rôle ISQLWrite est affecté à ce groupe.
Public	Le rôle Public est affecté à ce groupe. Tous les utilisateurs sont membres de ce groupe.
Normal	Les rôles CatalogUser, AlertsUser, ChannelUser et RegistryReader sont affectés à ce groupe. Ce groupe ne peut pas être supprimé ou renommé.
Administrateur	Les rôles CatalogUser, AlertsUser, ToolsAdmin, DesktopAdmin, ChannelUser, ChannelAdmin, RegistryAdmin et OSLCAdmin sont affectés à ce groupe. Ce groupe ne peut pas être supprimé ou renommé.
Système	Les rôles CatalogUser, AlertsUser, ToolsAdmin, DesktopAdmin, AlertsProbe, AlertsGateway, DatabaseAdmin, AutoAdmin, SecurityAdmin, ISQL, ISQLWrite, SuperUser, ChannelUser, ChannelAdmin, OSLCAdmin et RegistryAdmin sont affectés à ce groupe. Ce groupe ne peut pas être supprimé ou renommé.

Utilisation des groupes pour la sécurité de niveau ligne dans la liste d'événements

Les groupes Normal, Administrateur et Système fournissent aux groupes une sécurité de niveau ligne dans la liste d'événements. Ces groupes ne peuvent pas être supprimés ou renommés.

La propriété du serveur OBjectServer **AlertSecurityModel** détermine si la sécurité de niveau ligne du groupe est activée dans la liste d'événements. Par défaut, **AlertSecurityModel** est désactivé. Dans ce cas :

- Les membres du groupe Normal peuvent modifier une ligne qui leur est attribuée ou à l'utilisateur `nobody`.
- Les membres du groupe Administrateur peuvent modifier une ligne qui leur est attribuée, à l'utilisateur `nobody` ou à un membre du groupe Normal.

Si la propriété **AlertSecurityModel** est activée, seuls les utilisateurs du groupe qui possède la ligne peuvent la modifier. Dans ce cas, un membre du groupe Normal ou Administrateur peut modifier une ligne qui est attribuée à un groupe auquel il appartient.

Un membre du groupe Système peut toujours modifier n'importe quelle ligne.

Utilisateurs de Tivoli Netcool/OMNIbus par défaut

Lorsque vous exécutez l'utilitaire d'initialisation de la base de données (**nco_dbinit**) pour créer un serveur ObjectServer, un ensemble d'utilisateurs par défaut est créé.

Le tableau suivant décrit les utilisateurs par défaut, qui sont définis dans le script `security.sql`.

Tableau 71. Utilisateurs par défaut

Nom d'utilisateur	Description
root	Cet utilisateur est créé avec une chaîne vide comme mot de passe par défaut. Vous pouvez redéfinir le mot de passe à l'aide de Netcool/OMNIbus Administrator ou de la commande SQL du serveur ObjectServer ALTER USER.
nobody	Cet utilisateur est désactivé et ne peut pas être utilisé pour accéder au serveur ObjectServer. La propriété de chaque alerte dans la table alerts.status est affectée à un utilisateur lorsque la ligne est insérée. Par défaut, les sondes affectent des lignes à l'utilisateur `nobody`.

Les droits attribués aux utilisateurs par défaut sont présentés dans le tableau suivant.

Tableau 72. Droits des utilisateurs par défaut

Droit	Utilisateur root	Utilisateur nobody
Set enable or disable	Non	Non
Set full name	Oui	Non
Set password	Oui	Non
Set PAM	Oui	Non
Assign or remove restriction filter	Oui	Oui Notez,cependant, que vous ne pouvez pas vous connecter en tant qu'utilisateur `nobody`.
Drop user	Non	Non
Grant or revoke permission	Non	Non
Be a member of a group	Oui	Oui

Utilisation de filtres de restriction pour filtrer les informations de table

Un filtre de restriction est une façon de limiter les lignes qui s'affichent lorsqu'un utilisateur consulte des données tabulaires. Lorsque le filtre est attribué à un utilisateur ou à un groupe, le filtre contrôle les données qui s'affichent et qui sont modifiées à partir d'applications client et modifiées dans des commandes SQL.

Seules les lignes qui satisfont aux critères indiqués dans la condition de filtre sont renvoyées.

Définition et suivi d'une trace de contrôle

Lors vous sécurisez des applications, il est important de surveiller ou d'effectuer un audit de l'efficacité de votre sécurité. Pour ce faire, vous pouvez configurer le système de sorte à consigner certains types de messages. Vous pouvez ensuite surveiller les journaux pour voir si un événement intéressant ou préoccupant s'est produit.

Pour configurer les journaux d'audit de l'utilisateur, utilisez les propriétés ou les options de ligne de commande du serveur ObjectServer décrites dans le tableau suivant.

Tableau 73. Contrôle des propriétés et des options de ligne de commande de l'ObjectServer

Propriété	Option de ligne de commande	Description
Sec.AuditLog *chaîne*	`-secauditlog` *chaîne*	Indique le fichier dans lequel les informations de contrôle sont écrites. La valeur par défaut est `$NCHOME/omnibus/log/`*nom de serveur*`/audit.log`.
Sec.AuditLevel *chaîne*	`-secauditlevel` *chaîne*	Indique le niveau de contrôle de sécurité effectué. Les valeurs possibles sont `debug`, `info`, `warn` et `error`. La valeur par défaut est `warn`. Les niveaux `debug` et `info` génèrent des messages pour les échecs et les réussites d'authentification, alors que les niveaux `warn` et `error` génèrent des messages pour les échecs d'authentification uniquement.

Dans le cadre de votre processus de sécurité, consultez vos journaux fréquemment.

Chiffrement des valeurs de propriété

Vous pouvez utiliser le chiffrement des valeurs de propriété pour chiffrer les valeurs de chaîne d'un fichier de propriétés ou d'un fichier de configuration afin que les chaînes ne puissent être lues sans une clé. Au démarrage du processus utilisant le fichier de propriétés ou le fichier de configuration, les chaînes sont déchiffrées.

Vous pouvez utiliser le mécanisme de chiffrement dans les fichiers de propriétés du serveur ObjectServer, du serveur proxy, de la commande **nco_postmsg**, du protocole LDAP, de la sonde et des passerelles. Vous pouvez également utiliser ce mécanisme pour coder les mots de passe qui sont stockés dans les fichiers de configuration d'agent de processus.

Le mécanisme de chiffrement de valeur de propriété utilise la norme AES (Advanced Encryption Standard), qui prend en charge les clés de 128, 192 et 256 bits, un générateur de clé de ligne de commande (**nco_keygen**) et un utilitaire de chiffrement (**nco_aes_crypt**). Les algorithmes de cryptographie sont également disponibles en modes FIPS 140–2 et non-FIPS 140–2. La procédure est la suivante :

1. Générez une clé et stockez-la dans un fichier de clé en exécutant l'utilitaire **nco_keygen**.

2. Dans la valeur de la propriété **ConfigKeyFile**, définissez le chemin d'accès au fichier et le nom du fichier de clé que l'utilitaire **nco_keygen** génère. Cette étape ne s'applique pas si vous chiffrez des mots de passe dans le fichier de configuration d'agent de processus.
3. Chiffrez une valeur de chaîne avec la clé en exécutant l'utilitaire **nco_aes_crypt**.
4. Ajoutez la valeur de chaîne chiffrée dans un fichier de propriétés.

Référence associée:

«Basculement de votre installation vers le mode FIPS 140-2», à la page 289
Si vous souhaitez changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2, suivez les étapes décrites dans la liste de contrôle de la configuration de FIPS 140-2.

Génération d'une clé dans un fichier de clés

Exécutez l'utilitaire **nco_keygen** pour générer une clé dans un fichier de clés. Les options de ligne de commande sont disponibles pour spécifier une valeur hexadécimale pour la clé ou une longueur en octets pour la génération automatique de clé.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer une clé unique utilisée par tous les fichiers de propriétés ou créer une clé pour chaque fichier de propriétés.

Pour générer une clé dans un fichier de clés, procédez comme suit :

Procédure

Exécutez **nco_keygen** comme suit. Les entrées facultatives sont présentées entre crochets.
`$NCHOME/omnibus/bin/nco_keygen -o fichier_clés [-l longueur | -k clé]`
Dans cette commande :

- *fichier_clés* représente le chemin du fichier de sortie et le nom du fichier dans lequel la clé est enregistrée.
- *longueur* représente la longueur de la clé (en octets), telle que vous l'avez spécifiée. Ce nombre doit être divisible par 8 pour pouvoir obtenir un nombre entier d'octets. La valeur par défaut est 128. Seules les longueurs de clé 128, 192 et 256 sont valides pour le chiffrement AES.
- *clé* représente la valeur de la clé en chiffres hexadécimaux, telle que vous l'avez spécifiée.

  Vous pouvez utiliser les options de ligne de commande `-l` ou `-k`, mais pas les deux.

  Si vous utilisez l'option de ligne de commande `-o` pour spécifier un nom de fichier de sortie, et que vous ne sélectionnez ni l'option `-l` ni l'option `-k`, une clé de 128 octets générée de façon aléatoire est enregistrée dans le fichier.

Résultats

L'utilitaire **nco_keygen** enregistre la clé dans le fichier, en utilisant le format *longueur:clé*, où *longueur* correspond au nombre d'octets de la clé (représenté sous forme de nombres décimaux ASCII) et *clé* correspond aux données de la clé.

La clé peut être utilisée pour chiffrer et déchiffrer des données. Pour le déchiffrement, le fichier de clés doit être accessible au processus qui déchiffre les

données. L'accès au fichier de clés peut être contrôlé par les droits UNIX ou Windows ou par d'autres moyens, bien que non couverts par un schéma ou des outils Tivoli Netcool/OMNIbus.

Spécification du fichier de clés comme propriété

Dans le fichier de propriétés dans lequel vous souhaitez spécifier une valeur de chaîne chiffrée, attribuez le chemin et le nom du fichier de clés généré par l'utilitaire **nco_keygen** à la propriété **ConfigKeyFile**.

Pourquoi et quand exécuter cette tâche

Vous devez définir la propriété **ConfigKeyFile** dans les fichiers suivants :

- Fichiers de propriétés ObjectServer : `$NCHOME/omnibus/etc/nom_serveur.props`
- Fichiers de propriétés du serveur proxy : `$NCHOME/omnibus/etc/serveur_proxy.props`
- Fichier de propriétés **nco_postmsg** : `$NCHOME/omnibus/etc/nco_postmsg.props`
- Fichier de propriétés LDAP : `$NCHOME/omnibus/etc/ldap.props`
- Fichiers de propriétés de sonde : `$OMNIHOME/probes/archive/nom_sonde.props` où *archive* représente le répertoire du système d'exploitation
- Fichiers de propriétés de passerelle : `$OMNIHOME/etc/nom_passerelle.props`

Conseil : Ce paramètre de propriété est obligatoire pour permettre à la clé de déchiffrer les chaînes chiffrées du fichier de propriétés lors de la phase d'exécution.

Lors de l'exécution du démon d'agent de processus **nco_pad**, vous pouvez utiliser l'option de ligne de commande `-keyfile` afin de spécifier le chemin et le nom du fichier de clés.

Chiffrement d'une valeur de chaîne avec la clé

Utilisez **nco_aes_crypt** pour chiffrer une valeur de chaîne avec la clé générée par l'utilitaire **nco_keygen**.

Pourquoi et quand exécuter cette tâche

Pour chiffrer une valeur de chaîne, procédez comme suit :

Procédure

Exécutez **nco_aes_crypt** comme suit :
`$NCHOME/omnibus/bin/nco_aes_crypt -c chiffrement -k fichier_clés valeur_chaîne`
Dans cette commande :

- *chiffrement* correspond à l'algorithme utilisé pour chiffrer la valeur de chaîne. Indiquez l'une des valeurs suivantes pour *chiffrement*, selon le mode de fonctionnement :
  - Mode FIPS 140–2 : indiquez `AES_FIPS`.
  - Mode Non-FIPS 140–2 : indiquez `AES_FIPS` ou `AES`. Utilisez `AES` (valeur par défaut) uniquement si vous souhaiter maintenir la compatibilité avec les mots de passe codés à l'aide des outils fournis dans les versions antérieures à Tivoli Netcool/OMNIbus version 7.2.1.

- *fichier_clés* est le chemin et le nom du fichier de clés. Cette valeur doit correspondre à celle spécifiée pour la propriété **ConfigKeyFile** du fichier de propriétés.
- *chaîne_valeur* est la valeur de chaîne que vous souhaitez chiffrer.

  Restriction : En raison de l'ordre de démarrage, la propriété **MessageLevel** ne peut pas être chiffrée.

Résultats

La sortie est affichée dans la fenêtre de la console dans un format chiffré et est délimitée par des symboles @. Vous pouvez désormais copier le texte de sortie, y compris les symboles @, à utiliser dans les fichiers de propriétés concernés.

Conseil : L'utilitaire **nco_aes_crypt** comporte des options de ligne de commande supplémentaires que vous pouvez utiliser pour :

- chiffrer le contenu du fichier au lieu d'une valeur de chaîne.
- envoyer une sortie chiffrée à un fichier au lieu de la fenêtre de console.
- déchiffrer manuellement les valeurs chiffrées.

Référence associée:

«Options de ligne de commande nco_aes_crypt», à la page 370
Vous pouvez utiliser l'utilitaire **nco_aes_crypt** pour chiffrer et déchiffrer les valeurs de chaîne ou les données contenues dans un fichier.

Ajout d'une valeur chiffrée à un fichier de propriétés

Après avoir chiffré une valeur de chaîne, ajoutez-la au fichier de propriétés dans lequel vous souhaitez masquer la valeur réelle.

Pourquoi et quand exécuter cette tâche

Pour ajouter une valeur chiffrée à un fichier de propriétés, procédez comme suit :

Procédure

1. Ouvrez le fichier de propriétés à éditer.
2. Spécifiez (ou collez) la valeur de chaîne chiffrée, y compris les symboles délimiteurs @, comme paramètre de la propriété correspondante. Par exemple :

   ```
   Gate.ObjectServerA.Password : '@44:Kris2m3QLsy+dZYNt3/
   jptl8cd7c6Fmboaj+E6XrNw8=@'
   ```
3. Attribuez l'algorithme de cryptographie à utiliser lors du déchiffrement de la chaîne à la propriété **ConfigCryptoAlg** (AES_FIPS, par exemple). Cette valeur doit correspondre à celle spécifiée lorsque vous avez exécuté **nco_aes_crypt** avec le paramètre `-c` pour chiffrer la valeur de chaîne.

   La propriété **ConfigCryptoAlg** est exécutée conjointement avec la propriété **ConfigKeyFile** afin de déchiffrer la valeur de chaîne, le cas échéant.

Options de ligne de commande nco_aes_crypt

Vous pouvez utiliser l'utilitaire **nco_aes_crypt** pour chiffrer et déchiffrer les valeurs de chaîne ou les données contenues dans un fichier.

L'utilitaire **nco_aes_crypt** se trouve dans le répertoire `$NCHOME/omnibus/bin` et nécessite un fichier clé qui peut être généré via l'utilitaire **nco_keygen**.

La syntaxe de l'utilitaire **nco_aes_crypt** est la suivante (les valeurs facultatives sont indiquées entre crochets) :

```
nco_aes_crypt [-d] [-o chaîne] [-c chaîne] -k chaîne -f filename
nco_aes_crypt [-d] [-o chaîne] [-c chaîne] -k chaîne données
```

Les options de ligne de commande sont décrites dans le tableau suivant.

Tableau 74. options de ligne de commande nco_aes_crypt

Option de ligne de commande (ou valeur)	Description
`-d`	Définit le mode dans lequel l'utilitaire s'exécute pour déchiffrer le mode. La valeur par défaut est le mode de chiffrement. Cette option de ligne de commande n'est pas prise en charge par Windows.
`-o` *chaîne*	Indique le fichier de sortie dans lequel les données chiffrées sont écrites.
`-c` *chaîne*	Indique l'algorithme cryptographique à utiliser pour le chiffrement ou le déchiffrement. Les valeurs sont les suivantes : • `AES_FIPS` : utilisez cette valeur en mode FIPS 140–2. • `AES` : utilisez cette valeur uniquement pour gérer la compatibilité avec le chiffrement de propriété AES qui était disponible dans Tivoli Netcool/OMNIbus version 7.2. Cela ne s'applique qu'au mode non-FIPS 140–2.
`-k` *chaîne*	Indique le chemin et le nom du fichier contenant la clé qui chiffre ou déchiffre les données.
`-f` *chaîne*	Indique le chemin et le nom d'un fichier contenant des données à chiffrer ou déchiffrer.
données	Indique une valeur de chaîne à chiffrer ou déchiffrer.

Tâches associées:

«Génération d'une clé dans un fichier de clés», à la page 367
Exécutez l'utilitaire **nco_keygen** pour générer une clé dans un fichier de clés. Les options de ligne de commande sont disponibles pour spécifier une valeur hexadécimale pour la clé ou une longueur en octets pour la génération automatique de clé.

Référence associée:

«Basculement de votre installation vers le mode FIPS 140-2», à la page 289
Si vous souhaitez changer votre installation de la version 8.1 pour qu'elle s'exécute en mode FIPS 140-2, suivez les étapes décrites dans la liste de contrôle de la configuration de FIPS 140-2.

Chapitre 14. Utilisation du protocole SSL pour les communications serveur et client

Tivoli Netcool/OMNIbus prend en charge l'utilisation du protocole SSL pour la communication entre ses serveurs et ses clients.

SSL utilise des certificats numériques pour l'échange et l'authentification de clés. Lorsqu'un client initie une connexion SSL, le serveur présente au client un certificat signé par une autorité de certification. Une autorité de certification est une partie certifiée qui garantit l'identité du certificat et de son créateur. Le certificat serveur contient l'identité du serveur, la clé publique et la signature numérique de l'émetteur du certificat.

En lisant le certificat serveur, le client peut déterminer si le serveur est une source certifiée et accepter ou rejeter la connexion. Pour vérifier la signature sur le certificat serveur, le client a besoin de la clé publique de l'autorité de certification émettrice. Etant donné que les clés publiques sont distribuées dans les certificats, le client doit posséder un certificat pour l'autorité de certification émettrice. Ce certificat doit être signé par l'autorité de certification.

Les certificats serveur peuvent être généré pour des serveurs ObjectServer, des agents de processus, des serveurs proxy et des sondes à l'écoute sur des ports de commande bidirectionnels.

Les certificats ont deux objectifs :

- Ils fournissent une preuve authentifiée à un client que le serveur auquel il se connecte appartient à la société ou à l'individu qui a installé le certificat.
- Ils contiennent la clé publique que le client utilise pour établir une connexion cryptée avec le serveur.

En mode FIPS 140-2, toutes les fonctions de chiffrement et de génération de clés nécessaires pour les connexions SSL sécurisées sont fournies par les fournisseurs cryptographiques approuvés par la norme FIPS 140-2.

Pour configurer la communication SSL, vous devez exécuter les tâches suivantes :

1. Créez des entrées pour les connexions SSL dans l'éditeur de serveur.
2. Si vous êtes en mode FIPS 140–2, configurez les propriétés cryptographiques pour le chiffrement et la génération de clés.
3. Créez et distribuez des certificats et des clés aux serveurs et clients à l'aide de l'utilitaire graphique IBM Key Management (iKeyman) ou de l'utilitaire **nc_gskcmd**. Pour le mode FIPS 140-2, faites appel à l'utilitaire **nc_gskcmd**.

Concepts associés:

Chapitre 13, «Sécurité des accès utilisateur dans Tivoli Netcool/OMNIbus», à la page 337
Tivoli Netcool/OMNIbus offre des mécanismes de *sécurité des accès utilisateur* pour protéger votre système Tivoli Netcool/OMNIbus de dommages accidentels ou délibérés causés par les utilisateurs ou des utilisateurs potentiels de votre système.

Instructions de configuration de SSL rapide

Si vous êtes déjà habitué à utiliser la communication SSL dans Tivoli Netcool/OMNIbus, utilisez ces informations comme des instructions rapides relatives aux tâches que vous devez exécuter.

1. Avant de configurer un réseau protégé SSL

Pour configurer des communications SSL, créez des entrées pour SSL dans l'éditeur de serveur, définissez ces entrées dans le fichier de connexions de donnéesomni.dat, puis créez (et distribuez) le fichier d'interfaces.

```
[NCOMS]
{
 Primary: nocturama 3000 ssl 3500
}
```

Pour plus d'informations, voir «Configuration des informations de communication du serveur», à la page 209, «Utilisation de l'éditeur de serveur pour configurer SSL sous UNIX», à la page 375 et «Génération du fichier d'interfaces pour plusieurs plateformes (UNIX uniquement)», à la page 219.

2. Créer des bases de données de clés

Sur chaque ordinateur sur lequel un composant serveur (ObjectServer, agent de processus ou serveur proxy) est installé, créez une base de données de clés pour stocker les certificats numériques. Créez également une base de données de clés sur chaque ordinateur à partir duquel les clients se connectent au serveur à l'aide d'un port SSL. Utilisez un fichier de la base de données de clés dédié (omni.kdb) pour chaque installation Tivoli Netcool/OMNIbus sur un serveur ou un ordinateur client. L'exemple suivant montre comment créer une base de données de clés à l'aide de l'utilitaire **nc_gskcmd**.

```
$NCHOME/bin/nc_gskcmd -keydb -create -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-stash -expire 366
```

Pour plus d'informations, voir «Création d'une base de données de clés», à la page 381.

3. Créer des certificats autosignés

Si vous souhaitez configurer un réseau de certification privé dans lequel vous agissez comme autorité de certification émettrice pour vos certificats serveur, créez un certificat autosigné dans la base de données de clés de chaque ordinateur serveur. L'exemple suivant montre comment utiliser l'utilitaire **nc_gskcmd** pour créer un certificat autosigné.

```
$NCHOME/bin/nc_gskcmd -cert -create -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "NCOMS_CA" -size 1024 -ca true
-dn "CN=NCOMS_CA,O=IBM,OU=Support,L=SouthBank,ST=London,C=GB"
-expire 366 -x509version 3
```

Pour plus d'informations, voir «Création d'un certificat autosigné», à la page 385.

4. Distribuer les certificats

Pour utiliser un certificat autosigné en tant que certificat de signataire, distribuez le certificat autosigné à tous les clients en *récupérant* le certificat à partir de la base de

données de clés du serveur et en *ajoutant* le certificat récupéré à la base de données de clés sur chaque ordinateur client. L'exemple suivant montre comment extraire un certificat.

```
$NCHOME/bin/nc_gskcmd -cert -extract -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "NCOMS" -target "$NCHOME/etc/security/keys/ncomscert.arm"
```

L'exemple suivant montre comment ajouter un certificat.

```
$NCHOME/bin/nc_gskcmd -cert -add -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "NCOMS" -file "ncomscert.arm"
```

Pour plus d'informations, voir «Extraction des certificats d'une base de données de clés», à la page 397 et «Ajout de certificats d'autorités de certification», à la page 399.

5. Demander et envoyer les certificats

A partir de chaque ordinateur serveur, créez une demande de certificat numérique pour le serveur, et envoyez la demande de certificat à une autorité de certification certifiée à des fins d'autorisation. L'autorité de certification autorise la demande de certificat et utilise le certificat racine autosigné pour générer un certificat serveur. Elle renvoie ensuite le certificat serveur signé. L'exemple ci-dessous montre comment demander un certificat.

```
$NCHOME/bin/nc_gskcmd -certreq -create -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "PSERV" -size 1024
-dn "CN=NCOMS,O=IBM,OU=Support,L=SouthBank,ST=London,C=GB"
-file "$NCHOME/etc/security/keys/pservreq.arm"
```

Pour plus d'informations, voir «Demande de certificat serveur auprès d'une autorité de certification», à la page 388.

6. Recevoir les certificats

A la réception du certificat serveur provenant de l'autorité de certification émettrice, réceptionnez le certificat dans la base de données de clés du serveur. Le certificat serveur est utilisé pour authentifier le côté serveur des communications Tivoli Netcool/OMNIbus lorsqu'un client demande une connexion sécurisée. L'exemple suivant montre comment recevoir un certificat.

```
$NCHOME/bin/nc_gskcmd -cert -receive -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-file "$NCHOME/etc/security/keys/pservcert.arm"
```

Pour plus d'informations, voir «Réception de certificats de serveur d'autorités de certification», à la page 395.

7. Spécifier des noms usuels

Spécifiez des noms usuels acceptables pour des passerelles unidirectionnelles et bidirectionnelles et pour des analyses. Les exemples suivants montrent des modèles de configurations.

Exemple de configuration d'un paire de reprise en ligne pour une passerelle unidirectionnelle de serveur ObjectServer :

```
Gate.Reader.Server:   'PSERV'
Gate.Reader.CommonNames:  'NCOMS'
Gate.Writer.Server:   'BSERV'
Gate.Writer.CommonNames:  'NCOMS'
```

Utilisation de la propriété **SSLServerCommonName** pour spécifier des noms usuels SSL acceptables :

```
SSLServerCommonName:   'NCOMS'
```

Pour plus d'informations, voir «Configuration de la SSL pour les installations distribuées», à la page 378.

8. Configurer une connexion SSL entre Concentrateur des services d'application du tableau de bord et le référentiel d'utilisateurs

Configurez une connexion entre Concentrateur des services d'application du tableau de bord et le référentiel d'utilisateurs que vous avez défini dans le domaine. Ce référentiel peut être un annuaire LDAP ou un serveur ObjectServer. La configuration varie selon votre référentiel d'utilisateurs.

Pour plus d'informations, voir «Configuration d'une connexion SSL sur un serveur LDAP», à la page 522 et «Configuration d'une connexion SSL au serveur ObjectServer», à la page 523.

9. Configurer SSL pour le flux d'événements vers l'Interface graphique Web

Créez une connexion sécurisée entre l'Interface graphique Web et le serveur ObjectServer, de sorte que le flux de données d'événement dans l'Interface graphique Web soit protégé par SSL.

Pour plus d'informations, voir «Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer», à la page 525.

10. Remplacez le certificat par défaut pour les clients de l'Interface graphique Web

Concentrateur des services d'application du tableau de bord contient un certificat à utiliser pour l'authentification des connexions SSL aux clients de l'Interface graphique Webs. Vous pouvez remplacer ce certificat par l'un des vôtres, par un certificat créé par une autorité de certification ou par un certificat autosigné.

Pour plus d'informations, voir «Remplacement du certificat SSL par défaut pour les connexions aux clients d'interface graphique Web», à la page 527.

Tâches associées:

«Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer», à la page 525
Utilisez une connexion Secure Socket Layer (SSL) pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers l'Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez SSL dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

«Configuration d'une connexion SSL au serveur ObjectServer», à la page 523
Pour les environnements intégrant un registre d'utilisateurs Tivoli Netcool/OMNIbus ObjectServer, vous devez configurer des communications chiffrées sur le Jazz for Service Management.

«Configuration des connexions SSL en mode FIPS 140–2 pour le flux d'événements à partir du serveur ObjectServer», à la page 538
Pour plus de sécurité, utilisez une connexion Secure Socket Layer (SSL) avec le chiffrement FIPS 140-2 pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez le chiffrement FIPS 140-2 dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

Configuration des communications SSL

Pour configurer des communications SSL, créez des entrées pour SSL dans l'éditeur de serveur, modifiez le fichier de connexions de données`omni.dat`, puis créez (et distribuez) le fichier d'interfaces.

Utilisation de l'éditeur de serveur pour configurer SSL sous UNIX

Dans l'éditeur de serveur UNIX, vous pouvez activer des connexions cryptées et/ou non cryptées.

Sur l'ordinateur hôte du serveur, procédez comme suit :

- Vous pouvez définir le port non chiffré et laisser le port SSL non défini (ou le définir sur `0`). Dans ce cas, seules les connexions non cryptées sont autorisées.
- Vous pouvez définir le port SSL et laisser le port non chiffré non défini (ou le définir sur `0`). Dans ce cas, seules les connexions cryptées sont autorisées.
- Vous pouvez définir un port non chiffré et un port SSL. Dans ce cas, les connexions cryptées et non cryptées sont autorisées. Des pare-feux peuvent être configurés pour permettre l'accès aux ports adéquats à partir d'autres systèmes.

  Remarque : Si le serveur autorise les connexions cryptées et non cryptées, les clients qui utilisent le même fichier d'interfaces que le serveur (y compris les clients locaux) se connectent à l'aide du port non chiffré. Si vous souhaitez utiliser le port SSL pour vous connecter à ces ordinateurs, n'indiquez pas de port non chiffré pour le serveur.

Sur chaque ordinateur client, procédez comme suit :

- Si vous souhaitez que le client se connecte au serveur à partir de cet ordinateur sans utiliser de chiffrement, créez une entrée qui indique l'hôte du serveur, le nom de serveur et le port non chiffré.
- Si vous souhaitez que le client se connecte au serveur à partir de cet ordinateur en utilisant le chiffrement, créez une entrée qui indique l'hôte du serveur, le nom de serveur et le port SSL. Pour cette entrée, le nom de serveur que vous indiquez *doit* être identique au nom usuel qui est indiqué pour le serveur lors de la création et de l'autorisation d'une demande de certificat.

  Remarque : Si vous créez des entrées pour une connexion SSL et une connexion non cryptée sur le même ordinateur client pour le même serveur, utilisez le nom usuel de l'entrée SSL (comme indiqué lors de la création d'une demande de certificat) et un nom alternatif pour l'entrée non chiffrée.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

Utilisation de l'éditeur de serveur pour configurer SSL sous Windows

Dans l'éditeur de serveur Windows, vous pouvez activer des connexions cryptées et/ou non cryptées.

Sur l'ordinateur hébergeant le serveur, procédez comme suit :

- Si vous souhaitez que le serveur autorise les connexions cryptées de clients, créez une entrée Listener (Programme d'écoute) en cochant la case **Listener (Programme d'écoute)** et cochez également la case **SSL**.
- Si vous souhaitez que le serveur autorise les connexions non cryptées de clients, créez une entrée Listener (Programme d'écoute) en cochant la case **Listener (Programme d'écoute)** et cochez également la case **SSL**.

Sur chaque ordinateur client, procédez comme suit :

- Si vous souhaitez que le client se connecte au serveur à partir de cet ordinateur sans utiliser de chiffrement, décochez la case **SSL**.
- Si vous souhaitez que le client se connecte au serveur à partir de cet ordinateur en utilisant le chiffrement, cochez la case **SSL**.

  Remarque : Si vous créez des entrées pour une connexion SSL et une connexion non cryptée sur le même ordinateur client pour le même serveur, vous devez utiliser le nom usuel de l'entrée SSL (comme indiqué lors de la création d'une demande de certificat) et un nom alternatif pour l'entrée non chiffrée.

Tâches associées:

«Configuration des informations de communication du serveur», à la page 209
Vous pouvez utiliser l'éditeur de serveurs pour créer et modifier les détails de communication, tester l'activité du serveur et ajouter des serveurs de sauvegarde (reprise en ligne) ainsi que des programmes d'écoute. Vous pouvez également supprimer des définitions de serveur lorsque ces derniers ne font plus partie de votre configuration système.

UNIX : génération du fichier d'interfaces pour SSL

Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **`nco_igen`** pour générer le fichier d'interfaces.

Pourquoi et quand exécuter cette tâche

Procédure

- Modifiez le fichier `omni.dat` en spécifiant les ports SSL. Pour un serveur autorisant les connexions chiffrées et non chiffrées, les clients qui utilisent le même fichier d'interfaces que le serveur (clients locaux) se connectent à l'aide du port non chiffré. Si vous souhaitez utiliser le port SSL pour vous connecter localement, n'indiquez pas de port non chiffré pour le serveur.

- Générez le fichier d'interfaces en exécutant la commande **nco_igen**.

Exemple

L'exemple suivant présente une entrée du fichier omni.dat avec un port non chiffré et un port SSL définis. Lorsque vous exécutez l'utilitaire **nco_igen** pour cette entrée, il génère deux entrées serveur (master): l'une avec un port non chiffré 3000 et l'autre avec un port SSL 3500. Deux entrées client (query) sont également créées.

```
[NCOMS]
{
 Primary: nocturama 3000 ssl 3500
}
```

L'exemple suivant présente les entrées d'un fichier omni.dat pour lequel seuls les ports SSL sont spécifiés :

```
[PSERV]
{
Primary: hostname.ibm.com ssl 7100
}
[BSERV]
{
Primary: hostname.ibm.com ssl 8100
}
[NCOMS]
{
Primary: hostname.ibm.com ssl 7100
Backup: hostname.ibm.com ssl 8100
```

Tâches associées:

«Configuration de la SSL pour les installations distribuées», à la page 378
Si vous utilisez des ports SSL et des ports déchiffrés sur votre ordinateur hôte, créez un fichier d'interfaces pour les ordinateurs client distants qui utilisent des ports SSL. Distribuez ce fichier d'interfaces aux ordinateurs client distants plutôt que d'utiliser le fichier d'interfaces généré sur l'ordinateur hôte du serveur.

«Edition manuelle du fichier de données de connexions», à la page 217
Le fichier de données de connexions permet de créer le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus. Dans certains cas, il peut être nécessaire d'éditer le fichier de connexions directement ; par exemple sur les systèmes UNIX qui ne disposent pas d'interface graphique.

«Génération du fichier d'interfaces pour plusieurs plateformes (UNIX uniquement)», à la page 219
Après avoir utilisé l'éditeur de serveurs pour configurer des communications entre composants, les informations de communication sont sauvegardées dans un *fichier d'interfaces*.

«Etape 3 : distribution des fichiers d'interfaces (UNIX uniquement)», à la page 221
Après avoir généré des fichiers d'interfaces pour chaque système d'exploitation UNIX dans votre système Tivoli Netcool/OMNIbus, vous pouvez les distribuer. Vous pouvez ainsi facilement dupliquer des paramètres de communication pour chaque ordinateur UNIX Tivoli Netcool/OMNIbus.

«Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer», à la page 525
Utilisez une connexion Secure Socket Layer (SSL) pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers l'Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez SSL dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

«Configuration d'une connexion SSL au serveur ObjectServer», à la page 523
Pour les environnements intégrant un registre d'utilisateurs Tivoli Netcool/OMNIbus ObjectServer, vous devez configurer des communications chiffrées sur le Jazz for Service Management.

«Configuration des connexions SSL en mode FIPS 140–2 pour le flux d'événements à partir du serveur ObjectServer», à la page 538
Pour plus de sécurité, utilisez une connexion Secure Socket Layer (SSL) avec le chiffrement FIPS 140-2 pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez le chiffrement FIPS 140-2 dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

Configuration de la SSL pour les installations distribuées

Si vous utilisez des ports SSL et des ports déchiffrés sur votre ordinateur hôte, créez un fichier d'interfaces pour les ordinateurs client distants qui utilisent des ports SSL. Distribuez ce fichier d'interfaces aux ordinateurs client distants plutôt que d'utiliser le fichier d'interfaces généré sur l'ordinateur hôte du serveur.

Pourquoi et quand exécuter cette tâche

Dans une paire de reprise en ligne, les clients identifient les serveurs ObjectServer à l'aide du même nom de serveur. Ce nom doit être le nom usuel du serveur lorsque vous utilisez le port SSL pour vous connecter.

Procédure

- Vérifiez que le nom de serveur que vous spécifiez est identique au nom usuel spécifié pour le serveur lors de la création d'une demande de certificat. Dans une paire de reprise en ligne, les clients identifient les serveurs ObjectServer à l'aide du même nom de serveur. Ce nom doit être le nom usuel du serveur lorsque vous utilisez le port SSL pour vous connecter. Pour la passerelle unidirectionnelle, utilisez les propriétés **Gate.Reader.CommonNames** et **Gate.Writer.CommonNames** pour indiquer des noms usuels acceptables pour les serveurs ObjectServer principal et de sauvegarde. Pour la passerelle bidirectionnelle, utilisez les propriétés **Gate.ObjectServerA.CommonNames** et **Gate.ObjectServerB.CommonNames**. Pour de plus amples informations sur l'utilisation de ces propriétés de passerelle ObjectServer, voir *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*. L'exemple suivant présente un exemple de configuration du nom usuel d'une passerelle unidirectionnelle :

  ```
  Gate.Reader.Server:   'PSERV'
  Gate.Reader.CommonNames:  'NCOMS'
  Gate.Writer.Server:   'BSERV'
  Gate.Writer.CommonNames:  'NCOMS'
  ```

  Dans cet exemple, il est impossible d'effectuer de se connecter en spécifiant PSERV ou BSERV. Pour établir la connexion, spécifiez le nom virtuel NCOMS.
- Si une analyse est associée à un serveur ObjectServer à l'aide de la SSL et que la zone **CommonName** du certificat reçu ne correspond pas au nom spécifié par la propriété de serveur, utilisez la propriété **SSLServerCommonName** pour spécifier une liste séparée par des virgules des noms usuels SSL acceptables (par défaut, c'est la propriété de serveur qui est utilisée).

  ```
  SSLServerCommonName:   'NCOMS'
  ```

A propos des fichiers de la base de données de clés

Une base de données de clés CMS consiste en un certain nombre de fichiers portant la même racine de nom de fichier, mais avec des extensions différentes.

Ces fichiers sont décrits dans le tableau suivant.

Tableau 75. Fichiers de la base de données de clés

Extension de fichier	Description	Nom de fichier de Tivoli Netcool/OMNIbus
`.kdb`	Une base de données de clés stocke les clés et les certificats numériques et active les connexions réseau sécurisées entre les clients et les serveurs. En mode FIPS 140-2, les mots de passe pour les bases de données de clés doivent répondre aux exigences suivantes. Si les mots de passe ne respectent pas ces exigences, la base de données de clés est créée, mais vous ne pouvez pas créer, signer ni recevoir de certificats et une erreur est consignée dans le journal du serveur ObjectServer. • La longueur minimale du mot de passe est de 14 caractères. • Un mot de passe doit contenir au moins un caractère en minuscule, un caractère en majuscule et un chiffre ou caractère spécial. • Chaque caractère ne doit pas apparaître plus de trois fois dans un mot de passe. • Il ne peut pas y avoir plus de deux caractères consécutifs du mot de passe identiques. • Tous les caractères figurent dans le jeu de caractères imprimable ASCII standard compris entre 0x20 et 0x7E inclus.	`omni.kdb`
`.rdb`	Lorsqu'une demande certificat est créée, un fichier `.rdb` est créé pour stocker la paire de clés demandée et les données de demande de certificat. Lorsqu'un certificat signé est obtenu d'une autorité de certification et reçu dans la base de données de clés, il est mis en correspondance avec la clé privée figurant dans le fichier `.rdb`. Le certificat et la clé privés sont ensuite tous deux ajoutés au fichier `.kdb` en tant que certificat accompagné de ses informations de clé privée. L'entrée demande est ensuite supprimée de la base de données de clés de demande.	`omni.rdb`

Tableau 75. Fichiers de la base de données de clés (suite)

Extension de fichier	Description	Nom de fichier de Tivoli Netcool/OMNIbus
`.crl`	Un fichier `.crl` est créé pour des raisons d'héritage et n'est plus utilisé. Ce fichier était utilisé pour stocker une liste de révocation de certificat détaillant les certificats révoqués ou suspendus.	`omni.crl`
`.sth`	Vous pouvez sauvegarder le mot de passe d'une base de données de clés dans un fichier de dissimulation si vous avez besoin d'une connexion automatique à la base de données de clés afin d'avoir accès aux certificats numériques. Le mot de passe est stocké dans un format codé dans le fichier de dissimulation. Lors de l'accès à la base de données de clés, le système vérifie si un fichier de dissimulation existe. S'il en détecte un, le contenu du fichier est déchiffré et utilisé comme entrée pour le mot de passe. **Remarque :** Tivoli Netcool/OMNIbus exige un fichier de dissimulation.	`omni.sth`

Les fichiers de la base de données de clés sont stockés à l'emplacement suivant :

- Sous UNIX : `$NCHOME/etc/security/keys`
- Sous Windows : `%NCHOME%\ini\security\keys`

Configuration d'un réseau protégé SSL

Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

Pourquoi et quand exécuter cette tâche

Important : Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS 140-2, utilisez uniquement l'utilitaire **nc_gskcmd**. De plus, utilisez **nc_gskcmd** pour les réseaux comprenant des clients basés sur Java. N'utilisez pas iKeyman pour l'un de ces scénarios.

Les utilitaires font appel à une base de données de clés Certificate Management System (CMS) pour stocker les certificats numériques et les clés. La base de données de clés requiert un mot de passe pour protéger les clés privées, utilisées pour signer des documents et pour déchiffrer des messages chiffrés avec des clés publiques.

Dans une base de données de clés, les certificats numériques d'autorités de certification sont stockés sous forme de certificats de *signataire*. Tout certificat autosigné créé, ou tout certificat de serveur reçu des autorités de certification émettrices en réponse à une demande de certificat, est stocké comme certificat *personnel*.

Tâches associées:

«Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer», à la page 525
Utilisez une connexion Secure Socket Layer (SSL) pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers l'Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez SSL dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

«Configuration d'une connexion SSL au serveur ObjectServer», à la page 523
Pour les environnements intégrant un registre d'utilisateurs Tivoli Netcool/OMNIbus ObjectServer, vous devez configurer des communications chiffrées sur le Jazz for Service Management.

«Configuration des connexions SSL en mode FIPS 140–2 pour le flux d'événements à partir du serveur ObjectServer», à la page 538
Pour plus de sécurité, utilisez une connexion Secure Socket Layer (SSL) avec le chiffrement FIPS 140-2 pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez le chiffrement FIPS 140-2 dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

Création d'une base de données de clés

Sur chaque ordinateur sur lequel un composant serveur (ObjectServer, agent de processus ou serveur proxy) est installé, créez une base de données de clés pour stocker les certificats numériques. Créez également une base de données de clés sur chaque ordinateur à partir duquel les clients se connectent au serveur à l'aide d'un port SSL. Utilisez un fichier de la base de données de clés dédié (`omni.kdb`) pour chaque installation Tivoli Netcool/OMNIbus sur un serveur ou un ordinateur client.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez une base de données de clés, elle est automatiquement renseignée avec un certain nombre de certificats de signataire d'autorités de certifications publiques communes.

Création d'une base de données de clés à l'aide de nc_gskcmd

Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

Pourquoi et quand exécuter cette tâche

Pour de plus amples informations sur la l'utilitaire **nc_gskcmd**, voir les manuels «Options de ligne de commande nc_gskcmd», à la page 406 et *IBM Global Security Kit Secure Sockets Layer Introduction and iKeyman User's Guide*, SC32-1700.

En mode FIPS 140-2, les mots de passe pour les bases de données de clés doivent répondre aux exigences suivantes. Si les mots de passe ne respectent pas ces exigences, la base de données de clés est créée, mais vous ne pouvez pas créer, signer ni recevoir de certificats et une erreur est consignée dans le journal du serveur ObjectServer.

- La longueur minimale du mot de passe est de 14 caractères.

- Un mot de passe doit contenir au moins un caractère en minuscule, un caractère en majuscule et un chiffre ou caractère spécial.
- Chaque caractère ne doit pas apparaître plus de trois fois dans un mot de passe.
- Il ne peut pas y avoir plus de deux caractères consécutifs du mot de passe identiques.
- Tous les caractères figurent dans le jeu de caractères imprimable ASCII standard compris entre 0x20 et 0x7E inclus.

Procédure

Pour créer une base de données de clés en mode FIPS 140-2 :

Exécutez la commande suivante :
`$NCHOME/bin/nc_gskcmd -keydb -create -db "$NCHOME/etc/security/keys/omni.kdb" -pw mot_de_passe -stash -expire entier1`
Le tableau ci-dessous décrit les variables de cette instance de la commande et les valeurs possibles.

Tableau 76. Description des arguments de ligne de commande pour créer une base de données de clés

Variable	Explication
mot_de_passe	Mot de passe permettant d'accéder à la base de données de clés
entier1	Période d'expiration du certificat en jours. Indiquez une valeur comprise entre 366 jours et 7300 jours (c'est-à-dire 20 ans)

Exemple

L'exemple suivant montre comment utiliser l'utilitaire **nc_gskcmd** pour créer une base de données de clés valide pendant 366 jours.

```
$NCHOME/bin/nc_gskcmd -keydb -create -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-stash -expire 366
```

Que faire ensuite

Envisagez de définir des droits d'utilisateur appropriés sur le fichier stash afin d'empêcher les accès non autorisés. Si vous avez besoin de certificats de signataire supplémentaires, vous pouvez les demander et les ajouter dans la base de données de clés. Vous pouvez également afficher le contenu des certificats et supprimer des certificats.

Concepts associés:

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Tâches associées:

«Demande de certificat serveur auprès d'une autorité de certification», à la page 388
A partir de chaque ordinateur serveur, créez une demande de certificat numérique pour le serveur, et envoyez la demande de certificat à une autorité de certification certifiée à des fins d'autorisation. L'autorité de certification autorise la demande de certificat et utilise le certificat racine autosigné pour générer un certificat serveur. Elle renvoie ensuite le certificat serveur signé.

«Modification du mot de passe de la base de données de clés», à la page 405
Il est recommandé de modifier régulièrement le mot de passe de la base de données de clés. Dans l'interface graphique d'iKeyman, vous êtes également invité à modifier le mot de passe si vous tentez d'ouvrir la base de données de clés avec un mot de passe expiré.

«Affichage des détails du certificat», à la page 403
Vous pouvez examiner le contenu de tout certificat de signataire ou personnel stocké dans la base de données de clés. Lorsque vous examinez un tel certificat, vous pouvez choisir de le définir comme certificat racine de confiance ou comme certificat par défaut.

«Suppression de certificats», à la page 404
Vous pouvez supprimer des certificats de signataire ou personnel dont vous n'avez plus besoin de votre base de données de clés.

Création d'une base de données de clés à l'aide d'iKeyman

Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Procédure

Pour créer une base de données de clés à l'aide d'iKeyman :

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Nouveau**.
3. Complétez cette fenêtre comme suit :

   Key database type (Type de base de données de clés)
   Sélectionnez `CMS` dans cette liste.

   File Name (Nom de fichier)
   Entrez `omni.kdb` comme nom de fichier de la base de données de clés. La valeur par défaut est `key.kdb`.

   Emplacement
   Cet emplacement spécifie le répertoire dans lequel la base de données de clés est stockée. La valeur par défaut est généralement un des répertoires suivants :

   - UNIX : `$NCHOME/etc/security/keys/`
   - Windows : `%NCHOME%\ini\security\keys\`

   Remarque : Sous Windows, si vous avez démarré iKeyman depuis la ligne de commande en entrant `%NCHOME%\bin\nc_ikeyman.bat`, l'emplacement indiqué ci-dessus est la valeur par défaut. Si vous avez démarré iKeyman depuis l'Explorateur Windows en cliquant deux fois sur le fichier `%NCHOME%\bin\nc_ikeyman.vbs`, l'emplacement par défaut est `%NCHOME%\bin\`.

Si le codage UTF-8 est activé sous Windows, le chemin d'accès de la base de données de clés doit uniquement contenir des caractères pris en charge par la page de code par défaut du système.

Acceptez le répertoire par défaut sous UNIX. Sous Windows, assurez-vous que l'emplacement est `%NCHOME%\ini\security\keys\`.

OK Cliquez sur ce bouton pour accepter les paramètres du fichier de la base de données de clés.

La fenêtre Password Prompt (Invite de mot de passe) s'affiche pour vous permettre de spécifier un mot de passe destiné à contrôler l'accès à la base de données de clés.

4. Complétez cette fenêtre comme suit :

Mot de passe (Password)
Entrez un mot de passe. Au fur et à mesure que vous tapez les caractères, une indication de la force du mot de passe est fournie.

Remarque : Les mots de passe sont sensibles à la casse, de sorte que lorsque vous devez spécifier le mot de passe pour ouvrir la base de données de clés, vous devez utiliser la casse correcte pour éviter des erreurs.

Confirm Password (Confirmer le mot de passe)
Entrez de nouveau le mot de passe.

Set expiration time (Définir le délai d'expiration)
Cochez cette case pour spécifier une période après laquelle le mot de passe arrivera à expiration. Entrez la période en jours. La valeur par défaut est `60` jours. Si cette case est décochée, le mot de passe n'expirera jamais.

Stash the password to a file? (Stocker le mot de passe dans un fichier ?)
Cochez cette case pour enregistrer le mot de passe dans un format chiffré dans un fichier de dissimulation. Cette condition est obligatoire pour Tivoli Netcool/OMNIbus.

OK Cliquez sur ce bouton pour fermer la fenêtre et créer la base de données de clés.

Résultats

Le fichier de base de données de clés est créé dans le répertoire spécifié avec le nom `omni.kdb`, et des fichiers supplémentaires appelés `omni.crl` et `omni.rdb`. Le fichier stash est également sauvegardé au même emplacement avec le nom `omni.sth`. La fenêtre IBM Key Management (Gestion des clés IBM) affiche à présent l'emplacement du fichier et le nom de la base de données de clés ainsi que les certificats de signataire par défaut.

Important : Comme mesure de sécurité pour empêcher un abus d'utilisation des certificats de signataire par défaut, supprimez tous ces certificats de la base de données de clés.

Que faire ensuite

Envisagez de définir des droits d'utilisateur appropriés sur le fichier stash afin d'empêcher les accès non autorisés. Si vous avez besoin de certificats de signataire supplémentaires, vous pouvez les demander et les ajouter dans la base de données

de clés. Vous pouvez également afficher le contenu des certificats et supprimer des certificats.

Concepts associés:

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Demande de certificat serveur auprès d'une autorité de certification», à la page 388
A partir de chaque ordinateur serveur, créez une demande de certificat numérique pour le serveur, et envoyez la demande de certificat à une autorité de certification certifiée à des fins d'autorisation. L'autorité de certification autorise la demande de certificat et utilise le certificat racine autosigné pour générer un certificat serveur. Elle renvoie ensuite le certificat serveur signé.

«Modification du mot de passe de la base de données de clés», à la page 405
Il est recommandé de modifier régulièrement le mot de passe de la base de données de clés. Dans l'interface graphique d'iKeyman, vous êtes également invité à modifier le mot de passe si vous tentez d'ouvrir la base de données de clés avec un mot de passe expiré.

«Affichage des détails du certificat», à la page 403
Vous pouvez examiner le contenu de tout certificat de signataire ou personnel stocké dans la base de données de clés. Lorsque vous examinez un tel certificat, vous pouvez choisir de le définir comme certificat racine de confiance ou comme certificat par défaut.

«Suppression de certificats», à la page 404
Vous pouvez supprimer des certificats de signataire ou personnel dont vous n'avez plus besoin de votre base de données de clés.

Création d'un certificat autosigné

Si vous souhaitez configurer un réseau de certification privé dans lequel vous agissez comme autorité de certification émettrice pour vos certificats serveur, créez un certificat autosigné dans la base de données de clés de chaque ordinateur serveur.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez un certificat autosigné, indiquez des informations sur votre organisation, utilisées pour générer la paire de clés publique-privée associée. La clé publique est intégrée au certificat et elle est utilisée pour vérifier la validité d'autres certificats émis par l'autorité de certification. La clé privée est utilisée pour signer le certificat et elle est stockée localement et de manière sécurisée dans la base de données de clés.

Procédure

Pour créer un certificat autosigné :

Dans la ligne de commande, entrez la commande suivante :

```
$NCHOME/bin/nc_gskcmd -cert -create -db "filename"
-pw mot_de_passe -label "keylabel" -size keysize
-ca true -dn distinguishedname
-expire integer1 -x509version integer2
```

Important : Ne créez pas de certificat autosigné avec `-ca` défini sur `false`.
Le tableau ci-dessous décrit les variables de cette instance de la commande et les valeurs possibles.

Tableau 77. Variables. Description des arguments de ligne de commande pour créer un certificat autosigné

Variable	Explication
nom_fichier	Le nom et le chemin d'accès de la base de données de clés dans laquelle vous souhaitez stocker le certificat. Spécifiez cette valeur sous forme de chaîne entre guillemets, par exemple : • UNIX Linux `"$NCHOME/etc/security/keys/omni.kdb"` • Windows `"%NCHOME%\ini\security\keys\omni.kdb"`
mot_de_passe	Mot de passe permettant d'accéder à la base de données de clés
intitulé_de_clé	Brève description significative qui peut être utilisée pour identifier le certificat autosigné dans la base de données de clés. Spécifiez cette valeur sous forme de chaîne entre guillemets. Pour vous aider à identifier le certificat comme étant autosigné dans l'interface graphique iKeyman, vous pouvez ajouter les mots `Autorité de certification` ou `AC` dans le texte de l'étiquette.
taille_de_la_clé	Longueur de la clé en octets. Les valeurs sont `512`, `1024` et `2048`. Plus la clé est longue, plus le chiffrement est sécurisé. Notez qu'une plus longue clé peut aussi ralentir la performance.

Tableau 77. Variables (suite). Description des arguments de ligne de commande pour créer un certificat autosigné

Variable	Explication
nom_distinctif	Nom distinctif du titulaire de certificat sous forme de chaîne entre guillemets au format suivant :"CN=*chaîne1*, O=*chaîne2*, OU=*chaîne3*, L=*chaîne4*, ST=*chaîne5*, C=*chaîne6*". Dans cette chaîne, le paramètre nom commun (CN) est obligatoire, mais tous les autres paramètres sont facultatifs pour les certificats autosignés. Dans cet argument, les paramètres indiquent les informations suivantes : • *chaîne1* spécifie le nom commun du propriétaire du certificat. Il s'agit du nom du serveur sur lequel vos clients se connectent ; par exemple NCOMS. Le nom commun du serveur doit être le même que le nom du serveur du fichier de données des connexions ($NCHOME/etc/omni.dat ou %NCHOME%\ini\sql.ini) sur les machines client • *chaîne2* spécifie le nom de votre société. • *chaîne3* spécifie le nom de l'unité organisationnelle ou du service dans lequel le certificat est utilisé. • *chaîne4* indique la localité ou la ville de votre organisation. • *chaîne5* spécifie votre état ou votre province. • *chaîne6* spécifie le code ISO à deux lettres de votre pays.
entier1	Période d'expiration du certificat en jours. Indiquez une valeur comprise entre 366 jours et 7300 jours (c'est-à-dire 20 ans)
entier2	Version du certificat X.509 à créer. Les valeurs sont 1, 2 et 3. La valeur par défaut est 3.

Résultats

Si vous démarrez l'interface graphique iKeyman et ouvrez le fichier de base de données omni.kdb, les nouveaux certificats créés sont visibles dans la fenêtre IBM Key Management (Gestion des clés IBM), en tant qu'une de vos entrées dans la liste **Personal Certificates** (Certificats personnels). L'étiquette de clé est utilisée pour identifier le certificat.

Exemple

L'exemple suivant montre comment utiliser l'utilitaire **nc_gskcmd** pour créer un certificat autosigné.

```
$NCHOME/bin/nc_gskcmd -cert -create -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "NCOMS_CA" -size 1024 -ca true
-dn "CN=NCOMS_CA,O=IBM,OU=Support,L=SouthBank,ST=London,C=GB"
-expire 366 -x509version 3
```

Que faire ensuite

Distribuez ce certificat comme certificat de signataire à tous les clients qui doivent se connecter au serveur à l'aide de SSL. Pour distribuer le certificat autosigné, extrayez le certificat comme fichier dans un emplacement spécifié du réseau puis ajoutez le fichier extrait à la base de données de clés sur chaque ordinateur client.

Tâches associées:

«Extraction des certificats d'une base de données de clés», à la page 397
Vous pouvez extraire une copie d'un certificat de signataire ou personnel d'une base de données de clés et l'ajouter à une autre base de données de clés comme certificat de signataire. Lorsque vous extrayez un certificat, la clé publique est également extraite. Cette tâche vous permet de copier un certificat autosigné d'un ordinateur serveur vers un emplacement du réseau.

«Ajout de certificats d'autorités de certification», à la page 399
Lorsque vous recevez un certificat racine ou un certificat intermédiaire associé d'une autorité de certification émettrice, ajoutez le certificat à la base de données de clés sur tous les ordinateurs client et serveur qui requièrent une connexion SSL. De même, pour distribuer un certificat autosigné que vous avez extrait d'une base de données de clés de serveur, ajoutez le fichier de certificat extrait à tous les ordinateurs client.

Référence associée:

«Options de ligne de commande nc_gskcmd», à la page 406
L'utilitaire de ligne de commande **nc_gskcmd** fournit davantage de fonctionnalités que l'interface graphique iKeyman.

Demande de certificat serveur auprès d'une autorité de certification

A partir de chaque ordinateur serveur, créez une demande de certificat numérique pour le serveur, et envoyez la demande de certificat à une autorité de certification certifiée à des fins d'autorisation. L'autorité de certification autorise la demande de certificat et utilise le certificat racine autosigné pour générer un certificat serveur. Elle renvoie ensuite le certificat serveur signé.

Si vous agissez comme l'autorité de certification émettrice au sein d'un réseau de certification privé et que vous souhaitez utiliser un certificat autosigné pour générer un certificat serveur, signez le certificat et renvoyez-le en tant que certificat serveur signé.

Tâches associées:

«Création d'une base de données de clés à l'aide de nc_gskcmd», à la page 381
Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

Demande de certificat serveur auprès d'une autorité de certification à l'aide de`nc_gskcmd`

Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

Procédure

1. Pour demander un certificat serveur, exécutez la commande suivante :

   ```
   $NCHOME/bin/nc_gskcmd -certreq -create -db "filename"
   -pw password -label "keylabel"
   -size keysize -dn "distinguishedname"
   -file "$NCHOME/etc/security/keys/certname.arm"
   ```

   Le tableau ci-dessous décrit les variables de cette instance de la commande et les valeurs possibles.

Tableau 78. Description des arguments de ligne de commande pour demander un certificat serveur

Variable	Explication
nom_fichier	Le nom et le chemin d'accès de la base de données de clés dans laquelle vous souhaitez stocker le certificat. Spécifiez cette valeur sous forme de chaîne entre guillemets, par exemple : • UNIX Linux `"$NCHOME/etc/security/keys/omni.kdb"` • Windows `"%NCHOME%\ini\security\keys\omni.kdb"`
mot_de_passe	Mot de passe permettant d'accéder à la base de données de clés
intitulé_de_clé	Brève description significative qui peut être utilisée pour identifier le certificat autosigné dans la base de données de clés. Spécifiez cette valeur sous forme de chaîne entre guillemets. Pour vous aider à identifier le certificat comme étant autosigné dans l'interface graphique iKeyman, vous pouvez ajouter les mots `Autorité de certification` ou `AC` dans le texte de l'étiquette.
taille_de_la_clé	Longueur de la clé en octets. Les valeurs sont `512`, `1024` et `2048`. Plus la clé est longue, plus le chiffrement est sécurisé. Notez qu'une plus longue clé peut aussi ralentir la performance.

Tableau 78. Description des arguments de ligne de commande pour demander un certificat serveur (suite)

Variable	Explication
nom_distinctif	Nom distinctif du titulaire de certificat sous forme de chaîne entre guillemets au format suivant :"CN=*chaîne1*, O=*chaîne2*, OU=*chaîne3*, L=*chaîne4*, ST=*chaîne5*, C=*chaîne6*". Dans cette chaîne, le paramètre nom commun (CN) est obligatoire, mais tous les autres paramètres sont facultatifs pour les certificats autosignés. Dans cet argument, les paramètres indiquent les informations suivantes : • *chaîne1* spécifie le nom commun du propriétaire du certificat. Il s'agit du nom du serveur sur lequel vos clients se connectent ; par exemple NCOMS. Le nom commun du serveur doit être le même que le nom du serveur du fichier de données des connexions ($NCHOME/etc/omni.dat ou %NCHOME%\ini\sql.ini) sur les machines client • *chaîne2* spécifie le nom de votre société. • *chaîne3* spécifie le nom de l'unité organisationnelle ou du service dans lequel le certificat est utilisé. • *chaîne4* indique la localité ou la ville de votre organisation. • *chaîne5* spécifie votre état ou votre province. • *chaîne6* spécifie le code ISO à deux lettres de votre pays.
nom_certificat	Nom du fichier certificat (fichier .arm) que vous souhaitez demander. Le nom du fichier est le même que le nom de l'ObjectServer spécifié dans le fichier de connexion de données omni.dat. Spécifiez le chemin d'accès au fichier de certificat sous forme de chaîne entre guillemet.

2. Pour les paires de reprise en ligne, répétez l'étape 1 pour le serveur ObjectServer de secours. Changez la valeur de l'option -label et donnez-lui le nom du serveur ObjectServer de secours (comme indiqué dans le fichier de connexions de données omni.dat), conservez les valeurs de noms usuels pour l'option de ligne de commande -dn et changez la valeur de l'option de ligne de commande -file pour lui donner le nom du fichier de certificats pour le serveur ObjectServer de secours.

Exemple

L'exemple suivant présente une demande de certificat pour un serveur ObjectServer principal appelé «PSERV» faisant partie de la paire de reprise en ligne avec le nom usuel «NCOMS» :

```
$NCHOME/bin/nc_gskcmd -certreq -create -db "$NCHOME/etc/security/keys/omni.kdb"
-pw password -label "PSERV" -size 1024
-dn "CN=NCOMS, O=IBM, OU=Support, L=SouthBank, ST=London, C=GB"
-file "$NCHOME/etc/security/keys/pservreq.arm"
```

L'exemple suivant présente une demande de certificat pour un serveur ObjectServer de secours de la paire de reprise en ligne NCOMS appelé «BSERV» :

```
$NCHOME/bin/nc_gskcmd -certreq -create -db "$NCHOME/etc/security/keys/omni.kdb"
-pw password -label "BSERV" -size 1024
-dn "CN=NCOMS, O=IBM, OU=Support, L=SouthBank, ST=London, C=GB"
-file "$NCHOME/etc/security/keys/bservreq.arm"
```

Tâches associées:

«Signature d'un fichier de demande de certificat avec un certificat de signataire», à la page 393
Si vous agissez comme l'autorité de certification émettrice au sein d'un réseau de certification privé et que vous souhaitez utiliser un certificat autosigné pour générer un certificat serveur, signez le certificat et renvoyez-le en tant que certificat serveur signé.

«Réception de certificats de serveur d'autorités de certification», à la page 395
A la réception du certificat serveur provenant de l'autorité de certification émettrice, réceptionnez le certificat dans la base de données de clés du serveur. Le certificat serveur est utilisé pour authentifier le côté serveur des communications Tivoli Netcool/OMNIbus lorsqu'un client demande une connexion sécurisée. Si l'autorité de certification envoie des certificats de signataire supplémentaires ou des certificats d'autorités de certification intermédiaires, ajoutez ces certificats supplémentaires à la base de données de clés avant de recevoir le certificat de serveur.

Demande de certificat serveur auprès d'une autorité de certification à l'aide d'iKeyman

Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez une demande de certificat, vous êtes invité à entrer des informations sur votre organisation afin de générer une paire de clés publique-privée. La clé publique est intégrée à la demande de certificat envoyée à l'autorité de certification et la clé privée pour le serveur est stockée localement dans la base de données de clés.

Procédure

Pour créer une demande de certificat à partir d'un ordinateur serveur :

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés (`omni.kdb`) dans laquelle vous souhaitez créer la demande. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).

5. Dans la zone **Key database content (Contenu de base de données de clés)**, sélectionnez `Personal Certificate Request (Demande de certificat personnel)` dans la liste déroulante puis cliquez sur **Nouveau**. La fenêtre "Create New Key and Certificate Request" (Créer une demande de clé et de certificat) s'affiche.
6. Complétez cette fenêtre comme suit. Des entrées facultatives sont indiquées dans la fenêtre.

   Key Label (Etiquette de clé)
   Spécifiez le nom du serveur comme étiquette. Il s'agit du nom du serveur auquel vos clients se connectent et doit être identique au nom du serveur dans le fichier de données de connexions (`$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini`) de la machine serveur ; par exemple, `NCOMS`.

   Key Size (Taille de la clé)
   Sélectionnez la longueur de la clé (en octets) dans cette liste. La valeur par défaut est `1024`.

   Plus la clé est longue, plus le chiffrement est sécurisé. Cependant, une longue clé peut aussi ralentir les performances.

   Common Name (Nom usuel)
   Spécifiez le nom usuel du propriétaire du certificat. Ce nom doit correspondre au nom du serveur spécifié dans le fichier de données de connexions (`$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini`), ou le fichier de propriétés des ordinateurs client.

   Conseil : Certains clients d'une configuration virtuelle fournissent une propriété qui permet de spécifier une liste des noms usuels SSL acceptables ; par exemple, la propriété d'analyse **`SSLServerCommonName`**.

   Organization (Organisation)
   Indiquez le nom de votre entreprise.

   Organization Unit (Unité organisationnelle)
   Indiquez l'unité organisationnelle ou le nom du département où le certificat sera utilisé.

   Locality (Localité)
   Indiquez la localité ou la ville de votre entreprise.

   State/Province (Etat/Province)
   Indiquez votre état ou province.

   Zipcode (Code postal)
   Indiquez votre code postal.

   Country or region (Pays ou région)
   Sélectionnez le code ISO à deux lettres correspondant à votre pays.

   Entrez le nom d'un fichier dans lequel la demande de certificat doit être stockée
   Spécifiez le nom et l'emplacement du fichier dans lequel les détails de la demande doivent être sauvegardés. La valeur par défaut est :
   - UNIX : `$NCHOME/etc/security/keys/certreq.arm`
   - Windows : `%NCHOME%\ini\security\keys\certreq.arm`

   OK Cliquez sur ce bouton pour créer la demande et fermer la fenêtre.

Résultats

La nouvelle demande de certificat créée est répertoriée dans la fenêtre IBM Key Management (Gestion des clés IBM), comme une entrée de la liste **Personal Certificate Requests** (Demandes de certificat personnel). L'étiquette de clé est utilisée pour identifier la demande.

Que faire ensuite

Envoyez le fichier `.arm` à l'autorité de certification pour demander un certificat numérique pour le serveur. (Cette autorité de certification peut être une autorité de certification publique de confiance ou l'autorité de certification émettrice dans votre réseau de certification privé). Après avoir vérifié votre identité, l'autorité de certification vous envoie un certificat signé et chiffré avec sa clé privée. Recevez ensuite le certificat signé dans la base de données de clés sur le serveur.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Signature d'un fichier de demande de certificat avec un certificat de signataire»
Si vous agissez comme l'autorité de certification émettrice au sein d'un réseau de certification privé et que vous souhaitez utiliser un certificat autosigné pour générer un certificat serveur, signez le certificat et renvoyez-le en tant que certificat serveur signé.

«Réception de certificats de serveur d'autorités de certification», à la page 395
A la réception du certificat serveur provenant de l'autorité de certification émettrice, réceptionnez le certificat dans la base de données de clés du serveur. Le certificat serveur est utilisé pour authentifier le côté serveur des communications Tivoli Netcool/OMNIbus lorsqu'un client demande une connexion sécurisée. Si l'autorité de certification envoie des certificats de signataire supplémentaires ou des certificats d'autorités de certification intermédiaires, ajoutez ces certificats supplémentaires à la base de données de clés avant de recevoir le certificat de serveur.

Signature d'un fichier de demande de certificat avec un certificat de signataire

Si vous agissez comme l'autorité de certification émettrice au sein d'un réseau de certification privé et que vous souhaitez utiliser un certificat autosigné pour générer un certificat serveur, signez le certificat et renvoyez-le en tant que certificat serveur signé.

Pourquoi et quand exécuter cette tâche

Pour signer un fichier de demande de certificat avec un certificat autosigné :

Procédure

Dans la ligne de commande, entrez la commande suivante :

```
$NCHOME/bin/nc_gskcmd -cert -sign -db filename -pw mot_de_passe
-label étiquette_clé -target server_filename
-expire integer -file request_filename
```

Dans cette commande :

- *nom_fichier* spécifie le nom et le chemin d'accès de la base de données de clés dans laquelle le certificat autosigné est stocké. Spécifiez cette valeur sous forme de chaîne entre guillemets ; par exemple `"$NCHOME/etc/security/keys/omni.kdb"` (sous UNIX) ou `"%NCHOME%\ini\security\keys\omni.kdb"` (sous Windows).
- *mot_de_passe* spécifie le mot de passe à utiliser pour accéder à la base de données de clés.
- *étiquette_clé* spécifie l'étiquette du certificat autosigné dans la base de données de clés. Spécifiez cette valeur sous forme de chaîne entre guillemets.
- *nom_fichier_serveur* spécifie le nom et le chemin d'accès du certificat serveur que vous souhaitez générer. Spécifiez cette valeur sous forme de chaîne entre guillemets. Vous pouvez spécifiez un nom en tant que fichier `.arm`.
- *entier* spécifie une période d'expiration en jours pour le certificat serveur. Spécifiez une valeur comprise entre 366 jours et 7300 jours (c'est-à-dire 20 ans). La période d'expiration du certificat serveur doit être inférieure à celle du certificat autosigné.
- *nom_fichier_demande* spécifie le nom et le chemin d'accès du fichier de demande de certificat. Spécifiez cette valeur sous forme de chaîne entre guillemets. Par exemple, `"$NCHOME/etc/security/keys/certreq.arm"` sous UNIX ou `"%NCHOME%\ini\security\keys\certreq.arm"` sous Windows.

Résultats

Le fichier de certificat serveur est créé à l'emplacement spécifié.

Exemple

L'exemple suivant montre comment utiliser l'utilitaire **nc_gskcmd** pour signer une demande de certificat appelée `certreq.arm` avec le certificat du signataire `pservcert.arm`.

```
$NCHOME/bin/nc_gskcmd -cert -sign -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-label "NCOMS_CA"
-target "$NCHOME/etc/security/keys/pservcert.arm"
-file "$NCHOME/etc/security/certreq.arm"
```

Que faire ensuite

Recevez le certificat serveur dans la base de données de clés.

Tâches associées:

«Réception de certificats de serveur d'autorités de certification», à la page 395
A la réception du certificat serveur provenant de l'autorité de certification émettrice, réceptionnez le certificat dans la base de données de clés du serveur. Le certificat serveur est utilisé pour authentifier le côté serveur des communications Tivoli Netcool/OMNIbus lorsqu'un client demande une connexion sécurisée. Si l'autorité de certification envoie des certificats de signataire supplémentaires ou des certificats d'autorités de certification intermédiaires, ajoutez ces certificats supplémentaires à la base de données de clés avant de recevoir le certificat de serveur.

Référence associée:

«Options de ligne de commande nc_gskcmd», à la page 406
L'utilitaire de ligne de commande **nc_gskcmd** fournit davantage de fonctionnalités que l'interface graphique iKeyman.

Réception de certificats de serveur d'autorités de certification

A la réception du certificat serveur provenant de l'autorité de certification émettrice, réceptionnez le certificat dans la base de données de clés du serveur. Le certificat serveur est utilisé pour authentifier le côté serveur des communications Tivoli Netcool/OMNIbus lorsqu'un client demande une connexion sécurisée. Si l'autorité de certification envoie des certificats de signataire supplémentaires ou des certificats d'autorités de certification intermédiaires, ajoutez ces certificats supplémentaires à la base de données de clés avant de recevoir le certificat de serveur.

Réception de certificats serveur à l'aide de `nc_gskcmd`

Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **`nc_gskcmd`**.

Procédure

1. Pour recevoir le certificat serveur, exécutez la commande suivante :

   ```
   $NCHOME/bin/nc_gskcmd -cert -receive -db "nom_fichier" -pw mot_de_passe -file
   "$NCHOME/etc/security/keys/nom_certificat.arm"
   ```

   Le tableau ci-dessous décrit les arguments de ligne de commande de cette commande et les valeurs obligatoires.

Tableau 79. Description des arguments de ligne de commande pour demander un certificat serveur

Variable	Explication
nom_fichier	Le nom et le chemin d'accès de la base de données de clés dans laquelle vous souhaitez stocker le certificat. Spécifiez cette valeur sous forme de chaîne entre guillemets, par exemple : • UNIX Linux `"$NCHOME/etc/security/keys/omni.kdb"` • Windows `"%NCHOME%\ini\security\keys\omni.kdb"`
mot_de_passe	Mot de passe permettant d'accéder à la base de données de clés
nom_certificat	Nom du fichier certificat (fichier `.arm`) que vous souhaitez demander. Le nom du fichier est le même que le nom de l'ObjectServer spécifié dans le fichier de connexion de données `omni.dat`. Spécifiez le chemin d'accès au fichier de certificat sous forme de chaîne entre guillemet.

2. Pour les paires de reprise en ligne, répétez l'étape 1 pour le serveur ObjectServer de sauvegarde. Changez la valeur de l'option de ligne de commande `-file` et donnez-lui le nom du fichier certificat du serveur ObjectServer de sauvegarde.

Résultats

Le certificat signé de l'autorité de certification est fusionné avec la demande correspondante et ajouté à la base de données de clés comme certificat serveur avec ses informations de clé privée. L'entrée de la demande est ensuite supprimée de la base de données de clés.

Exemple

L'exemple suivant présente un certificat reçu pour un serveur ObjectServer principal appelé «PSERV».

```
$NCHOME/bin/nc_gskcmd -cert -receive -db
"$NCHOME/etc/security/keys/omni.kdb" -pw password
-file "$NCHOME/etc/security/keys/pservcert.arm"
```

L'exemple suivant présente un certificat reçu pour un serveur ObjectServer de sauvegarde appelé «BSERV».

```
$NCHOME/bin/nc_gskcmd -cert -receive -db
"$NCHOME/etc/security/keys/omni.kdb" -pw mot_de_passe -file
"$NCHOME/etc/security/keys/bservcert.arm"
```

Que faire ensuite

Si ce certificat n'a pas encore été défini comme certificat par défaut, définissez-le comme certificat par défaut dans la base de données de clés du serveur.

Réception de certificats de serveur à l'aide d'iKeyman

Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Pourquoi et quand exécuter cette tâche

Pour recevoir un certificat serveur dans la base de données de clés :

Procédure

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés dans laquelle vous souhaitez ajouter le certificat serveur. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Dans la zone **Key database content (Contenu de base de données de clés)**, sélectionnez `Personal Certificates (Certificats personnels)` dans la liste déroulante puis cliquez sur **Receive (Recevoir)**.
6. Indiquez les informations suivantes :

   Certificate file name (Nom du fichier du certificat)
   Spécifiez le nom du fichier de certificat, généralement au format `.arm` ou à un autre format acceptable, tel que `.cer`.

   Emplacement
   Spécifiez l'emplacement dans lequel vous avez sauvegardé le fichier.

   Conseil : Vous pouvez également utiliser le bouton **Browse** (Parcourir) pour sélectionner le fichier et son emplacement.

   OK Cliquez sur ce bouton pour accepter ces détails et sauvegarder le fichier dans la base de données de clés.

Résultats

Le certificat signé de l'autorité de certification est fusionné avec la demande correspondante et ajouté à la base de données de clés comme certificat serveur avec ses informations de clé privée. L'entrée de la demande est ensuite supprimée de la base de données de clés. Dans la fenêtre IBM Key Management (Gestion de clés IBM), le certificat serveur est affiché dans la liste **Personal Certificates** (Certificats personnels) avec l'étiquette affectée à la demande.

Que faire ensuite

Si ce certificat n'a pas encore été défini comme certificat par défaut (indiqué par un astérisque à gauche de l'étiquette), définissez-le comme certificat par défaut dans la base de données de clés du serveur.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

Distribution des certificats

Pour utiliser un certificat autosigné en tant que certificat de signataire, distribuez le certificat autosigné à tous les clients en *récupérant* le certificat à partir de la base de données de clés du serveur et en *ajoutant* le certificat récupéré à la base de données de clés sur chaque ordinateur client.

Extraction des certificats d'une base de données de clés

Vous pouvez extraire une copie d'un certificat de signataire ou personnel d'une base de données de clés et l'ajouter à une autre base de données de clés comme certificat de signataire. Lorsque vous extrayez un certificat, la clé publique est également extraite. Cette tâche vous permet de copier un certificat autosigné d'un ordinateur serveur vers un emplacement du réseau.

Extraction des certificats d'une base de données de clés à l'aide de `nc_gskcmd` :

Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **`nc_gskcmd`**.

Procédure

Pour extraire le certificat d'une base de données de clés, exécutez la commande suivante :

```
$NCHOME/bin/nc_gskcmd -cert -extract -db "$NCHOME/etc/security/keys/omni.kdb"
-pw password -label "keylabel" -target "$NCHOME/etc/security/keys/certname.arm"
```

Où *password* est le mot de passe de la base de données de clés, *keylabel* est la description du certificat dans la base de données de clés (définissez cette valeur sous forme de chaîne entre guillemets) et *certname* est le nom du certificat que vous souhaitez extraire. Spécifiez le chemin d'accès au certificat sous forme de chaîne entre guillemets.

Que faire ensuite

Ouvrez à présent chaque base de données de clés dans laquelle vous souhaitez ajouter le certificat extrait et ajouter ce dernier en tant que certificat de signataire.

Tâches associées:

«Ajout de certificats d'autorités de certification», à la page 399
Lorsque vous recevez un certificat racine ou un certificat intermédiaire associé d'une autorité de certification émettrice, ajoutez le certificat à la base de données de clés sur tous les ordinateurs client et serveur qui requièrent une connexion SSL. De même, pour distribuer un certificat autosigné que vous avez extrait d'une base de données de clés de serveur, ajoutez le fichier de certificat extrait à tous les ordinateurs client.

Extraction des certificats d'une base de données de clés à l'aide d'iKeyman :

Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Procédure

Pour extraire le certificat :

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés (`omni.kdb`) à partir de laquelle vous souhaitez extraire le certificat. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Dans la zone **Key database content (Contenu de la base de données de clés)** effectuez les actions correspondantes comme suit :
   - Pour extraire un certificat personnel (comme un certificat autosigné), sélectionnez `Personal Certificates` (Certificats personnels) dans la liste déroulante. Sélectionnez le certificat que vous souhaitez extraire et cliquez sur **Extract Certificate** (Extraire le certificat).
   - Pour extraire un certificat de signataire, sélectionnez `Signer Certificates (Certificats de signataires)` dans la liste déroulante. Sélectionnez le certificat que vous souhaitez extraire et cliquez sur **Extract** (Extraire).

   La fenêtre "Extract Certificate to a File" (Extraire le certificat dans un fichier) s'affiche.
6. Complétez la fenêtre comme suit :

   Type de données
   Sélectionnez un type de données qui correspond à celui du certificat.

   Certificate file name (Nom du fichier du certificat)
   Spécifiez le nom du fichier dans lequel vous souhaitez extraire le certificat. Vous pouvez sauvegarder le fichier en tant que fichier `.arm`.

   Emplacement
   Spécifiez l'emplacement dans lequel vous souhaitez sauvegarder le fichier de certificat extrait.

   OK Cliquez sur ce bouton pour sauvegarder le certificat dans le fichier spécifié et revenir à la fenêtre IBM Key Management (Gestion des clés IBM).

Que faire ensuite

Ouvrez à présent chaque base de données de clés dans laquelle vous souhaitez ajouter le certificat extrait et ajouter ce dernier en tant que certificat de signataire.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Ajout de certificats d'autorités de certification»
Lorsque vous recevez un certificat racine ou un certificat intermédiaire associé d'une autorité de certification émettrice, ajoutez le certificat à la base de données de clés sur tous les ordinateurs client et serveur qui requièrent une connexion SSL. De même, pour distribuer un certificat autosigné que vous avez extrait d'une base de données de clés de serveur, ajoutez le fichier de certificat extrait à tous les ordinateurs client.

Ajout de certificats d'autorités de certification

Lorsque vous recevez un certificat racine ou un certificat intermédiaire associé d'une autorité de certification émettrice, ajoutez le certificat à la base de données de clés sur tous les ordinateurs client et serveur qui requièrent une connexion SSL. De même, pour distribuer un certificat autosigné que vous avez extrait d'une base de données de clés de serveur, ajoutez le fichier de certificat extrait à tous les ordinateurs client.

Avant de commencer

Si vous avez obtenu un certificat requis (ou les détails du certificat) d'une autorité de certification, sauvegardez d'abord les informations sous la forme d'un fichier texte `.arm` ou d'un autre format accepté comme `.cer`, dans un emplacement temporaire. Votre certificat autosigné extrait est déjà au format `.arm`.

Tâches associées:

«Extraction des certificats d'une base de données de clés à l'aide d'iKeyman», à la page 398
Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Ajout de certificats aux bases de données de clés à l'aide de `nc_gskcmd` :

Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS 140-2 ou si votre réseau comprend des clients Java, faites appel à l'utilitaire **`nc_gskcmd`**. **`nc_gskcmd`** ajoute une extension Basic Constraints (Contraintes de base) au certificat de l'autorité de certification.

Procédure

Pour ajouter le certificat à une base de données de clés, exécutez la commande suivante :

```
$NCHOME/bin/nc_gskcmd -cert -add -db "$NCHOME/etc/security/keys/omni.kdb"
-pw mot_de_passe -label "intitulé_de_clé" -file "nom_certificat.arm"
```

Où *mot_de_passe* est le mot de passe de la base de données de clés, *intitulé_de_clé* est la description du certificat dans la base de données de clés (définissez cette valeur sous forme de chaîne entre guillemets) et *nom_certificat* est le nom du certificat que vous souhaitez extraire. Spécifiez le nom du fichier certificat sous

forme de chaîne entre guillemet.

Ajout de certificats aux bases de données de clés à l'aide d'iKeyman :

Pour les déploiements ne fonctionnant pas en mode FIPS 140-2 ou ne contenant pas de client Java nécessitant des communications chiffrées, vous pouvez utiliser l'outil graphique iKeyman.

Procédure

Pour ajouter un certificat à une base de données de clés :

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom du fichier et l'emplacement de la base de données de clés (`omni.kdb`) à laquelle vous souhaitez ajouter le certificat. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Dans la zone **Key database content (Contenu de base de données de clés)**, sélectionnez `Signer Certificates (Certificats de signataires)` dans la liste déroulante puis cliquez sur **Ajouter**.
6. Indiquez les informations suivantes :

   Certificate file name (Nom du fichier du certificat)
   Spécifiez le nom du fichier autosigné (ou autre) que vous souhaitez ajouter à cette base de données.

   Emplacement
   Spécifiez l'emplacement dans lequel vous avez sauvegardé le fichier.

   Conseil : Vous pouvez également utiliser le bouton **Browse** (Parcourir) pour sélectionner le fichier et son emplacement.

   OK Cliquez sur ce bouton pour acceptez ces détails.

   La fenêtre "Enter a Label" (Entrer une étiquette) s'ouvre.
7. Entrez une étiquette significative pour le certificat et cliquez sur **OK** pour sauvegarder le fichier dans la base de données de clés.

Résultats

Le certificat est répertorié dans la fenêtre IBM Key Management (Gestion des clés IBM), comme une de vos entrées de la liste **Signer Certificates** (Certificats de signataires). L'étiquette que vous avez entré est utilisée pour identifier le certificat.

Que faire ensuite

Après avoir ajouté le certificat à la base de données de clés, vérifiez que l'extension Basic Constraints (Contraintes de base) a été définie pour le certificat. Une extension Basic Constraints (Contraintes de base) est requise pour tous les certificats d'autorité de certification utilisés pour signer les certificats de serveur. Pour rechercher l'extension Basic Constraints :

1. Dans l'interface graphique iKeyman, sélectionnez le certificat concerné dans la liste des certificats de signataires et cliquez sur **View/Edit**(Afficher/Editer).
2. Dans la fenêtre Key Information (Informations sur la clé) cliquez sur **View Details**(Afficher les détails).
3. Dans la fenêtre suivante, recherchez dans la liste **Zone** un nœud appelé **Basic Constraints** (Contraintes de base) et cliquez sur l'élément **Valeur** sous ce nœud. Dans la zone **Valeur** sous la liste **Zone**, l'entrée suivante doit être affichée : **CA:true**.

Tâches associées:

«Démarrage d'iKeyman»
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

Gestion des certificats numériques

Exécutez ces tâches dans le cadre de la gestion d'un réseau protégé SSL.

Démarrage d'iKeyman

Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

Pourquoi et quand exécuter cette tâche

Pour démarrer iKeyman :

Procédure

Effectuez les actions correspondant à votre système d'exploitation :

Système d'exploitation	Action
UNIX	Dans la ligne de commande, entrez la commande suivante : `$NCHOME/bin/nc_ikeyman`
Windows	Effectuez une des actions suivantes : • Dans la ligne de commande, entrez la commande suivante : `%NCHOME%\bin\nc_ikeyman.bat` **Conseil :** Utilisez cette option comme option privilégiée pour démarrer iKeyman afin de garantir que l'emplacement de la base de données de clé par défaut soit toujours défini sur `%NCHOME%\ini\security\keys\` dans l'interface graphique. • Dans l'Explorateur Windows, accédez à l'emplacement `%NCHOME%\bin` et cliquez deux fois sur le fichier `nc_ikeyman.vbs`.

La fenêtre IBM Key Management (Gestion des clés IBM) s'ouvre.

Spécification du certificat par défaut

Vous pouvez spécifier un certificat par défaut si plusieurs certificats personnels sont stockés dans la base de données de clés. Par exemple, après avoir reçu un certificat serveur d'une autorité de certification, vous pouvez commencer à l'utiliser en le définissant par défaut.

Pourquoi et quand exécuter cette tâche

Pour spécifier le certificat par défaut :

Procédure

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés qui contient le certificat que vous souhaitez définir comme certificat par défaut. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Dans la zone **Key database content (Contenu de base de données de clés)**, sélectionnez `Personal Certificates (Certificats personnels)` dans la liste déroulante.
6. Sélectionnez le certificat que vous souhaitez définir par défaut et cliquez sur **View/Edit** (Afficher/Editer). La fenêtre Key Information (Informations sur la clé) s'ouvre. Elle fournit un récapitulatif des détails du certificat.
7. Cochez la case **Set the certificate as the default** (Définir comme certificat par défaut) et cliquez sur **OK**.

Résultats

Dans la fenêtre IBM Key Management (Gestion des clés IBM), l'étiquette est annotée avec un astérisque (*) .

Ce certificat est affiché pour les clients qui se connectent au serveur Tivoli Netcool/OMNIbus et ils peuvent utiliser la clé publique du certificat pour chiffrer les données qu'ils envoient au serveur.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

Affichage des détails du certificat

Vous pouvez examiner le contenu de tout certificat de signataire ou personnel stocké dans la base de données de clés. Lorsque vous examinez un tel certificat, vous pouvez choisir de le définir comme certificat racine de confiance ou comme certificat par défaut.

Pourquoi et quand exécuter cette tâche

Pour afficher les détails d'un certificat :

Procédure

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés (`omni.kdb`) qui contient le certificat à afficher. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Dans la zone **Key database content (Contenu de la base de données de clés)** effectuez les actions correspondantes comme suit :
   - Pour afficher un certificat de signataire, sélectionnez `Signer Certificates (Certificats de signataires)` dans la liste déroulante.
   - Pour afficher un certificat personnel, sélectionnez `Personal Certificates (Certificats personnels)` dans la liste déroulante.
6. Sélectionnez le certificat que vous souhaitez afficher et cliquez sur **View/Edit** (Afficher/Editer). La fenêtre Key Information (Informations sur la clé) s'ouvre. Elle fournit un récapitulatif des détails du certificat.
7. Si vous affichez un certificat de signataire, vous pouvez le définir comme certificat racine de confiance en cochant la case **Set the certificate as a trusted root** (Définir le certificat comme racine de confiance). Si vous affichez un certificat personnel qui n'est pas celui par défaut, vous pouvez le définir comme certificat par défaut en cochant la case **Set the certificate as the default root** (Définir le certificat comme racine par défaut).
8. Pour afficher les détails complets sur le certificat, cliquez sur **View Details** (Afficher les détails).

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Création d'une base de données de clés à l'aide de nc_gskcmd», à la page 381
Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

Suppression de certificats

Vous pouvez supprimer des certificats de signataire ou personnel dont vous n'avez plus besoin de votre base de données de clés.

Pourquoi et quand exécuter cette tâche

Pour supprimer un ou plusieurs certificats de la base de données de clés :

Procédure

1. Facultatif : Créez une sauvegarde du certificat en l'extrayant dans un emplacement différent, au cas où vous en avez besoin ultérieurement. Vous pouvez effectuer cette procédure pour un ou plusieurs certificats à supprimer.
2. Démarrez iKeyman.
3. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
4. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés (`omni.kdb`) qui contient des certificats à supprimer. Cliquez ensuite sur **OK**.
5. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
6. Dans la zone **Key database content (Contenu de la base de données de clés)** effectuez les actions correspondantes comme suit :
   - Pour supprimer des certificats de signataire, sélectionnez l'option `Signer Certificates (Certificats de signataires)` dans la liste déroulante.
   - Pour supprimer des certificats numériques personnels, sélectionnez l'option `Personal Certificates (Certificats personnels)` dans la liste déroulante.
7. Sélectionnez les certificats à supprimer. Vous pouvez sélectionner plusieurs certificats en utilisant la touche Ctrl ou Maj.
8. Cliquez sur **Supprimer** et confirmez la suppression.

Résultats

Chaque certificat supprimé est supprimé de la fenêtre IBM Key Management (Gestion des clés IBM) et de la base de données.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Création d'une base de données de clés à l'aide de nc_gskcmd», à la page 381
Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

«Extraction des certificats d'une base de données de clés», à la page 397
Vous pouvez extraire une copie d'un certificat de signataire ou personnel d'une base de données de clés et l'ajouter à une autre base de données de clés comme certificat de signataire. Lorsque vous extrayez un certificat, la clé publique est également extraite. Cette tâche vous permet de copier un certificat autosigné d'un ordinateur serveur vers un emplacement du réseau.

Modification du mot de passe de la base de données de clés

Il est recommandé de modifier régulièrement le mot de passe de la base de données de clés. Dans l'interface graphique d'iKeyman, vous êtes également invité à modifier le mot de passe si vous tentez d'ouvrir la base de données de clés avec un mot de passe expiré.

Pourquoi et quand exécuter cette tâche

Pour modifier le mot de passe de la base de données de clés comme partie de votre procédure standard :

Procédure

1. Démarrez iKeyman.
2. Dans la fenêtre IBM Key Management (Gestion des clés IBM), cliquez sur **Key Database File (Fichier de la base de données de clés)** > **Ouvrir**.
3. Dans la fenêtre Ouvrir, spécifiez le nom et l'emplacement du fichier de la base de données de clés (`omni.kdb`) dont le mot de passe doit être modifié. Cliquez ensuite sur **OK**.
4. Entrez le mot de passe actuel de la base de données de clés dans la fenêtre Password Prompt (Invite du mot de passe) et cliquez sur **OK**. Le contenu de la base de données de clés s'affiche dans la fenêtre IBM Key Management (Gestion des clés IBM).
5. Cliquez sur **Key Database File (Fichier de base de données de clés)** > **Modifier le mot de passe**. La fenêtre Modifier le mot de passe s'affiche.
6. Complétez cette fenêtre comme suit :

   Nouveau mot de passe
   Entrez un mot de passe. Au fur et à mesure que vous tapez les caractères, une indication de la force du mot de passe est fournie.

   Remarque : Les mots de passe sont sensibles à la casse, de sorte que lorsque vous devez spécifier le mot de passe pour ouvrir la base de données de clés, vous devez utiliser la casse correcte pour éviter des erreurs.

   Confirmer le nouveau mot de passe
   Entrez de nouveau le mot de passe.

   Set expiration time (Définir le délai d'expiration)
   Cochez cette case pour spécifier une période après laquelle le mot de passe arrivera à expiration. Entrez la période en jours. La valeur par défaut est `60` jours. Si cette case est décochée, le mot de passe n'expirera jamais.

   Stash the password to a file? (Stocker le mot de passe dans un fichier ?)
   Cochez cette case pour enregistrer le mot de passe dans un format chiffré dans un fichier de dissimulation. Cette condition est obligatoire pour Tivoli Netcool/OMNIbus.

   OK Cliquez sur ce bouton pour sauvegarder le mot de passe et fermer la fenêtre.

Résultats

Le mot de passe est chiffré et sauvegardé dans le fichier stash `omni.sth` au même emplacement que la base de données de clés.

Tâches associées:

«Démarrage d'iKeyman», à la page 401
Vous pouvez effectuer la majorité des tâches de gestion de certificat depuis l'interface graphique d'iKeyman.

«Création d'une base de données de clés à l'aide de nc_gskcmd», à la page 381
Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

Options de ligne de commande nc_gskcmd

L'utilitaire de ligne de commande **nc_gskcmd** fournit davantage de fonctionnalités que l'interface graphique iKeyman.

Pour gérer les certificats à partir de la ligne de commande, exécutez la commande suivante :

```
$NCHOME/bin/nc_gskcmd objet action options
```

Dans cette commande :

- *objet* est une option de ligne de commande qui indique qu'une action est requise sur un objet, généralement une base de données de clés, un certificat ou une demande de certificat. Cette option doit être la première option de ligne de commande indiquée.
- *action* est une option de ligne de commande qui définit une action spécifique à prendre sur l'objet. Cette option doit être la deuxième option de ligne de commande indiquée.
- *options* sont des options de ligne de commande obligatoires et facultatives qui sont valides pour la paire *objet*/*action* indiquée. Ces options de ligne de commande peuvent être dans n'importe quel ordre.

Remarque : Toutes les actions et leurs options associées ne sont pas applicables à une utilisation dans Tivoli Netcool/OMNIbus.

Pour plus d'informations sur la syntaxe de ces options de ligne de commande, voir *IBM Global Security Kit Secure Sockets Layer Introduction and iKeyman User's Guide*.

Le tableau suivant répertorie chaque *objet* et son jeu d'*actions* associées pour la commande **nc_gskcmd**.

Tableau 80. Objets et actions correspondantes pour nc_gskcmd

Objet	Action	Description
-keydb	-changepw	Modifie le mot de passe d'une base de données de clés.
	-convert	Convertit le format de la base de données de clés.
	-create	Crée une base de données de clés.
	-delete	Supprime la base de données de clés.
	-expiry	Affiche la date d'expiration du mot de passe d'une base de données de clés.
	-list	Affiche les types pris en charge de base de données de clés.
	-stash	Dissimule le mot de passe d'une base de données de clés dans un fichier.
-cert	-add	Ajoute un certificat d'autorité de certification d'un fichier dans une base de données de clés.

Tableau 80. Objets et actions correspondantes pour nc_gskcmd (suite)

Objet	Action	Description
	`-create`	Crée un certificat autosigné.
	`-delete`	Supprime un certificat.
	`-details`	Affiche les détails d'un certificat spécifique.
	`-export`	Exporte un certificat personnel et sa clé privée associée d'une base de données de clés vers un fichier PKCS#12 ou une autre base de données de clés.
	`-extract`	Extrait un certificat d'une base de données de clés.
	`-getdefault`	Affiche le certificat personnel par défaut.
	`-import`	Importe un certificat d'une base de données de clés ou un fichier PKCS#12.
	`-list` *chaîne*	Répertorie les certificats dans la base de données de clés. Les valeurs sont `all`, `personal`, `CA` et `site`. La valeur par défaut est de répertorier tous les certificats. Si vous indiquez `-list` tout seul, tous les certificats sont également répertoriés.
	`-modify`	Modifie un certificat. **Remarque :** Actuellement, la seule zone qui peut être modifiée est la zone Certificate Trust (Certificat de confiance).
	`-receive`	Reçoit un certificat d'un fichier dans la base de données de clés.
	`-setdefault`	Définit un certificat personnel en tant que certificat par défaut.
	`-sign`	Signe un certificat qui est stocké dans un fichier avec un certificat lui-même stocké dans la base de données de clés, puis stocke le certificat signé en résultant dans un fichier.
`-certreq`	`-create`	Crée une demande de certificat.
	`-delete`	Supprime une demande de certificat d'une base de données de demandes de certificats.
	`-details`	Affiche les détails d'une demande de certificat spécifique.
	`-extract`	Extrait une demande de certificat d'une base de données de demandes de certificats vers un fichier.
	`-list`	Répertorie toutes les demandes de certificats dans la base de données de demandes de certificats.
	`-recreate`	Recrée une demande de certificat.
`-help`		Affiche les informations d'aide de la commande **`nc_gskcmd`**.
`-version`		Affiche les informations de version de la commande **`nc_gskcmd`** et quitte.

Le tableau suivant répertorie les *options* valides pour la paire *objet*/*action* indiquée.

Tableau 81. Options pour les paires objet/action

Option	Description
`-ca` TRUE | FALSE	Ajoute l'extension Basic Constraint (contrainte de base) au certificat autosigné. **Remarque :** Ne créez pas de certificats autosignés avec `-ca` paramétré sur `false`.
`-crypto` *chaîne*	Indique une opération d'unité cryptographique PKCS#11.
`-db` *chaîne*	Indique le nom de chemin qualifié complet d'une base de données de clés.

Tableau 81. Options pour les paires objet/action (suite)

Option	Description
`-default_cert` YES | NO	Définit un certificat en tant que certificat par défaut pour l'utiliser lors de l'authentification client. La valeur par défaut est `no`.
`-dn` *chaîne*	Indique le nom distinctif X.500. Entrez la valeur sous forme de chaîne entre guillemets au format suivant : "CN=*nom_usuel*, O=*organisation*, OU=*unité_organisationnelle*, L=*emplacement*, ST=*province_état*, ZIP=*code_postal*, C=*pays*" Par exemple : "CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott,ST=NY,ZIP=13760,C=country" Seul CN est obligatoire.
`-encryption` *chaîne*	Indique la longueur du chiffrement qui est utilisée dans la commande d'exportation du certificat. La valeur peut être `strong` ou `weak`. La valeur par défaut est `strong`.
`-expire` *entier*	Indique la durée avant l'expiration d'un mot de passe de certificat ou de base de données de clés (en jours). La durée est de `0` à `7300` jours (soit 20 ans). La valeur par défaut est de `60` jours pour un mot de passe de base de données de clés. Une expiration de `0` signifie que le mot de passe associé à la base de données de clés n'expire jamais. Pour un certificat autosigné, indiquez un intervalle entre `366` et `7300`.
`-file` *chaîne*	Indique le nom de fichier d'un certificat ou d'une demande de certificat (en fonction de l'*objet* indiqué).
`-format` *chaîne*	Indique le format d'un certificat. La valeur peut être `ascii` pour le code ASCII Base64_encoded ou `binary` pour les données DER binaires. La valeur par défaut est `ascii`.
`-label` *chaîne*	Indique le texte descriptif utilisé pour identifier un certificat ou une demande de certificat dans la base de données de clés. **Conseil :** Pour vous aider à identifier le certificat comme étant autosigné dans l'interface graphique utilisateur iKeyman, vous pouvez ajouter les mots `Autorité de certification` ou `AC` dans le texte de l'étiquette.
`-new_format` *chaîne*	Indique le nouveau format de la base de données de clés.
`-new_label` *chaîne*	Indique un nouveau label de certificat ou un alias pour remplacer le label de certificat existant.
`-new_pw` *chaîne*	Indique un nouveau mot de passe de base de données de clés.
`-old_format` *chaîne*	Indique l'ancien format de la base de données de clés.
`-pfx`	Indique un fichier PKCS#12 sous forme de fichier Microsoft `.pfx`.

Tableau 81. Options pour les paires objet/action (suite)

Option	Description
`-pw` *chaîne*	Indique le mot de passe de la base de données de clés ou du fichier PKCS#12. En mode FIPS 140-2, les mots de passe pour les bases de données de clés doivent répondre aux exigences suivantes. Si les mots de passe ne respectent pas ces exigences, la base de données de clés est créée, mais vous ne pouvez pas créer, signer ni recevoir de certificats et une erreur est consignée dans le journal du serveur ObjectServer. • La longueur minimale du mot de passe est de 14 caractères. • Un mot de passe doit contenir au moins un caractère en minuscule, un caractère en majuscule et un chiffre ou caractère spécial. • Chaque caractère ne doit pas apparaître plus de trois fois dans un mot de passe. • Il ne peut pas y avoir plus de deux caractères consécutifs du mot de passe identiques. • Tous les caractères figurent dans le jeu de caractères imprimable ASCII standard compris entre 0x20 et 0x7E inclus.
`-size` *entier*	Indique la taille de clé. Les valeurs sont `512`, `1024` et `2048`. La valeur par défaut est `1024`.
`-stash`	Dissimule le mot de passe de la base de données de clés dans un fichier *nom_base-de-données_clés*`.sth` dans le même emplacement que le fichier de base de données de clés.
`-san_dnsname`	Ajoute un ou plusieurs noms de serveur de nom de domaine à l'attribut Subject Alternate Name (Nom alternatif du sujet). Doit être dans la "syntaxe préférentielle pour les noms" conformément à la norme RFC 1034.
`-san_emailaddr`	Ajoute une ou plusieurs adresses email à l'attribut Subject Alternate Name (Nom alternatif du sujet). Doit être une adresse "addr-spec" conformément à la norme RFC 822.
`-san_ipaddr`	Ajoute une ou plusieurs adresses IP à l'attribut Subject Alternate Name (Nom alternatif du sujet). Doit être une chaîne conformément aux normes RFC 1338 et RFC 1519.
`-secondaryDB`	Indique la prise en charge d'une deuxième base de données de clés pour les opérations d'unités PKCS#11.
`-secondaryDBpw`	Indique le mot de passe de la deuxième base de données de clés pour les opérations d'unités PKCS#11.
`-showOID`	Affiche l'intégralité du certificat ou de la demande de certificat.
`-target` *chaîne*	Indique le fichier ou la base de données de clés de destination où un certificat est exporté ou importé.
`-target_pw` *chaîne*	Indique le mot de passe de la base de données de clés si `-target` indique une base de données de clés.
`-target_type` *chaîne*	Indique un type pour la base de données indiquée par l'option de ligne de commande `-target`. La valeur admissible pour Tivoli Netcool/OMNIbus est `cms`, qui indique une base de données de clés CMS.
`-tokenlabel` *chaîne*	Indique le libellé d'une unité cryptographique PKCS#11.
`-trust` *chaîne*	Indique le statut de confiance d'un certificat d'une autorité de certification. Cette valeur peut être `enable` ou `disable`. La valeur par défaut est `enable`.

Tableau 81. Options pour les paires objet/action (suite)

Option	Description
`-type` *chaîne*	Indique le type de base de données. La valeur admissible pour Tivoli Netcool/OMNIbus est `cms`, qui indique une base de données de clés CMS.
`-usereasoncode`	Renvoie un code d'erreur à valeurs multiples si la commande **`nc_gskcmd`** échoue ou `0` si elle aboutit.
`-x509version` *entier*	Indique la version du certificat X.509 à créer. Les valeurs sont `1`, `2` et `3`. La valeur par défaut est `3`.

Exemple de fichiers de clés

Tivoli Netcool/OMNIbus inclut un script de démonstration qui génère des exemples de fichiers de clés. Le script est destiné à être utilisé dans des preuves de concept et à fournir des recommandations sur l'utilisation de l'utilitaire de gestion de ligne de commande **`nc_gskmd`**.

Pour exécuter le script, utilisez la commande suivante :

UNIX `$NCHOME/bin/create_example_keys.sh`

Windows `%NCHOME%\bin\create_example_keys.bat`

Pour utiliser le script avec des paramètres différents, faites une copie du script puis éditez et exécutez la copie.

Le script crée un ensemble d'exemples de magasins de clés qui contiennent un certificat d'autorité de certification (CA) avec une clé privée et un certificat serveur avec une clé privée. Les exemples de fichiers de clés sont créés dans le répertoire suivant :

UNIX `$NCHOME/etc/security/keys`

Windows `%NCHOME%\ini\security\keys`

Remarque : Le script n'écrase aucun des fichiers de clés existants. Si vous stockez déjà des fichiers de clés dans ce répertoire, vous devrez peut-être les supprimer avant d'exécuter le script. Vous pouvez également modifier les chemins de répertoire spécifiés par les paramètres de script suivants avant d'exécuter le script :

- `CA_KDB`
- `OMNI_KDB`
- `CLIENT_KDB`

A des fins de démonstration, le script s'exécute dans une installation unique de Tivoli Netcool/OMNIbus. Trois fichiers de clés différents sont créés et utilisés. Dans un système réel, chaque fichier de clés serait situé sur un ordinateur différent. Le certificat et les fichiers de demande de certificat identifiés par `$CERT_FILE` et `$REQ_FILE` seraient envoyés d'un ordinateur à l'autre à l'aide d'un mécanisme tel que la messagerie électronique sécurisée ou le protocole FTP. Notez que, dans les systèmes réels, les composants Tivoli Netcool/OMNIbus peuvent uniquement accéder à un fichier de clés qui doit être nommé `omni.kdb`.

Les fichiers de clés suivants (`.kdb`) sont créés :

- `ca.kdb` contient le certificat de l'autorité de certification et une clé privée.

  Il s'agit d'informations extrêmement sensibles qui sont utilisées pour signer des certificats de serveur. Vous devez garantir la sécurité de ce fichier de clés, conformément à la politique de sécurité de votre organisation. Ce fichier de clés n'est pas accessible par Tivoli Netcool/OMNIbus.
- `omni.kdb` contient le certificat de l'autorité de certification, le certificat du serveur et la clé privée.

  Conservez ce fichier de clés uniquement sur l'ordinateur serveur. Ce fichier de clés est nommé `omni.kdb` de sorte qu'il peut être utilisé par les deux programmes client et serveur dans cette installation Tivoli Netcool/OMNIbus.
- `client/omni.kdb` contient le certificat de l'autorité de certification.

  Vous devez distribuer ce fichier de clés, ou son contenu, à chaque installation de Tivoli Netcool/OMNIbus à partir de laquelle les programmes client vont se connecter au serveur. Pour permettre aux programmes client de Tivoli Netcool/OMNIbus d'utiliser ce fichier de clés, tous les fichiers qui constituent le fichier de clés doivent être placés dans le répertoire suivant de l'installation du client :

  UNIX `$NCHOME/etc/security/keys`

  Windows `%NCHOME%\ini\security\keys`

Chaque fichier de clés comprend un fichier principal appelé *nom_base*`.kdb` et un certain nombre d'autres fichiers ayant le même *nom_base* mais des extensions différentes. Tous les fichiers sont requis et doivent être transférés ou sauvegardés ensemble.

Si plusieurs serveurs différents doivent être exécutés dans la même installation de Tivoli Netcool/OMNIbus, créez leurs demandes de certificat à partir du même fichier de clés. Pour chaque serveur, répétez les commandes `-certreq -create`, `-cert -sign` et `-cert -receive` illustrées dans le script.

Si les programmes client se connectent à plusieurs serveurs, avec des certificats signés par différentes autorités de certification, importez le certificat de chaque autorité de certification dans le fichier de clés de l'installation client. Pour chaque autorité de certification, répétez les commandes `-cert -extract` et `-cert -add` illustrées dans le script.

Chapitre 15. Configuration IPv6

Tivoli Netcool/OMNIbus offre la prise en charge des protocoles IPv4 et IPv6. Les composants peuvent à présent fonctionner et coexister sur un réseau prenant en charge une configuration IPv4 seulement, IPv6 seulement ou IPv4 et IPv6.

Les composants serveur Tivoli Netcool/OMNIbus fonctionnent dans des environnements IPv6 et IPv4 de la manière suivante :

- Le serveur ObjectServer peut traiter des événements qui proviennent de réseaux IPv4 et IPv6. Lorsque le serveur ObjectServer s'exécute sur un hôte à double pile, le nom d'hôte renvoyé au client en réponse à une commande est le nom d'hôte du serveur correspondant à la version IP que le client exécute. Par exemple, un client exécutant IPv4 reçoit le nom d'hôte IPv4 du serveur ObjectServer, et un client exécutant IPv6 reçoit le nom d'hôte IPv6 du serveur ObjectServer.
- Dans des environnements doubles IPv4 et IPv6, les passerelles unidirectionnelles et bidirectionnelles du serveur ObjectServer peuvent écouter sur les deux interfaces, sur le socket de communication.
- Le serveur proxy peut prendre en charge les connexions entre les sondes et les serveurs ObjectServer qui s'exécutent sur des hôtes IPv4 et IPv6.
- Dans des environnements doubles IPv4 et IPv6, l'agent de processus peut écouter sur les deux interfaces, sur le socket de communication.

Les formats d'adresse IPv6 suivants sont pris en charge :

- Huit groupes de quatre caractères hexadécimaux, séparés par deux points, par exemple ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
- Les segments de 16 bits égaux à zéro peuvent être remplacés par deux points (:).

  Par exemple, l'adresse 1010:0000:0000:0000:ABCD:EF01:2345:6789 peut être écrite de la manière suivante : 1010::ABCD:EF01:2345:6789.
- Les adresses IPv4 peuvent être représentées en tant qu'adresses IPv6. Par exemple :
  - 0:0:0:0:0:0:192.101.50.5
  - 0:0:0:0:0:FFFF:103.27.35.8

    Ces adresses peuvent également être représentées de la manière suivante :
  - ::192.101.50.5
  - ::FFFF:103.27.35.8

Configuration de la prise en charge d'IPv6

Lorsque vous installez ou modifiez un composant serveur sur n'importe quel hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour communiquer avec d'autres composants. Les informations de communication des serveurs sont configurées à l'aide de l'éditeur de serveur.

Lors de la configuration des informations pour les communications serveur dans un environnement double IPv6 et IPv4, vous pouvez utiliser des adresses IPv6, des adresses IPv4 ou des noms d'hôte pour indiquer le nom de l'ordinateur sur lequel

le composant serveur est installé. Si vous souhaitez utiliser un nom d'hôte au lieu d'une adresse IPv6, vous devez configurer la recherche d'hôtes sur votre système d'exploitation.

Configuration UNIX

Après avoir utilisé l'éditeur de serveur (ou **nco_xigen**) pour configurer les communications entre composants avec des adresses IPv6 ou IPv4, les informations pour les communications entre serveurs sont sauvegardées dans un fichier d'interfaces $NCHOME/etc/interfaces.*arch*, où *arch* représente le répertoire de votre système d'exploitation. Si vous avez une installation répartie, comprenant différents composants Tivoli Netcool/OMNIbus s'exécutant sur plusieurs systèmes de votre réseau, vous devez distribuer le fichier d'interfaces qui contient les informations de communication à chaque système Tivoli Netcool/OMNIbus.

Si vous exécutez des composants Tivoli Netcool/OMNIbus sur plusieurs systèmes d'exploitation UNIX, vous devez générer des fichier d'interfaces compatibles pour chaque système d'exploitation et distribuer les fichiers aux hôtes pertinents. Vous pouvez configurer les communications entre composants sur un ordinateur Tivoli Netcool/OMNIbus et, à partir de cet ordinateur, générer des fichiers d'interfaces pour tous les systèmes d'exploitation disponibles. Vous pouvez générer des fichiers d'interfaces pour chaque système d'exploitation à partir de la ligne de commande ou utiliser l'éditeur de serveur pour générer des fichiers d'interfaces de la manière suivante :

- A partir de la ligne de commande, entrez la commande suivante :

  ```
  $NCHOME/bin/nco_igen -all
  ```

  Un fichier d'interfaces appelé $NCHOME/etc/interfaces.*archive* est généré pour chaque système d'exploitation, où *archive* représente le nom du système d'exploitation UNIX, par exemple, interfaces.hpux11 et interfaces.solaris2. Copiez le fichier d'interfaces du système d'exploitation pertinent vers le répertoire $NCHOME/etc sur chaque ordinateur hôte.
- A partir de l'éditeur de serveur, indiquez vos paramètres de communication puis cochez la case **Generate All (Générer tout)**. Cliquez sur le bouton **Appliquer** pour générer des fichiers d'interfaces appelés $NCHOME/etc/interfaces.*archive*, où *archive* représente les noms des systèmes d'exploitation UNIX individuels. Copiez le fichier d'interfaces du système d'exploitation pertinent vers le répertoire $NCHOME/etc sur chaque ordinateur hôte.

Exemple de configurations IPv4 et IPv6 dans le fichier omni.dat

Sous UNIX, le fichier de données de connexion $NCHOME/etc/omni.dat est utilisé pour créer le fichier d'interfaces pour les communications Tivoli Netcool/OMNIbus. Voici des exemples de paramètres IPv4 et IPv6 dans ce fichier.

Exemple : configuration du fichier omni.dat avec un nom d'hôte et une adresse IPv6

Voici des exemples d'entrées dans le fichier omni.dat avec un nom d'hôte et une adresse IPv6 :

```
[NCOMS]
{
        Primary:        presley 9000
}
```

```
[BARROW]
{
        Primary:        fec0:0000:0000:7777:0218:fcef:fe8c:4f3b 8002
}
```

Exemple : configuration du serveur ObjectServer IPv4 et IPv6 double pile pour écouter sur les ports IPv4 et IPv6

Pour activer les sondes sur un ordinateur IPv6 en vue d'une connexion à un ordinateur ObjectServer IPv4 et IPv6 double pile, vous devez configurer un serveur ObjectServer de sauvegarde à l'aide de l'adresse IPv6 du serveur ObjectServer. Dans l'exemple de fichier `omni.dat`, 192.168.0.1 est l'adresse IPv4 du serveur ObjectServer IPv4 et IPv6 double pile et 2094:82a:2a6e:123:503:badd:fe43:f552 est son adresse IPv6.

```
[MAINOBJ]
{
        Primary:        192.168.0.1 4100
        Backup:         2094:82a:2a6e:123:503:badd:fe43:f552 4100
}
```

Si les noms de domaine IPv4 et IPv6 sont configurés sur votre réseau, vous pouvez également utiliser le nom de domaine qualifié complet (FQDN) de l'ordinateur ObjectServer en tant qu'entrée `Primary` dans `omni.dat`. Par exemple sf0.ipv4.*domaine*.com ou sf0.ipv6.*domaine*.com.

Configuration Windows

Sur chaque ordinateur Windows, utilisez l'éditeur de serveur pour configurer les communications entre composants avec des adresses IPv6 ou IPv4 comme requis.

Sur les ordinateurs Windows 2003, vous devez aussi installer le pilote de protocole IPv6 et configurer une adresse IPv6 externe. Vous pouvez effectuer cette tâche à partir du Panneau de configuration à l'aide de l'utilitaire **Connexions réseau**. Ouvrez la fenêtre Propriétés sous Connexion au réseau local et dans l'onglet **Général**, installez le pilote de protocole IPv6 et configurez l'adresse IPv6 externe. Pour obtenir des informations complètes sur la configuration IPv6, reportez-vous à la documentation de votre système d'exploitation.

Chargement des configurations de listes d'événements distantes à l'aide de HTTP ou de FTP sous Windows

Si vous souhaitez charger une configuration de liste d'événements (`.elc`) à partir d'un serveur distant à l'aide de HTTP ou de FTP, vous pouvez indiquer une adresse IPv4 ou IPv6 pour le nom de serveur.

Sous Windows, si vous souhaitez accéder à un fichier `.elc` sur un serveur distant à l'aide de l'adresse IPv6 du serveur, notez que la liste d'événements Windows requiert la version 7 du fichier système Windows, `wininet.dll`. Cette version du fichier prend en charge les adresses littérales IPv6 dans les noms d'hôte et est disponible à partir d'Internet Explorer 7. Par conséquent, vous devez vérifier que l'une des conditions suivantes est remplie :

- La version 7 de `wininet.dll` est installée sur l'ordinateur à partir duquel vous exécutez la commande **`NCOEvent`**. Ce fichier est généralement stocké dans `C:\WINDOWS\system32`.
- Internet Explorer 7 est installé.

Conseil : Il peut également être utile de vérifier si la liste d'événements peut charger le fichier `.elc`. Pour ce faire, entrez le format IPv6 de l'adresse URL vers le fichier dans la zone d'**adresse** d'un navigateur Web pour voir si vous pouvez accéder au fichier `.elc`.

Pour de plus amples informations sur l'ouverture des configurations de listes d'événements à partir de serveurs distants, voir *IBM Tivoli Netcool/OMNIbus User's Guide*.

Configuration du fichier de règles de la sonde

Vous pouvez inclure un certain nombre de fichiers de règles secondaires dans votre fichier de règles principal à l'aide de l'instruction `include`.

Si vous souhaitez inclure un fichier de règles de sonde distant stocké sur un serveur Web IPv6, utilisez des crochets [] pour délimiter l'adresse IPv6 dans l'adresse Web. Exemple :

```
include "http://[fed0::7887:234:5edf:fe65:348]:8080/probewatch.rules"
```

Pour de plus amples informations sur l'imbrication de plusieurs fichiers de règles dans un fichier de règles, voir le manuel *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*.

Concepts associés:

«Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207
Lorsque vous installez ou modifiez un composant serveur sur un hôte de votre système Tivoli Netcool/OMNIbus, vous devez configurer le composant pour qu'il communique avec d'autres composants à l'aide de l'éditeur de serveur.

Tâches associées:

«Configuration d'installations réparties», à la page 218
Vous pouvez exécuter différents composants Tivoli Netcool/OMNIbus sur plusieurs systèmes de votre réseau. Vous pouvez par exemple exécuter un serveur ObjectServer sur un ordinateur, une passerelle sur un autre ordinateur et un serveur proxy sur un troisième ordinateur.

Chapitre 16. Support multiculturel

Tivoli Netcool/OMNIbus utilise la bibliothèque ICU (International Components for Unicode) pour la conversion des jeux de caractères et prend en charge les codages de caractères prenant en charge ICU.

ICU est une bibliothèque de globalisation multiplateforme, basée sur Unicode, qui inclut la prise en charge de la comparaison de chaînes dépendant des paramètres régionaux, la mise en forme de la date, de l'heure, des nombres, de la devise, des messages, la détection des frontières de texte et la conversion des jeux de caractères. Pour obtenir une liste des codages de caractères pris en charge, voir le site Web d'ICU à l'adresse suivante : http://www.icu-project.org/.

Les données texte sont automatiquement converties entre les codages de caractères si un client et un serveur ObjectServer utilisent des codages différents. Exécutez le serveur ObjectServer dans un codage qui inclut tous les caractères utilisés dans tous les emplacements de votre déploiement de Tivoli Netcool/OMNIbus. Si votre déploiement utilise des données en langues différentes, exécutez le serveur ObjectServer au codage UTF-8 (8-bit Unicode Transition Format) pour garantir le traitement de toutes les données texte.

Remarque : Si vous utilisez des sources d'authentification externes pour vérifier les données d'identification de l'utilisateur, vous devez établir si ces sources d'authentification prennent également en charge les caractères multi-octets. Si les caractères multi-octets ne sont pas pris en charge, vous devez spécifier les noms d'utilisateur et les mots de passe à l'aide de caractères ASCII.

Configuration de polices pour l'affichage de l'historique du client AEN

Si un événement accéléré contient des caractères en langue nationale, ces caractères peuvent être affichés de manière incorrecte dans la fenêtre Historical Data Viewer du client AEN (Accelerated Event Notification). Pour résoudre ce problème, modifiez la police utilisée dans la fenêtre Historical Data Viewer. Cette police est définie dans le fichier de propriétés AEN. Pour changer la police, procédez comme suit :

1. Ouvrez le fichier suivant :
   - UNIX *rép_base_utilisateur*/.netcool/nco_aen_settings/aen.properties
   - Windows *rép_base_utilisateur*\.netcool\nco_aen_settings\aen.properties
2. Ajoutez une ligne à la fin du fichier au format suivant :
   `system.List.font=`*`nom_police`*`,`*`style_police`*`,`*`taille_police`*

   Par exemple, si les caractère de chinois simplifié s'affichent mal, ajoutez la ligne suivante : `system.List.font=courier,BOLD,11`
3. Redémarrez le client AEN.

Configuration de votre environnement local

Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Sous UNIX et Linux

Sous UNIX et Linux, définissez une ou plusieurs variables d'environnement de localisation pour vous aider à définir les paramètres d'environnement local de votre environnement. Par exemple, sous Solaris, vous pouvez définir les variables dans `/etc/default/init`, et sous AIX, vous pouvez les définir dans `/etc/environment`.

Tableau 82. Variables d'environnement de localisation pour UNIX et Linux

Variables d'environnement	Description
LC_ALL	La valeur LC_ALL est prioritaire sur les autres valeurs de toutes les variables d'environnement. Si elle est définie, elle détermine la langue, le jeu de caractères, l'ordre de tri et les formats de données.
LC_COLLATE	Cette variable d'environnement détermine la séquence de classement (ou l'ordre de tri).
LC_CTYPE	Cette variable d'environnement définit la classification des caractères et la conversion de la casse.
LC_MESSAGES	Cette variable d'environnement définit le langage et le jeu de caractères pour les messages.
LC_MONETARY	Cette variable d'environnement définit le format des informations numériques monétaires.
LC_NUMERIC	Cette variable d'environnement définit le formatage numérique, non monétaire.
LC_TIME	Cette variable d'environnement définit les formats de date et d'heure.
LANG	Si la variable LC_ALL n'est pas définie, la valeur LANG détermine la langue, le jeu de caractères et l'ordre de tri. Différents éléments de la valeur LANG peuvent être ignorés en définissant les variables d'environnement LC_COLLATE, LC_CTYPE, LC_MESSAGE et LC_TIME.

Sous Windows

Pour définir votre environnement local sous Windows, utilisez l'élément **Paramètres régionaux** ou **Options régionales et linguistiques** du Panneau de configuration. Configurez vos paramètres de la manière suivante dans la fenêtre qui s'affiche :

1. Dans l'onglet **Formats**, sélectionnez la langue à utiliser pour afficher les dates, les heures, les monnaies et les nombres.
2. Dans la zone **Langue pour les programmes non Unicode** de l'onglet **Options avancées** ou **Administration**, sélectionnez la langue dans laquelle exécuter Tivoli Netcool/OMNIbus.

Vous devrez réamorcer votre ordinateur afin que les nouveaux paramètres prennent effet.

Leslangues définies dans ces étapes doivent être identiques.

Vous pouvez choisir d'exécuter le serveur ObjectServer, la passerelle de serveur ObjectServer, l'utilitaire **nco_dbinit**, l'utilitaire **nco_postmsg** et les sondes et passerelles individuelles au codage UTF-8 à l'aide d'une option de ligne de commande spécifique à Windows, `-utf8enabled`. Cette option de ligne de commande contrôle le codage des données transmises dans ou générées par ces applications et doit être définie sur `TRUE` pour une exécution en UTF-8. Lorsque l'option `-utf8enabled` est définie sur `FALSE` (la valeur par défaut), la page de codes système par défaut est utilisée.

Le tableau suivant décrit les codages pouvant être utilisés pour les données transmises dans ces applications et les données générées par ces applications.

Tableau 83. Codages admissibles pour l'entrée et la sortie

Application	Ligne de commande d'entrée	Fichier en entrée	Fichier de sortie
serveur ObjectServer	Les options de ligne de commande basées sur des chaînes entrées dans la ligne de commande sont codées dans la page de codes par défaut du système uniquement.	Fichier affecté : fichier de propriétés (`.props`) Si l'option `-utf8enabled` est définie sur `TRUE`, vos paramètres de propriété sont codés en UTF-8. Si l'option `-utf8enabled` est définie sur `FALSE`, vos paramètres de propriété sont codés dans la page de codes par défaut du système.	Fichiers affectés : fichier de propriétés et fichier journal (`.props` et `.log`) Si l'option `-utf8enabled` est définie sur `TRUE`, la sortie écrite dans ces fichiers est codée en UTF-8. Si l'option `-utf8enabled` est définie sur `FALSE`, les sorties du fichier sont codées dans la page de codes par défaut du système.

Tableau 83. Codages admissibles pour l'entrée et la sortie (suite)

Application	Ligne de commande d'entrée	Fichier en entrée	Fichier de sortie
Passerelle ObjectServer	Les options de ligne de commande basées sur des chaînes entrées dans la ligne de commande sont codées dans la page de codes par défaut du système uniquement.	Fichiers affectés : fichier de mappage et fichier de propriétés (`.map` et `.props`) Si l'option `-utf8enabled` est définie sur `TRUE`, les paramètres de votre fichier de propriétés et de votre fichier de mappage sont codés en UTF-8. Si l'option `-utf8enabled` est définie sur `FALSE`, les paramètres de votre fichier de propriétés et de votre fichier de mappage sont codés dans la page de codes par défaut du système.	Fichier affecté : fichier journal (`.log`) Si l'option `-utf8enabled` est définie sur `TRUE`, la sortie écrite dans ce fichier est codée en UTF-8. Si l'option `-utf8enabled` est définie sur `FALSE`, la sortie du fichier est codée dans la page de codes par défaut du système.
`nco_dbinit`	Les options de ligne de commande basées sur des chaînes entrées dans la ligne de commande sont codées dans la page de codes par défaut du système uniquement.	Fichiers affectés : fichiers d'importation SQL et fichier de propriétés (`.sql` et `.props`) Si l'option `-utf8enabled` est définie sur `TRUE`, vos paramètres de propriété et SQL sont codés en UTF-8. Si l'option `-utf8enabled` est définie sur `FALSE`, vos paramètres de propriété et SQL sont codés dans la page de codes par défaut du système.	Non applicable

Tableau 83. Codages admissibles pour l'entrée et la sortie (suite)

Application	Ligne de commande d'entrée	Fichier en entrée	Fichier de sortie
nco_postmsg	Les options de ligne de commande basées sur des chaînes entrées dans la ligne de commande sont codées dans la page de codes par défaut du système uniquement.	Fichier affecté : fichier de propriétés (.props) Si l'option -utf8enabled est définie sur TRUE, vos paramètres de propriété sont codés en UTF-8. Si l'option -utf8enabled est définie sur FALSE, vos paramètres de propriété sont codés dans la page de codes par défaut du système.	Fichier affecté : fichier journal (.log) Si l'option -utf8enabled est définie sur TRUE, la sortie écrite dans ce fichier est codée en UTF-8. Si l'option -utf8enabled est définie sur FALSE, la sortie du fichier est codée dans la page de codes par défaut du système.

Pour utiliser le codage UTF-8, créez et exécutez le serveur ObjectServer dans ce codage et déterminez si les sondes et passerelles prises en charge et l'utilitaire **nco_postmsg** doivent aussi être exécutés en UTF-8, ou si ces applications client doivent être exécutées dans l'environnement local du système par défaut. Pour obtenir des informations sur les sondes et les passerelles qui peuvent s'exécuter au codage UTF-8 sous Windows, consultez les publications des sondes et passerelles individuelles. Si vous utilisez SSL, notez que le chemin d'accès à la base de données de clés (%NCHOME%\ini\security\keys) doit contenir uniquement des caractères pris en charge par la page de codes système par défaut.

Notez également que les agents de processus et les serveurs proxy ne prennent pas en charge le codage UTF-8 sous Windows et s'exécutent dans le codage système par défaut uniquement.

Informations supplémentaires

Sous Windows, l'exécution au codage UTF-8 garantit la conformité avec la norme GB18030 pour les caractères chinois. Sous UNIX et Linux, vous pouvez utiliser les variables de localisation pour indiquer un environnement local conforme à la norme GB18030. Pour l'Interface graphique Web, des étapes supplémentaires sont nécessaires pour assurer la conformité à la norme GB18030.

Si vous souhaitez ajouter un nouvel environnement local, vous devez installer le module d'environnement local ou le module de langue approprié sur votre ordinateur. Pour de plus amples informations, voir la documentation de votre système d'exploitation.

Remarque : Si vous utilisez Netcool/OMNIbus Administrator, vous devez vous assurer que le codage du jeu de caractères de chaque ObjectServer géré possède une entrée correspondante dans le fichier $NCHOME/omnibus/java/jars/csemap.dat. Ce fichier fournit un mappage entre les conventions de dénomination de codage Sybase et du jeu de caractères de l'environnement d'exécution Java. Si le codage du jeu de caractères d'un serveur ObjectServer ne figure pas dans le fichier csemap.dat, vous devez ajouter un mappage à ce fichier au format suivant :

codage_Sybase codage_Java

Par exemple :

```
ascii_7 ASCII
```

Tâches associées:

«Création d'une base de données de clés à l'aide de nc_gskcmd», à la page 381
Si vous exécutez Tivoli Netcool/OMNIbus en mode FIPS-0142 ou si votre réseau comprend des clients Java, utilisez le programme **nc_gskcmd**.

«Configuration de l'Interface graphique Web pour les caractères GB18030», à la page 187
Pour que votre installation de l'Interface graphique Web en chinois soit conforme à la norme GB18030 pour les caractères chinois, vous devez installer le jeu de caractères GB18030 sur votre système client et configurer les systèmes clients de façon à ce qu'ils affichent ces caractères.

Référence associée:

«Propriétés et options de ligne de commande de nco_dbinit», à la page 198
Lorsque l'utilitaire d'initialisation de la base de données **nco_dbinit** démarre, il lit un fichier de propriétés. Si une propriété n'est pas indiquée dans ce fichier, la valeur par défaut est utilisée à moins que vous l'écrasiez par une option de ligne de commande.

«Erreurs d'authentification LDAP communes», à la page 660
Erreurs d'authentification LDAP communes

Identification des environnements locaux pris en charge sur votre ordinateur

Vous pouvez exécuter la commande **locale** sous UNIX, ou utiliser le Panneau de configuration de Windows pour répertorier tous les environnements locaux pris en charge sur votre ordinateur.

Pourquoi et quand exécuter cette tâche

Pour vérifier les environnement locaux qui sont pris en charge sur votre ordinateur :

Procédure

- Sous UNIX, exécutez la commande suivante :

  ```
  locale -a
  ```

  Conseil : Vous pouvez également utiliser la commande **locale** sans option de ligne de commande pour répertorier l'environnement local actuel et la commande **locale charmap** pour afficher le codage.
- Sous Windows, utilisez l'élément **Paramètres régionaux** ou **Options régionales et linguistiques** du Panneau de configuration.

Que faire ensuite

Vous pouvez affecter n'importe quel environnement local répertorié à la variable d'environnement LANG ou LC_*. Les environnements locaux répertoriés sont sensibles à la casse, veillez donc à utiliser la casse correcte lorsque vous les affectez à des variables d'environnement. Vous pouvez également afficher les environnements locaux pris en charge pour la configuration du bureau et pour les composants du bureau UNIX.

Tâches associées:

«Identification des environnements locaux pris en charge pour le bureau UNIX» Tous les environnements locaux pris en charge pour l'utilisation dans le bureau UNIX sont installés dans `$NCHOME/omnibus/desktop/locale/arch`, où *arch* représente le répertoire du système d'exploitation.

Activation ou désactivation du tri localisé

La propriété ObjectServer **Store.LocalizedSort** vous permet d'activer ou de désactiver le tri localisé. Cette fonction est désactivée par défaut pour obtenir des performances optimales.

Pourquoi et quand exécuter cette tâche

La propriété ObjectServer **Store.LocalizedSort** vous permet d'effectuer des comparaisons de chaîne de bibliothèque C standard (valeur par défaut) ou d'activer le tri localisé. Lorsque le tri localisé est activé, vous pouvez également utiliser la propriété **Store.LocalizedSortCaseSensitive** pour contrôler la sensibilité à la casse de l'ordre de tri.

Exemple

Exemple de tri localisé

Lorsque la localisation est désactivée, Å est traité comme une variante de A et les deux caractères seront triés à proximité l'un de l'autre.

Lorsque la localisation est activée dans un environnement local en danois, Å est traité comme une lettre distincte, triée après Z.

Identification des environnements locaux pris en charge pour le bureau UNIX

Tous les environnements locaux pris en charge pour l'utilisation dans le bureau UNIX sont installés dans `$NCHOME/omnibus/desktop/locale/arch`, où *arch* représente le répertoire du système d'exploitation.

Pourquoi et quand exécuter cette tâche

Dans cet emplacement, il existe un répertoire ou un lien symbolique pour chaque environnement local pour lequel la configuration du bureau est prise en charge.

Configuration de polices pour le bureau UNIX

Si vous souhaitez afficher le bureau UNIX dans votre environnement local, il peut être nécessaire de configurer les polices requises pour afficher le texte dans le codage de votre environnement local.

Pourquoi et quand exécuter cette tâche

L'installation Tivoli Netcool/OMNIbus inclut des fichiers de ressources qui contiennent des définitions pour les éléments de l'interface utilisateur des applications du bureau UNIX ; par exemple, les définitions des dimensions de fenêtre, les sélections de polices, les couleurs, les valeurs de chaîne des titres de fenêtre, les menus, les boutons, les icônes, les étiquettes de zone et les chaînes de message.

Des traductions des fichiers de ressources sont disponibles pour les environnements locaux suivants : , anglais, français, allemand, japonais, coréen, russe, espagnol, chinois simplifiée et chinois traditionnel. De plus, les environnements locaux qui utilisent le jeu de caractères ISO-8859-1 doivent afficher les polices correctement, avec le paramètre Anglais activé. Les autres jeux de caractères peuvent nécessiter une configuration.

Les fichiers de ressources sont stockés à l'emplacement suivant :

```
$NCHOME/omnibus/desktop/locale/arch/nom_environnement_local/app-defaults
```

Où *arch* est le nom du répertoire du système d'exploitation et *nom_environnement_local* est le nom complet de l'environnement local ; par exemple, en_GB.ISO8859-1. Notez que certains noms d'environnements locaux peuvent être des liens symboliques avec des noms abrégés.

Les fichiers de ressources incluent :

- `NCO` : définitions du Conductor, du Générateur de filtres et du Générateur de vues associés
- `NCOBanner` : définitions pour l'écran d'accueil du Conductor
- `NCOELCT` : définitions de la liste d'événements transitoires
- `NCOEvent` : définitions pour la fenêtre d'écran de surveillance Liste d'événements, de la liste d'événements et des fenêtre associées telles que la fenêtre Ouverture de session, du Générateur de filtres et du Générateur de vues
- `NCOHelp` : définitions liés à l'aide en ligne. Il est possible que ce fichier ne contienne aucune définition
- `NCOMessage` : définitions pour la boîte de dialogue de messagerie qui peut être utilisée avec des outils
- `NCOXigen` : définitions pour l'éditeur de serveurs
- `NCOXprops` : définitions pour l'éditeur de propriétés

Si votre environnement local n'est pas inclus dans le package d'installation de Tivoli Netcool/OMNIbus, les fichiers de ressources de l'environnement local en_US.ISO8859-1 sont utilisés par défaut. Vous pouvez configurer votre installation pour utiliser un autre environnement local, non fourni dans le package d'installation. Si votre environnement local utilise un codage de jeu de caractères différent d'ISO-8859-1, vous devez également vous assurer de définir une police qui peut rendre de manière précise les caractères du fichier de ressources dans les caractères de votre environnement local.

Pour configurer un autre environnement local et jeu de polices :

Procédure

1. Exécutez la commande suivante pour répertorier tous les environnements locaux pris en charge :

   ```
   locale -a
   ```

2. Définissez la variable d'environnement LC_ALL sur un de ces environnements locaux.
3. Exécutez la commande suivante pour afficher votre codage de caractères :

   ```
   locale charmap
   ```

   Notez le codage, car il sera requis ultérieurement.

4. Pour créer un jeu de fichiers de ressources localisés dans une police rendue correctement, accédez au répertoire `$NCHOME/omnibus/desktop/locale/arch`, où *arch* représente le répertoire de votre système d'exploitation. Vous devez copier un jeu de fichiers de ressources à partir d'un environnement local qui contient des polices adaptées à votre codage, puis personnaliser les fichiers copiés. Par exemple, pour créer des fichiers pour l'environnement local arabe (ar), créez un répertoire avec le nom de l'environnement local et copiez les fichiers de ressources pour l'environnement en_US.ISO8859-1 :

   ```
   cd $NCHOME/omnibus/desktop/locale/arch
   mkdir ar
   cd ar
   cp -r ../en_US.ISO8859-1/* .
   ```

   Les fichiers de ressources (avec le préfixe NCO), le sous-répertoire d'images et les fichiers de configuration de liste d'événements par défaut sont copiés dans le répertoire `ar`. Vous devez à présent rechercher un jeu de polices approprié pour votre système, qui correspond à la police d'application du fichier de ressources.

5. A partir de la ligne de commande, entrez la commande appropriée à votre système d'exploitation :

Système d'exploitation	**Commande**
AIX	`/usr/X11R6/bin/xlsfonts -fn "nom_police"`
HP-UX	`/usr/bin/X11/xlsfonts -fn "nom_police"`
Linux (Red Hat)	`/usr/X11R6/bin/xlsfonts -fn "nom_police"`
Solaris	`/usr/openwin/bin/xlsfonts -fn "nom_police"`

   Dans cette commande, *nom_police* est le codage de caractères trouvé à l'étape 3, à la page 424. Spécifiez cette valeur en tant qu'expression générique à l'aide d'astérisques (*). Notez que vous devez inclure la valeur entre guillemets pour empêcher l'interpréteur de commandes d'interpréter les astérisques du texte. Par exemple :

   `/usr/openwin/bin/xlsfonts -fn "*-iso8859-6"` La liste des polices correspondantes est affichée.

6. Prévisualisez chaque police pour déterminer si elle est adaptée. Pour chaque police, entrez la commande suivante :

   ```
   xfd -fn nom_police
   ```

   Où *nom_police* est l'un des noms de police correspondants renvoyé à l'étape précédente. Une fenêtre s'ouvre et affiche le nom complet de la police ainsi qu'une grille qui contient un caractère par cellule. Il peut être nécessaire d'utiliser les boutons **Next Page** (Page suivante) et **Previous Page** (Page précédente) pour afficher tous les caractères. Lorsque vous avez identifié les polices adaptées, vous pouvez ajouter le jeu de polices à votre fichier de ressources.

7. Ouvrez chaque fichier de ressources appelé `NCO` l'un après l'autre pour modifier la police. Par exemple, dans les ressources de la liste d'événements, vous devez définir `NCOEvent*fontList`, `NCOEvent*sub_matrix.labelFont`, `*view_builder*display_matrix.labelFont`, et `NCOEvent*info_matrix.labelFont` sur des jeux de polices qui contiennent toutes les polices requises pour l'environnement local.

   Les noms de polices UNIX sont au format :

```
-foundry-font family-weight-slant-set width-serif-pixels-points-hres-vres-spacing-average
width-character set-encoding
```

Vous pouvez spécifier des noms de police avec des caractères génériques. Par exemple, la police par défaut de la liste d'événements est :

```
-adobe-helvetica-bold-r-normal--12-*-75-75-*-*-iso*-*
```

Pour l'arabe, vous pouvez remplacer cette valeur par :

```
-dt-interface user-bold-r-normal-m serif-14-140-75-75-p-188-iso8859-6
```

Lorsque vous utilisez des jeux de caractères EUC, plusieurs polices sont requises simultanément ; par exemple EUCJIS (japonais) requiert les polices iso8859-1, jisx0201.1976-0, jisx0208.1983-0 et jisx0212.1990-0. Vous pouvez spécifier un tel jeu de polices avec un ou plusieurs noms de police contenant des caractères spéciaux. (Les polices comprises dans un jeu de polices sont séparées par un point-virgule et les jeux de polices se terminent par un signe deux-points).

8. Le cas échéant, modifiez d'autres paramètres dans les ressources comme suit :
   - Spécifiez les largeurs par défaut (en pixels) des fenêtres. Il peut être nécessaire d'ajuster ces valeurs pour s'adapter à votre police et garantir que le texte de la fenêtre s'affiche correctement.
   - Remplacez les valeurs de chaîne des titres de fenêtre (`*.title`), des noms de boutons (`*.labelString`), des messages (`*.messageString`) et d'autres éléments textuels par votre texte traduit. Assurez-vous que le texte traduit utilise le codage de caractères de votre environnement local.
9. Sauvegardez les modifications apportées aux fichiers. Vous pouvez maintenant exécuter Tivoli Netcool/OMNIbus avec l'environnement local et les polices corrects.

Configuration du serveur ObjectServer pour utiliser le texte d'interface utilisateur traduit dans le bureau

La base de données ObjectServer contient des données de configuration affichées dans le bureau UNIX et Windows (c'est-à-dire dans la liste d'événements et Conductor). Lorsque vous initialisez la base de données ObjectServer, ces données de configuration sont lues dans le fichier de définitions SQL, qui insère les valeurs par défaut dans les tables du bureau, y compris les couleurs par défaut, les visuels de colonne, les conversions, les outils et les menus.

Pourquoi et quand exécuter cette tâche

Le fichier de définition SQL du bureau est par défaut `$NCHOME/omnibus/etc/desktop.sql`.

Le serveur ObjectServer utilise un seul fichier `desktop.sql`. Toutes les listes d'événements et tous les conducteurs connectés à un serveur ObjectServer affichent les chaînes dans la même langue.

Les traductions des données de configuration par défaut sont disponibles dans les langues suivantes : japonais, coréen, chinois simplifié et chinois traditionnel. Les chaînes traduites sont fournies dans des fichiers `desktop.sql` distincts pour :

- Les visuels de colonne utilisés comme noms de colonnes par défaut dans la liste d'événements
- Les conversions qui provoquent l'affichage des données d'événement numériques sous forme de chaîne pour les zones comme Gravité, Avec acc de réception, Type et NmosManagedStatus

- Les noms d'éléments dans les menus **Outil**

Les fichiers traduits pour chaque langue prise en charge sont stockés dans `$NCHOME/omnibus/etc/locale/`*`nom_environnement_local`*`/desktop.sql`, où *nom_environnement_local* est le nom complet de l'environnement local. Pour utiliser un de ces fichiers, spécifiez celui que vous souhaitez utiliser lors de l'initialisation de la base de données ObjectServer. Pour cela, utilisez la commande **nco_dbinit**.

Important : Vous devez exécuter **nco_dbinit** dans l'environnement local dans lequel vous allez démarrer et exécuter le serveur ObjectServer. Si vous souhaitez exécuter le codage UTF-8, vous devez convertir en UTF-8 les fichiers `.sql` codés en langue naturelle telles que le chinois ou le japonais. Spécifiez ensuite l'option de ligne de commande `-utf8enabled` avec la valeur `TRUE` lorsque vous exécutez **nco_dbinit**.

Pour initialiser la base de données dans votre environnement local requis, exécutez la commande **nco_dbinit** avec l'option de ligne de commande `-desktopfile` comme suit :

```
$NCHOME/omnibus/bin/nco_dbinit -server nom_serveur -desktopfile chaîne
```

Dans cette commande, *nom_serveur* est le nom du nouveau serveur ObjectServer et *chaîne* est le chemin d'accès et le nom du fichier `desktop.sql` correspondant à l'environnement local requis. Par exemple :

```
$NCHOME/omnibus/bin/nco_dbinit -server DENCO -desktopfile
$NCHOME/omnibus/etc/locale/zh_TW.EUC/desktop.sql
```

Ensuite, démarrez le serveur ObjectServer dans le même environnement local que celui utilisé lors de l'exécution de la commande **nco_dbinit**. Par exemple :

```
$NCHOME/bin/nco_objserv -name DENCO
```

Vous pouvez modifier les données de configuration après la création du serveur ObjectServer créé à l'aide de Netcool/OMNIbus Administrator et traduire les chaînes dans d'autres langues.

Tâches associées:

«Création d'un serveur ObjectServer», à la page 197
Vous créez un ou plusieurs serveurs ObjectServer sur un poste de travail hôte en exécutant l'utilitaire d'initialisation de base de données (**nco_dbinit**).

Chapitre 17. Extension des fonctionnalités de Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus inclut un ensemble de ressources qui vous permettent de développer les fonctionnalités du produit. L'intégration à d'autres produits Tivoli est requise pour certaines personnalisations.

Les ressources sont installées dans le répertoire `$NCHOME/omnibus/extensions`, et incluent des personnalisations pour :

- Configurer un environnement à plusieurs niveaux permettant d'augmenter les performances et la capacité de gestion des événements.
- Configurer la haute disponibilité.
- Etendre les règles de sonde pour détecter les rafales d'événements et les débits d'événements anormalement élevés ou faibles.
- Configurer l'auto-surveillance des sondes pour collecter des métriques sur la quantité de mémoire utilisée par diverses opérations de traitement ainsi que le nombre d'événements reçus, supprimés et générés.
- Recharger simultanément plusieurs fichiers de règles de sonde.
- Prendre en charge des analyses prévisibles dans un environnement Tivoli Netcool/OMNIbus et IBM Tivoli Monitoring intégré.
- Activer des événements à partir d'IBM Tivoli Application Dependency Discovery Manager (TADDM) afin qu'ils soient surveillés dans Tivoli Netcool/OMNIbus.
- Activer la gestion des événements d'un environnement virtuel à l'aide des capacités jointes de Tivoli Netcool/OMNIbus et d'IBM Tivoli Monitoring.

Ces ressources sont toujours installées, quelle que soit la fonction d'installation choisie.

Concepts associés:

«Intégration à d'autres produits Tivoli», à la page 62
Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

Présentation du répertoire $NCHOME/omnibus/extensions

Le répertoire `$NCHOME/omnibus/extensions` contient un ensemble de fichiers exemples et modèles. Lorsque vous configurez Tivoli Netcool/OMNIbus, utilisez ces fichiers pour étendre la fonction du produit.

Le répertoire `$NCHOME/omnibus/extensions` contient les deux sous-répertoires suivants :

- `control_shutdown`
- `eventflood`
- `itmdeploy`

- `itmpredictive`
- `multitier`
- `roi`
- `taddm`
- `virtualization`
- `xiny`

Chacun de ces sous-répertoires contient des fichiers en lecture seule qui fournissent un modèle de configuration. Traitez les fichiers originaux comme des modèles disponibles à des fins de référence. Si vous souhaitez étendre les capacités des modèles, faites des copies des fichiers et, avant de les modifier, supprimez les droits en lecture seule. Dans certains cas, vous pouvez exécuter des commandes qui désignent ces fichiers.

Remarque : Les droits d'accès en lecture seule ne sont pas appliqués sous Windows.

Contenu du répertoire control_shutdown

Le répertoire `control_shutdown` contient un script SQL qui peut être utilisé pour mettre à jour le schéma ObjectServer avec les personnalisations requises pour configurer l'arrêt contrôlé d'un serveur ObjectServer.

Des informations supplémentaires sur la configuration de l'arrêt contrôlé sont disponibles dans le présent guide d'installation.

Contenu du répertoire eventflood

Le répertoire `eventflood` contient des modèles de fichiers de règles secondaires pouvant être utilisés lorsqu'une sonde est sujette à un débordement d'événements ou à un débit anormal de réception d'événements. Le fichier de règles de débordement contient toutes les règles permettant de déterminer les débits d'événements actuels et l'action à prendre durant un débordement d'événements, ou un débit anormalement élevé ou faible de réception d'événements. Le fichier de configuration de règles de débordement contient les variables utilisées pour configurer le fichier de règles de débordement.

Pour de plus amples informations sur la configuration et la détection de débordement d'événements ou de débits d'événements anormaux, voir la rubrique *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*.

Contenu du répertoire itmdeploy

Le répertoire `itmdeploy` contient les modèles de fichiers permettant de :

- Récupérer les fichiers que vous souhaitez consulter ou mettre à jour, pour les installations de sonde et de Tivoli Netcool/OMNIbus déployées sur des ordinateurs distants.
- Transférer des fichiers mis à jour vers les ordinateurs distants.

Les fichiers externes au répertoire d'installation de Tivoli Netcool/OMNIbus peuvent également être récupérés et remplacés sur des ordinateurs distants.

Cette personnalisation requiert une intégration dans IBM Tivoli Monitoring. L'utilitaire de fichier de transfert et son fichier de propriétés correspondant, ainsi qu'un fichier `.jar` sont fournis pour effectuer les opérations de transfert de fichier.

Des informations supplémentaires sur le déploiement distant des sondes et des opérations de transfert de fichiers sont fournies dans ce chapitre du guide d'installation.

Contenu du répertoire itmpredictive

Le répertoire `itmpredictive` contient les modèles de fichiers requis pour configurer Tivoli Netcool/OMNIbus pour que les événements prévisibles générés dans IBM Tivoli Monitoring puissent être affichés dans la liste des événements actifs ou la liste d'événements de bureau. La capacité d'afficher les événements prévisibles exige une intégration à IBM Tivoli Monitoring et à Probe for Tivoli EIF.

Les modèles de fichier sont fournis pour :

- ajouter dans le serveur ObjectServer des déclencheurs, des zones, un ID de classe et sa conversion, et des outils ;
- traiter et mapper des données d'événements prévisibles à des données d'alerte qui peuvent être insérées dans la table alerts.status du serveur ObjectServer ;
- créer le filtre, la vue et la configuration de liste d'événements à utiliser pour la liste d'événements ;
- créer le filtre, la vue, les outils, les invites et le menu à utiliser avec la lise d'événements actifs.

Pour de plus amples informations sur la configuration des événements prévisibles, consultez ce chapitre du guide d'installation et le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* . Pour de plus amples informations sur la surveillance des événements prévisibles, voir *IBM Tivoli Netcool/OMNIbus User's Guide* et le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Contenu du répertoire multitier

Le répertoire `multitier` contient les modèles de fichiers permettant de configurer une architecture à plusieurs niveaux de serveurs et passerelles ObjectServer installés dans les couches de collecte, d'agrégation et d'affichage. Les fichiers de définition de mappe, les fichiers de propriétés et les fichiers de définition de réplication de table sont fournis pour configurer les passerelles ObjectServer. Les scripts SQL permettent également de mettre à jour le schéma ObjectServer et d'annuler les modifications effectuées.

Des informations supplémentaires sur la configuration d'une architecture à plusieurs niveaux sont fournies dans ce guide d'installation.

Contenu du répertoire roi

Le répertoire `roi` contient un script SQL permettant de mettre à jour le schéma ObjectServer et un modèle de fichier de règles secondaire permettant de configurer une sonde pour l'auto-surveillance. Il contient également les fichiers nécessaires pour mettre en place une procédure pour recharger les fichiers de règles de plusieurs sondes simultanément.

Un ensemble de modèles de rapports est également fourni et doit être personnalisé par l'utilisateur. Ces rapports proposent également une intégration à Tivoli Data Warehouse et Tivoli Common Reporting. Pour procéder à la configuration, vous devez savoir utiliser ces composants.

Pour des informations supplémentaires sur la configuration de sondes pour l'auto-surveillance, consultez le *Guide des sondes et des passerelles d'IBM Tivoli Netcool/OMNIbus*.

Contenu du répertoire taddm

Le répertoire `taddm` contient des modèles de fichier permettant de configurer Tivoli Netcool/OMNIbus afin que les événements générés dans TADDM puissent être affichés dans la liste des événements actifs ou la liste d'événements. Pour pouvoir afficher ces événements, ils doivent être intégrés dans TADDM et Probe for Tivoli EIF.

Les modèles de fichier sont fournis pour :

- ajouter dans le serveur ObjectServer l'ID de classe, la conversion, le menu et les outils requis ;
- traiter et mapper les données d'événements TADDM à des données d'alerte qui peuvent être insérées dans la table alerts.status du serveur ObjectServer ;
- ajouter le menu et les outils au composant d'Interface graphique Web.

Des informations supplémentaires sur la configuration des événements TADDM sont disponibles dans ce chapitre du guide d'installation et dans le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* . Pour plus d'informations sur la surveillance des événements TADDM, voir *IBM Tivoli Netcool/OMNIbus User's Guide* et le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Contenu du répertoire virtualization

Le répertoire `virtualization` et ses sous-répertoires contiennent les modèles de fichiers requis pour configurer Tivoli Netcool/OMNIbus afin de prendre en charge la gestion des événements pour un environnement virtuel. Cette personnalisation peut être configurée de deux manières : en utilisant Netcool/OMNIbus Knowledge Library et la sonde pour SNMP avec VMware vSphere 5.0, ou dans un environnement intégré qui inclut IBM Tivoli Monitoring et Probe for Tivoli EIF.

Les modèles de fichier sont fournis pour :

- ajouter des déclencheurs et une base de données au serveur ObjectServer ;
- traiter et mapper des données d'événements à des données d'alerte qui peuvent être insérées dans la table alerts.status et une table personnalisée dans le serveur ObjectServer ;
- traiter et mapper des interceptions SNMP sur des données d'alerte qui peuvent être insérées dans la table alerts.status et une table personnalisée dans le serveur ObjectServer ;
- annuler les modifications apportées au schéma ObjectServer.

Des informations supplémentaires sur la configuration de gestion d'événements dans un environnement virtuel sont disponibles dans ce chapitre du guide d'installation.

Contenu du répertoire xiny

Le répertoire `xiny` contient les fichiers requis pour l'activation du débit d'événements X en Y.

Concepts associés:

Chapitre 9, «Configuration de la haute disponibilité», à la page 267
Lorsque Tivoli Netcool/OMNIbus est configuré pour la haute disponibilité, la perte d'événements est réduite, l'intégrité des données, optimisée et les performances sont accrues.

«Activation des événements prévisibles et de l'analyse prévisionnelle»
Dans un environnement intégré Tivoli Netcool/OMNIbus et IBM Tivoli Monitoring, la fonction d'analyse prévisionnelle intégrée vous permet d'identifier les problèmes de performances et de capacité potentiels qui pourraient provoquer une dégradation des performances ou une indisponibilité du service. Dans cet environnement, vous pouvez générer des événements qui représentent des prédictions pour les systèmes en danger de dépassement de seuil imminent et nécessitant une certaine attention.

«Gestion d'environnements virtuels», à la page 465
Vous pouvez configurer Tivoli Netcool/OMNIbus afin qu'il exécute la gestion des événements d'un environnement virtuel. Tivoli Netcool/OMNIbus peut être configuré pour effectuer ce type de gestion d'événements à l'aide d'une sonde personnalisée pour SNMP, ou dans le cadre d'une solution intégrée à IBM Tivoli Monitoring.

Chapitre 8, «Configuration et déploiement d'une architecture à plusieurs niveaux», à la page 223
Tivoli Netcool/OMNIbus peut être déployé dans une configuration à plusieurs niveaux pour augmenter les performances et la capacité de gestion des événements. Dans un environnement à plusieurs niveaux, le contrôle du flux d'événements entre les serveurs ObjectServer doit être géré avec précaution pour préserver l'intégrité des données et assurer que des conditions d'indétermination ne se produisent pas.

«Activation de la prise en charge des événements TADDM», à la page 456
IBM Tivoli Application Dependency Discovery Manager (TADDM) est un outil de gestion des configurations qui reconnaît les systèmes matériels et logiciels d'un environnement informatique. TADDM est un sous-système du produit IBM Tivoli Change and Configuration Management Database .

Activation des événements prévisibles et de l'analyse prévisionnelle

Dans un environnement intégré Tivoli Netcool/OMNIbus et IBM Tivoli Monitoring, la fonction d'analyse prévisionnelle intégrée vous permet d'identifier les problèmes de performances et de capacité potentiels qui pourraient provoquer une dégradation des performances ou une indisponibilité du service. Dans cet environnement, vous pouvez générer des événements qui représentent des prédictions pour les systèmes en danger de dépassement de seuil imminent et nécessitant une certaine attention.

Remarque : La présente section suppose que vous disposez d'une connaissance pratique de IBM Tivoli Monitoring.

Evénement prévisible

IBM Tivoli Monitoring et Probe for Tivoli EIF peuvent être configurés pour réacheminer les événements prévisibles vers Tivoli Netcool/OMNIbus. Les alertes en résultant peuvent ensuite être surveillées dans la liste d'événements actifs ou dans la liste d'événements de bureau.

Selon les fonctions d'analyse et d'événements prévisionnels que vous configurez, les types d'événements prévisionnels suivants peuvent être générés :

- Evénéments prévisionnels basés sur le débit d'événements : si la fonction de tendance linéaire est configurée, ces événements prévisionnels affichent les prévisions. Par exemple, si une unité surveillée affiche un débit d'événements d'erreur croissant et qu'elle dépassera un seuil défini dans les sept jours.
- Evénements prévisionnels basés sur les écarts de base de référence : si la fonction de base de référence est configurée, ces événements prévisionnels affichent les écarts par rapport à un débit d'événements moyen défini, qui est calculé à partir des données archivées.
- Evénements prévisibles basés sur une tendance linéaire utilisant des données historiques collectées à partir des agents de surveillance dans l'environnement IBM Tivoli Monitoring.

Le scénario d'utilisation suivant décrit les actions possibles à prendre lorsque des événements prévisibles sont réacheminés vers Tivoli Netcool/OMNIbus afin d'être affichés dans la liste d'événements et dans la liste d'événements actifs :

- Lorsque des données d'alerte d'un événement prévisible s'affichent dans la liste d'événements ou dans la liste d'événements actifs, commencez à collecter les informations d'origine relatives au problème prévu, notamment l'emplacement du problème et le nombre de jours avant la violation du seuil.
- Recherchez les raisons de la prédiction en consultant les événements réels et les autres événements prévisibles générés pour l'entité ou le nœud géré(e).
- Lorsque vous êtes suffisamment satisfait de la validité de la prédiction, prenez des mesures correctives au niveau de l'entité gérée avant la survenue du problème.
- Sinon, ignorez temporairement l'événement prévisible lorsque vous surveillez les prédictions de suivi et les événements réels qui se produisent sur l'entité gérée dans la période entre la génération de l'événement prévisible et le dépassement du seuil.
- En cas de plusieurs événements prévisibles, accordez une priorité à votre réponse en fonction de l'ordre dans lequel les événements s'affichent dans la liste d'événements ou dans la liste d'événements actifs.

Tendance linéaire des débits d'événements de l'unité

La tendance linéaire des débits d'événements de l'unité utilise la fonction d'analyse prévisionnelle IBM Tivoli Monitoring pour déterminer si les débits d'événements reçus par le serveur ObjectServer sont susceptibles de dépasser les seuils maximaux au cours d'une période de temps définie. Tivoli Performance Analyzer utilise les débits d'événements reçus du serveur ObjectServer pour produire des tendances. Si un seuil a été violé au cours d'un laps de temps défini, un événement prévisible est envoyé au serveur ObjectServer. Une assistance est proposée pour calculer les prévisions à sept, 30, ou 90 jours. Vous pouvez définir des seuils critiques et d'avertissement ; lorsque ces seuils sont dépassés, l'événement prévisible qui en résulte aura le niveau de gravité correspondant.

Le calcul des tendances linéaires utilise la méthode de régression des moindres carrés. Cette méthode évoque un modèle linéaire d'utilisation dans le temps pour les attributs sélectionnés en fonction de leurs valeurs passées.

Remarque : La méthode de régression des moindres carrés fournit des données approximatives. Il est recommandé d'appliquer une marge de 12 heures aux événements prévisibles générés.

Planification des débits d'événements d'une unité

La planification du débit d'événements par unité client permet de calculer le débit moyen d'événements par unité sur un laps de temps défini. Les données de débit d'événements, archivées dans Tivoli Data Warehouse, permettent de construire un couloir de normalité. Les débits d'événements actuels sont comparés à la base de référence moyenne sur un nombre de semaine défini pour la période de temps actuel. A vous de définir les écarts par rapport au taux moyen, c'est-à-dire les seuils que le débit d'événements doit dépasser. Si un seuil est dépassé, IBM Tivoli Monitoring génère une situation, qui est ensuite reçue par Probe for Tivoli EIF. A son tour, Probe for Tivoli EIF génère un événement dans Tivoli Netcool/OMNIbus. La période minimum de génération des données est de sept jours. Idéalement, vous devriez autoriser 14 jours de données.

Installation et configuration des événements prévisibles

Pour configurer et surveiller les événements prévisibles, Tivoli Netcool/OMNIbus, Probe for Tivoli EIF et IBM Tivoli Monitoring doivent être installés dans un environnement intégré.

La figure suivante illustre la configuration requise pour les composants produit dans l'environnement intégré.

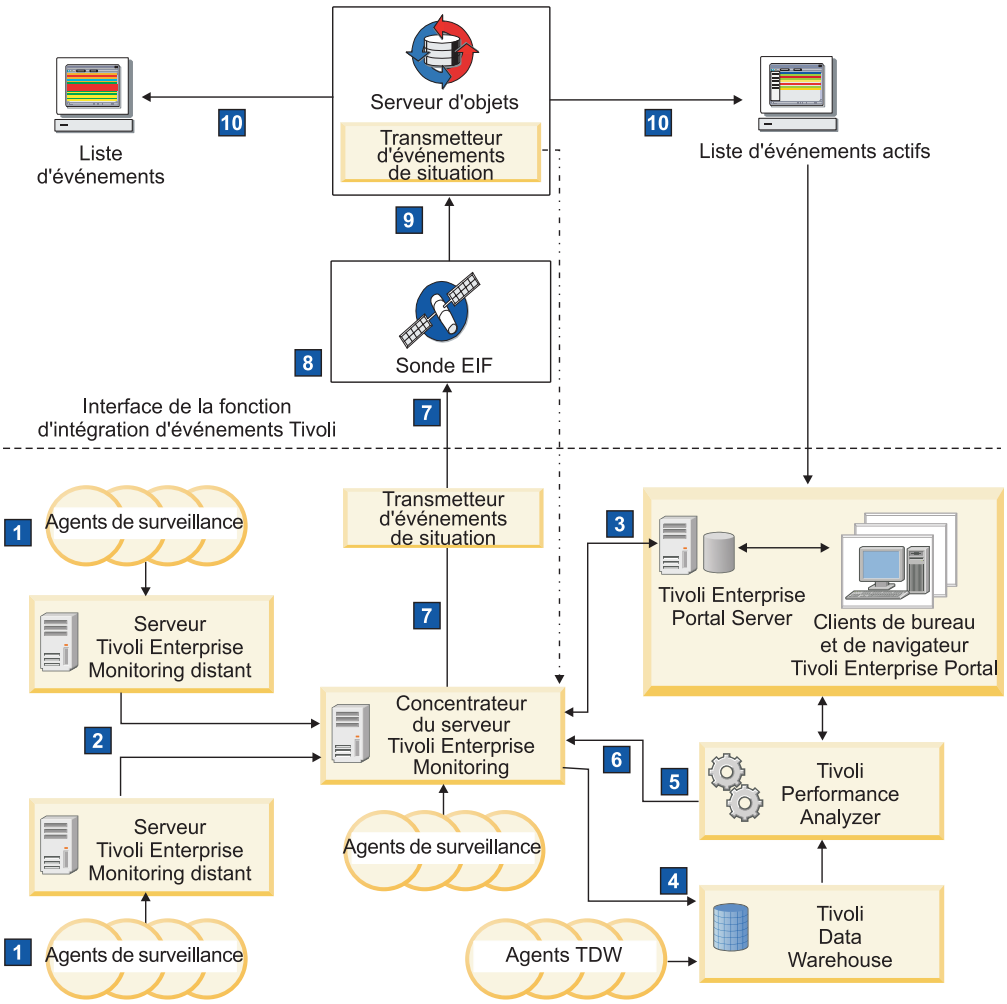

Figure 14. Configuration de Tivoli Netcool/OMNIbus et d'IBM Tivoli Monitoring pour les événements prévisibles

Le flux de configuration est le suivant :

1 Les agents de surveillance Tivoli Enterprise sont installés sur les systèmes ou sous-systèmes à surveiller. Ces agents collectent des données sur les systèmes surveillés ou gérés et les envoient à un ou plusieurs serveurs de surveillance Tivoli Enterprise.

2 Les serveurs Tivoli Enterprise Monitoring collectent les alertes reçues des agents de surveillance ainsi que les données de performances et de disponibilité. Les serveurs de surveillance gèrent également l'état de connexion des agents. Un serveur de surveillance dans chaque environnement doit être désigné comme le concentrateur. Le serveur de surveillance concentrateur contrôle les serveurs de surveillance distants et tous les agents de surveillance connectés directement au serveur de surveillance concentrateur.

3 Un serveur de portail Tivoli Enterprise fournit la couche présentation des données collectées. Le serveur de portail extrait des données du serveur de surveillance concentrateur en réponse à des actions de l'utilisateur à partir des clients Tivoli Enterprise Portal et présente les données aux clients de portail dans une interface utilisateur Java.

4 Tivoli Data Warehouse stocke les données historiques collectées par les

agents de surveillance dans votre environnement. Vous devez configurer IBM Tivoli Monitoring pour conserver des modèles de données dans des fichiers historiques et sauvegarder régulièrement ces fichiers dans Tivoli Data Warehouse. Deux agents spécialisés (l'agent proxy de Tivoli Data Warehouse et l'agent de regroupement et d'élagage) interagissent avec Tivoli Data Warehouse pour recevoir, regrouper et supprimer les données.

5 Le composant Tivoli Performance Analyzer offre une fonction de prédiction qui vous permet de surveiller les tendances de consommation des ressources, d'anticiper les problèmes de performances à venir et d'éviter ou de résoudre des problèmes plus rapidement. Tivoli Performance Analyzer effectue une tendance linéaire par rapport aux données historiques existant dans Tivoli Data Warehouse et vous permet de simuler des situations et des événements en fonction du comportement prévu. Par défaut, la tendance est calculée pour l'espace disque, l'utilisation de l'unité centrale et de la mémoire ainsi que pour le trafic réseau. Vous pouvez définir une tâche de tendance linéaire analytique qui précise les données à analyser, les seuils d'avertissement et critique ainsi que les périodes de prévision.

Tivoli Performance Analyzer est composé d'un outil de configuration et de tâches, situations et espaces de travail prédéfinis, qui sont tous accessibles depuis le portail Tivoli Enterprise. En outre, un agent Tivoli Performance Analyzer Warehouse interagit avec :

- Tivoli Data Warehouse pour récupérer les données historiques stockées collectées par d'autres agents
- le serveur de portail pour recevoir l'instruction d'exécuter la tâche d'analyse et les calculs analytiques sur les données
- le serveur de surveillance concentrateur pour transmettre les résultats de la tendance

6 Lorsque la tâche d'analyse s'exécute à sa fréquence et son planning indiqués, les valeurs de prévision sont calculées pour un ensemble d'attributs de sortie prédéfinis. Ces attributs sont récupérés par le serveur de surveillance concentrateur. En voici la liste :

- attributs stockés dans Tivoli Data Warehouse en tant que nouveaux attributs Tivoli Performance Analyzer
- attributs disponibles pour être affichés dans Tivoli Enterprise Portal
- attributs évalués lors de l'exécution de situations prédéfinies (ou personnalisées) afin de générer des événements prévisibles qui fournissent un avertissement avancé sur les problèmes potentiels

7 Le serveur de surveillance concentrateur peut être configuré pour réacheminer ces événements prévisibles vers les serveurs ObjectServer de Tivoli Netcool/OMNIbus à des fins d'affichage. Le serveur de surveillance concentrateur utilise un redirecteur d'événement de situation vers les événements Event Integration Facility (EIF) et l'interface Tivoli EIF pour réacheminer les événements EIF vers un récepteur EIF, qui est, dans ce cas, Probe for Tivoli EIF.

8 Probe for Tivoli EIF reçoit les événements, traite les données d'événement prévisible, mappe les données aux zones du serveur ObjectServer puis envoie des alertes au serveur ObjectServer. Il est nécessaire d'apporter des modifications au fichier de règles de sonde pour mapper les données d'événement prévisible aux zones du serveur ObjectServer.

9 Le serveur ObjectServer nécessite une certaine configuration pour interpréter et stocker les alertes. Les zones dédiées de la table alerts.status

sont également utilisées pour stocker des données uniques relatives aux événements prévisibles reçus de IBM Tivoli Monitoring. Le composant de synchronisation des événements IBM Tivoli Monitoring doit également être installé sur l'hôte du serveur ObjectServer. Ce composant offre des ressources de personnalisation qui permettent au serveur ObjectServer et à Probe for Tivoli EIF de gérer des événements de situation génériques et des événements prévisibles. Le composant de synchronisation des événements inclut également un processus SUF (Situation Update Forwarder) qui permet le renvoi des mises à jour des alertes vers le serveur de surveillance concentrateur d'origine.

Restriction : Il n'existe aucune fonction de mise à jour des événements prévisibles dans Tivoli Netcool/OMNIbus ou pour réacheminer ces mises à jour vers le serveur de surveillance concentrateur d'origine. Cette fonction existe uniquement pour les autres types d'événements de situation reçus d' IBM Tivoli Monitoring. En tant que telles, certaines actions relatives aux événements prévisibles doivent être exécutées dans IBM Tivoli Monitoring.

10 Les données d'état et de performances sont collectées depuis le serveur ObjectServer par l'agent de performance et d'état Tivoli Netcool/OMNIbus IBM Tivoli Monitoring et envoyées au serveurTivoli Enterprise Monitoring.

11 Les événements prévisibles insérés dans la table alerts.status peuvent être affichés, filtré et triés dans la liste d'événements actifs dans l'Interface graphique Web ou dans la liste d'événements. La fonctionnalité de lancement en contexte est également activée des événements prévisibles de la liste d'événements actifs vers le portail Tivoli Enterprise. Cette fonction vous permet d'afficher des détails sur un événement prévisible dans l'espace de travail du portail Tivoli Enterprise pertinent. Pour utiliser la fonctionnalité de lancement en contexte, une connexion unique doit être configurée.

Tâches associées:

«Configuration des événements prévisibles dans votre environnement intégré», à la page 448
Une événement prévisible est une alerte qui prévient les opérateurs qu'un incident peut se produire à l'avenir. Les événements prévisibles sont générés dans IBM Tivoli Monitoring et peuvent être transmis à Tivoli Netcool/OMNIbus pour être affichés dans la liste d'événements ou dans la Liste d'événements actifs.

Référence associée:

«Ressources de configuration de Tivoli Netcool/OMNIbus pour les événements prévisibles», à la page 444
Tivoli Netcool/OMNIbus fournit un certain nombre de ressources pour activer les événements prévisionnels. Ces ressources sont disponibles en tant que modèles de fichiers se trouvant dans le répertoire `$NCHOME/omnibus/extensions/itmpredictive`.

Installation et configuration de la tendance linéaire

Pour configurer et surveiller les analyses prévisionnelles de la tendance linéaire, Tivoli Netcool/OMNIbus, la sonde pour Tivoli EIF et IBM Tivoli Monitoring doivent être installés dans un environnement intégré.

La figure suivante illustre la configuration requise pour les composants produit dans l'environnement intégré.

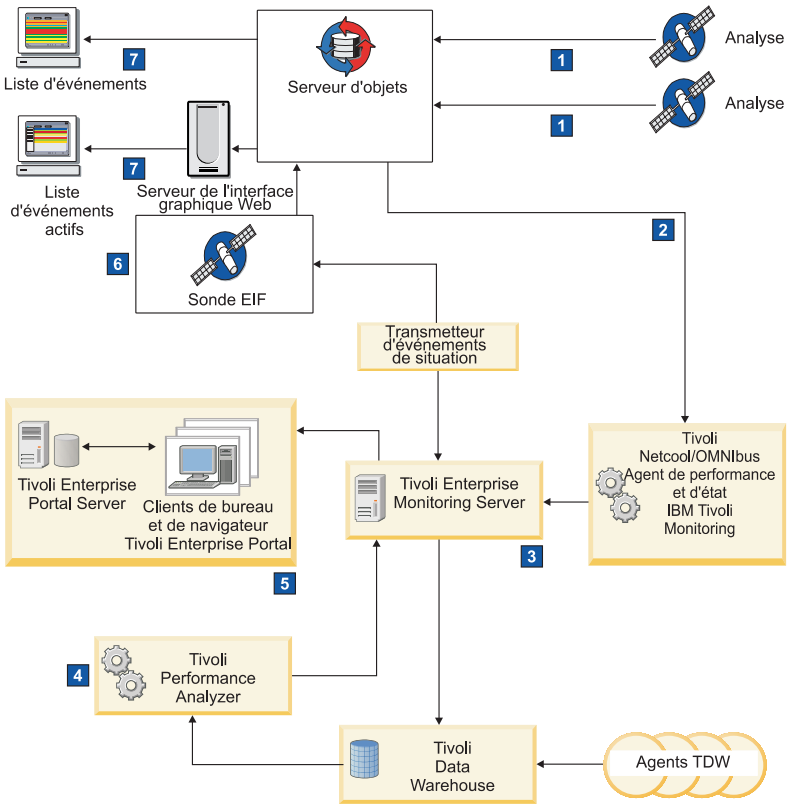

Figure 15. Configuration de Tivoli Netcool/OMNIbus et d'IBM Tivoli Monitoring pour les événements prévisibles

Le flux de configuration est le suivant :

1. Les sondes sont installées sur les unités ou les systèmes que vous souhaitez surveiller ; elles envoient les événements vers le serveur ObjectServer. Les automatisations dans le serveur ObjectServer détectent les débits d'événements de chaque unité surveillée.
2. Le serveur ObjectServer écrit les données de débit d'événements aux fichiers journaux des événements et l'agent IBM Tivoli surveillant l'état de santé lit ces fichiers. Pour transformer les événements en situations relevant d'IBM Tivoli Monitoring, le langage SQL et les automatisations des analyses prévisionnelles doivent être exécutés sur le serveur ObjectServer, ainsi que sur les classes de situations appropriées. L'analyseur de l'état de santé alimente le serveur Tivoli Enterprise Monitoring en situations.
3. Tivoli Data Warehouse archive les données de débit d'événements historiques. Vous devez configurer IBM Tivoli Monitoring de façon à conserver des échantillons de données dans les fichiers historiques et à enregistrer ces fichiers régulièrement dans Tivoli Data Warehouse . Deux

agents spécialisés (l'agent d'archivage et l'agent de regroupement et d'élagage) interagissent avec Tivoli Data Warehouse afin de recevoir, regrouper, et supprimer des données.

4 Tivoli Data Warehouse alimente en données de débits d'événements archivés Tivoli Performance Analyzer, où une tendance utilise les données pour calculer le débit d'événements futur. Il est possible de configurer des seuils qui, s'ils sont violés, génèrent une situation.

Tivoli Performance Analyzer est composé d'un outil de configuration et de tâches, situations et espaces de travail prédéfinis, qui sont tous accessibles depuis le portail Tivoli Enterprise. En outre, un agent Tivoli Performance Analyzer Warehouse interagit avec :

- Tivoli Data Warehouse pour récupérer les données historiques stockées collectées par d'autres agents
- le serveur de portail pour recevoir l'instruction d'exécuter la tâche d'analyse et les calculs analytiques sur les données
- le serveur de surveillance concentrateur pour transmettre les résultats de la tendance

5 Toutes les situations sont analysées et transmises à Tivoli Enterprise Portal. La tendance peut s'afficher dans deux espaces de travail par défaut.

6 Le serveur Tivoli Enterprise Monitoring réachemine les situations créées par l'agent Tivoli Performance vers la sonde de Tivoli EIF. La sonde reçoit les situations, traite les données d'attribut des situation, mappe les données aux zones du serveur ObjectServer, puis envoie des alertes au serveur ObjectServer. La sonde utilise la configuration du fichier de règles pour convertir les données de situation en données d'événement.

7 Les événements insérés dans la table alerts.status peuvent être affichés, filtrés et triés dans la liste d'événements actifs dans l'interface graphique Web ou dans la liste d'événements. La fonctionnalité de lancement en contexte est également activée des événements prévisibles de la liste d'événements actifs vers Tivoli Enterprise Portal. Cette fonctionnalité vous permet d'afficher les caractéristiques d'un événement dans l'espace de travail Tivoli Enterprise Portal approprié. DansTivoli Enterprise Portal, vous pouvez identifier la tendance à laquelle correspondent les événements prévisionnels.

Conditions préalables pour les événements prévisibles et les analyses prévisionnelles

Pour pouvoir configurer l'environnement, IBM Tivoli Netcool/OMNIbus, IBM Tivoli Monitoring, IBM DB2 sont requis avec une version particulière et des niveaux de groupes de correctifs avec des configurations spécifiques.

Au minimum, les versions et les produits suivants doivent être installés avec les configurations requises :

- «IBM DB2», à la page 441
- «IBM Tivoli Monitoring», à la page 441
- «Tivoli Netcool/OMNIbus», à la page 442
-

IBM DB2

La base de données IBM DB2 version 9.1 doit être installée et configurée avec tous les utilisateurs et les groupes par défaut. Pour plus d'informations sur l'installation de IBM DB2 version 9.1, consultez le centre de documentation *IBM DB2* sur : http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/index.jsp

IBM Tivoli Monitoring

La version 6.2.3 de IBM Tivoli Monitoring au minimum est requise. Configurez le produit avec un ou plusieurs serveurs distants et serveurs de surveillance concentrateur, Tivoli Enterprise Portal (serveur et client), Tivoli Data Warehouse et Tivoli Performance Analyser version 6.2.2 Groupe de correctifs 2.

Pour la configuration de IBM Tivoli Monitoring, utilisez la clé de chiffrement par défaut, IBMTivoliMonitoringEncryptionKey. Vous devez spécifier les fonctions suivantes pour l'installation :

- TEMA
- TEPS
- TEMS
- TEPD
- ECLIPSE

Sélectionnez l'agent TIVOLI ENTERPRISE USER EXTENSION. Après l'installation, l'agent de regroupement et d'élagage doit être configuré.

Pour Tivoli Enterprise Portal, spécifiez le nom d'hôte du serveur sur lequel Tivoli Enterprise Portal doit être installé. Indiquez DB2 en tant type de base de données.

Pour Tivoli Data Warehouse, toutes les bases de données doivent se trouver dans la base de données DB2.

Pour Tivoli Performance Analyzer, toutes les fonctions doivent être installées. Tivoli Performance Analyzer doit utiliser toutes les bases de données DB2 qui ont été configurées pendant l'installation d'IBM Tivoli Monitoring. Utilisez le pilote JDBC suivant pour la connexion à Tivoli Data Warehouse :

- Linux UNIX `/opt/IBM/sqllib/java/db2jcc.jar; /opt/IBM/sqllib/java/db2jcc_license_cu.jar`
- Windows `C:\Fichiers programmes\IBM\sqllib\java\db2jcc.jar; c:\Fichiers programmes\IBM\sqllib\java\db2jcc_license_cu.jar`

Windows Sur les ordinateurs 64 bit, utilisez les répertoires `Fichiers programmes` 32 bits. Les sources de données créées par l'applet Administrateur de sources de données ODBC par défaut disponible dans le panneau de contrôle, ne sont pas disponibles pour les applications 32 bits. Par conséquent, utilisez la version 32 bits de l'applet Administrateur de sources de données ODBC de *WINDOWS*`\SysWOW64\odbcad32.exe`.

Après l'installation de IBM Tivoli Monitoring, vérifiez que la base de données et les tables Tivoli Enterprise Portal ont été créées et connectez-vous au bureau Tivoli Enterprise Portal. En outre, si Eclipse ne démarre pas après l'installation, changez de numéro de port. Si Warehouse Proxy ne s'exécute pas après l'installation, vous pouvez le démarrer dans l'interface graphique Gérer les services Tivoli Enterprise

Monitoring. Si une erreur se produit pendant la configuration de Warehouse Proxy, vous pouvez le recréer manuellement à l'aide de l' Assistant Création de bases de données.

Indiquez également le nom et le port du serveur sur lesquels Probe for Tivoli EIF s'exécute sur le serveur Tivoli Enterprise Monitoring.

Pour de plus amples informations sur l'installation et la configuration de IBM Tivoli Monitoring, consultez le centre de documentation *IBM Tivoli Monitoring* sur http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.2fp2/welcome.htm.

Pour de plus amples informations sur l'installation et la configuration de l'analyseur de performance Tivoli version 6.2.2, consultez le centre de documentation *Tivoli Performance Analyzer V6.2.2* sur http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp?topic=/com.ibm.kpa.ovr.doc/c_ovr_product_overview.html

Dans votre installation IBM Tivoli Monitoring, vous devez activer la transmission des événements aux serveurs ObjectServer Tivoli Netcool/OMNIbus . Pour chaque serveur de surveillance de concentrateur à partir duquel vous souhaitez que les événements prévisibles soient transmis, activez la fonctionTivoli Event Integration Facility. Indiquez ensuite le nom d'hôte de l'ordinateur sur lequel se trouve Probe for Tivoli EIF et le numéro de port sur lequel la sonde est en mode écoute. Pour plus d'informations, recherchez le nœud de la version du produit IBM Tivoli Monitoring dans le centre de documentation. Puis, développez les sous-nœuds comme suit : *Guides d'installation et de configuration> Guide d'installation> Intégration des systèmes de gestion des événements > Configuration de la transmission des événements à Netcool/OMNIbus > Configuration du serveur de surveillance pour transmettre les événements*.

Tivoli Netcool/OMNIbus

La version 7.3.1 de Tivoli Netcool/OMNIbus au minimum est requise. Vérifiez que le produit est déployé et configuré comme suit.

Configurez les serveurs ObjectServer auxquels vous souhaitez transmettre les événements prévisibles sur les ordinateurs hôte désignés. Configurez les serveurs ObjectServer comme suit :

- Importez le fichier `tec_db_update.sql` dans chaque serveur ObjectServer afin que le schéma de base de données ObjectServer puisse stocker des données d'alerte provenant des événements de situation. Le fichier `tec_db_update.sql` fournit un mappage entre les zones de Tivoli Enterprise Console et les zones ObjectServer. Pour plus d'informations sur la mise à jour de ce mappage, voir «Informations complémentaires», à la page 443.
- Installez le composant de synchronisation d'événements IBM Tivoli Monitoring sur l'ordinateur hôte de chaque ObjectServer. Le composant de synchronisation des événements envoie des modifications de statut des événements de situation de Tivoli Netcool/OMNIbus vers le serveur de surveillance d'origine. Lors de l'installation du composant, entrez les informations demandées concernant les serveurs de surveillance concentrateur avec lesquels vous souhaitez que les événements de situation soient synchronisés. Le Transmetteur d'événements de situation est également installé, avec les fichiers binaires de support et de configuration. En outre, les fichiers sont installés et peuvent être utilisés pour

configurer Probe for Tivoli EIF. Pour plus d'informations sur le composant de synchronisation d'événements, consultez «Informations complémentaires».

Installez et configurez l' Interface graphique Web, y compris le client Interface graphique Web Administration Application Programming Interface (WAAPI) installé. Le client WAAPI est nécessaire pour charger les personnalisations des événements prévisibles. Pour plus d'informations, voir «Activation des événements prévisibles dans l'Interface graphique Web», à la page 587. Si vous souhaitez activer la fonctionnalité de lancement en contexte entre la liste d'événements actifs (AEL) et Tivoli Enterprise Portal, vérifiez que l'authentification unique est configurée.

Configurez les postes de travail client et vérifiez qu'ils ont accès aux outils de bureau Tivoli Netcool/OMNIbus et à l'Interface graphique Web.

Installez une ou plusieurs instances de Probe for Tivoli EIF. Pour plus d'informations sur l'installation, consultez les fichiers `README.txt` et `description.txt` dans le module de téléchargement de sonde. Une instance de Probe for Tivoli EIF doit être associée à chaque serveur ObjectServer auquel vous souhaitez transmettre les événements prévisibles. Des fichiers de règles personnalisés pouvant traiter des événements prévisibles sont fournis pour être utilisés avec Probe for Tivoli EIF. Le fichier `tivoli_eif.règles` est développé afin de mapper des attributs d'événements de situation générique à des zones ObjectServer de la table alerts.status. Ce fichier de règles contient également une instruction include commentée pour incorporer le fichier`événement_prévisibles.règles` fourni avec Tivoli Netcool/OMNIbus. Vérifiez que cette instruction n'est pas mise en commentaire. Pour plus d'informations sur la mise à jour de schéma qui est requise pour les événements de situation, voir «Informations complémentaires».

Installez IBM Tivoli Monitoring for Tivoli Netcool/OMNIbus Agent. Avant de démarrer l'agent, configurez-le, comme suit :

- Chargez les déclencheurs d'agent et les fichiers journaux à partir du fichier `itm_os.sql` dans le serveur ObjectServer.
- Indiquez le nom d'hôte de Tivoli Enterprise Monitoring Server, le nom du serveur ObjectServer et l'emplacement du fichier journal d'ObjectServer, lequel se trouve généralement dans `$NCHOME/omnibus/log`.

Une fois que vous avez démarré l'agent à partir de Tivoli Enterprise Monitoring Server, vérifiez que les éléments de l'agent OMNIbus sont affichés sur l'espace de travail du bureau Tivoli Enterprise Portal Server. Vérifiez également que les éléments correspondent aux événements de l'AEL et des listes d'événements de bureau.

Informations complémentaires

Pour plus d'informations, consultez les site Web suivants :

- Pour plus d'informations sur la configuration d'un environnement intégré avec IBM Tivoli Netcool/OMNIbus et IBM Tivoli Monitoring, voir le centre de documentation *IBM Tivoli Monitoring* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp.
- Pour plus d'informations sur l'installation d'un composant de synchronisation d'événements, localisez **IBM Tivoli Monitoring** dans le panneau de navigation de gauche du centre de documentation *IBM Tivoli Monitoring*. Développez ensuite les sous-nœuds comme suit :

Guides d'installation et de configuration > **Guide d'installation et de paramétrage** > **Intégration des systèmes de gestion des événements** > **Configuration de la transmission des événements à Netcool/OMNIbus** > **Installation du composant de synchronisation d'événements**

- Pour plus d'informations sur la configuration du mappage entre les zones Tivoli Enterprise Console et ObjectServer, voir la section *Configuration du serveur ObjectServer pour gérer des événements à partir de TEC* dans *IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF Reference Guide*. Ce guide est disponible sur le centre de documentation Network Availability Management à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp
- Pour plus d'informations sur la mise à jour de schéma requise pour les événements de situation et sur l'utilisation du fichier `tivoli_eif.rules` personnalisé, recherchez le nœud de la version du produit **IBM Tivoli Monitoring** du centre de documentation *IBM Tivoli Monitoring*. Développez ensuite les sous-nœuds comme suit :

  Guide d'installation et de configuration > **Guides d'installation et de paramétrage** > **Intégration des systèmes de gestion des événements** > **Configuration de la transmission des événements vers Netcool/OMNIbus** > **Configuration du serveur Netcool/OMNIbus Object**

  Dans cet emplacement référencé du centre de documentation, seules les sous-tâches intitulées **Mise à jour du schéma de base de données OMNIbus** et **Configuration de la sonde EIF** sont obligatoires pour les événements prévisibles et les analyses prévisionnelles. Les autres sont redondantes et ne sont importantes que si vous utilisez s'autres types d'événements de situation.

Ressources de configuration de Tivoli Netcool/OMNIbus pour les événements prévisibles

Tivoli Netcool/OMNIbus fournit un certain nombre de ressources pour activer les événements prévisionnels. Ces ressources sont disponibles en tant que modèles de fichiers se trouvant dans le répertoire `$NCHOME/omnibus/extensions/itmpredictive`.

Ressources du serveur ObjectServer

Les ressources Objectserver suivantes prennent en charge les événements prévisionnels :

- Un ID de classe de 89300 est réservé aux événements prévisibles.
- Dans la table alerts.status, les colonnes suivantes sont ajoutées afin de stocker les données spécifiques aux événements prévisibles :

Nom de colonne	Type de données	Obligatoire	Description
TrendDirection	integer	Non	Applicable aux événements prévisibles reçus d' IBM Tivoli Monitoring. Indique la tendance de prévision. Les valeurs sont les suivantes : `-1` : En baisse `0` : Constante `1` : En hausse

Nom de colonne	Type de données	Obligatoire	Description
Heure de l'estimation	taper	Oui	Applicable aux événements prévisibles reçus d' IBM Tivoli Monitoring. Spécifie le délai en jours, défini par Tivoli Performance Analyser, pour lequel les seuils définis seront dépassés. Il est recommandé d'appliquer une marge de 12 heures aux événements prévisibles générés.

- Les conversions suivantes mappent des valeurs entières à des valeurs de chaîne :
  - Conversion pour l'ID de classe ID 89300: `Evénements prévisibles`
  - Conversions pour la colonne TrendDirection : 1 = `Rising`, 0 = `Constant` et -1 = `Falling`
  - Conversion pour les colonnes DaysToCriticalThreshold et DaysToWarningThreshold : 9999 est convertie en chaîne vide car cette chaîne représente l'absence de valeur DaysToCriticalThreshold ou DaysToWarningThreshold.
- Les déclencheurs new_row_predictive et deduplicate_predictive sont fournis. Ces déclencheurs sont attribués au groupe de déclencheurs default_triggers. Le nouveau déclencheur new_row_predictive garantit que lors de l'insertion d'un nouvel événement prévisible dans le serveur ObjectServer, les zones correctes et le temps d'expiration de l'événement sont définis. Le déclencheur deduplicate_predictive garantit que les zones correctes sont copiées lors du dédoublonnage et que le temps d'expiration de l'événement est défini.

Ces ressources sont ajoutées au serveur ObjectServer lorsque vous importez le fichier de package `predictive_events_menutools_native_gui.jar`, qui est l'un des modèles de fichier du répertoire `$NCHOME/omnibus/extensions/itmpredictive`.

Ressources de visualisation des événements

Les ressources suivantes prennent en charge l'affichage des événements prévisibles dans la liste d'événements et dans la liste d'événements actifs :

- Un fichier de filtre, `predictive_event.elf`, un fichier de vue, `predictive_event.elv`, et un fichier de configuration de liste d'événements, `predictive_event.elc`, sont fournis pour filtrer et trier les événements prévisibles dans la liste d'événements. Le filtre et la vue sont définis de la manière suivante :
  - Le filtre **Predictions (Prévisions)** est défini par la clause WHERE suivante :
    ```
    where Class = 89300
    ```
  - La vue **Predictions** (Prévisions) contient les colonnes par défaut suivantes, qui s'affichent ainsi de gauche à droite : Node, TrendDirection, Summary, FirstOccurrence, LastOccurrence, Count, PredictionTime.

    La priorité et l'ordre de tri des colonnes sont les suivants :

    1. Gravité par ordre décroissant
    2. LastOccurrence par ordre croissant

3. PredictionTime par ordre croissant

- Les ressources de configuration de la liste d'événements actifs sont fournis sous la forme d'une fichier de commandes WAAPI appelé `predictive_events_web_gui.xml`, qui crée un filtre, une vue, des outils, des invites et des options de menu pour les événements prévisibles et ajoute des ressources Web (un fichier `.jsp`, des images et une feuille de style) au serveur de l'Interface graphique Web. Les informations sur WAAPI (Web GUI Administration Application Program Interface) sont disponibles dans le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Ressources du fichier de règles

Un fichier de règles personnalisées, qui peut traiter les événements prévisibles, est fourni pour Probe for Tivoli EIF. Ce fichier de règles est appelé `predictive_event.rules`.

Le fichier `predictive_event.rules` mappe spécifiquement les attributs d'événement prévisible (de Tivoli Performance Analyzer) aux zones du serveur ObjectServer. Les mappages des attributs aux colonnes entre les attributs Tivoli Performance Analyzer calculés à partir de l'analyse de tendance et les colonnes de la table alerts.status sont les suivants :

Tableau 84. Mappages du fichier de règles pour les événements prévisibles

Attribut Tivoli Performance Analyzer	**Colonne de la table alerts.status**	**Remarques sur le mappage**
Direction	TrendDirection	Indique une prévision ascendante ou descendante ou une ligne plate. Nouvelle colonne de la table alerts.status.
Confidence	ExtendedAttr	Valeur sous forme de pourcentage comprise entre 0 et 100 qui désigne le niveau de confiance en la tendance prévisible. Dans cette plage, 0 décrit aucune confiance et 100 décrit une fonction parfaitement bien prévue. Pas promu en colonne.
Strength	ExtendedAttr	Puissance de la tendance, en fonction d'une corrélation entre la confiance et le nombre d'échantillons analysés. Pas promu en colonne.
TimeStamp	LastOccurrence	Horodatage indiquant le moment où la prévision a été calculée.

Tableau 84. Mappages du fichier de règles pour les événements prévisibles (suite)

Attribut Tivoli Performance Analyzer	Colonne de la table alerts.status	Remarques sur le mappage
Num_Of_Samples	ExtendedAttr	Nombre d'échantillons (ou de points de données) utilisés pour établir la tendance. Plus le nombre d'échantillons est élevé, plus la prévision estimée est précise. Pas promu en colonne.
Node	Agent	Nom de l'hôte sur lequel Tivoli Performance Analyzer s'exécute. Il s'agit de l'unité produisant les événements d'erreur sur laquelle la tendance est basée.
system_name	Node	Nom d'hôte sur lequel les métriques prévisibles ont été réalisées.
89300	Class	ID de classe réservé, qui est alloué aux événements prévisibles.
Valeurs de chaîne littérales	Summary	Tivoli Performance Analyzer fournit un ensemble de valeurs de chaîne littérales insérées dans la colonne Summary de la table alerts.status.
Tous les autres attributs	ExtendedAttr	Attributs étendus supplémentaires.
3 (WARNING)	Severity	Niveau de gravité, comme indiqué dans IBM Tivoli Monitoring. La valeur peut être 3 ou 5.
5 (CRITIQUE)	Severity	Niveau de gravité, comme indiqué dans IBM Tivoli Monitoring. La valeur peut être 3 ou 5.

Tâches associées:

«Configuration des événements prévisibles dans votre environnement intégré», à la page 448

Une événement prévisible est une alerte qui prévient les opérateurs qu'un incident peut se produire à l'avenir. Les événements prévisibles sont générés dans IBM Tivoli Monitoring et peuvent être transmis à Tivoli Netcool/OMNIbus pour être affichés dans la liste d'événements ou dans la Liste d'événements actifs.

Configuration des événements prévisibles dans votre environnement intégré

Une événement prévisible est une alerte qui prévient les opérateurs qu'un incident peut se produire à l'avenir. Les événements prévisibles sont générés dans IBM Tivoli Monitoring et peuvent être transmis à Tivoli Netcool/OMNIbus pour être affichés dans la liste d'événements ou dans la Liste d'événements actifs.

Avant de commencer

Vous devez avoir au minimum les versions de produit suivantes : Tivoli Netcool/OMNIbus version 7.3.1 et IBM Tivoli Monitoring version 6.2.3. Vérifiez que vous avez installé et configuré ces deux produits, de sorte qu'ils soient à l'état opérationnel. Pour plus d'informations sur la configuration des systèmes, voir «Conditions préalables pour les événements prévisibles et les analyses prévisionnelles», à la page 440.

Procédure

Pour configurer la gestion des événements prévisibles :

1. Copiez le fichier `itm_event.rules` de votre installation IBM Tivoli Monitoring dans le répertoire suivant sur chaque ordinateur hôte sur lequel Probe for Tivoli EIF est installé :

   `$NCHOME/omnibus/probes/`*`arch`*

2. Sur chaque hôte du serveur ObjectServer, importez la configuration de gestion d'événements prévisibles dans le schéma ObjectServer en accédant au répertoire `$NCHOME/omnibus/bin` et en exécutant la commande suivante :

   ```
   nco_confpack -import -server nom_serveur -user nom_utilisateur -password
   mot_de_passe -package $NCHOME/omnibus/extensions/itmpredictive/
   predictive_events_menutools_native_gui.jar -nowarn
   ```

   Où *nom_serveur* est le nom du serveur ObjectServer, et *nom_utilisateur* et *mot_de_passe* sont les identifiants de connexion ObjectServer.

3. Accédez au répertoire `$NCHOME/omnibus/extensions/itmpredictive`.
4. Copiez le fichier `predictive_event.rules` personnalisé dans le répertoire suivant sur chaque ordinateur hébergeant Probe for Tivoli EIF :

   `$NCHOME/omnibus/probes/`*`arch`*

   Ce répertoire contient déjà le fichier personnalisé `tivoli_eif.rules`.
5. Supprimez les droits d'accès en lecture par défaut dans le fichier `predictive_event.rules`.
6. Modifiez le fichier `tivoli_eif.rules`.
   a. Supprimez la mise en commentaire de l'instruction `include` commentée qui intègre le fichier `predictive_event.rules`.
   b. Supprimez la mise en commentaire de l'instruction `include` commentée qui intègre le fichier `itm_event.rules`.
   c. Si la sonde est en cours d'exécution, lisez à nouveau le fichier de règles.
7. Pour la visualisation d'événements dans la liste d'événements, copiez les fichiers suivants dans un emplacement préconisé et supprimez les droits de lecture seule par défaut de ces fichiers.
   - `predictive_event.elc`
   - `predictive_event.elv`
   - `predictive_event.elf`

8. Facultatif : Mettez le fichier `predictive_event.elc` à disposition des opérateurs de liste d'événements. Ce fichier est une configuration de liste d'événements pouvant être chargée dans la fenêtre de la zone de surveillance Liste des événements. Cette configuration comporte un seul écran de surveillance **Predictions** (Prévisions) avec un filtre Predictions et une vue Predictions (Prévisions). La configuration peut être chargée à partir du menu **Fichier** > **Ouvrir**.
9. Pour charger le filtre `predictive_event.elf` et la vue `predictive_event.elv` dans une configuration de liste d'événements existante, procédez comme suit :
   a. Dans la fenêtre d'écrans de surveillance Liste d'événements, cliquez sur **Fenêtres** > **Configuration** pour ouvrir la fenêtre Configuration de la liste d'événements
   b. Lorsque vous affichez les filtres qui font partie de cette configuration de liste d'événements :
      - UNIX Linux Cliquez sur **Charger**.
      - Windows Cliquez sur **Ouvrir**.
   c. Accédez à l'emplacement où le fichier de filtre `predictive_event.elf` est sauvegardé, sélectionnez le fichier et cliquez sur **OK**.
   d. Lorsque vous affichez les vues qui font partie de cette configuration de liste d'événements :
      - UNIX Linux Cliquez sur **Charger**.
      - Windows Cliquez sur **Ouvrir**.
   e. Accédez à l'emplacement où le fichier de vue `predictive_event.elv` est sauvegardé, sélectionnez le fichier et cliquez sur **OK**.
   f. Sauvegardez la configuration de liste d'événements. Le filtre et la vue sont ajoutés en tant qu'écran de surveillance **Predictions** (Prévisions) et peuvent également être sélectionnés dans toutes les listes d'événements de cette configuration de liste d'événements.
   g. Appliquez les colonnes d'événements prévisibles à la table alerts.status puis activez les déclencheurs d'événements prévisibles à l'aide de la commande suivante pour votre système d'exploitation :
      - UNIX Linux `./nco_sql -user root -password` *`mot de passe`* `-server` *`NCOMS`* `< /opt/IBM/tivoli/netcool/omnibus/extensions/itmpredictive/predictive_event.sql`
      - Windows `isql -S` *`NCOMS`* `-U root -P` *`mot_de_passe`* `-i C:\IBM\Tivoli\Netcool\omnibus\extensions\itmpredictive\predictive_event.sql`

      Où *NCOMS* est le nom du serveur ObjectServer et où *mot de passe* est le mot de passe du superutilisateur.

Résultats

Vous pouvez à présent surveiller les événements prévisibles dans la liste d'événements.

Que faire ensuite

Configurez la liste AEL pour la gestion d'événements prévisibles.

Vous pouvez désormais également suivre la procédure de configuration pour l'analyse prévisionnelle.

Pour obtenir plus d'informations sur la surveillance des événements prévisibles dans la liste d'événements, voir *IBM Tivoli Netcool/OMNIbus User's Guide*. Pour obtenir plus d'informations sur la surveillance des événements prévisibles dans la liste d'événements AEL, voir *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Tâches associées:

«Configuration de l'authentification unique (SSO)», à la page 576
Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

Référence associée:

«Ressources de configuration de Tivoli Netcool/OMNIbus pour les événements prévisibles», à la page 444
Tivoli Netcool/OMNIbus fournit un certain nombre de ressources pour activer les événements prévisionnels. Ces ressources sont disponibles en tant que modèles de fichiers se trouvant dans le répertoire `$NCHOME/omnibus/extensions/itmpredictive`.

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Configuration des tendances linéaires

Après avoir configuré les événements prévisibles, vous pouvez effectuer la configuration de la tendance linéaire, qui permet de déceler les problèmes liés aux débits d'événements d'unités avant que ces problèmes ne se produisent.

Avant de commencer

Votre environnent doit respecter les conditions préalables pour pouvoir générer des événements prévisibles et effectuer des analyses prévisionnelles. En outre, vous devez avoir configuré les événements prévisibles pour votre environnement intégré et Tivoli Netcool/OMNIbus doit être en cours d'exécution. Les étapes suivantes expliquent la marche à suivre pour installer et configurer les événements prévisibles.

Remarque : Il est supposé que vous possédez des connaissances de base sur IBM Tivoli Monitoring.

Pourquoi et quand exécuter cette tâche

Pour installer une tendance linéaire, vous devez installer un domaine fourni, mais non installé, avec Tivoli Netcool/OMNIbus dans IBM Tivoli Monitoring. Le domaine installe les dispositifs suivants, qui sont obligatoires pour permettre le calcul d'une tendance linéaire :

- Deux espaces de travail pour afficher et analyser les données de tendance
- Deux situations : l'une est générée jusqu'à sept jours avant que le seuil d'avertissement ne soit dépassé ; l'autre est générée jusqu'à sept jours avant que le seuil critique ne soit dépassé, d'après les prévisions de la courbe de tendance.

- Une tendance. La tendance prend en charge les prévisions tous les sept, 30 et 90 jours. Les situations ne sont fournies que pour des prévisions à sept jours.

Lorsque vous installez Tivoli Netcool/OMNIbus, le domaine est installé par défaut.

Certaines des instructions suivantes ne sont applicables que dans le cadre d'un environnement de test ; cela sera indiqué le cas échéant.

Pour configurer les événements prévisibles dans un environnement Tivoli Netcool/OMNIbus intégré et un environnement IBM Tivoli Monitoring :

Procédure

1. Dans Tivoli Enterprise Portal, configurez la collecte de données historiques dans l'agent IBM Tivoli Monitoring pour Tivoli Netcool/OMNIbus. Cette étape s'effectue dans la fenêtre History Collection Configuration (Configuration de collecte historique).
   a. Vous devez définir le groupe d'attributs KNO EVENT RATE BY NODE de façon à ce qu'il soit archivé toutes les heures et définir l'élagage sur une semaine ou plus. Créez ensuite de nouveaux paramètres de collecte, dans lesquels les intervalles de collecte et de l'entrepôt de données sont aussi rapprochés que possible. Définissez le groupe d'attributs pour les paramètres de collecte sur KNO EVENT RATE BY NODE. Dans l'onglet **Distribution**, démarrez la collecte sur le groupe OMNIBUS_SERVER_AGENT.

      Dans le panneau de gauche, une icône est affichée à côté de l'élément **Tivoli Netcool/OMNIbus** pour indiquer que des données sont en train d'être collectées. L'agent IBM Tivoli Monitoring pour Tivoli Netcool/OMNIbus crée plusieurs tables et vues dans la base de données IBM DB2. Les tables sont les suivantes :
      - KNO_EVENT_RATE_BY_NODE
      - KNO_EVENT_RATE_BY_NODE _H

      La vue est : KNO_EVENT_RATE_BY_NODE_HV.
   b. Vérifiez que les tables et vues ont été créées dans la base de données IBM DB2. Les tables et vues ne sont pas immédiatement créées.
   c. Répétez l'étape 1a pour les groupes d'attributs KPA_T_NO8099_LTF et KPA_T_NO8099_LTS.
2. Dans votre installation Tivoli Netcool/OMNIbus, accédez au répertoire `extensions/itmpredictive` et copiez le répertoire `itpa_tendance` dans votre installation IBM Tivoli Monitoring.
3. Dans votre installation IBM Tivoli Monitoring, accédez au répertoire `itpa_tendance` et exécutez la commande suivante pour démarrer l'installation :
   - UNIX `domaintool.sh`
   - Windows `domaintool.bat`

   Remarque : Ignorez le répertoire `corbeille`.
4. Entrez l'emplacement où vous avez installé IBM Tivoli Monitoring. Par exemple, sous Windows, `C:\IBM\ITM`.

   L'outil d'activation de domaine ITPA détecte l'installation de Tivoli Enterprise Portal Server et de Tivoli Performance Analyzer.

5. Dans la prochaine fenêtre, acceptez les options **Tivoli Enterprise Portal Server (TEPS)**, **Tivoli Performance Analyzer (TPA)** et **Tivoli Enterprise Monitoring Server (TEMS)**.

   Si une de ces options est grisée, l'utilisateur exécutant l'installation ne dispose pas des droits pour modifier la base de données concernée. Vous devez ajouter ces droits dans la base de données IBM DB2 et dans Tivoli Enterprise Portal Server, puis exécuter à nouveau la commande **domaintool**.

6. Sélectionnez le domaine **omnibus_event_rate**.

   Le domaine est installé. Une fois l'installation terminée, un message de réussite s'affiche.

7. Cliquez sur **Finish** (Terminer) et redémarrez manuellement Tivoli Enterprise Portal Server et Tivoli Performance Analyzer.

8. Pour vérifier que l'installation du domaine a été réussie, connectez-vous au serveur Tivoli Enterprise Portal Server et procédez comme suit :

   - Pour vérifier que les espaces de travail sont installés : A partir du panneau de navigation de gauche, développez le nœud pour l'ordinateur sur lequel IBM Tivoli Monitoring est installé. Cliquez avec le bouton droit de la souris sur **Performance Analyzer Warehouse Agent** et cliquez sur **Workspaces** (Espaces de travail). Les espaces de travail suivants devraient s'afficher pour la sélection :
     - **Event_Rate Details (Détails du taux d'événements)** : Cet espace de travail affiche un graphique qui illustre les prévisions de la tendance. Il est conçu pour afficher les données par nœud (ou unité). Par conséquent, sélectionnez-le uniquement à l'aide de l'icône de lien d'une tendance affichée dans l'espace de travail Event_Rate Overview.
     - **Event_Rate Overview** : Cet espace de travail affiche une liste de prévisions, par exemple, la prévision à sept jours. Les prévisions à 30 et 90 jours sont également fournies.

     Les espaces de travail afficheront des erreurs jusqu'à ce que suffisamment de données aient été archivées par l'agent de regroupement et d'élagage.
   - Pour vérifier que les situations sont installées : Cliquez sur **Situation Editor** (Editeur de situations). Sous **Performance Analyzer Warehouse Agent**, vous devriez voir les deux situations suivantes :
     - **Event_Rate_TTCT_1W** : Ce nom correspond à la «durée avant le seuil critique : une semaine.»
     - **Event_Rate_TTWT_1W**: Ce nom correspond à «durée avant le seuil d'avertissement : une semaine.»

     Ces situations sont générées lorsqu'il est prévu que la tendance dépasse les seuils définis (en nombre d'événements) dans les sept jours suivants. Pour savoir comment changer les seuils par défaut, reportez-vous à l'étape 9.
   - Pour vérifier que la tendance est installée : Cliquez sur **Performance Analyzer Configuration** (Configuration de l'analyseur de performances) puis sur **Analytics** (Analyse). Dans la fenêtre Performance Analyzer Configuration (Configuration de l'analyseur de performances), vous devriez voir une tendance appelée **Event Rate Forecast** (Prévision de débit d'événements).

   Si le message d'erreur suivant s'affiche, il peut être ignoré en toute sécurité :

   ```
   SQL Error $KPACNO08099 AGENTNODE$ not valid in context.
   ```

9. Facultatif : Pour changer les valeurs des seuils pour lesquelles des situations sont générées, dans Situation Editor (Editeur de situation), cliquez sur **Sortie**.

Changez le nombre d'événements pour **Décompte avant seuil critique** et **Décompte avant seuil d'avertissement** si nécessaire.

La valeur par défaut pour Time to Critical threshold (décompte avant seuil critique) est de 10 000 événements et la valeur par défaut pour Time to Warning threshold (décompte avant seuil d'avertissement) est 8000 événements.

10. Facultatif : Dans un environnement de test, simulez des tendances linéaires en installant une sonde dans votre Tivoli Netcool/OMNIbus pour effectuer une simulation, ou en utilisant votre environnement de simulation existant. Simulez un débit d'événements en hausse qui atteindra le seuil d'avertissement et le seuil critique d'ici une période raisonnable pour effectuer un test.

    Conseil : Par défaut, l'agent de collecte Tivoli Data Warehouse collecte des données toutes les 15 minutes et enregistre les valeurs minimale, maximale et moyenne sur la base de données Tivoli Data Warehouse DB2 toutes les heures. Si d'importants volumes de données sont générés, il est possible que la charge du serveur augmente. Dans un environnent qui subit déjà de lourdes charges, vous pouvez réduire ces charges en réduisant l'intervalle de collecte de l'agent de collecte Tivoli Data Warehouse.

11. Attendez que l'environnement génère des données archivées et crée une tendance de données. En règle générale, 10 heures sont nécessaires avant de générer suffisamment de données.

    Pour effectuez un test, définissez l'élagage de sorte qu'il ait lieu toutes les deux semaines. Notez que, dans un environnement de production, si vous autorisez la génération d'un trop grand nombre de données archivées, la courbe de tendance deviendra de plus en plus horizontale. Les intervalles de collecte et celles de Tivoli Data Warehouse doivent être définies sur des valeurs aussi basses que possible, de manière à ce que les intervalles soient aussi rapprochés que possible. L'agent de collecte Tivoli Data Warehouse collecte des données toutes les 15 minutes et enregistre les valeurs minimale, maximale et moyenne sur la base de données Tivoli Data Warehouse DB2 toutes les heures. Si d'importants volumes de données sont générés, il est possible que la charge du serveur augmente. Dans un environnent qui subit déjà de lourdes charges, vous pouvez réduire la charge en réduisant l'intervalle de collecte de l'agent de collecte Tivoli Data Warehouse.

12. Vérifiez que le flot de données fonctionne correctement. Pour vérifier le flot de données, procédez comme suit :
    - Pour vérifier que les données correctes sont archivées dans la base de données DB2 utilisée par Tivoli Data Warehouse, utilisez le Centre de contrôle DB2. Sous WAREHOUS, vérifiez les tables et KNO_EVENT_RATE_BY_NODE_H pour consultez les archives horaires des débits d'événements.
    - Pour vérifier que ces données sont chargées via l'agent Tivoli Performance, dans la fenêtre Performance Analyzer Agent Statistics (Statistiques de l'agent analyseur de performances), vérifiez que l'état de la tâche analytique est défini sur `Calculé`.

Que faire ensuite

Pour afficher le graphique d'une tendance particulière, dans l'espace de travail Event_Rate Overview, cliquez sur **Link (Lien)** > **Détails**. Si un message d'erreur s'affiche lorsque vous affichez le graphique dans l'espace de travail Event_Rate Details, vérifiez que les données Tivoli Performance Analyzer sont correctement

archivées. Plus particulièrement, vérifiez les groupes d'attributs KPA_T_NO80099_LTF et KPA_T_NO80099_LTS pour Performance Analyzer Warehouse Agent dans Tivoli Enterprise Portal.

Si nécessaire, vous pouvez créer des situations qui sont générées jusqu'à 30 ou 90 jours avant que le seuil ne soit dépassé.

Vous pouvez aussi configurer une base de référence qui établit en temps réel des rapports sur les débits d'événements d'unités.

Résolution des problèmes

Si les performances de votre système sont lentes, ne paramétrez pas l'archivage pour qu'il s'exécute à un débit rapide car cela pourrait surcharger les performances du système, surtout à mesure que des données sont générées dans la base de données DB2.

Concepts associés:

«Conditions préalables pour les événements prévisibles et les analyses prévisionnelles», à la page 440
Pour pouvoir configurer l'environnement, IBM Tivoli Netcool/OMNIbus, IBM Tivoli Monitoring, IBM DB2 sont requis avec une version particulière et des niveaux de groupes de correctifs avec des configurations spécifiques.

Tâches associées:

«Configuration de la base de référence»
Vous pouvez surveiller les débits d'événements reçus depuis les sondes par Tivoli Netcool/OMNIbus en temps réel, en configurant la fonctionnalité de base de référence dans votre IBM Tivoli Monitoring intégré. Vous pouvez définir les écarts supérieur et inférieur sur la base de référence qui, lorsqu'ils sont dépassés, déclenchent une situation depuis IBM Tivoli Monitoring. Probe for Tivoli EIF convertit la situation en un événement qui est reçu par le serveur ObjectServer.

«Configuration des événements prévisibles dans votre environnement intégré», à la page 448
Une événement prévisible est une alerte qui prévient les opérateurs qu'un incident peut se produire à l'avenir. Les événements prévisibles sont générés dans IBM Tivoli Monitoring et peuvent être transmis à Tivoli Netcool/OMNIbus pour être affichés dans la liste d'événements ou dans la Liste d'événements actifs.

Configuration de la base de référence

Vous pouvez surveiller les débits d'événements reçus depuis les sondes par Tivoli Netcool/OMNIbus en temps réel, en configurant la fonctionnalité de base de référence dans votre IBM Tivoli Monitoring intégré. Vous pouvez définir les écarts supérieur et inférieur sur la base de référence qui, lorsqu'ils sont dépassés, déclenchent une situation depuis IBM Tivoli Monitoring. Probe for Tivoli EIF convertit la situation en un événement qui est reçu par le serveur ObjectServer.

Avant de commencer

Assurez-vous que l'on vous demande l'identificateur et le mot de passe IBM Tivoli Enterprise Portal, ainsi que le nom d'hôte ou adresse IP IBM Tivoli Enterprise Portal. Vous aurez également besoin du nom du répertoire dans lequel Tivoli Netcool/OMNIbus est installé.

En outre, vous devez effectuer les étapes de configuration décrites dans le paragraphe suivant :

- «Conditions préalables pour les événements prévisibles et les analyses prévisionnelles», à la page 440
- «Configuration des événements prévisibles dans votre environnement intégré», à la page 448
- «Configuration des tendances linéaires», à la page 450

Pourquoi et quand exécuter cette tâche

Configurez la base de référence en installant deux situations par défaut dans IBM Tivoli Monitoring. Ces situations sont générées comme suit :

- High_Event_Rate_Baseline est générée lorsque le seuil supérieur, défini par l'écart déduit du couloir de normalité, est dépassé.
- Low_Event_Rate_Baseline est générée lorsque le seuil inférieur, défini par l'écart déduit du couloir de normalité, est dépassé.

Installez ces situations dans IBM Tivoli Monitoring à l'aide du script fourni avec Tivoli Netcool/OMNIbus. Ce script permet de définir les seuils supérieur et inférieur. Il permet également de définir une tâche (un travail cron sous UNIX, une tâche panifiée sous Windows) qui met à jour les situations avec des débits d'événements horaires moyens qui sont comparés aux seuils. Ces valeurs moyennes sont basées sur les débits d'événements reçus pendant l'heure en cours lors des semaines précédentes, par exemple, entre 14h et 15h les jeudis. Le débit d'événements en cours est calculé toutes les 15 minutes. Le script s'exécute sur l'hôte Tivoli Netcool/OMNIbus et peut se connecter à l'hôte IBM Tivoli Monitoring à distance.

Pour configurer une base de référence :

Procédure

1. Sur l'ordinateur hôte Tivoli Netcool/OMNIbus, accédez au répertoire `$NCHOME\itmpredictive\baseline` et exécutez le script `init_baseline.sh`.
2. A l'invite du script, donnez les informations suivantes :
   - Le nom du répertoire où Tivoli Netcool/OMNIbus est installé (la valeur par défaut est `$OMNIHOME`)
   - Le nombre de semaines précédentes, obligatoire pour permettre le calcul du débit d'événements moyen correspond à l'heure en cours (la valeur par défaut est de cinq semaines)
   - Le niveau d'écart du débit d'événements moyen obligatoire pour dépasser le seuil inférieur et déclencher la situation Low_Event_Rate_Baseline. Cette valeur est définie comme le débit d'événements auquel le *nombre_écarts* est soustrait. La valeur par défaut est `2.0`.
   - Le niveau d'écart par rapport au débit d'événements moyen obligatoire pour dépasser le seuil supérieur et déclencher la situation High_Event_Rate_Baseline. Cette valeur est définie comme le débit d'événements auquel le *nombre_écarts* est additionné. La valeur par défaut est `2.0`.
   - L'identificateur et le mot de passe IBM Tivoli Enterprise Portal (l'utilisateur par défaut est `sysadmin`)
   - Le nom d'hôte ou l'adresse IP IBM Tivoli Enterprise Portal (la valeur par défaut est `localhost`)
3. Confirmez que les situations et le travail cron ou la tâche planifiée ont été ajoutés :

a. Dans Tivoli Enterprise Portal, démarrez l'éditeur de situations et vérifiez que les situations High_Event_Baseline et Low_Event_Baseline ont été ajoutées à l'élément **Tivoli OMNIbus Server**.
b. Vérifiez l'existence du travail cron ou de la tâche planifiée comme suit :
   - UNIX Exécutez la commande `crontab -l` et vérifiez la ligne suivante :

     ```
     1 * * * * $OMNIHOME/extensions/itmpredictive/baseline/
     dynamic_event_rate_baseline.sh
     ```

   - Windows Dans la liste **Scheduled Tasks (Tâches planifiées)**, vérifiez la tâche **Dynamic Event Rate Baseline**.
4. Autorisez les données d'événement à dépasser le nombre de semaines spécifié pour permettre le calcul des débits d'événements moyens.

Concepts associés:

«Conditions préalables pour les événements prévisibles et les analyses prévisionnelles», à la page 440
Pour pouvoir configurer l'environnement, IBM Tivoli Netcool/OMNIbus, IBM Tivoli Monitoring, IBM DB2 sont requis avec une version particulière et des niveaux de groupes de correctifs avec des configurations spécifiques.

Tâches associées:

«Configuration des tendances linéaires», à la page 450
Après avoir configuré les événements prévisibles, vous pouvez effectuer la configuration de la tendance linéaire, qui permet de déceler les problèmes liés aux débits d'événements d'unités avant que ces problèmes ne se produisent.

«Configuration des événements prévisibles dans votre environnement intégré», à la page 448
Une événement prévisible est une alerte qui prévient les opérateurs qu'un incident peut se produire à l'avenir. Les événements prévisibles sont générés dans IBM Tivoli Monitoring et peuvent être transmis à Tivoli Netcool/OMNIbus pour être affichés dans la liste d'événements ou dans la Liste d'événements actifs.

Activation de la prise en charge des événements TADDM

IBM Tivoli Application Dependency Discovery Manager (TADDM) est un outil de gestion des configurations qui reconnaît les systèmes matériels et logiciels d'un environnement informatique. TADDM est un sous-système du produit IBM Tivoli Change and Configuration Management Database .

Vous pouvez configurer TADDM afin qu'il génère des événements de notification lors de la reconnaissance de modifications apportées à un élément de configuration de votre environnement informatique et qu'il réachemine les événements vers Probe for Tivoli EIF. La sonde peut ensuite réacheminer les événements vers le serveur ObjectServer de Tivoli Netcool/OMNIbus à des fins de surveillance dans la liste d'événements actifs ou dans la liste d'événements de bureau. Les outils du menu de lancement en contexte vous permettent de naviguer de la liste d'événements ou de la liste d'événements actifs vers l'interface graphique TADDM afin de récupérer des informations complémentaires sur les modifications reconnues.

Certains scénarios courants sont les suivants :

- Lorsque votre infrastructure d'applications informatiques change, vous souhaitez recevoir des alertes afin de rester informé des modifications de configuration apportées à votre infrastructure d'applications informatiques. De telles alertes

sont générées à la suite d'une reconnaissance TADDM et identifient les modifications qui se sont produites depuis la dernière reconnaissance.

- A partir de Tivoli Netcool/OMNIbus, vous souhaitez récupérer les informations détaillées sur l'infrastructure d'applications informatiques connexes à une modification de configuration spécifique afin de savoir ce qui a été modifié.
- Dans Tivoli Netcool/OMNIbus, vous souhaitez récupérer l'historique des changements d'un élément de l'infrastructure d'applications informatiques connexe à une alerte de modification de configuration afin de pouvoir analyser la stabilité de votre infrastructure d'applications informatiques.

Remarque : Il est supposé que vous possédez des connaissances de base sur TADDM.

Installation et configuration des événements TADDM

Pour surveiller les événements TADDM dans Tivoli Netcool/OMNIbus, Tivoli Netcool/OMNIbus, la Probe for Tivoli EIF et TADDM doivent être installés dans un environnement intégré.

La figure suivante illustre la configuration requise pour les composants produit dans l'environnement intégré.

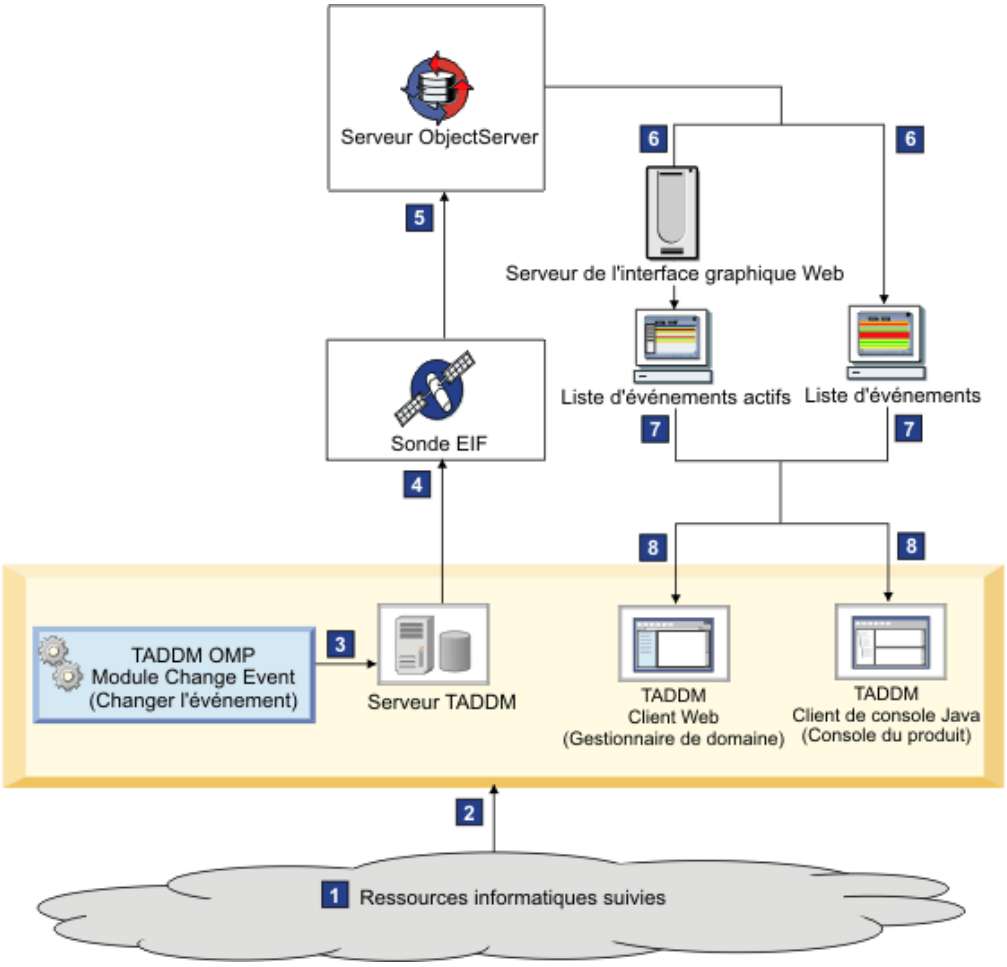

Figure 16. Configuration de Tivoli Netcool/OMNIbus et de TADDM pour surveiller les événements TADDM

Le flux de configuration est le suivant :

1. La configuration d'une ressource (ou d'un élément) informatique est modifiée par un utilisateur.
2. La modification est reconnue par un capteur TADDM lors du processus de reconnaissance.
3. Une fois le processus de reconnaissance terminé, un module complémentaire configuré pour TADDM recherche des modifications apportées aux éléments dont vous souhaitez effectuer le suivi. (Ce module s'appelle TADDM OMP Change Event Module.) Si des modifications sont détectées pour l'un des éléments suivis, le module Change Event génère un événement EIF qui contient les détails des modifications de configuration.
4. L'événement EIF est réacheminé vers Probe for Tivoli EIF.
5. Probe for Tivoli EIF traite les données d'événement, mappe les données aux zones du serveur ObjectServer, puis envoie une alerte au serveur ObjectServer.
6. L'alerte s'affiche en tant qu'événement TADDM dans la liste d'événements actifs ou dans la liste d'événements de bureau.
7. Dans la liste d'événements actifs ou dans la liste d'événements, les outils de menu de lancement en contexte vous permettent de demander des détails complémentaires sur les attributs de l'élément de configuration ou son historique des changements.
8. Vous pouvez afficher les détails dans l'application Web ou Console TADDM.

Tâches associées:

«Configuration du support pour les événements TADDM dans votre environnement intégré», à la page 459
Vous pouvez configurer Tivoli Netcool/OMNIbus, Probe for Tivoli EIF, et TADDM afin de surveiller les événements de TADDM dans la liste d'événements de Tivoli Netcool/OMNIbus ou la liste d'événements actifs.

Référence associée:

«Fichiers de configuration Tivoli Netcool/OMNIbus pour les événements TADDM»
Lorsque vous installez Tivoli Netcool/OMNIbus, un certain nombre de fichiers de configuration permettent de surveiller les événements TADDM. Ces fichiers de configuration se situent dans le répertoire `$NCHOME/omnibus/extensions/taddm`.

Fichiers de configuration Tivoli Netcool/OMNIbus pour les événements TADDM

Lorsque vous installez Tivoli Netcool/OMNIbus, un certain nombre de fichiers de configuration permettent de surveiller les événements TADDM. Ces fichiers de configuration se situent dans le répertoire `$NCHOME/omnibus/extensions/taddm`.

Les détails des fichiers de configuration sont les suivants :

- `taddm.elf` : Ce fichier de filtre peut être utilisé pour filtrer les événements TADDM dans la liste d'événements. Le filtre est défini par la clause WHERE suivante :

  ```
  where Class = 87721
  ```

- Fichier `taddm_menutools_native_gui.jar` : ce fichier de package crée les ressources ObjectServer suivantes :

  - Un menu et des outils peuvent être appliqués aux événements TADDM de la liste d'événements
  - L'ID de classe réservé 87721 pour les événements TADDM
  - Une conversion pour l'ID de classe 87721 : `Tivoli Application Dependency Discovery Manager`
- Fichier `taddm_menutools_web_gui.xml` : ce fichier de commandes WAAPI crée le menu, les outils et le filtre qui peut être appliqué aux événements TADDM de la liste d'événements actifs. Le menu, les outils et le filtre sont ajoutés au serveur d'Interface graphique Web. Les informations sur l'interface WAAPI (Web GUI Administration Application Program Interface) sont disponibles dans le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .
- Fichier `tivoli_eif_taddm.rules` : ce fichier de règles personnalisé est destiné à Probe for Tivoli EIF, et doit être inséré dans le fichier `tivoli_eif.rules` principal. Le fichier `tivoli_eif_taddm.rules` contient la logique permettant de traiter les détails de modification de configuration détectés lors de la reconnaissance TADDM, et de mapper les données aux zones ObjectServer. Ce fichier de règles attribue également l'ID de classe 87721 aux événements.

Tâches associées:

«Configuration du support pour les événements TADDM dans votre environnement intégré»
Vous pouvez configurer Tivoli Netcool/OMNIbus, Probe for Tivoli EIF, et TADDM afin de surveiller les événements de TADDM dans la liste d'événements de Tivoli Netcool/OMNIbus ou la liste d'événements actifs.

Configuration du support pour les événements TADDM dans votre environnement intégré

Vous pouvez configurer Tivoli Netcool/OMNIbus, Probe for Tivoli EIF, et TADDM afin de surveiller les événements de TADDM dans la liste d'événements de Tivoli Netcool/OMNIbus ou la liste d'événements actifs.

Avant de commencer
«Configuration supplémentaire de TADDM version 7.1.2», à la page 461
«Etapes de configuration pour la prise en charge des événements TADDM», à la page 462

Avant de commencer

Au minimum, cette configuration nécessite les produits et les versions suivants :

- Tivoli Netcool/OMNIbus version 7.3.1
- TADDM : utilisez l'une des versions suivantes :
  - V7.1.22 avec TADDM OMP Change Event Module
  - TADDM version 7.2 ou ultérieure

  Le module d'événement de changement TADDM OMP peut être téléchargé séparément pour TADDM version 7.1.2, mais il est intégré dans TADDM version 7.2 ou une version ultérieure. Pour plus d'informations, consultez la documentation de TADDM.

Pour procéder, Tivoli Netcool/OMNIbus et TADDM doivent être installés et configurés, et doivent être à l'état opérationnel suivant :

- Les hôtes ObjectServer désignés auxquels vous souhaitez que les événements TADDM soient transmis, sont configurés.

- La fonction **nco_confpack** est installée sur chaque hôte ObjectServer.
- Le serveur de l'Interface graphique Web est installé et configuré sur un ordinateur hôte. Par défaut, le serveur de l'Interface graphique Web contient le client Administration Application Program Interface (WAAPI) de l'Interface graphique Web, à partir duquel vous pouvez charger les personnalisations prenant en charge des événements TADDM. Pour plus d'informations sur le client WAAPI, voir *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus*
- Les postes de travail client sont configurés avec un accès aux outils de bureau de Tivoli Netcool/OMNIbus ou à l'Interface graphique Web.

  Sur tous les ordinateurs qui exécutent la liste d'événements de bureau, vérifiez que Java Runtime Environment (JRE) est installé. Vérifiez également que l'emplacement de répertoire de l'utilitaire Java Web Start (**javaws**) figure dans la variable d'environnement PATH. Les outils de menu qui démarrent la console Java de TADDM requièrent la présence de cet utilitaire dans l'environnement PATH où la liste d'événements est démarrée. L'utilitaire **javaws** se trouve généralement dans le répertoire `/bin` de l'environnement d'exécution Java.
- TADDM est installé. Pour plus d'informations sur l'installation et la configuration de TADDM, consultez le centre de documentation ITSM (IT Service Management) à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp, ouvrez le nœud *Application Dependency Discovery Manager* dans le panneau de navigation de gauche, et recherchez les informations sur la version requise.
- Facultatif : l'authentification unique est configurée entre le serveur de l'Interface graphique Web et le serveur TADDM. Si l'authentification unique est configurée, les utilisateurs AEL peuvent accéder à TADDM sans avoir à se connecter à TADDM séparément.
  - Pour plus d'informations sur la configuration de l'authentification unique pour le serveur de l'Interface graphique Web, voir «Configuration de l'authentification unique (SSO)», à la page 576.
  - Pour plus d'informations sur la configuration de TADDM pour l'authentification unique, voir le centre de documentation ITSM (IT Service Management) à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp. Pour configurer TADDM pour une connexion unique, vous devez configurer TADDM pour qu'il utilise les référentiels fédérés de WebSphere

En outre, Probe for Tivoli EIF doit être installé dans votre environnement Tivoli Netcool/OMNIbus, comme décrit dans les fichiers `README.txt` et `description.txt` du package de téléchargement de sonde. Modifiez le fichier de propriétés de sonde afin d'inclure les détails du serveur ObjectServer sur lequel vous souhaitez transmettre les événements TADDM. La sonde comprend un fichier de règles personnalisé destiné au traitement d'événements TADDM. Pour plus d'informations, voir «Etapes de configuration pour la prise en charge des événements TADDM», à la page 462.

Référence associée:

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Configuration supplémentaire de TADDM version 7.1.2

Si vous utilisez TADDM version 7.1.2, vous devez configurer TADDM avec le module TADDM OMP Change Event Module.

Avant de commencer

Vérifiez que vous disposez d'un ID et d'un mot de passe IBM afin de pouvoir accéder au téléchargement d'OMP Change Event Module.

Pourquoi et quand exécuter cette tâche

Le module d'événements de TADDM est un module complémentaire qui permet d'envoyer des notifications aux systèmes de gestion d'événements externes lorsque TADDM détecte des modifications de configuration dans votre environnement.

Procédure

Pour définir la configuration requise :

1. Téléchargez TADDM OMP Change Event Module à l'adresse : http://www-01.ibm.com/software/brandcatalog/portal/opal/details?catalog.label=1TW10CC1Q.
2. Extrayez les fichiers du package de téléchargement dans un emplacement temporaire, et accédez au sous-répertoire `doc`.
3. Ouvrez le fichier `index.html` pour obtenir les instructions relatives à l'intégration dans Tivoli Netcool/OMNIbus.

   Conseil : Les instructions pertinentes se trouvent dans la section appelée *Sending change events to ITM, TEC, and OMNIBus* (Envoi d'événements de changement à ITM, TEC et OMNIbus). Si vous cliquez sur l'un des liens, vous remarquerez que le texte est stocké dans le fichier `change_events.html` qui se trouve également dans le sous-répertoire `doc` . Vous pouvez lire le texte pour vous familiariser avec le contenu, mais seul le contenu de la section *Configuration de TADDM* est pertinent.
4. Dans le fichier `change_events.html`, suivez toutes les instructions de la section *Configuration de TADDM* pour ajouter les fichiers de module d'événements à votre serveur TADDM, et pour configurer le serveur.
5. Mettez à jour le fichier `$MODULE_PATH/taddmomp/properties/EventConfig.xml` comme suit :
   a. Dans la section sur les programmes d'écoute d'événement, utilisez l'élément <listener> pour spécifier des détails sur les ressources dont les modifications doivent être suivies.
   b. Dans la section sur les destinataires d'événements, utilisez l'élément <recipient> pour indiquer les détails du système auquel les données d'événement doivent être transmises et la configuration à appliquer. La valeur <recipient name=> de cette section doit être identique à la valeur de <alert recipient=> dans la section sur les programmes d'écoute d'événement ; exemple : `omnibus`.
   c. Supprimez les éléments <address> et <port>. Généralement, ces éléments peuvent être utilisés pour indiquer les détails de connexion de l'ordinateur hôte Probe for Tivoli EIF , mais il sont redondants dans ce cas.
   d. Utilisez l'élément <config> pour indiquer le chemin vers le fichier de configuration extrait dans `$MODULE_PATH/taddmomp/properties/`

omnibus.eif.properties. Vous devez utiliser ce fichier pour indiquer les détails de connexion de Probe for Tivoli EIF et les autres paramètres de configuration EIF.

6. Mettez à jour le fichier $MODULE_PATH/taddmomp/properties/omnibus.eif.properties par défaut, désigné dans le fichier EventConfig.xml), comme suit :
   a. Indiquez le nom qualifié complet de l'ordinateur hôte de Probe for Tivoli EIF en tant la valeur de la propriété **ServerLocation**.
   b. Indiquez le port sur lequel la sonde écoute en tant que valeur de la propriété **ServerPort** .
   c. Indiquez les emplacements de répertoire appropriés pour la mémoire tampon, le fichier de trace et le fichier journal.
   d. Complétez le reste du fichier comme indiqué dans l'exemple suivant. Dans cet exemple, certains des commentaires par défaut sont modifiés.

```
...
# La classe d'événement
TADDMEventClass=TADDM

# Définitions d'attribut EIF pour l'événement

# Remplacements pris en charge pour les données d'événements dans TADDM EIF Adapter.
# Elles peuvent être utilisées pour générer la valeur des attributs d'événement.
# Le nom d'attribut TEC doit être précédé de TADDMEvent_Slot_
#
# Les valeurs d'attribut correspondent aux zones traitées dans le fichier
# tivoli_eif_taddm.rules.
#
TADDMEvent_Slot_object_name=$TADDM_OBJECT_NAME
TADDMEvent_Slot_change_type=$TADDM_CHANGE_TYPE
TADDMEvent_Slot_change_time=$TADDM_CHANGE_TIME
TADDMEvent_Slot_class_name=$TADDM_CLASS_NAME
TADDMEvent_Slot_attribute_name=$TADDM_ATTRIBUTE_NAME
TADDMEvent_Slot_old_value=$TADDM_OLD_VALUE
TADDMEvent_Slot_new_value=$TADDM_NEW_VALUE
TADDMEvent_Slot_host=$TADDM_HOST
TADDMEvent_Slot_port=$TADDM_PORT
TADDMEvent_Slot_guid=$TADDM_GUID

# la source doit être définie pour identifier les événements TADDM dans la sonde
TADDMEvent_Slot_source=TADDM
```

Etapes de configuration pour la prise en charge des événements TADDM

Pourquoi et quand exécuter cette tâche

Pour activer la surveillance des événements TADDM dans Tivoli Netcool/OMNIbus, procédez comme suit :

Procédure

1. Sur l'hôte Tivoli Netcool/OMNIbus ObjectServer, accédez au répertoire $NCHOME/omnibus/extensions/taddm.
2. Copiez le modèle de fichier tivoli_eif_taddm.rules dans le répertoire suivant de l'ordinateur où Probe for Tivoli EIF est installé, ou sur un autre emplacement privilégié.

   $NCHOME/omnibus/probes/*arch*
3. Facultatif : Modifiez le fichier tivoli_eif_taddm.rules en définissant un délai d'expiration pour les événements TADDM sur le serveur ObjectServer. Sinon, ces événements sont conservés sur le serveur ObjectServer car il n'y a pas d'événements de résolution pour les événements TADDM.

a. Supprimez les droits d'accès en lecture seule par défaut dans le fichier `tivoli_eif_taddm.rules`.
b. Trouvez la ligne commentée suivante à la fin du fichier de règles.

```
# @ExpireTime = 7 * 24 * 60 * 60
```

c. Annulez la mise en commentaire de cette ligne et indiquez un délai d'expiration en secondes pour les événements TADDM. L'exemple de configuration définit le délai d'expiration sur une semaine (à savoir, 60 secondes * 60 minutes * 24 heures * 7 jours).
d. Enregistrez et fermez le fichier.

4. Modifiez le fichier `tivoli_eif.rules` principal pour Probe for Tivoli EIF.
   a. Localisez la section `switch($source)` du fichier.
   b. Supprimez la mise en commentaires qui contient l'instruction `include` du fichier `tivoli_eif_taddm.rules`. Insérez le chemin de répertoire de ce fichier, si nécessaire.

      ```
      include "tivoli_eif_taddm.rules"
      ```

   c. Commentez la ligne suivante, ou laissez-la sans commentaires si vous avez configuré votre système pour recevoir des événements à partir de Tivoli Enterprise Console.

      ```
      include "tivoli_eif_default.rules"
      ```

      Si la ligne n'est pas commentée, vous devez mettre à jour le schéma de base de données ObjectServer en appliquant le fichier d'importation `tec_db_update.sql` inclus dans la sonde. Pour plus d'informations, consultez la publication relative à Probe for Tivoli EIF. Vous pouvez accéder à cette publication de la manière suivante, à partir du centre de documentation IBM Tivoli Network Management (http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp) :
      1) Développez le nœud *IBM Tivoli Netcool/OMNIbus* dans le panneau de navigation située sur la gauche.
      2) Développez le nœud *Tivoli Netcool/OMNIbus probes and TSMs*.
      3) Accédez au nœud *IBM*.
5. Editez le fichier `$NCHOME/omnibus/probes/archive/tivoli_eif.props` pour mette à jour la valeur de la propriété **`Inactivity`**. Par défaut, la sonde s'arrête si son port d'écoute est inactif pendant 10 minutes. La génération d'événements peut être sporadique en fonction des plannings de reconnaissance de TADDM ; vous devez donc configurer la sonde pour qu'elle s'exécute en continu lorsqu'elle est à l'écoute des événements TADDM. Pour configurer ce paramètre, définissez la propriété **`Inactivity`** sur 0 (zéro).
6. Exécutez (ou redémarrez) la sonde.
7. Ajoutez la configuration TADDM au serveur ObjectServer vers lequel les événements sont envoyés et auquel les listes d'événements se connectent. Cette configuration inclut la classe réservée ainsi que le menu et les outils pour les événements TADDM.
   a. Sur l'hôte du serveur ObjectServer, accédez au répertoire `$NCHOME/omnibus/bin`.
   b. Entrez la commande suivante :

      ```
      nco_confpack -import -server nom_serveur -user nom_utilisateur
      -password mot_de_passe -package $NCHOME/omnibus/extensions/taddm/
      taddm_menutools_native_gui.jar -nowarn
      ```

      Dans cette commande, *nom_serveur* est le nom du serveur ObjectServer, et *nom_utilisateur* et *mot_de_passe* sont vos identifiants de connexion.

Lorsque l'importation est terminée, un sous-menu TADDM est disponible dans le menu **Alertes** de la liste d'événements.

8. Pour ajouter le filtre TADDM à vos listes d'événements, copiez le fichier `$NCHOME/omnibus/extensions/taddm/taddm.elf` sur un emplacement privilégié. Le filtre est ajouté avec le nom **TADDM**, et peut être sélectionné dans toutes les listes d'événements de cette configuration de liste d'événements.
9. Pour charger le filtre `taddm.elf` dans une configuration de liste d'événements existante, procédez comme suit :
   a. Dans la fenêtre d'écrans de surveillance Liste d'événements, cliquez sur **Fenêtres** > **Configuration** pour ouvrir la fenêtre Configuration de la liste d'événements.
   b. Lorsque vous affichez les filtres faisant partie de la configuration de listes d'événements, cliquez sur **Load** (Charger) (sous UNIX ou Linux), ou cliquez sur **Ouvrir** (sous Windows).
   c. Dans la fenêtre qui s'affiche, accédez à l'emplacement où vous avez sauvegardé le fichier de filtre `taddm.elf`, sélectionnez le fichier, puis cliquez sur **OK**.
   d. Sauvegardez la configuration de liste d'événements.
10. Pour ajouter le menu, les outils et un filtre pour les événements TADDM au serveur d'Interface graphique Web, consultez «Activation de la prise en charge des événements TADDM dans l'Interface graphique Web», à la page 590.
11. Sur tous les ordinateurs UNIX et Linux qui exécutent la liste d'événements de bureau, vérifiez que la variable d'environnement OMNIBROWSER est définie. Définissez la variable d'environnement OMNIBROWSER pour indiquer l'emplacement et le nom de fichier sur le navigateur Web par défaut, comme suit : Le paramètre OMNIBROWSER est requis pour effectuer un lancement à partir d'un événement TADDM de la liste d'événements sur le client Web TADDM.
    - Pour un utilisateur csh, ajoutez la ligne suivante au fichier `$HOME/.login` :
      `setenv OMNIBROWSER` *`chemin_exécutable_navigateur`*
    - Pour un utilisateur ksh ou sh, ajoutez la ligne suivante au fichier `$HOME/.profile` :
      `OMNIBROWSER=`*`chemin_exécutable_navigateur`*`;export OMNIBROWSER`
12. A partir de TADDM, configurez le planning de reconnaissance pour les éléments de configuration à surveiller.

    Des informations supplémentaires sur la configuration de reconnaissance dans TADDM sont disponibles dans le centre de documentation TADDM à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/index.jsp. Lorsque le processus de reconnaissance se termine, les détails des modifications détectées sont transmis à Probe for Tivoli EIF. La sonde mappe les données sur les zones ObjectServer et insère les données dans le serveur ObjectServer en tant qu'événements.

Que faire ensuite

Vous pouvez maintenant surveiller les événements TADDM dans la liste d'événements et l'AEL.

Pour plus d'informations sur la surveillance d'événements TADDM dans la liste d'événements, voir *IBM Tivoli Netcool/OMNIbus User's Guide*. Pour plus d'informations sur la surveillance d'événements TADDM dans la liste d'événements actifs, consultez le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Gestion d'environnements virtuels

Vous pouvez configurer Tivoli Netcool/OMNIbus afin qu'il exécute la gestion des événements d'un environnement virtuel. Tivoli Netcool/OMNIbus peut être configuré pour effectuer ce type de gestion d'événements à l'aide d'une sonde personnalisée pour SNMP, ou dans le cadre d'une solution intégrée à IBM Tivoli Monitoring.

Parmi les scénarios d'utilisation d'un environnement virtuel figurent :

- La corrélation d'événements d'incident. Les événements d'incident connexes au même incident initial peuvent être dus à l'hyperviseur, à l'ordinateur physique ou à la machine virtuelle. Une corrélation doit être établie entre ces événements de sorte que seuls les événements de cause première s'affichent dans la liste d'événements ou dans la liste d'événements actifs.
- Réduction de la gravité après une migration de machine virtuelle. La gravité des problèmes liés au matériel peut être automatiquement diminuée lorsque la machine virtuelle est déplacée vers un nouvel ordinateur hôte physique.

Important : Il est supposé que vous possédez des connaissances pratiques sur les environnements virtuels et IBM Tivoli Monitoring.

Configuration de la gestion d'événements dans un environnement virtuelà l'aide d'une sonde pour SNMP et IBM Tivoli Netcool/OMNIbus Knowledge Library

Vous pouvez exécuter Tivoli Netcool/OMNIbus avec IBM Tivoli Netcool/OMNIbus Knowledge Library et avec une sonde personnalisée pour SNMP afin de surveiller et de gérer un environnement virtuel VMware vSphere utilisant des hyperviseurs ESXi.

Un hyperviseur VMware ESXi est installé sur chaque serveur physique. L'hyperviseur est utilisé pour partitionner les serveurs en plusieurs machines virtuelles (VM) qui partagent les ressources matérielles. Le cluster VMware ESXi est géré à partir d'un seul centre de contrôle ESXi central. L'application VMware VirtualCenter vous permet de gérer et de surveiller les serveurs VMware et les machines virtuelles, et de migrer les machines virtuelles entre les serveurs. Le VirtualCenter et les clusters hyperviseur ESXi transmettent tous deux des alertes SNMP à la sonde Tivoli Netcool/OMNIbus pour SNMP. La sonde pour SNMP reçoit les alertes et utilise des fichiers de règles personnalisées, qui doivent être ajoutés à Netcool/OMNIbus Knowledge Library, pour traiter les alertes. Ensuite, la sonde pour SNMP transmet les alertes sous forme d'événements au serveur ObjectServer, qui les stocke dans la table alerts.status et dans une table personnalisée appelée custom.vmstatus. Les alertes résultantes peuvent ensuite être surveillées dans la liste d'événements de bureau ou dans l'afficheur d'événements. Vous pouvez ajouter, à la liste d'événements et à l'afficheur d'événements, un outil qui met en corrélation les événements de symptôme avec les événements de cause première.

Les fichiers de règles personnalisées activent uniquement les alertes SNMP de gestion virtuelle, et cela pour VMware uniquement.

Pour configurer cette fonctionnalité de surveillance, Tivoli Netcool/OMNIbus version 8.1 Netcool/OMNIbus Knowledge Library version 3.7 et VMware vSphere V5.0 avec des hyperviseurs ESXi sont requis, ainsi qu'une sonde Probe for SNMP

Tivoli Netcool/OMNIbus. Etant donné que le système VMware génère de grandes quantités de données, utilisez une instance dédiée de la sonde pour SNMP pour surveiller votre environnement virtuel.

Avant de commencer

Vérifiez que Tivoli Netcool/OMNIbus est installé, configuré et dans un état opérationnel, comme suit :

- Les hôtes ObjectServer désignés, auxquels vous souhaitez que les événements de virtualisation soient transmis, sont configurés.
- Les postes de travail client sont configurés avec un accès aux outils de bureau de Tivoli Netcool/OMNIbus et à l'Interface graphique Web.

Vérifiez que Netcool/OMNIbus Knowledge Library est installé et configuré comme suit :

- La variable d'environnement NC_RULES_HOME est définie.
- Le module de configuration `advcorr.sql` est appliqué aux serveurs ObjectServer qui doivent surveiller le système VMware.
- Des conversions sont ajoutées au serveur ObjectServer pour prendre en charge les colonnes AdvCorrCauseType et CauseType.

Pour plus d'informations sur Netcool/OMNIbus Knowledge Library, voir le manuel *Netcool/OMNIbus Knowledge Library Reference Guide*, qui est disponible dans le centre de documentation Network Availability Management à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp.

Pourquoi et quand exécuter cette tâche

Pour vous assurer que la table custom.vmstatus contient des données exactes, installez la sonde pour SNMP lorsque vous installez le système VMWare. Si vous installez la sonde sur un système VMWare qui est déjà en cours d'exécution, la corrélation entre les événements des machines virtuelles et des hôtes peut être inexacte lors des opérations initiales. Ce problème se produit uniquement si vous installez la sonde sur un système VMWare qui est déjà en cours d'exécution et qu'une application de surveillance indépendante est installée sur une machine virtuelle qui s'exécute sur le cluster. Une sonde ou un agent IBM Tivoli Monitoring sont des exemples d'application de surveillance indépendante. Ce problème se produit parce que la table custom.vmstatus ne contient pas initialement tous les mappages des machines virtuelles vers les hôtes. Lorsque le système s'exécute et que les machines virtuelles changent d'état ou se déplacent entre les hôtes, la table custom.vmstatus peut construire un mappage complet. Dans ce cas, les événements sont corrélés avec précision.

Procédure

Pour configurer l'environnement virtuel :

1. Configurez votre infrastructure informatique virtuelle avec les machines virtuelles, les serveurs VMware ESXi et VMware VirtualCenter :
   a. Installez et configurez le cluster VMWare ESXi.
   b. Installez l'application VMware VirtualCentre sur l'hôte désigné à partir duquel le cluster sera géré de façon centralisée.
   c. Vérifiez que le nom qui identifie une machine virtuelle dans le centre de contrôle ESXi correspond au nom d'hôte réseau qui est défini pour la machine virtuelle.

d. Vérifiez que le client vSphere est connecté au VirtualCenter et le VirtualCenter est configuré pour générer des alertes SNMP.
e. Assurez-vous que chaque nœud hyperviseur ESXi est configuré comme suit. Pour configurer des nœuds hyperviseur ESXi, utilisez l'utilitaire de ligne de commande VMware vSphere.
   - Le démon SNMP est configuré pour envoyer des alertes SNMP à l'ordinateur hôte sur lequel la sonde pour SNMP est installée.
   - Le démon SNMP est activé.
f. Veillez à ce que les définitions des alarmes dont vous avez besoin soient modifiées de façon à ce que toutes les transitions d'alarme génèrent une alerte SMMP correspondante.
g. Vérifiez que les noms qui sont utilisés dans le vCenter pour identifier les machines virtuelles sont identiques aux noms d'hôte utilisés par les machines virtuelles.

2. Installez la sonde pour SNMP sur un ordinateur hôte auquel le démon SNMP VMware envoie des alertes SNMP.
3. Facultatif : Sur l'hôte Netcool/OMNIbus Knowledge Library, effectuez des copies de sauvegarde des fichiers suivants :
   - `NC_RULES_HOME/include-snmptrap/AssignCorrectAdvValue.include.snmptrap.rules`
   - `NC_RULES_HOME/snmptrap.rules`
4. Copiez le fichier de règles personnalisées qui est inclus dans Tivoli Netcool/OMNIbus sur Netcool/OMNIbus Knowledge Library :
   a. Sur l'hôte ObjectServer, accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/snmp`.
   b. Copiez le fichier `AssignCorrectAdvValue.include.snmptrap.rules` dans le répertoire `NC_RULES_HOME/include-snmptrap`.
   c. Copiez tous les autres fichiers, notamment le fichier `snmptrap.rules`, dans le répertoire `NC_RULES_HOME`.
5. Dans le fichier de propriétés de la sonde pour SNMP, `mttrapd.props`, configurez la sonde comme suit :
   - Utilisez la propriété **`RulesFile`** pour indiquer le chemin d'accès au fichier `snmptrap.rules`. Pour plus d'informations sur la manière de configurer la sonde pour SNMP de cette manière, consultez la section relative à la *configuration des sondes afin d'utiliser les fichiers de règles mis à jour* dans le manuel *Netcool/OMNIbus Knowledge Library Reference Guide*.
   - Utilisez la propriété **`Port`** pour configurer la sonde afin qu'elle écoute le port spécifié lorsque le démon VMware a été configuré pour envoyer des alertes à la sonde.
6. Appliquez la configuration au serveur ObjectServer qui crée les ressources ObjectServer requises pour un environnement virtuel :
   a. Vérifiez que le serveur ObjectServer est en cours d'exécution.
   b. Accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/common` et copiez le fichier `virtualization_automations.sql` dans le répertoire `$NCHOME/omnibus/etc` ou dans l'emplacement de votre choix.
   c. Appliquez la configuration de virtualisation au serveur ObjectServer en exécutant la commande suivante à partir de l'interface SQL interactive :
      - UNIX Linux `$NCHOME/omnibus/bin/nco_sql -user` *`nom_utilisateur`* `-password` *`mot_de_passe`* `-server` *`nom_serveur`* `<` *`chemin_répertoire`*`/virtualization_automations.sql`

- Windows `"%NCHOME%\omnibus\bin\isql" -U nom_utilisateur -P mot_de_passe -S nom_serveur -i chemin_répertoire\virtualization_automations.sql`

  Dans ces commandes, *nom_utilisateur* est un nom d'utilisateur valide, *mot_de_passe* est le mot de passe correspondant, *nom_serveur* est le nom du serveur ObjectServer et *chemin_répertoire* est le chemin qualifié complet du répertoire du fichier `.sql`.

d. Si le serveur ObjectServer fait partie d'une paire de reprise en ligne, vérifiez que la table custom.vmstatus (ajoutée au schéma) est également répliquée par la passerelle OjectServer. Pour plus d'informations sur le mappage de la passerelle, voir le manuel *IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*.

Pendant l'application de la configuration, des messages d'erreur similaires aux exemples suivants peuvent s'afficher. Ce messages d'erreur sont sans gravité et peuvent être ignorés.

```
ERROR=Object exists on line 3 of statement
'alter table alerts.status add column
CauseType int...', at or near 'CauseType'
(1 row affected)
ERROR=Attempt to insert duplicate row on line 2 of statement 'insert into
alerts.conversions values ( 'CauseType0','CauseType',0,'Unknown' );...'
```

7. Ajoutez le menu et les outils pour la corrélation des événements symptôme et des événements de cause première sur le serveur ObjectServer auquel les événements sont envoyés :
   a. Sur l'hôte du serveur ObjectServer, accédez au répertoire `$NCHOME/omnibus/bin`.
   b. Entrez la commande suivante :

      `nco_confpack -import -server nom_serveur -user nom_utilisateur -password mot_de_passe -package $NCHOME/omnibus/extensions/virtualization/common/ShowRootCauseTool.jar -nowarn`

      Dans cette commande, *nom_serveur* est le nom du serveur ObjectServer, et *nom_utilisateur* et *mot_de_passe* sont vos identifiants de connexion.
8. Démarrez la sonde pour SNMP.
9. Démarrez les machines virtuelles.
10. Assurez-vous que chaque nœud hyperviseur ESXi est correctement configuré en envoyant à la sonde pour SNMP une alerte de test SNMP à partir du nœud.

Résultats

Votre système Tivoli Netcool/OMNIbus peut maintenant surveiller les événements reçus à partir de la sonde pour SNMP, qui sont émis sous forme d'alertes SNMP à partir du système VMware. Certains des événements SNMP qui proviennent de VMware vSphere comportent des textes récapitulatifs longs. Si un tel événement est envoyé au serveur ObjectServer, le texte récapitulatif complet est ajouté à la table alerts.details et une version abrégée du texte figure dans l'événement. Vous pouvez désormais utiliser l'outil RCA dans la liste d'événements pour identifier l'événement de cause première à l'origine des événements de symptôme. Dans la liste d'événements, un sous-menu **Show Root Cause** (Afficher la cause première) s'affiche lorsque vous cliquez avec le bouton droit de la souris sur un événement de symptôme.

Que faire ensuite

Dans l'Interface graphique Web, vous pouvez configurer l'Afficheur d'événements pour corréler les événements de symptôme et de cause première.

Tâches associées:

«Activation de la corrélation d'événements de gestion virtuels dans l'Interface graphique Web», à la page 589
Vous pouvez configurer l'Interface graphique Web pour gérer des événements qui sont issus d'un environnement virtuel. Copiez un fichier de commandes WAAPI de l'hôte Tivoli Netcool/OMNIbus vers l'hôte de l'Interface graphique Web et exécutez le client WAAPI sur le fichier. Des colonnes sont ajoutées à l'Afficheur d'événements pour définir la relation entre les événements de cause première et les événements symptôme qui sont issus d'un environnement virtuel

Référence associée:

«Ressources de configuration Tivoli Netcool/OMNIbus pour la gestion de la virtualisation», à la page 477
Lorsque vous installez Tivoli Netcool/OMNIbus, des fichiers de configuration sont fournis afin de gérer les événements dans les environnements virtuels. Ces ressources sont disponibles sous forme de modèles de fichiers dans le répertoire `$NCHOME/omnibus/extensions/virtualization` et ses sous-répertoires.

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Configuration de la gestion d'événements dans un environnement virtuel à l'aide de IBM Tivoli Monitoring

IBM Tivoli Monitoring peut être configuré pour utiliser la sonde Probe for Tivoli EIF pour transmettre au serveur ObjectServer les événements de situation (incidents) qui se produisent dans un environnement virtuel. Les alertes en résultant peuvent ensuite être surveillées dans la liste d'événements actifs ou dans la liste d'événements de bureau.

Dans cette configuration, un agent IBM Tivoli Monitoring for Virtual Servers est obligatoire pour fournir les événements de situation. Ces événements peuvent vous aider à identifier et à résoudre les problèmes de disponibilité et de performances du serveur virtuel.

Vous devez avoir au minimum les versions de produit suivantes : Tivoli Netcool/OMNIbus version 7.3.1. IBM Tivoli Monitoring version 6.2.3 et VMware ESXi version 4.0.

Avant de commencer

Vérifiez que Tivoli Netcool/OMNIbus est installé, configuré et dans un état opérationnel, comme suit :

- Les hôtes ObjectServer désignés, vers lesquels les événements de virtualisation doivent être transmis, sont configurés.
- Les postes de travail clients sont configurés avec l'accès aux outils de bureau de Tivoli Netcool/OMNIbus et à l'Interface graphique Web.

En outre, une ou plusieurs sondes pour Tivoli EIF doivent être installées dans votre environnement Tivoli Netcool/OMNIbus, comme décrit dans les fichiers `README.txt` et `description.txt` du package de téléchargement de sonde. Chaque serveur ObjectServer auquel vous souhaitez transmettre les événements de situation doit être associé à Probe for Tivoli EIF. Un fichier de règles personnalisées destiné à traiter les événements de situation est fourni pour une utilisation avec les sondes.

Vous devez être familiarisé avec la configuration de cet environnement, qui est décrite dans «Flot de données de configuration pour la surveillance d'un environnement virtuel avec IBM Tivoli Monitoring», à la page 475.

Pourquoi et quand exécuter cette tâche

Cette procédure présente un modèle de configuration de bout en bout de l'environnement virtuel VMware. Les étapes de configuration décrites concernent spécifiquement l'utilisation de VMWare ESXi et de l'agent VMware VI. Cependant, vous pouvez modifier les étapes de configuration afin d'utiliser l'un des hyperviseurs pris en charge et leur agent IBM Tivoli Monitoring for Virtual Servers associé. Les hyperviseurs suivants sont pris en charge par IBM Tivoli Monitoring for Virtual Environments version 7.1 :

- VMware ESXi
- Citrix
- Serveur virtuel Microsoft
- Hyper-V Microsoft
- Système P (AIX Premium, CEC Base, HMC Base, et VIOS Premium)
- z/VM
- Agent KVM (agent de machine virtuelle basé sur le noyau Linux)

De plus, l'agent du système d'exploitation UNIX IBM Tivoli Monitoring peut capturer les données de zone Solaris.

Utilisez la documentation IBM Tivoli Monitoring pour vous aider à configurer cet environnement intégré. Vous la trouverez dans le centre de documentation *IBM Tivoli Monitoring* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/index.jsp. Veillez à rechercher les informations correspondant à votre version prise en charge de IBM Tivoli Monitoring.

- Pour plus d'informations sur l'installation et la configuration de IBM Tivoli Monitoring, voir le *Guide d'installation et de configuration*.
- Pour plus d'informations sur la configuration de la transmission des événements au serveur ObjectServer, localisez les informations dans les nœuds suivants : *Installation and Configuration Guides (Guide d'installation et de configuration) > Installation and Setup Guide (Guide d'installation et de configuration) > Integrating event management systems (Intégration des systèmes de gestion d'événements) > Setting up event forwarding to Netcool/OMNIbus (Configuration de la transmission d'événements à Netcool/OMNIbus)> Configuring the monitoring server [to forward events] (Configuration du serveur de surveillance (pour la transmission d'événements)*.
- Pour plus d'informations sur l'installation et la configuration d'IBM Tivoli Monitoring for Virtual Servers: VMware VI Agent, voir le manuel *IBM Tivoli Monitoring for Virtual Servers: VMware VI Agent User's Guide*.
- Pour plus d'informations sur la création de situations, voir le manuel *IBM Tivoli Monitoring User's Guide*.

Pour plus d'informations sur l'activation de la communication SSL pour l'agent VI IBM Tivoli Monitoring version 6.2.1, voir le centre de documentation *Composite Application Manager for Applications* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v24r1/topic/com.ibm.tivoli.itmvs.doc_6.2.2/vmware622_user.htm.

Procédure

Pour configurer la gestion d'événements dans votre environnement virtuel :

1. Configurez votre infrastructure informatique virtuelle avec les machines virtuelles, les serveurs VMware ESXi et VMware VirtualCenter :
   a. Installez et configurez le cluster VMWare ESXi.
   b. Installez l'application VMware VirtualCentre sur l'hôte désigné à partir duquel le cluster est géré de façon centrale.
   c. Vérifiez que le nom qui identifie une machine virtuelle dans le centre de contrôle ESXi correspond au nom d'hôte du réseau qui est défini pour la machine virtuelle.

   Assurez-vous que, à ce stade, aucune machine virtuelle n'est en cours d'exécution sur le cluster. Pour qu'une machine virtuelle puisse être démarrée, l'agent VI VMWare, le serveur ObjectServer et la sonde Probe for Tivoli EIF doivent être configurés et en cours d'exécution. S'ils ne le sont pas, la table d'état de virtualisation, custom.vmstatus, risque de ne pas être remplie correctement. Si des machines virtuelles sont en cours d'exécution sur le cluster à ce stade, suspendez-les pendant la durée du processus de configuration. Si un service ininterrompu est nécessaire, vous pouvez faire migrer les machines virtuelles vers un autre hôte.
2. Installez et configurez votre environnement IBM Tivoli Monitoring :
   a. Vérifiez que IBM DB2 est installé en tant que système RDBMS prérequis pour IBM Tivoli Monitoring.
   b. Installez IBM Tivoli Monitoring.
   c. Configurez un ou plusieurs serveurs distants ou serveurs de surveillance concentrateurs, ainsi que Tivoli Enterprise Portal (serveur et clients).
3. Installez le composant de synchronisation d'événements IBM Tivoli Monitoring sur l'hôte de chaque serveur ObjectServer auquel vous souhaitez transmettre les événements de situation IBM Tivoli Monitoring. Lors de l'installation du composant, entrez les informations concernant chaque serveur de surveillance concentrateur avec lequel les événements de situation doivent être synchronisés. Lorsque vous installez le composant de synchronisation d'événements, le processus Situation Update Forwarder est installé avec ses fichiers binaires et de configuration. Les fichiers qui peuvent être utilisés pour configurer le serveur ObjectServer et Probe for Tivoli EIF sont également installés.
4. A partir de l'installation de IBM Tivoli Monitoring, activez la transmission des événements au serveur ObjectServer :
   a. Sur le serveur de surveillance à partir duquel les événements de situation doivent être transmis, activez l'utilitaire Tivoli Event Integration Facility.
   b. Indique le nom d'hôte de l'ordinateur sur lequel s'exécute la sonde Probe for Tivoli EIF et le numéro de port sur lequel la sonde est en mode écoute.
5. Installez IBM Tivoli Monitoring for Virtual Servers: VMware VI Agent. Cet agent est capable de surveiller le cluster ESXi à l'aide de l'application VMware VirtualCenter et de réaliser des actions de base à l'aide de VMware VirtualCenter.

Important : Lors de l'installation, vérifiez que vous sélectionnez le modèle `Monitoring Agent for VMware VI Agent`, conçu pour se connecter à VMware VirtualCenter. Ne choisissez pas le modèle `Monitoring Agent for VMware ESXi` .

6. Activez la communication SSL entre l'agent VMware VI et la source de données VMware VirtualCenter en ajoutant le certificat de signataire de la source de données VMware VirtualCenter à la base de données de clés de l'agent VMware VI : Si vous exécutez IBM Tivoli Monitoring version 6.2.1 VI Agent, exécutez les étapes suivantes pour activer SSL :
   a. A partir de l'hôte VMware VirtualCentre, recherchez le fichier de certificat VMware par défaut appelé `rui.crt`. Par exemple, sous Windows, son emplacement par défaut est `C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\rui.crt`.
   b. Copiez ce fichier à un emplacement temporaire de l'ordinateur hôte de l'agent VMware VI.
   c. A partir de l'ordinateur hôte de l'agent VMware VI, exécutez la commande **gsk7capicmd** pour ajouter le certificat de signataire à la base de données de clés de l'agent.
7. Démarrez l'agent de surveillance.
8. Dans la fenêtre Gérer les services Tivoli Monitoring de l'installation IBM Tivoli Monitoring, effectuez la configuration de l'agent :
   a. Créez une instance de l'agent de surveillance pour VMware VI et définissez les sources de données à surveiller.
   b. Indiquez un exemple d'intervalle d'une minute.
   c. Vérifiez que la connexion SSL est définie sur `Oui`.
   d. Vérifiez que le nom d'utilisateur et le mot de passe pour le VirtualCenter sont spécifiés.
9. Lancez Tivoli Enterprise Portal et vérifiez si les événements de situation sont reçus à partir de l'hôte VMware VirtualCentre après un délai d'une minute. Dans le panneau Situation Event Console (Console d'événements de situation), les noms de situation pertinents portent le préfixe `KVM_`.
10. A partir du portail Tivoli Enterprise Portal, créez deux situations supplémentaires, qui sont requises pour configurer la virtualisation de Tivoli Netcool/OMNIbus :
    a. Ouvrez l'éditeur de situations.
    b. Dans l'arborescence Situation, développez le nœud **VMware VI**.
    c. Cliquez avec le bouton droit sur la situation KVM_VM_Powered_Off et cliquez sur **Create Another** (Créer autre) dans le menu contextuel.
    d. Créez une situation appelée KVM_VM_Down avec une formule `!='poweredOn'` et un intervalle d'échantillonnage d'1 minute. Sélectionnez également **Run at startup** (Exécuter au démarrage).
    e. Sous l'onglet **EIF**, vérifiez que les événements sont transmis à un destinataire EIF avec un niveau de gravité EIF critique (Critical).
    f. Cliquez sur le bouton **EIF Slot Customization** (Personnalisation d'attribut EIF) et vérifiez que l'option **Map all attributes** (Mapper tous les attributs) est sélectionnée.
    g. Créez une autre situation appelée KVM_VM_Up avec des paramètres identiques à la situation KVM_VM_Down, à l'exception des paramètres suivants : définissez la formule sur `=='poweredOn'` et définissez le niveau de gravité EIF sur anodin (Harmless).

11. Appliquez la configuration au serveur ObjectServer qui crée les ressources ObjectServer requises pour un environnement virtuel :
    a. Vérifiez que le serveur ObjectServer est en cours d'exécution.
    b. Accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/common` et copiez le fichier `virtualization_automations.sql` dans le répertoire `$NCHOME/omnibus/etc` ou dans l'emplacement de votre choix.
    c. Appliquez la configuration de virtualisation au serveur ObjectServer en exécutant la commande suivante à partir de l'interface SQL interactive :
        - UNIX Linux `$NCHOME/omnibus/bin/nco_sql -user` *nom_utilisateur* `-password` *mot_de_passe* `-server` *nom_serveur* `<` *chemin_répertoire*`/virtualization_automations.sql`
        - Windows `"%NCHOME%\omnibus\bin\isql" -U` *nom_utilisateur* `-P` *mot_de_passe* `-S` *nom_serveur* `-i` *chemin_répertoire*`\virtualization_automations.sql`

        Dans ces commandes, *nom_utilisateur* est un nom d'utilisateur valide, *mot_de_passe* est le mot de passe correspondant et *nom_serveur* est le nom du serveur ObjectServer et *chemin_répertoire* est le chemin qualifié complet du répertoire du fichier `.sql`.
    d. Si le serveur ObjectServer fait partie d'une paire de reprise en ligne, vérifiez que la table custom.vmstatus (ajoutée au schéma) est également répliquée par la passerelle ObjectServer. Pour plus d'informations sur ces mappages, consultez le manuel*IBM Tivoli Netcool/OMNIbus ObjectServer Gateway Reference Guide*.
12. Copiez le fichier `itm_event.rules` de IBM Tivoli Monitoring dans le répertoire suivant de chaque ordinateur sur lequel la sonde Probe for Tivoli EIF est installée :

    `$NCHOME/omnibus/probes/`*arch*
13. Accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/itm` et copiez le fichier personnalisé `tivoli_eif_virtualization_pt1.rules` et le fichier `tivoli_eif_virtualization_pt2.rules` dans le répertoire `$NCHOME/omnibus/probes/`*arch* de l'ordinateur sur lequel la sonde Probe for Tivoli EIF est installée.
14. Modifiez le fichier de règles `tivoli_eif.règles`, qui est inclus dans la sonde Probe for Tivoli EIF, comme suit :
    a. Supprimez la mise en commentaire des lignes qui contiennent une instruction include pour les fichiers `tivoli_eif_virtualization_pt1.rules` et `tivoli_eif_virtualization_pt1.rules`.
    b. Supprimez également la mise en commentaire de l'instruction `include` qui inclut le fichier `itm_event.rules`.
    c. Si la sonde Probe for Tivoli EIF est en court d'exécution, relisez le fichier de règles.
15. Supprimez les droits d'accès en lecture seule par défaut dans les fichiers copiés `tivoli_eif_virtualisation_pt1.règles` et `tivoli_eif_virtualisation_pt2.règles`. Lisez le contenu du fichier, et modifiez-le ou personnalisez-le en fonction des besoins. Modifiez notamment les instructions `registertarget` en indiquant le nom du serveur ObjectServer auquel vous souhaitez transmettre les événements de situation.
16. Modifiez le fichier de propriétés de la sonde Probe for Tivoli EIF, situé dans `$NCHOME/omnibus/probes/`*arch*`/nco_p_tivoli_eif.props` :

a. Définissez la valeur de la propriété **RulesFile** par le chemin et le nom du fichier `tivoli_eif.rules`. Vérifiez que la propriété **RulesFile** est indiquée après la propriété **Name**.
b. Définissez la valeur de la propriété **Inactivity** par `0` (zéro). Par défaut, la sonde s'arrête si son port d'écoute est inactif pendant 10 minutes. Le fait de définir cette propriété sur `0` permet de configurer une exécution continue de la sonde lorsqu'elle est à l'écoute des événements de situation.
c. Vérifiez que les autres propriétés de la sonde, comme **Server** et **PortNumber**, sont définies correctement.

17. Ajoutez le menu et l'outil pour la corrélation des événements symptôme et des événements de cause première sur le serveur ObjectServer auquel les événements sont envoyés :
    a. Sur l'hôte du serveur ObjectServer, accédez au répertoire `$NCHOME/omnibus/bin`.
    b. Entrez la commande suivante :

       ```
       nco_confpack -import -server nom_serveur -user nom_utilisateur
       -password mot_de_passe -package $NCHOME/omnibus/extensions/
       virtualization/common/ShowRootCauseTool.jar -nowarn
       ```

       Dans cette commande, *nom_serveur* est le nom du serveur ObjectServer, et *nom_utilisateur* et *mot_de_passe* sont vos identifiants de connexion.
18. Vérifiez que l'ordinateur hôte de Probe for Tivoli EIF exécute Java version 1.5 ou version ultérieure, en entrant `java -version`. Démarrez ensuite la sonde Probe for Tivoli EIF.
19. Démarrez les machines virtuelles.

Résultats

Vous pouvez désormais surveiller les événements de situation depuis votre environnement virtuel dans la liste d'événements. Vous pouvez désormais utiliser l'outil RCA dans la liste d'événements pour identifier l'événement de cause première à l'origine des événements symptôme. Dans la liste d'événements, un sous-menu **Show Root Cause** (Afficher la cause première) s'affiche lorsque vous cliquez avec le bouton droit de la souris sur un événement symptôme.

Que faire ensuite

Installez les autres sondes sur les machines virtuelles du cluster. Dans le modèle de configuration fourni, les incidents dus à une utilisation élevée de la mémoire et de l'unité centrale sont corrélés. Dans les fichiers de règles des sondes, paramétrez @AlertGroup sur `Memory Allocation Status` ou `CPU Status` pour activer la corrélation entre ces types d'erreur.

Dans l'Interface graphique Web, vous pouvez configurer l'Afficheur d'événements pour corréler des événements symptôme et de cause première.

Référence associée:

«Ressources de configuration Tivoli Netcool/OMNIbus pour la gestion de la virtualisation», à la page 477
Lorsque vous installez Tivoli Netcool/OMNIbus, des fichiers de configuration sont fournis afin de gérer les événements dans les environnements virtuels. Ces ressources sont disponibles sous forme de modèles de fichiers dans le répertoire `$NCHOME/omnibus/extensions/virtualization` et ses sous-répertoires.

«Importation des configurations», à la page 317
Pour importer une configuration, exécutez l'utilitaire **nco_confpack** sur l'installation de Tivoli Netcool/OMNIbus qui contient le serveur ObjectServer dans lequel vous souhaitez importer la configuration. Vous pouvez importer un package de configuration vers n'importe quel ObjectServer version 8.1. Vous pouvez importer des informations depuis un package de configuration dans un seul serveur ObjectServer à la fois.

Flot de données de configuration pour la surveillance d'un environnement virtuel avec IBM Tivoli Monitoring

Vous pouvez définir un système virtuel de gestion des événements d'incident en intégrant Tivoli Netcool/OMNIbus, Probe for Tivoli EIF, IBM Tivoli Monitoring et un agent IBM Tivoli Monitoring for Virtual Servers.

Les divers composants de ce système peuvent être répartis sur plusieurs ordinateurs hôte ou tous s'exécuter sur un seul hôte puissant. A des fins de test, les composants peuvent également s'exécuter sur des ordinateurs virtuels dans le cluster qui est géré. Cependant, cette configuration n'est pas recommandée pour un environnement de production.

L'installation et la configuration de base pour les composants dans l'environnement intégré, où le logiciel VMware Virtualization est utilisé pour créer un environnement virtuel, sont les suivantes.

1. Un cluster VMware ESXi est configuré avec deux hôtes de serveur physique ou plus. Un hyperviseur VMware ESXi est installé sur chaque serveur physique. L'hyperviseur est utilisé pour partitionner les serveurs en plusieurs machines virtuelles (VM) qui partagent les ressources matérielles. Les machines virtuelles exécutent également toutes les sondes, qui sont configurées pour acquérir les données d'événement et les réacheminer directement vers le serveur ObjectServer en tant qu'alertes.
2. Le cluster VMware ESXi est géré à partir d'un seul centre de contrôle ESXi central. L'application VMware VirtualCenter vous permet de gérer et de surveiller les serveurs VMware et les machines virtuelles, et de migrer les machines virtuelles entre les serveurs. Le centre de contrôle ESXi peut être exécuté sur une machine virtuelle sur le cluster.
3. L'agent VMware VI surveille le centre de contrôle ESXi à partir d'un hôte distant. L'agent collecte les informations de surveillance relatives à la mémoire, à l'unité centrale, au système, au disque dur et à l'utilisation du réseau pour les serveurs VMware ESXi et les machines virtuelles. L'agent surveille également les événements et les alarmes connexes aux incidents sur les serveurs VMware ESXi et les machines virtuelles.
4. Le serveur Tivoli Enterprise Monitoring Server agit comme un point de collecte et de contrôle pour les événements de situation reçus de l'agent VMware VI. Un ou plusieurs serveurs de surveillance distants et concentrateurs peuvent être configurés en fonction de vos exigences. Un serveur de portail Tivoli Enterprise fournit la couche présentation des données collectées. Ce serveur de portail récupère des données à partir du serveur de surveillance en réponse aux actions de l'utilisateur à partir d'un ou plusieurs clients Tivoli Enterprise Portal. Le serveur de portail envoie les données aux clients de portail à des fins de présentation, d'analyse et de manipulation.
5. Le serveur de surveillance peut être configuré pour réacheminer les événements de situation vers les serveurs ObjectServer de Tivoli Netcool/OMNIbus. Le serveur de surveillance utilise l'interface Tivoli Event Integration Facility (EIF) pour réacheminer des événements de situation vers un récepteur EIF. Dans ce cas, le récepteur est Probe for Tivoli EIF.

6. Probe for Tivoli EIF reçoit les événements de situation, traite les données d'événement et mappe les données sur les zones ObjectServer. La sonde envoie alors des alertes au serveur ObjectServer. Le fichier de règles de sonde doit être modifié pour garantir le mappage des données d'événement sur les zones du serveur ObjectServer. Le serveur ObjectServer doit être configuré pour traiter et stocker les alertes. Le composant de synchronisation des événements IBM Tivoli Monitoring doit être installé sur l'hôte du serveur ObjectServer. Ce composant offre des ressources de personnalisation qui permettent au serveur ObjectServer et à Probe for Tivoli EIF de gérer des événements de situation génériques et des événements prévisibles. Le composant de synchronisation des événements inclut également un processus SUF (Situation Update Forwarder) qui permet le renvoi des mises à jour des alertes vers le serveur de surveillance concentrateur d'origine.
7. Les événements de situation insérés dans la table alerts.status peuvent être affichés dans la Liste d'événements actifs ou dans la liste d'événements du bureau.

Tâches associées:

«Configuration de la gestion d'événements dans un environnement virtuel à l'aide de IBM Tivoli Monitoring», à la page 469
IBM Tivoli Monitoring peut être configuré pour utiliser la sonde Probe for Tivoli EIF pour transmettre au serveur ObjectServer les événements de situation (incidents) qui se produisent dans un environnement virtuel. Les alertes en résultant peuvent ensuite être surveillées dans la liste d'événements actifs ou dans la liste d'événements de bureau.

Référence associée:

«Ressources de configuration Tivoli Netcool/OMNIbus pour la gestion de la virtualisation», à la page 477
Lorsque vous installez Tivoli Netcool/OMNIbus, des fichiers de configuration sont fournis afin de gérer les événements dans les environnements virtuels. Ces ressources sont disponibles sous forme de modèles de fichiers dans le répertoire `$NCHOME/omnibus/extensions/virtualization` et ses sous-répertoires.

Application des déclencheurs de virtualisation à un environnement mis à niveau

Si vous avez effectué une mise à niveau vers Tivoli Netcool/OMNIbus 8.1 à partir de la version 7.3 ou 7.3.1 et que vous utilisez l'environnement intégré avec IBM Tivoli Monitoring pour surveiller les environnements virtuels, mettez à niveau la configuration du serveur ObjectServer vers la version 8.1. Les déclencheurs inclus dans les ressources de configuration 8.1 sont plus efficaces que dans les versions précédentes.

Avant de commencer

Vérifiez que Tivoli Netcool/OMNIbus est mis à niveau et que les hôtes ObjectServer désignés, vers lesquels les événements de virtualisation doivent être réacheminés, sont configurés. Vérifiez que les serveurs ObjectServer sont en cours d'exécution.

Procédure

1. Accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/common` et copiez le fichier `virtualization_automations.sql` dans le répertoire `$NCHOME/omnibus/etc` ou dans l'emplacement de votre choix.

2. Appliquez la configuration de virtualisation au serveur ObjectServer en exécutant la commande suivante à partir de l'interface SQL interactive :
   - UNIX Linux `$NCHOME/omnibus/bin/nco_sql -user nom_utilisateur -password mot_de_passe -server nom_serveur < chemin_répertoire/virtualization_automations.sql`
   - Windows `"%NCHOME%\omnibus\bin\isql" -U nom_utilisateur -P mot_de_passe -S nom_serveur -i chemin_répertoire\virtualization_automations.sql`

   Dans ces commandes, *nom_utilisateur* est un nom d'utilisateur valide, *mot_de_passe* est le mot de passe correspondant, *nom_serveur* est le nom du serveur ObjectServer et *chemin_répertoire* est le chemin qualifié complet du répertoire du fichier .sql.
3. Si le serveur ObjectServer fait partie d'une paire de reprise en ligne, vérifiez que la table custom.vmstatus (ajoutée au schéma) est également répliquée par la passerelle.

Ressources de configuration Tivoli Netcool/OMNIbus pour la gestion de la virtualisation

Lorsque vous installez Tivoli Netcool/OMNIbus, des fichiers de configuration sont fournis afin de gérer les événements dans les environnements virtuels. Ces ressources sont disponibles sous forme de modèles de fichiers dans le répertoire `$NCHOME/omnibus/extensions/virtualization` et ses sous-répertoires.

Les détails des fichiers de configuration sont les suivants :

- Fichier `$NCHOME/omnibus/extensions/virtualization/common/virtualization_automations.sql` : ce fichier crée les ressources Objectserver suivantes :
  - Les colonnes de table ci-dessous sont ajoutées à la table alerts.status :

Nom de colonne	Type de données	Description
CauseType	integer	Dénote les événements de symptôme et de cause première. Les valeurs possibles sont les suivantes : • `0` : Inconnue • `1` : Cause première • `2` : Symptôme
ParentIdentifier	varchar(255)	Associe les événements de symptôme à l'événement de cause première. Pour un événement de symptôme, la valeur de cette zone est la valeur Identifier de l'événement de cause première.
ParentServerSerial	integer	Associe les événements de symptôme à l'événement de cause première. Pour un événement de symptôme, la valeur de cette zone est la valeur ServerSerial de l'événement de cause première.

– La table custom.vmstatus. Cette table est utilisée pour stocker les détails sur l'état des machines virtuelles de l'environnement. L'état des machines virtuelles est actualisé par les événements de situation de l'agent VMware VI. Les informations de cette table peuvent être dupliquées car des situations différentes peuvent générer des informations identiques. La table custom.vmstatus contient les colonnes suivantes :

Nom de colonne	Type de données	Description
VMHostName	varchar(64)	Nom d'hôte de la machine virtuelle. Clé principale.
HyperHostName	varchar(64)	Nom d'hôte du serveur physique sur lequel la machine virtuelle est configurée.
VMStatus	int	Etat de la machine virtuelle. Les valeurs sont les suivantes : • 0 : hors ligne. Indique que la machine virtuelle est hors tension, bloquée ou en veille. • 1 : active
StateChange	heure	Heure de la dernière modification de l'entrée.

– Déclencheurs vms_new_row, vms_deduplication, vms_state_change, vms_remove_old_enties et vm_correlate. Ces déclencheurs effectuent des corrélations et des résolutions d'événements d'erreur en fonction du nom d'hôte de la machine virtuelle et de l'hyperviseur. Les déclencheurs sont attribués au groupe de déclencheurs vm_triggers.

- Fichier `$NCHOME/omnibus/extensions/virtualization/common/ShowRootCauseToo.jar`. Ce fichier crée un élément et un outil de menu qui sont ajoutés à la liste d'événements pour identifier les événements de cause première sous-jacents aux événements de symptôme.
- Fichier `$NCHOME/omnibus/extensions/virtualization/common/remove_virtualization_automations.sql` : Ce fichier supprime la table de virtualisation et les automatisations du schéma ObjectServer, si nécessaire.
- Fichier `$NCHOME/omnibus/extensions/virtualization/snmp/snmp.rules` et fichiers associés dans le répertoire `$NCHOME/omnibus/extensions/virtualization/snmp`. Ce fichier de règles personnalisé ainsi que les fichiers de règles associés sont dans un format compatible avec IBM Tivoli Netcool/OMNIbus Knowledge Library. Ces fichiers contiennent la logique permettant de traiter les interceptions SNMP qui proviennent de machines virtuelles VMware vSphere V5.0.
- Fichiers `$NCHOME/omnibus/extensions/virtualization/itm/tivoli_eif_virtualization_pt1.rules` et `$NCHOME/omnibus/extensions/virtualization/itm/tivoli_eif_virtualization_pt1.rules/tivoli_eif_virtualization_pt2.rules` : Ces fichiers de règles personnalisées sont fournis pour Probe for Tivoli EIF et peuvent être utilisés en supprimant la mise en commentaire des lignes appropriées dans le fichier de règles standard (`tivoli_eif.règles`), fourni avec la sonde. Les fichiers `tivoli_eif_virtualization_pt1.rules` et `tivoli_eif_virtualization_pt2.rules` contiennent la logique permettant de contrôler les événements de situation pour relever les erreurs et les résolutions générées par un agent Hyperviseur IBM

Tivoli Monitoring. En outre, ces fichiers mappent les données de situation aux zones ObjectServer de la table alerts.status et insèrent ces données dans la table custom.vmstatus.

Récapitulatif du modèle de configuration fourni

Le fichier `virtualization_automations.sql` vise à corréler les événements entre les machines virtuelles et l'hyperviseur, et à traiter les événements associés aux machines virtuelles migrées. Cet exemple de configuration a été écrit pour l'agent VMware VI, mais il peut être adapté à d'autres environnements de virtualisation, à condition que le fichier de règles pour le Probe for Tivoli EIF soit écrit correctement.

Les incidents matériels peuvent être collectés par des sondes s'exécutant sur des machines virtuelles, ou par l'agent VMware VI. Une fois les événements insérés dans la table alerts.status, ils sont corrélés à l'aide d'un déclencheur temporel s'exécutant toutes les 20 secondes. Si un événement de situation d'hyperviseur est corrélé avec un événement de situation de même type à partir d'une machine virtuelle en cours d'exécution, les deux événements sont modifiés de la façon suivante :

- L'événement d'hyperviseur est signalé comme cause première avec la valeur de la zone CauseType définie sur 1. La gravité passe sur 5 car l'événement de cause première entraîne d'autres incidents sur les machines virtuelles et il doit être résolu rapidement.
- Les événements de machine virtuelle sont signalés comme symptômes avec la valeur de la zone CauseType définie sur 2. La gravité passe sur 2 car le symptôme est résolu en même temps que la cause première. La valeur de la zone ParentServerSerial est définie sur la valeur de la zone ServerSerial de l'événement d'hyperviseur. Enfin, la zone ParentIdentifier est définie sur la valeur de la zone Identifier de l'événement de cause première.

Si une machine virtuelle est migrée, tout événement connexe avec une valeur AlertGroup `Memory Allocation Status`, `CPU Status`, ou `Network Link Status` est signalé avec un niveau de gravité 2 pour indiquer qu'il n'est plus un problème important. En effet, la migration de la machine virtuelle corrige ces incidents en temps voulu.

Remarque : Consultez le fichier `virtualization_automations.sql` pour comprendre le fonctionnement des automatisations et pour déterminer si le modèle de configuration répond à vos exigences ou si des tâches de configuration supplémentaires sont nécessaires pour traiter d'autres types d'incidents matériels. Vous pouvez copier le modèle de fichier fourni, supprimer ses droits d'accès en lecture seule par défaut, puis modifier votre copie du fichier en fonction de vos besoins.

Tâches associées:

«Configuration de la gestion d'événements dans un environnement virtuel à l'aide de IBM Tivoli Monitoring», à la page 469
IBM Tivoli Monitoring peut être configuré pour utiliser la sonde Probe for Tivoli EIF pour transmettre au serveur ObjectServer les événements de situation (incidents) qui se produisent dans un environnement virtuel. Les alertes en résultant peuvent ensuite être surveillées dans la liste d'événements actifs ou dans la liste d'événements de bureau.

«Configuration de la gestion d'événements dans un environnement virtuelà l'aide d'une sonde pour SNMP et IBM Tivoli Netcool/OMNIbus Knowledge Library», à la page 465
Vous pouvez exécuter Tivoli Netcool/OMNIbus avec IBM Tivoli Netcool/OMNIbus Knowledge Library et avec une sonde personnalisée pour SNMP afin de surveiller et de gérer un environnement virtuel VMware vSphere utilisant des hyperviseurs ESXi.

Rechargement de plusieurs fichiers de règles de sonde

Le fichier `$OMNIHOME/extensions/roi/probemanagement.sql` contient une procédure `reloadrules_allprobes` ainsi que les déclencheurs de serveur ObjectServer qui la prennent en charge. Ce code utilise les interface de commande HTTP de sonde. Une fois que vous avez chargé la procédure dans un serveur ObjectServer, vous pouvez l'utiliser pour donner simultanément l'ordre à plusieurs sondes de recharger leur fichier de règles. Cela est utile lorsque vous modifiez les fichiers de règles de plusieurs sondes et que vous voulez que vos modifications entrent en vigueur toutes en même temps.

Avant de commencer

Effectuez les actions suivantes :

- Configurez le serveur ObjectServer pour qu'il exécute les procédures externes avec le démon d'agent de processus (**nco_pad**).
- Configurez les sondes cible en vue de leur administration avec l'interface HTTP de sonde. Etant donné que la procédure de rechargement ne prend pas en charge l'authentification, ne configurez pas l'interface HTTP pour qu'elle demande un nom d'utilisateur ou un mot de passe.

Pourquoi et quand exécuter cette tâche

Les étapes ci-dessous expliquent comment configurer et exécuter la procédure `reloadrules_allprobes`.

Les fichiers nécessaires pour configurer et exécuter la procédure sont stockés dans le répertoire `$OMNIHOME/extensions/roi`. La procédure `reloadrules_allprobes` fait appel à l'utilitaire **nco_http** pour envoyer des commandes aux sondes.

Si vous avez besoin d'une connexion sécurisée, configurez le chiffrement SSL sur la sonde et dans l'utilitaire **nco_http**, comme expliqué aux étapes 4 à 7. Si vous activez HTTP et HTTPS sur la même sonde, HTTPS est utilisé par défaut.

Remarque : Les sondes ne traitent pas immédiatement la commande de rechargement. Lorsqu'une sonde la reçoit, elle note que le fichier de règles doit être rechargé. Lorsqu'elle détecte un nouvel événement, elle recharge le fichier de règles et le traite avec le nouvel événement.

Procédure

Configuration de l'environnement pour exécuter la procédure

1. Pour rediriger les événements ProbeWatch vers le fichier journal de gestion de sonde, modifiez le fichier de règles de chaque sonde pour inclure le fichier suivant :

   `$OMNIHOME/extensions/roi/probewatch.include`

   Exemple :

```
if(match(@Manager, "ProbeWatch"))
{
    include "$OMNIHOME/extensions/roi/probewatch.include"
    break
}
```

2. Configurez et démarrez l'agent de contrôle du processus **nco_pad**.

   Si vous exécutez **nco_pad** sur un ordinateur différent de celui où s'exécute le serveur ObjectServer, procédez comme suit :

   a. Sur l'ordinateur qui héberge le serveur ObjectServer, faites une copie du fichier `$OMNIHOME/extensions/roi/probemanagement.sql`.

   b. Modifiez cette copie en donnant au paramètre `host` de la procédure `do_probereloadrules` le nom d'hôte de l'ordinateur sur lequel **nco_pad** s'exécute.

3. Utilisez l'interface interactive SQL pour exécuter le fichier `probemanagement.sql`. Exemple :

   - UNIX Linux `$OMNIHOME/bin/nco_sql -user` *nom-utilisateur-administrateur* `-password` *mot-de-passe* `-server` *nom-serveur-d'objets* `< $OMNIHOME/extensions/roi/probemanagement.sql`
   - Windows `%OMNIHOME%\bin\isql -S` *nom-serveur-d'objets* `-U` *nom-utilisateur-administrateur* `-P` *mot-de-passe* `-i %OMNIHOME%\extensions\roi\probemanagement.sql`

     Où *nom-utilisateur-administrateur* représente un utilisateur administrateur autorisé à créer des déclencheurs, des fichiers et des procédure stockées.

   Cette commande crée les artefacts suivants :

   - Un fichier journal de gestion de sonde, `$OMNIHOME/log/`*nom-serveur-d'objets*`_probemanagement.log`.
   - Un groupe de déclencheurs probe_management comportant des déclencheurs qui journalisent les événements ProbeWatch relatifs au chargement des fichiers de règles.
   - Une procédure `reloadrules_allprobes` qui demande à toutes les sondes de recharger leur fichier de règles.
   - Une procédure externe que la procédure `reloadrules_allprobes` utilise pour appeler l'utilitaire **nco_probereloadrules**. L'utilitaire **nco_probereloadrules** demande le rechargement via l'interface HTTP de la sonde.

Facultatif : Configuration du chiffrement SSL

4. Créez la base de données de clés et les certificats requis pour une connexion SSL.

5. Ouvrez le fichier `$OMNIHOME/etc/nco_http.props` et définissez les valeurs de propriété suivantes :

   ```
   NHttpd.SSLCertificatePwd : mot-de-passe-certificat
   NHttpd.SSLEnable : TRUE
   ```

   Où *mot-de-passe-certificat* représente le mot de passe du certificat SSL pour l'ordinateur sur lequel **nco_http** est installé.

   La propriété **NHttpd.SSLEnable** permet les connexions SSL entre l'utilitaire **nco_http** et les sondes configurées pour SSL.

6. Ouvrez en édition le fichier de propriétés de chaque sonde et définissez les valeurs de propriété suivantes :

   ```
   NHttpd.SSLCertificate : nom-certificat
   NHttpd.SSLCertificatePwd : mot-de-passe-certificat
   NHttpd.SSLEnable : TRUE
   NHttpd.SSLListeningPort : port
   ```

Où *nom-certificat* représente le nom du certificat SSL pour l'ordinateur sur lequel la sonde est installée, et *mot-de-passe-certificat* représente le mot de passe du certificat. *port* représente le numéro du port sur lequel la sonde est à l'écoute du trafic HTTPS.

La propriété **NHttpd.SSLEnable** permet les connexions SSL entre la sonde et l'utilitaire **nco_http**.

Exécution de la procédure

7. Pour demander à toutes les sondes en cours d'exécution de recharger leur fichier de propriétés, utilisez la commande SQL suivante :

   ```
   execute reloadrules_allprobes
   ```

   Par exemple, pour exécuter la procédure avec l'interface interactive SQL, utilisez les commandes suivantes :

   ```
   1> execute reloadrules_allprobes;
   2> go
   ```

8. Examinez le fichier $OMNIHOME/log/*nom-serveur-d'objets*_probemanagement.log pour vous assurer que les sondes ont bien rechargé leur fichier de règles.

Résultats

Les informations suivantes sont journalisées dans le fichier journal de gestion de sonde :

- La date et l'heure auxquelles le rechargement a été demandé.
- Les informations concernant chaque sonde configurée pour HTTP pour laquelle une demande de rechargement est envoyée.
- Un récapitulatif qui contient les informations suivantes :
  - Le nombre de sondes ayant une interface HTTP activée (gérée).
  - Le nombre de sondes n'ayant pas d'interface HTTP activée (non gérée).
  - Le nombre de sondes qui sont répertoriées dans la table registry.probes mais qui ne sont pas en cours d'exécution.
- L'état de chaque tentative de rechargement. Comme le rechargement est traité avec le prochain événement reçu par une sonde, ces entrées de journal peuvent être écrites un certain temps après l'émission de la demande de rechargement initiale.

Si vous avez configuré le chiffrement SSL, les entrées de journal font référence à HTTPS et non à HTTP.

Lorsqu'un rechargement échoue, le message de journal indique la cause de l'échec. Pour plus d'informations concernant un échec, examinez le fichier journal local de la sonde.

Si aucun message d'état n'est journalisé après une commande de rechargement, procédez comme suit pour identifier le problème :

1. Assurez-vous que le journal contient bien une entrée montrant qu'une demande HTTP a été faite. Exemple :

   ```
   Tue Jul 23 12:46:27 2013 Sent HTTP reload rules request
    to nom-sonde on test_server:28888
   ```

   Si ce message de demande n'a pas été journalisé, assurez-vous que la sonde est en cours d'exécution et est connectée au serveur ObjectServer.

2. Assurez-vous que le processus **nco_pad** est en cours d'exécution et examinez son fichier journal à la recherche d'éventuelles erreurs.

3. Si **nco_pad** s'exécute correctement, vérifiez que le nom d'hôte journalisé dans le fichier journal de gestion de sonde est correct (*nom-sonde* on *nom-d'hôte*:*port*).

   Il se peut que la sonde ne puisse pas trouver le nom de l'hôte sur lequel elle s'exécute lorsqu'elle s'exécute dans un environnement virtualisé ou dans un environnement comportant plusieurs cartes réseau, ou si aucun service de nommage n'est disponible. Dans ces cas-là, spécifiez le nom d'hôte dans la propriété **Nhttpd.ListeningHostname**.

Remarque : Lorsque la procédure de rechargement est lancée sur des sondes installées sous Tivoli Netcool/OMNIbus version 7.4, les messages qui sont écrits dans le journal diffèrent légèrement de ceux qui sont écrits par les sondes de la version 8.1. Les messages font alors référence à SIGHUP au lieu de HTTP, que le rechargement ait été déclenché par une demande HTTP ou par un signal SIGHUP. Par exemple :

```
Tue Jul 23 12:47:28 2013 simnet2 probe on test_server:28148 :
 Rules file reread upon SIGHUP request successful
```

En outre, si le rechargement d'un fichier de règles échoue pour une raison autre qu'une erreur de syntaxe, le nom du fichier n'est pas inclus dans le message. Le message signalant l'échec ressemble au message suivants :

```
Tue Jul 23 18:20:24 2013 simnet_my probe on test_server:6790 :
 Rules file reread upon HTTP request failed ... (  in file  )
```

Pour résoudre ces problèmes, installez les sondes dans un environnement Tivoli Netcool/OMNIbus version 8.1.

Exemple

L'exemple suivant montre le type des messages qui sont journalisés lors de l'envoi de la commande de rechargement à trois sondes ayant des interfaces HTTP actives :

```
Tue Jul 23 12:46:27 2013 Reload all probe rules request
Tue Jul 23 12:46:27 2013 Sent HTTP reload rules request to simnet1 on
 test_server:28888
Tue Jul 23 12:46:27 2013 Sent HTTP reload rules request to simnet3 on
 test_server:28316
Tue Jul 23 12:46:27 2013 Sent HTTP reload rules request to simnet2 on
 test_server:28602
Tue Jul 23 12:46:27 2013 Reload all rules summary: managed probes 3,
 unmanaged probes 0, probes not running 0
Tue Jul 23 12:46:31 2013 simnet2 probe on test_server:28602 : Rules file reread
 upon HTTP request successful ...
Tue Jul 23 12:46:31 2013 simnet3 probe on test_server:28316 : Rules file reread
 upon HTTP request successful ...
Tue Jul 23 12:46:31 2013 simnet1 probe on test_server:28888 : Rules file reread
 upon HTTP request successful ...
```

L'exemple suivant montre le type des messages qui sont journalisés lorsque certaines sondes ont des interfaces HTTP actives et d'autres pas :

```
Tue Jul 23 12:47:24 2013 Reload all probe rules request
Tue Jul 23 12:47:24 2013 Sent HTTP reload rules request to simnet1 on
 test_server:29420
Tue Jul 23 12:47:24 2013 Sent HTTP reload rules request to simnet3 on
 test_server:28863
Tue Jul 23 12:47:24 2013 Sent HTTP reload rules request to simnet2 on
 test_server:28148
Tue Jul 23 12:47:24 2013 HTTP interface not active for notmgd_simnet1
 on test_server
Tue Jul 23 12:47:24 2013 HTTP interface not active for notmgd_simnet2
```

```
 on test_server
Tue Jul 23 12:47:24 2013 Reload all rules summary: managed probes 3,
 unmanaged probes 2, probes not running 0
Tue Jul 23 12:47:27 2013 simnet3 probe on test_server:28863 : Rules file reread
 upon HTTP request successful ...
Tue Jul 23 12:47:28 2013 simnet1 probe on test_server:29420 : Rules file reread
 upon HTTP request successful ...
Tue Jul 23 12:47:28 2013 simnet2 probe on test_server:28148 : Rules file reread
 upon HTTP request successful ...
```

L'exemple suivant montre le type des messages qui sont journalisés lorsqu'un fichier de règles contient une erreur de syntaxe :

```
Tue Jul 23 18:20:24 2013 simnet_my probe on test_server:6790 : Rules file reread
 upon HTTP request failed ... ( parse error at line 6 in file simnet.rules )
```

Tâches associées:

«Configuration d'un réseau protégé SSL», à la page 380
Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

Importation des rapports récapitulatifs des événements dans Tivoli Common Reporting

Pour exécuter les rapports récapitulatifs des événements, connectez Tivoli Common Reporting à une base de données relationnelle via une passerelle. Puis, importez le module de rapports qui est fourni avec Tivoli Netcool/OMNIbus dans Tivoli Common Reporting.

Avant de commencer

Plusieurs produits et composants doivent être installés et configurés de sorte que les données d'événement peuvent être stockées et affichées. Ces produits sont répertoriés dans le tableau ci-dessous :

Produit ou composant	Instructions
Tivoli Netcool/OMNIbus Gateway Configuration Scripts (mode génération de rapport)	Vous pouvez obtenir ces scripts à partir d'IBM Passport Advantage Online, à l'adresse http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. Pour trouver les scripts sur Passport Advantage Online, recherchez *nco-g-jdbc-reporting-scripts 1_0*. Configurez le serveur ObjectServer, la passerelle et la base de données relationnelle, selon les instructions fournies avec ces scripts.
Tivoli Netcool/OMNIbus	Un serveur ObjectServer doit être créé et en cours d'exécution.

Produit ou composant	Instructions
Tivoli Common Reporting	V3.1 est obligatoire. Pour plus d'informations sur l'installation et la configuration de Tivoli Common Reporting, voir http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.0/com.ibm.psc.doc_1.1.0/install/tcr_t_install.html. Tivoli Common Reporting est hébergé sur une instance de Concentrateur des services d'application du tableau de bord.
Base de données relationnelle	Vous pouvez utiliser une base de données IBM DB2 ou Microsoft SQL, Sybase ou Oracle.
Passerelle Tivoli Netcool/OMNIbus	Utilisez la passerelle pour JDBC. Si la base de données relationnelle est Oracle, vous pouvez également utiliser la passerelle Gateway for Oracle. Exécutez la passerelle en mode génération de rapport. Pour plus d'informations sur la passerelle, voir *IBM Tivoli Netcool/OMNIbus Gateway for JDBC Reference Guide* qui contient des informations sur les pilotes JDBC requis. Sinon, voir *IBM Tivoli Netcool/OMNIbus Gateway for Oracle Reference Guide*. Ces publications sont accessibles dans le centre de documentation Tivoli Netcool/OMNIbus à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp.

Pourquoi et quand exécuter cette tâche

Pour afficher les rapports dans Tivoli Common Reporting, vous devez créer une connexion entre Tivoli Common Reporting et la base de données relationnelle. Ensuite, vous devez importer le module de rapports qui est fourni avec Tivoli Netcool/OMNIbus dans Tivoli Common Reporting et vérifier que l'importation a réussi.

Conseil : Utilisez Internet Explorer pour gérer Tivoli Common Reporting.

Procédure

Pour importer les rapports, procédez comme suit. Ces étapes supposent que votre base de données relationnelle est DB2. Si vous utilisez une autre base de données, faites un autre choix à l'étape 2b, à la page 486. Les zones de la fenêtre New Data Source Wizard (Assistant de nouvelle source de données) reflètent votre choix.

1. Connectez-vous à Concentrateur des services d'application du tableau de bord en tant qu'utilisateur tipadmin ou un autre utilisateur approprié, puis accédez à la page Administration comme suit :
   a. Dans le panneau de navigation de gauche, cliquez sur **Reporting** > **Common Reporting**.
   b. Dans la barre des tâches située dans la partie supérieure droite, cliquez sur **Launch** > **Administration**
   c. Sur la page Administration, cliquez sur l'onglet **Configuration**.

2. Ajoutez la connexion de source de données. Effectuez ces étapes avec les informations fournies dans le centre de documentation Tivoli Common Reporting à l'adresse http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_21/ttcr_config_db.html.
   a. Sélectionnez **Data Source Connections (Connexions de source de données)** et cliquez sur **Add (Ajouter)**.
   b. Dans la fenêtre New Data Source Wizard (Assistant de nouvelle source de données), complétez les zones comme suit à mesure que vous progressez dans les panneaux.

      Name Entrez `Reporter`. Le nom doit être Reporter car il doit être identique au nom utilisé dans le module de rapports.

      Type Sélectionnez le type de base de données relationnelle, par exemple **DB2**.

      Use the default object gateway (Utiliser la passerelle d'objet par défaut)
      Cochez cette case.

      DB2 database field (Zone de base de données DB2)
      Entrez `REPORTER`. Le nom de la base de données DB2 doit correspondre au nom du schéma de base de données de Gateway for JDBC.

      Signon (Connexion)
      Sélectionnez ce bouton d'option.

      Password
      Cochez cette case.

      Create a signon that the Everyone group can use (Créer un code d'accès que le groupe Tous peut utiliser)
      Cochez cette case.
   c. Entrez votre nom d'utilisateur DB2, puis entrez et confirmez votre mot de passe. Le nom d'utilisateur DB2 doit correspondre au schéma DB2 qui contient les tables du schéma de base de données Gateway for JDBC. En général, ce nom d'utilisateur correspond à l'utilisateur DB2 qui a exécuté le script de base de données de passerelle.
   d. Cliquez sur **Test the connection (Tester la connexion)**, puis cliquez sur le bouton **Test**. Cliquez ensuite sur **Close (Fermer)** > **Close (Fermer)**.
   e. Cliquez sur **Next (Suivant)** > **Finish (Terminer)**.
3. Sur l'hôte de Tivoli Netcool/OMNIbus, copiez le module de rapports `Netcool_OMNIbus.zip` du répertoire `$NCHOME/omnibus/extensions/tcr_event_reports` vers l'hôte Tivoli Common Reporting.
   - UNIX Linux `/opt/IBM/JazzSM/reporting/cognos/deployment`
   - Windows `C:\IBM\JazzSM\reporting\cognos\deployment`
4. En tant qu'utilisateur smadmin, ou un autre utilisateur approprié, accédez à l'emplacement indiqué à l'étape 1, à la page 485 et cliquez sur **New Import (Nouvelle importation)**  .
5. Vérifiez que le fichier `Netcool_OMNIbus.zip` est sélectionné et cliquez sur **Next (Suivant)**. Ensuite, entrez un nom pour la spécification de déploiement et cliquez sur **Next (Suivant)**. Si le module n'est pas disponible pour sélection, assurez-vous qu'il est copié dans l'emplacement spécifié à l'étape 3.
6. Cochez la case en regard du module se trouvant dans le fichier `Netcool_OMNIbus.zip` et cliquez sur **Next (Suivant)**.

7. Cliquez sur **Suivant** > **Suivant**. Cliquez ensuite sur **Save only (Sauvegarder uniquement)** > **Finish (Terminer)**.
8. Cliquez sur **Play (Lecture)**  en regard du module importé. Sélectionnez **Now (Maintenant)** puis cliquez sur **Run (Exécuter)** Pour revenir à la page Content Administration (Administration du contenu), cliquez sur **Back (Retour)**  .

Résultats

Les rapports sont ajoutés à Tivoli Common Reporting. Vous pouvez afficher les rapports dans la zone Public folders (Dossiers publics) dans Tivoli Common Reporting.

Que faire ensuite

Vous pouvez effectuer les opérations suivantes :

- Lisez les descriptions de rapport afin de vous familiariser avec les rapports et leurs paramètres.
- Modifiez les rapports. Pour éditer des rapports, cliquez sur **Report Studio** dans la liste de rapports ou dans la partie droite du rapport HTML.
- Modifiez le modèle Tivoli Common Reporting. Pour plus d'informations, consultez l'article IBM DeveloperWorks *Tivoli Common Reporting Event Reports for Netcool OMNIbus* à l'adresse https://www.ibm.com/developerworks/mydeveloperworks/wikis/. Pour rechercher l'article sur DeveloperWorks, utilisez la fonction de recherche à droite de la page pour rechercher les éléments identifiés par **omnibus-tcr**.

Tâches associées:

«Création et exécution de serveurs ObjectServer», à la page 193
Chaque installation Tivoli Netcool/OMNIbus peut avoir au moins un serveur ObjectServer pour stocker et gérer les informations d'alerte. Vous pouvez également configurer plusieurs serveurs ObjectServer sur un ou plusieurs ordinateurs hôtes.

Référence associée:

Annexe D, «Rapports Tivoli Common Reporting pour Tivoli Netcool/OMNIbus», à la page 701
Utilisez ces informations pour vous familiariser avec les rapports Tivoli Netcool/OMNIbus fournis pour Tivoli Common Reporting (TCR).

Activation des métriques de débit d'événements X en Y

Les environnements Tivoli Netcool/OMNIbus comportent généralement sur leurs réseaux des unités qui génèrent de nombreuses alertes. La plupart de ces alertes représentent des problèmes de violation des seuils de performances, par exemple un commutateur qui atteint sa capacité de bande passante maximale pendant une période de pointe. Ces violations de seuil temporaires sont souvent prévues et la stratégie métier consiste à les ignorer sauf si la violation se poursuit pendant une période prolongée mais spécifique. Si ces alertes se poursuivent au-delà de ces périodes spécifiées, les opérateurs doivent intervenir. Cette section décrit un scénario de débit d'événements 'X' en 'Y' classique dans lequel l'opérateur n'est intéressé que par les alertes qui se produisent plus de X fois en Y secondes. Lorsque le débit d'événements dépasse le seuil, l'événement doit être escaladé. Cependant, tant que le seuil n'est pas dépassé, il n'est pas nécessaire de traiter les événements.

Présentation

La clé de calcul des métriques X en Y est la possibilité de capturer et de stocker les horodatages successifs à mesure que chaque occurrence de chaque événement est reçue. Il suffit de stocker les horodatages X les plus récents dans la mesure où il s'agit d'horodatages indiquant si une violation a eu lieu.

Remarque : Le fait de stocker plusieurs horodatages X augmente également l'espace mémoire utilisé par le serveur ObjectServer et n'est donc pas réalisé dans cette solution.

Lors de la réception de chaque événement, l'horodatage de la date/heure de réception de l'événement est ajouté à l'ensemble des horodatages stockés. Un calcul est effectué pour vérifier si les X derniers événements ont eu lieu en Y secondes. Ce processus est répété pour chaque occurrence de chaque événement reçu.

La solution X en Y utilise les fonctions de paire valeur-nom (NVP) sur le serveur ObjectServer pour stocker et extraire les horodatages d'occurrence d'événement à partir d'une zone de chaîne et vers celle-ci. En conséquence, aucune analyse de table dans le serveur ObjectServer n'est nécessaire pour effectuer des vérifications X en Y dans la mesure où toutes les informations requises sont stockées dans un seul emplacement dans chaque événement. La solution a donc un léger impact sur les performances d'un serveur ObjectServer sur lequel elle est installée. Les déclencheurs ajoutés au serveur ObjectServer sont toujours actifs et n'agissent sur les événements que lorsque les critères suivants sont définis :

- Une valeur différente de zéro pour la zone `XEvents` est définie.
- Une valeur différente de zéro pour la zone `YSeconds` est définie.
- La gravité de l'événement entrant n'est pas égale à zéro.

Remarque : Les événements dont la gravité est égale à zéro ne doivent pas être comptabilisés dans la mesure où ils sont généralement une incidence d'un événement d'effacement lors de l'utilisation de l'effacement par dédoublonnage. Etant donné que l'événement d'effacement n'est pas un événement à “problème”, il ne doit pas être “comptabilisé”.
Ces zones doivent être définies dans les règles de la sonde ou par n'importe quelle source d'événement insérant l'événement. Sous réserve que ces zones soient définies, la fonctionnalité X en Y est automatiquement activée pour ces événements par événement.

Composants de la solution X en Y

La solution X en Y comprend quatre zones ObjectServer supplémentaires, deux déclencheurs ObjectServer et deux procédures.

Un autre facteur essentiel de la fonctionnalité est un fichier de réplication de table modifié pour les passerelles entre la couche Collection et la couche Agrégation à utiliser dans un environnement multiniveau. Enfin, un fichier de mappage de passerelle est fourni pour être utilisé dans les fichiers de mappage de la passerelle entre la couche Collection et la couche Agrégation et la couche Agrégation de basculement.

Quatre zones

La solution X en Y ajoute les quatre zones suivantes au serveur ObjectServer.

XinY VARCHAR(4096)

Cette zone correspond à la zone de chaîne qui stocke les horodatages successifs. La façon dont cette zone est utilisée conjointement avec les fonctions NVP se comporte efficacement comme un tableau. Les horodatages sont stockés dans la zone par les fonctions NVP au format suivant :

```
t1="1332419954";t2="1332419954";t3="1332419954";t4="1332419954"
```

16 caractères sont requis par horodatage pour les 9 premiers horodatages (c'est-à-dire t1 à t9), 17 caractères sont requis par horodatage pour les 90 horodatages suivants (c'est-à-dire t10 à t99) et, par la suite, 18 caractères sont requis par horodatage. Sur cette base, jusqu'à 234 horodatages peuvent être stockés dans la zone de 4096 caractères, afin de prendre en charge une valeur XEvents maximale de 234.

Remarque : C'est la raison pour laquelle 234 est la valeur maximale qui doit être utilisée pour la zone `XEvents`.

NumXinY INTEGER

Il est noter qu'il est possible de recevoir plusieurs instances du même événement (c'est-à-dire, possédant le même ID (`Identifier`)) qui comportent des valeurs `XEvents` et `YSeconds` valides, ainsi que celles comportant des valeurs `XEvents` et `YSeconds` différentes de zéro non valides. Les horodatages ne sont collectés pour les événements dont les zones `XEvents` et `YSeconds` comportent toutes deux des valeurs différentes de zéro valides. En conséquence, la zone `Tally` stocke le nombre total d'occurrences de n'importe quel événement, mais `NumXinY` stocke le nombre d'événements dont les valeurs de zone `XEvents` et `YSeconds` sont valides. Cette zone est utilisée par la fonctionnalité X en Y afin de déterminer si le d'horodatages stockés est suffisant pour permettre des calculs de seuil. Les calculs de seuil ne sont effectués qu'une fois qu'il y a `XEvents` horodatages.

XEvents INTEGER

Cette zone stocke la première partie du seuil : le nombre d'événements.

YSeconds INTEGER

Cette zone stocke la seconde partie du seuil : le nombre de secondes. Cette zone est utilisée conjointement avec la zone `XEvents` pour déterminer s'il y a eu une violation de seuil. Cette zone ainsi que la zone `XEvents` doivent être paramétrées sur des valeurs différentes de zéro valides de sorte que la fonctionnalité X en Y soit activée pour un événement donné.

Deux procédures

La solution X en Y ajoute les deux procédures ci-dessous à chaque serveur ObjectServer.

xiny_add_time stamp

Cette procédure a pour but d'ajouter un horodatage à la zone d'horodatage `XinY`. Si aucun horodatage n'est fourni lorsque la procédure est appelée (c'est-à-dire, une valeur égale à zéro est reçue), la procédure ajoute l'horodatage en cours dans la zone d'horodatage.

La procédure ne stocke qu'un maximum de `XEvents` horodatages dans la mesure où ce nombre est le minimum requis pour déterminer s'il y a eu ou non une violation de seuil. Le fait de stocker un nombre supérieur augmente inutilement la taille de zone de la mémoire et, par conséquent, l'encombrement de mémoire du serveur ObjectServer.

La procédure va stocker les horodatages successifs dans l'ordre chronologique, du plus récent au plus ancien, et ne va stocker que XEvents horodatages les plus récents. Si la procédure est appelée à l'aide d'un horodatage antérieur à la valeur la plus ancienne actuellement stockée que la zone d'horodatage comporte déjà XEvents horodatages, la valeur entrante est supprimée.

xiny_calculate_breach
Cette procédure utilise la zone d'horodatage XinY, les valeurs de seuil XEvents et YSeconds et détermine si une violation de seuil a eu lieu. Si une violation de seuil a eu lieu, cela est indiqué et retransmis à l'emplacement à partir duquel la procédure a été appelée. Si une violation de seuil est détectée, la zone SuppressEscl est paramétrée sur 1, ce qui signifie qu'elle est désormais à l'état "Escaladé". Les opérateurs peuvent ensuite voir que l'événement est escaladé dans la liste d'événements et prendre des mesures.

Remarque : La procédure xiny_calculate_breach n'est incluse que dans les serveurs ObjectServer de la couche Agrégation dans la mesure où les calculs de violation ne sont effectués qu'au niveau de la couche d'agrégation.

Deux déclencheurs de base de données ObjectServer

La solution X en Y ajoute les deux déclencheurs de base de données ci-dessous à chaque serveur ObjectServer.

xiny_on_insert
Ce déclencheur de base de données se déclenche avant qu'un événement soit inséré dans le serveur ObjectServer qui comporte des valeurs différentes de zéro valides pour les deux zones XEvents et YSeconds, et la valeur Severity de l'événement entrant est différente de zéro. Si ces conditions sont remplies, l'horodatage en cours est ajouté à la zone d'horodatage XinY.

Sur un serveur ObjectServer de la couche Agrégation, cette procédure n'insère un horodatage que si l'événement entrant ne provient pas d'une passerelle. En effet, si l'événement entrant provient d'une passerelle, il est issu d'un autre serveur ObjectServer et va donc déjà inclure un ensemble de valeurs XinY. Dans tous les cas, un calcul de violation est effectué pour chaque insertion dans un serveur ObjectServer de la couche Agrégation.

Remarque : Les calculs de violation de seuil ne sont effectués qu'au niveau de la couche Agrégation.
Si une violation est détectée, ce qui est possible si un événement contenant un certain nombre d'horodatages a été reçu de la couche Collection, une entrée de journal est ajoutée et l'événement est escaladé.

Remarque : Au niveau de la couche Agrégation, ce déclencheur n'est émis que sur le serveur principal actif.

xiny_on_reinsert
Ce déclencheur de base de données se déclenche chaque fois qu'un événement est *réinséré* dans le serveur ObjectServer qui comporte des valeurs différentes de zéro pour les deux zones XEvents et YSeconds, et la valeur Severity de l'événement entrant est différente de zéro. Si ces conditions sont remplies, l'horodatage en cours est ajouté à la zone d'horodatage XinY.

Sur un serveur ObjectServer de la couche Agrégation, cette procédure traite les réinsertions provenant de la passerelle Collection différemment des événements réinsérés à partir d'autres sources. Etant donné que la collecte d'horodatages se produit également au niveau des serveurs ObjectServer de la couche Collection, les réinsertions entrantes à partir de la couche Collection incluent un ensemble de valeurs `XinY` à fusionner avec les valeurs figurant déjà au niveau de la couche Agrégation.

Pour réaliser cette opération, la procédure effectue une itération sur l'ensemble de valeurs `XinY` entrant et l'ajoute à l'ensemble local via la procédure `xiny_on_reinsert`. Cela garanti que toutes les valeurs entrantes sont stockées dans un ordre de tri chronologique. Si la copie locale de l'événement comporte déjà `XEvents` horodatages stockés et que l'une des valeurs entrantes est antérieure à la valeur la plus ancienne déjà présente, ces valeurs entrantes individuelles sont supprimées.

Remarque : La solution comprend un fichier de définition de réplication de table modifié pour les passerelles entre la couche Collection et la couche Agrégation qui efface les zones `XinY` et `NumXinY` au niveau de la copie de la couche Collection de l'événement une fois que l'événement est transmis à la couche Agrégation. Ainsi, les déclencheurs de la couche Agrégation peuvent supposer que toutes les valeurs entrantes dans la couche Agrégation n'ont pas été traitées précédemment et doivent être ajoutées à l'ensemble actuel des horodatages collectés.
Les réinsertions provenant d'autres sources, à l'exception de la passerelle ObjectServer de la couche Agrégation de basculement, par exemple une sonde, déclenchent une insertion dans la zone d'horodatage `XinY` contenant l'horodatage en cours.

Les réinsertions provenant du serveur ObjectServer de la couche Agrégation de basculement sont ignorées en ce qui concerne les calculs de seuil dans la mesure où la source d'événement est le serveur ObjectServer homologue de la couche Agrégation qui réplique ses événements.

Dans tous les cas où un horodatage est inséré, une vérification de violation de seuil est effectuée par le biais de la procédure `xiny_calculate_breach` et l'événement est escaladé, si nécessaire.

Remarque : Les calculs de violation de seuil ne sont effectués qu'au niveau de la couche Agrégation.
Si l'événement est escaladé, une entrée de journal est également ajoutée à l'événement pour indiquer que c'est la fonctionnalité X en Y qui a escaladé l'événement et à quelle heure.

Remarque : Au niveau de la couche Agrégation, ce déclencheur n'est émis que sur le serveur principal actif.

Définition modifiée de la réplication de table de passerelle entre la couche Collection et la couche Agrégation

Dans un environnement multiniveau, les serveurs ObjectServer de la couche Collection collectent également des horodatages pour les événements dont les zones appropriées sont définies. Les violations de seuil ne sont pas effectuées au niveau de la couche Collection ; cependant, les horodatages sont transmis à la couche Agrégation à des fins d'inclusion dans les calculs de seuil.

Chaque fois que la passerelle entre la couche Collection et la couche Agrégation transmet la copie Collection de l'événement jusqu'à la couche Agrégation, le fichier de définition de réplication de table de passerelle inclut du code effaçant les zones XinY (chaîne) et NumXinY (entier) après le transfert :

```
AFTER IDUC DO 'Tally = 0, SentToAgg = 1, XinY = \'\', NumXinY = 0'
```

La raison pour laquelle les zones X en Y dans la copie Collection de l'événement sont effacées est de permettre à la couche Agrégation de supposer que toutes les valeurs entrantes sont nouvelles et doivent donc être toutes incluses dans l'ensemble local. Sinon, il n'y a aucun moyen de savoir quelles entrées sont nouvelles et doivent être fusionnées dans l'ensemble local de valeurs et quelles entrées ont déjà été vues. Cela est important dans la mesure où le même événement peut provenir de plusieurs sources.

Exemple : basculement ou reprise en ligne d'une sonde entre une paire de serveurs ObjectServer de la couche Collection. Dans ce cas, il peut y avoir des occurrences d'un même événement provenant de plusieurs serveurs ObjectServer de la couche Collection, chacun possédant un ensemble d'horodatages, convergeant sur la couche Agrégation qui doit être fusionnée.

Exemples de scénarios

La présente section contient quelques exemples du comportement de la solution dans des circonstances différentes.

Les deux exemples de scénarios suivants sont explorés :

- «Insertion ou réinsertion standard à partir d'une sonde»
- «Insertion ou réinsertion à partir d'une passerelle entre la couche Collection et la couche Agrégation», à la page 494

Insertion ou réinsertion standard à partir d'une sonde

Dans cet exemple, un événement valide est reçu d'une sonde où `XEvents` est paramétré sur 3 et `YSeconds` sur 10 secondes.

Lors de la réception du premier événement, l'heure en cours est ajoutée à la zone d'horodatage, ce qui donne lieu à la valeur de zone `XinY` suivante :

```
t1="1111111110"
```

Etant donné que moins de `XEvents` horodatages sont stockés, aucun calcul de seuil n'est effectué à ce stade.

Dix secondes plus tard, une autre occurrence de l'événement est reçue de la sonde. L'horodatage existant est “inséré” le long d'un emplacement à droite et le nouvel horodatage est inséré à l'avant de la zone d'horodatage `XinY` :

```
t1="1111111120";t2="1111111110"
```

Etant donné que moins de `XEvents` horodatages sont stockés, aucun calcul de seuil n'est effectué à ce stade.

Trois secondes plus tard, une autre occurrence de l'événement est reçue de la sonde. Les horodatages existants sont “insérés” le long d'un emplacement à droite et le nouvel horodatage est inséré à l'avant de la zone d'horodatage `XinY` :

```
t1="1111111123";t2="1111111120";t3="1111111110"
```

Etant donné que `XEvents` horodatages sont désormais stockés, un calcul de seuil est effectué. Cependant, étant donné que le delta entre l'horodatage le plus ancien et l'horodatage le plus récent est de 13 secondes, il n'existe donc aucune condition de violation.

Trois secondes plus tard, une autre occurrence de l'événement est reçue de la sonde. Les horodatages existants sont “insérés” le long d'un emplacement à droite et le nouvel horodatage est inséré à l'avant de la zone d'horodatage `XinY`. Dans la mesure où `XEvents` est paramétré sur 3, seuls les 3 horodatages les plus récents sont stockés. La valeur "1111111110" de l'horodatage le plus ancien est ignorée, ce qui donne lieu à la valeur suivante :

```
t1="1111111126";t2="1111111123";t3="1111111120"
```

Dans la mesure où `XEvents` horodatages sont stockés, un calcul de seuil est effectué. Etant donné que le delta entre l'horodatage le plus ancien et l'horodatage

le plus récent est à présent de 6 secondes uniquement, il existe donc une condition de violation. Il en résulte que la zone SuppressEscl est paramétrée sur 1, ce qui signifie que l'événement est désormais à l'état “escaladé”. Cela apparaît dans les listes d'événements des opérateurs qui peuvent intervenir.

Insertion ou réinsertion à partir d'une passerelle entre la couche Collection et la couche Agrégation

Dans cet exemple, plusieurs instances du même événement supprimé sont reçues dans le serveur ObjectServer principal de la couche Agrégation à partir de deux passerelles différentes entre la couche Collection et la couche Agrégation. Cet exemple illustre comment les zones d'horodatage entrantes sont fusionnées avec la zone d'horodatage Agrégation locale.

Au départ, un événement valide est reçu du serveur ObjectServer principal de la couche Collection COL_P_1 via sa passerelle entre la couche Collection et la couche Agrégation C_TO_A_GATE_P_1, où XEvents est paramétré sur 5 et YSeconds sur 10 secondes. Lorsque la première instance de l'événement est reçue au niveau de la couche Agrégation, toutes les zones sont conservées en l'état, à l'aide de la valeur de zone XinY reçue de la couche Collection :

```
t1="1111111110"
```

Etant donné que moins de XEvents horodatages sont stockés, aucun calcul de seuil n'est effectué.

Deux autres occurrences du même événement sont ensuite insérées par la sonde dans le serveur ObjectServer de la couche Collection COL_P_1 donnant lieu à un ensemble d'horodatages XinY des valeurs suivantes :

```
t1="1111111114";t2="1111111112"
```

A ce stade, la sonde bascule sur le serveur ObjectServer de secours de la couche Collection COL_B_1 et insère trois autres occurrences du même événement donnant lieu à l'ensemble d'horodatages XinY suivant :

```
t1="1111111120";t2="1111111118";t3="1111111116"
```

Le cycle IDUC de la passerelle entre la couche Collection et la couche Agrégation C_TO_A_GATE_B_1 connectée au serveur ObjectServer de secours de la couche Collection COL_B_1 est déclenché en premier, ce qui donne lieu à la transmission de sa configuration XinY au serveur ObjectServer principal de la couche Agrégation.

Remarque : L'ensemble d'horodatages qui se trouve actuellement dans COL_B_1 contient des horodatages plus récents que ceux dans COL_P_1 mais ils sont transmis à la couche Agrégation en premier. Cet exemple montre donc qu'il n'est pas important que les horodatages soient reçus au niveau de la couche Agrégation dans l'ordre chronologique, dans la mesure où la procédure qui insère chacun des horodatages conserve néanmoins l'ordre de tri.
L'ensemble des horodatages de trois valeurs dans la zone d'horodatage COL_B_1 sont reçus par le serveur ObjectServer principal de la couche Agrégation et ajoutés un à un dans la zone d'horodatage de la couche Agrégation dans l'ordre chronologique descendant donnant lieu à l'ensemble d'horodatages XinY suivant :

```
t1="1111111120";t2="1111111118";t3="1111111116";t4="1111111110"
```

Il est à noter que l'horodatage existant était le plus ancien et a donc été réorganisé dans l'emplacement t4, afin de conserver l'ordre de tri. Etant donné que moins de XEvents horodatages sont stockés, aucun calcul de seuil n'est effectué à ce stade.

Ensuite, le cycle IDUC de la passerelle entre la couche Collection et la couche Agrégation C_TO_A_GATE_P_1 connectée au serveur ObjectServer principal de la couche Collection COL_P_1 est déclenché, ce qui donne lieu à la transmission de sa configuration XinY au serveur ObjectServer principal de la couche Agrégation.

L'ensemble des horodatages de deux valeurs dans la zone d'horodatage COL_P_1 sont ajoutés un à un dans la zone d'horodatage de la couche Agrégation dans l'ordre chronologique descendant donnant lieu à l'ensemble d'horodatages XinY suivant :

```
t1="1111111120";t2="1111111118";t3="1111111116";t4="1111111114";t5="1111111112"
```

Il est à noter que l'horodatage de "1111111110" précédemment stocké dans l'emplacement t4 était le plus ancien des horodatages et a donc été supprimé car seul XEvents horodatages les plus récents sont conservés. Dans ce cas, XEvents est égal à 5, ce qui signifie que seuls les 5 horodatages les plus récents sont conservés.

Il est également à noter que, malgré le fait que les horodatages de l'ensemble XinY entrant sont plus anciens que certains des horodatages déjà présents dans l'ensemble XinY de la couche Agrégation, les valeurs entrantes ont simplement été insérées une à une dans le bon emplacement pour garantir que l'ensemble résultant au niveau de la couche Agrégation conserve un ordre de tri. Etant donné que XEvents horodatages sont désormais stockés, un calcul de seuil est effectué. Etant donné que le delta entre l'horodatage le plus ancien et l'horodatage le plus récent est à présent de 8 secondes, il existe donc une condition de violation. Il en résulte que la zone SuppressEscl est mise à jour à 1, ce qui signifie que l'événement est désormais à l'état “escaladé”. Cela apparaît dans les listes d'événements des opérateurs qui peuvent intervenir.

Configuration des actions d'escalade personnalisées

L'escalade par défaut pour un événement qui ne respecte pas son seuil consiste à paramétrer SuppressEscl sur 1, ce qui signifie qu'il est dans un état escaladé. Il est prévu d'ajouter d'autres actions d'escalade personnalisées dans la solution X en Y. Le fichier SQL intitulé xiny_aggregation.sqlcontient un déclencheur d'insertion et un déclencheur de réinsertion. Toutes les actions d'escalade personnalisées doivent être ajoutées à ces deux déclencheurs dans la mesure où l'escalade peut avoir lieu dans le cas d'une insertion ou d'une réinsertion d'un événement, en fonction de sa source.

Un événement peut être escaladé immédiatement lors de l'insertion car le seuil (c'est-à-dire xevents) est paramétré sur 1 ou lorsque plusieurs occurrences d'un même événement arrivent au niveau de la couche Agrégation à partir de la couche Collection ; par conséquent, la ligne entrante peut contenir plusieurs horodatages. Les actions d'escalade d'insertion sont traitées dans le déclencheur intitulé xiny_on_insert. Les actions d'escalade personnalisées doivent être placées dans l'emplacement désigné suivant :

```
-----------------------------------------
-- INSEREZ LES ACTIONS D'ESCALADE PERSONNALISEES ICI
-----------------------------------------
-- EXEMPLE : -- RAISE SEVERITY
-- EXEMPLE : set new.Severity = 5;
-- ...
-----------------------------------------
```

Remarque : Vous devez définir les valeurs new.* pour mettre à jour les zones lors de l'insertion.

Les actions d'escalade de réinsertion sont traitées dans le déclencheur intitulé `xiny_on_reinsert`. Les actions d'escalade personnalisées doivent être placées dans l'emplacement désigné suivant :

```
----------------------------------------
-- INSEREZ LES ACTIONS D'ESCALADE PERSONNALISEES ICI
----------------------------------------
-- EXEMPLE : -- RAISE SEVERITY
-- EXEMPLE : set old.Severity = 5;
-- ...
----------------------------------------
```

Remarque : Vous devez définir les valeurs old.* pour mettre à jour les zones lors de la réinsertion.

Installation de la solution X dans Y

Cette section contient des instructions pour l'installation et l'utilisation de la solution X dans Y.

Les composants de la solution X dans Y se trouvent dans les répertoires d'extensions Tivoli Netcool/OMNIbus :

- UNIX `$NCHOME/omnibus/extensions/xiny`
- Windows `$NCHOME\omnibus\extensions\xiny`

Le répertoire contient les fichiers suivants :

- `xiny_collection.sql`
- `xiny_aggregation.sql`
- `xiny_C_TO_A_GATE_B_1.tblrep.def`
- `xiny_C_TO_A_GATE_P_1.tblrep.def`
- `xiny_GATEWAY.map`
- `xiny_collection_rollback.sql`
- `xiny_aggregation_rollback.sql`

Vous pouvez importer les fichiers SQL dans les serveurs ObjectServer Collection ou Agrégation pour créer des zones, des procédures et des déclencheurs. Les fichiers DEF remplacent les fichiers DEF fournis dans l'architecture multiniveau standard et comprennent une petite modification du comportement de l'interaction de la passerelle entre la couche Collection et la couche Agrégation avec les serveurs ObjectServer de la couche Collection. Le fichier MAP contient quatre mappages de zones supplémentaires qui doivent être ajoutés à tous les fichiers de mappage de passerelle entre la couche Collection et la couche Agrégation ou la couche Agrégation de basculement.

Les sections suivantes décrivent les procédures d'installation de la solution X dans Y :

- «Configuration de la paire d'agrégation», à la page 497
- «Configuration de la paire de collection», à la page 498
- «Activation de la solution X en Y», à la page 499

Configuration de la paire d'agrégation

Suivez les étapes décrites dans cette section pour installer la solution X en Y dans une paire de serveurs ObjectServer de la couche Agrégation.

Procédure

1. Installez et configurez une paire de serveurs ObjectServer de basculement de la couche Agrégation à l'aide de la configuration de l'architecture multiniveau standard. Pour plus d'informations, voir Configuration et déploiement d'une architecture à plusieurs niveaux dans le *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.
2. Importez le fichier `xiny_aggregation.sql` dans le serveur ObjectServer principal de la couche Agrégation :
   - UNIX `$OMNIHOME/bin/nco_sql –server AGG_P –user root < xiny_aggregation.sql`
   - Windows `"%OMNIHOME%\bin\isql" -S AGG_P -U root -i xiny_aggregation.sql`
3. Importez le fichier `xiny_aggregation.sql` dans le serveur ObjectServer de secours de la couche Agrégation :
   - UNIX `$OMNIHOME/bin/nco_sql –server AGG_B –user root < xiny_aggregation.sql`
   - Windows `"%OMNIHOME%\bin\isql" -S AGG_B -U root -i xiny_aggregation.sql`
4. Copiez les mappages de zone dans `xiny_GATEWAY.map` vers le fichier de mappage de passerelle de basculement de la couche Agrégation.

   Remarque : Faites une copie de sauvegarde du fichier de mappage existant avant d'apporter des modifications.

   - UNIX `$OMNIHOME/etc/AGG_GATE.map`
   - Windows `%OMNIHOME%\etc\AGG_GATE.map`

   Les zones à ajouter sont les suivantes :

```
################################################################################
#
# EMPLACEMENT DES MAPPAGES DE ZONES PERSONNALISEES DE LA TABLE alerts.status
#
################################################################################
'XinY' = '@XinY',
'NumXinY' = '@NumXinY',
'XEvents' = '@XEvents',
'YSeconds' = '@YSeconds',
################################################################################
```

5. Redémarrez la passerelle ObjectServer de basculement de la couche Agrégation : `AGG_GATE`.

Configuration de la paire de collection

Suivez les étapes décrites dans cette section pour installer la solution X en Y dans une paire de serveurs ObjectServer de la couche Collection.

Procédure

1. Installez et configurez une paire de serveurs ObjectServer principal et de secours de la couche Collection à l'aide de la configuration de l'architecture multiniveau standard. Pour plus d'informations, voir Configuration et déploiement d'une architecture à plusieurs niveaux dans le *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.
2. Importez le fichier `xiny_collection.sql` dans le serveur ObjectServer principal de la couche Collection :
   - UNIX `$OMNIHOME/bin/nco_sql –server COL_P_1 –user root < xiny_collection.sql`
   - Windows `"%OMNIHOME%\bin\isql" -S COL_P_1 -U root -i xiny_collection.sql`
3. Importez le fichier `xiny_collection.sql` dans le serveur ObjectServer de secours de la couche Collection :
   - UNIX `$OMNIHOME/bin/nco_sql –server COL_B_1 –user root < xiny_collection.sql`
   - Windows `"%OMNIHOME%\bin\isql" -S COL_B_1 -U root -i xiny_collection.sql`
4. Copiez les mappages de zone dans `xiny_GATEWAY.map` vers le fichier de mappage de passerelle de la couche Collection.

   Remarque : Faites une copie de sauvegarde du fichier de mappage existant avant d'apporter des modifications.

   - UNIX `$OMNIHOME/etc/C_TO_A_GATE.map`
   - Windows `%OMNIHOME%\etc\C_TO_A_GATE.map`

   Les zones à ajouter sont les suivantes :

```
################################################################################
#
# EMPLACEMENT DES MAPPAGES DE ZONES PERSONNALISEES DE LA TABLE alerts.status
#
################################################################################
'XinY' = '@XinY',
'NumXinY' = '@NumXinY',
'XEvents' = '@XEvents',
'YSeconds' = '@YSeconds',
################################################################################
```

5. Copiez les deux fichiers de réplication de table inclus dans le répertoire `$OMNIHOME/etc/` en remplaçant les fichiers existants :

   Remarque : Faites une copie de sauvegarde des fichiers existants avant d'effectuer l'opération de copie.

   - UNIX

```
cp xiny_C_TO_A_GATE_P_1.tblrep.def $OMNIHOME/etc/C_TO_A_GATE_P_1.tblrep.def
cp xiny_C_TO_A_GATE_B_1.tblrep.def $OMNIHOME/etc/C_TO_A_GATE_B_1.tblrep.def
```

   - Windows

```
copy xiny_C_TO_A_GATE_P_1.tblrep.def %OMNIHOME%\etc\C_TO_A_GATE_P_1.tblrep.def
copy xiny_C_TO_A_GATE_B_1.tblrep.def %OMNIHOME%\etc\C_TO_A_GATE_B_1.tblrep.def
```

Remarque : Les personnalisations de fichier de réplication de table précédemment effectuées doivent être réalisées à nouveau dans les nouveaux fichiers de réplication de table.

6. Redémarrez les passerelles ObjectServer entre la couche Collection et la couche Agrégation : `C_TO_A_GATE_P_1` et `C_TO_A_GATE_B_1`.

Activation de la solution X en Y

Définissez les zones XEvents et YSeconds pour activer la solution X en Y.

Pour activer la solution X en Y pour un événement donné, définissez les zones ci-dessous dans vos sources d'événement. Par exemple, dans les fichiers de règles de la sonde :

XEvents
Paramétrée sur une valeur différente de zéro pour le nombre d'événements à recevoir afin de déclencher une violation de seuil.

YSeconds
Paramétrée sur une valeur différente de zéro pour le nombre de secondes devant s'écouler afin de déclencher une violation de seuil.

Remarque : Les horodatages ne sont enregistrés que pour les événements entrants dont la gravité n'est pas égale à zéro. Les événements d'effacement ne sont pas pris en compte pour les violations de seuil.

Désinstallation de la solution X en Y

Suivez les étapes décrites dans cette section pour désinstaller la solution X en Y.

Procédure

1. Restaurez les fichiers de mappage d'origine de la couche Collection et de la couche Agrégation à partir des sauvegardes :
   - UNIX
     ```
     $OMNIHOME/etc/AGG_GATE.map
     $OMNIHOME/etc/C_TO_A_GATE.map
     ```
   - Windows
     ```
     %OMNIHOME%\etc\AGG_GATE.map
     %OMNIHOME%\etc\C_TO_A_GATE.map
     ```
2. Restaurez les fichiers de réplication de table de passerelle d'origine de la couche Collection à partir des sauvegardes (le cas échéant) :
   - UNIX
     ```
     $OMNIHOME/etc/C_TO_A_GATE_P_1.tblrep.def
     $OMNIHOME/etc/C_TO_A_GATE_B_1.tblrep.def
     ```
   - Windows
     ```
     %OMNIHOME%\etc\C_TO_A_GATE_P_1.tblrep.def
     %OMNIHOME%\etc\C_TO_A_GATE_B_1.tblrep.def
     ```
3. Redémarrez les passerelles dans lesquelles les modifications ont été apportées.
4. Importez le fichier SQL d'annulation respectif dans tous les serveurs ObjectServer de la couche Collection et de la couche Agrégation :
   - UNIX
     ```
     $OMNIHOME/bin/nco_sql -server AGG_P -user root
     < xiny_aggregation_rollback.sql
     $OMNIHOME/bin/nco_sql -server AGG_B -user root
     < xiny_aggregation_rollback.sql
     ```

```
$OMNIHOME/bin/nco_sql –server COL_P_1 –user root
< xiny_collection_rollback.sql
$OMNIHOME/bin/nco_sql –server COL_B_1 –user root
< xiny_collection_rollback.sql
```

- Windows

```
"%OMNIHOME%\bin\isql" -S AGG_P -U root -i xiny_aggregation_rollback.sql
"%OMNIHOME%\bin\isql" -S AGG_B -U root -i xiny_aggregation_rollback.sql

"%OMNIHOME%\bin\isql" -S COL_P_1 -U root -i xiny_collection_rollback.sql
"%OMNIHOME%\bin\isql" -S COL_B_1 -U root -i xiny_collection_rollback.sql
```

Chapitre 18. Configuration de l'Interface graphique Web

Le niveau de configuration que vous appliquez à l'Interface graphique Web après l'installation dépend de votre mode d'authentification des utilisateurs et du niveau de sécurité que vous souhaitez appliquer. Il est également important de tenir compte de la façon dont vous souhaitez utiliser l'Interface graphique Web dans votre environnement de production. Par exemple, considérez de quelles sources de données vous souhaitez recevoir des événements, si vous souhaitez effectuer une intégration à d'autres produits IBM et si vous souhaitez utiliser le haut niveau de résilience dans votre environnement qui est fourni par la fonctionnalité d'équilibrage de charge.

Configuration de l'authentification des utilisateurs

Les utilisateurs peuvent s'authentifier auprès d'un ObjectServer, un référentiel externe, tel qu'un annuaire LDAP, ou le référentiel de fichiers par défaut. Un ObjectServer ou le référentiel de fichiers peut être sélectionné pendant l'installation. Si l'option que vous avez sélectionnée pendant l'installation est la source d'authentification que vous souhaitez utiliser, aucune configuration supplémentaire n'est nécessaire. Si vous souhaitez utiliser LDAP ou modifier la sélection que vous avez effectuée, les étapes sont décrites ici.

Avant de commencer

Familiarisez-vous avec le concept de référentiel fédéré VMM (Virtual Member Manager) ou de *domaine*. Voir Authentification d'utilisateur de l'Interface graphique Web.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les étapes que vous devez effectuer pour configurer un annuaire LDAP pour l'authentification d'utilisateur et les étapes si vous souhaitez modifier la source d'authentification.

Tableau 85. Options de configuration pour l'authentification d'utilisateur de l'Interface graphique Web

Source d'authentification en cours d'utilisation	**Source d'authentification que vous souhaitez utiliser**	**Etapes**
Référentiel de fichiers	ObjectServer	1. Supprimez les utilisateurs par défaut du référentiel de fichiers. 2. Ajoutez l'ObjectServer au domaine en configurant le plug-in VMM. 3. Facultatif : autorisez les utilisateurs de l'ObjectServer à s'authentifier sur un annuaire LDAP.

Tableau 85. Options de configuration pour l'authentification d'utilisateur de l'Interface graphique Web (suite)

Source d'authentification en cours d'utilisation	Source d'authentification que vous souhaitez utiliser	Etapes
Référentiel de fichiers	LDAP	1. Supprimez les utilisateurs par défaut du référentiel de fichiers. 2. Ajoutez l'annuaire LDAP au domaine. Une configuration supplémentaire est requise pour OpenLDAP. 3. Configurez le plug-in VMM pour écrire dans l'annuaire LDAP. 4. Affectez les rôles de l'Interface graphique Web aux utilisateurs et les groupes LDAP. 5. Facultatif : synchronisez les utilisateurs LDAP avec l'ObjectServer.
ObjectServer	LDAP	1. Supprimez l'ObjectServer du domaine. 2. Ajoutez l'annuaire LDAP au domaine. Une configuration supplémentaire est requise pour OpenLDAP. 3. Configurez le plug-in VMM pour écrire dans l'annuaire LDAP. 4. Affectez les rôles de l'Interface graphique Web aux utilisateurs et les groupes LDAP. 5. Facultatif : synchronisez les utilisateurs LDAP avec l'ObjectServer.
LDAP	ObjectServer	1. Supprimez l'annuaire LDAP du domaine. 2. Ajoutez l'ObjectServer au domaine en configurant le plug-in VMM. 3. Facultatif : autorisez les utilisateurs de l'ObjectServer à s'authentifier sur un annuaire LDAP.

Tâches associées:

«Identification et résolution des problèmes concernant les registres d'utilisateur», à la page 516
Si vous ne pouvez pas vous connecter par l'intermédiaire du registre d'utilisateurs spécifié, désactivez la fonction de connexion, puis modifiez les paramètres de configuration de du registre.

«Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe», à la page 343
Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

Configuration de l'authentification d'utilisateurs sur un annuaire LDAP

Vous pouvez configurer l'interface graphique Web pour authentifier les utilisateurs et les groupes auprès d'un annuaire LDAP. Les étapes de configuration impliquent l'ajout de l'annuaire LDAP au domaine du gestionnaire VMM (Virtual Member Manager) et la configuration de VMM pour inscrire de nouveaux utilisateurs dans l'annuaire LDAP. Vous devez ensuite attribuer des rôles de l'interface graphique Web aux utilisateurs LDAP et synchroniser ces utilisateurs avec le serveur ObjectServer. La synchronisation permet aux utilisateurs d'écrire sur le serveur ObjectServer afin qu'ils puissent utiliser les fonctions de l'interface graphique Web qui nécessitent des droits d'écriture sur le serveur ObjectServer.

Avant de commencer

- Familiarisez-vous avec le concept du domaine VMM. Voir Authentification d'utilisateur de l'Interface graphique Web
- Assurez-vous que l'annuaire LDAP est en cours d'exécution et qu'il est accessible à partir de l'ordinateur hôte de l'interface graphique Web.
- Si un serveur ObjectServer a déjà été ajouté au domaine en tant que référentiel d'utilisateurs, il doit être supprimé. Voir «Suppression de référentiels d'utilisateurs», à la page 517.
- Si le référentiel d'utilisateurs précédent était le référentiel de fichiers par défaut, supprimez les utilisateurs par défaut qui ont été créés lorsque le référentiel de fichiers a été ajouté. Vous devez supprimer ces utilisateurs pour éviter les noms en double dans les référentiels du domaine.
- Obtenez les informations suivantes à propos de l'annuaire LDAP : Vous aurez besoin de ces informations pour configurer l'annuaire LDAP dans le domaine.
  - Nom d'hôte et numéro de port du serveur principal qui héberge l'annuaire LDAP et le serveur de secours, le cas échéant. Les noms d'hôte ne doivent pas contenir d'espace.
  - Type et version de l'annuaire LDAP qui est utilisé, par exemple IBM Tivoli Directory Server V6.2 ou Microsoft Active Directory.
  - ID utilisateur et mot de passe utilisés pour la liaison au serveur LDAP. Cet ID utilisateur doit être unique. Par exemple, cn=root. Important : pour créer des utilisateurs et des groupes dans l'interface graphique Web, l'ID de liaison LDAP doit disposer des droits d'accès appropriés dans l'annuaire LDAP. L'ID de liaison ne doit pas contenir d'espace.
  - Sous-arborescence de l'annuaire LDAP que vous souhaitez utiliser pour l'authentification des utilisateurs.

Exemple de données LDAP

Les tâches de configuration suivantes utilisent les exemples de données à partir d'une sous-arborescence dans un annuaire LDAP. Lorsque vous exécutez les tâches de configuration, remplacez les exemples de données par vos données.

L'annuaire LDAP est identifié en tant que TIVIDS. TIVIDS contient la sous-arborescence ou=NetworkManagement,dc=myco=dc=com qui contient les utilisateurs et les groupes qui seront authentifiés par l'interface graphique Web. Dans cette sous-arborescence, les objets LDAP sont définis comme suit :

- Le préfixe utilisateur est uid
- Le suffixe utilisateur est cn=users
- Le préfixe de groupe est cn

- Le suffixe de groupe est cn=groups

Dans la sous-arborescence, l'utilisateur administrateur doté du nom d'utilisateur Administr8or est donc défini comme uid=Administr8or,cn=users,ou=NetworkManagement,dc=myco,dc=com. Le groupe d'utilisateurs de l'administrateur doté du nom AdminGroup est défini comme cn=AdminGroup,cn=groups,ou=NetworkManagement,dc=myco,dc=com.

Ajout de l'annuaire LDAP au domaine

Pour authentifier les utilisateurs à partir d'un annuaire LDAP, l'Interface graphique Web a besoin de lire les données utilisateur LDAP. Pour ce faire, ajoutez l'annuaire LDAP au domaine Virtual Member Manager (VMM) en tant que référentiel.

Avant de commencer

Vous aurez besoin des informations suivantes pour configurer l'annuaire LDAP dans le domaine:

- Nom d'hôte et numéro de port du serveur principal qui héberge l'annuaire LDAP et le serveur de sauvegarde, le cas échéant. Les noms d'hôte ne doivent pas contenir d'espace.
- Type et version de l'annuaire LDAP qui est utilisé, par exemple IBM Tivoli Directory Server V6.2 ou Microsoft Active Directory.
- ID utilisateur et mot de passe utilisés pour la liaison au serveur LDAP. Cet ID utilisateur doit être unique, par exemple cn=root. Important : pour créer des utilisateurs et des groupes dans l'Interface graphique Web, l'ID de liaison LDAP doit disposer des droits d'accès appropriés dans l'annuaire LDAP. L'ID de liaison ne doit pas contenir d'espace.
- Sous-arborescence de l'annuaire LDAP que vous souhaitez utiliser pour l'authentification des utilisateurs.

Pourquoi et quand exécuter cette tâche

Les étapes de configuration présentées dans cette tâche utilisent l'annuaire LDAP exemple décrit dans «Exemple de données LDAP», à la page 503. Remplacez les valeurs de cet exemple par les vôtres.

Procédure

1. Effectuez une copie de sauvegarde du fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/wim/config/wimconfig.xml.
2. Connectez-vous en tant qu'utilisateur tipadmin et lancez la console d'administration :
   a. Dans le menu de gauche, cliquez sur **Paramètres** > **Console d'administration WebSphere**.
   b. Cliquez sur **Lancer la console d'administration WebSphere**.
3. Cliquez sur **Sécurité** > **Sécurité globale**
4. Sous Référentiel de comptes utilisateur, sélectionnez Référentiels fédérés dans la liste **Définitions de domaines disponibles**, puis cliquez sur **Configurer**.
5. Cliquez sur **Add repositories (LDAP, custom, etc)...**, puis sur **New Repository** > **LDAP repository**.
6. Ajoutez l'annuaire LDAP en tant que référentiel dans le domaine en renseignant les zones suivantes :

Identificateur de référentiel
Entrez `TIVIDS`. L'identificateur de référentiel identifie de manière unique le référentiel dans le domaine.

Type de répertoire
Sélectionnez le type de serveur LDAP. Le type de serveur LDAP détermine les filtres par défaut utilisés par le serveur d'applications WebSphere. Les utilisateurs IBM Tivoli Directory Server peuvent sélectionner **IBM Tivoli Directory Server** ou **SecureWay**, mais **IBM Tivoli Directory Server** offre des performances. Pour les annuaires OpenLDAP, sélectionnez **Personnalisé**.

Nom d'hôte principal
Entrez le nom d'hôte qualifié complet du serveur LDAP principal. Vous pouvez entrer l'adresse IP ou le nom DNS (Domain Name System).

Port Entrez le port de l'annuaire LDAP. Le nom d'hôte et le numéro de port représentent le domaine du serveur LDAP dans la cellule de noeuds de version mixte. La valeur du port par défaut est 389 ; il ne s'agit pas d'un port de connexion SSL (Secure Sockets Layer). Utilisez le port 636 pour une connexion SSL (Secure Sockets Layer). Sur certains serveurs LDAP, vous pouvez spécifier un port différent.

Nom dinstinctif de liaison
Entrez l'ID de liaison du serveur LDAP. Si les liaisons anonymes sont impossibles sur le serveur LDAP, le nom distinctif de liaison est destiné aux opérations d'écriture ou à l'obtention des informations d'utilisateurs et de groupes. Indiquez toujours un nom distinctif de liaison et un mot de passe de liaison, sauf si une liaison anonyme peut satisfaire toutes les fonctions. Si le serveur LDAP est configuré pour utiliser des liaisons anonymes, vous pouvez laisser ces zones vides.

Mot de passe de liaison
Entrez le mot de passe de l'ID de liaison.

Une fois que vous avez rempli les zones, cliquez sur **Appliquer**, puis cliquez sur **Sauvegarder**. L'annuaire LDAP est ajouté aux référentiels dans le domaine.

7. Définissez le référentiel en complétant les zones suivantes :

Nom distinctif d'une entrée de base qui identifie de manière unique le groupe d'entrées du domaine.
Exemple : `o=TIVIDS`. Ce nom distinctif (DN) définit une entrée pour l'annuaire LDAP dans le domaine.

Nom distinctif d'une entrée de base dans ce référentiel
Exemple : `o=NetworkManagement,dc=myco,dc=com`. Ce nom distinctif est la racine de la sous-arborescence dans l'annuaire LDAP que vous souhaitez utiliser pour l'authentification.

Important : Si vous laissez cette zone vide, l'entrée de base est mappée sur la racine de l'annuaire LDAP. Toutes les opérations sont effectuées à la racine, ce qui entraîne des erreurs sur la plupart des serveurs LDAP.

Une fois que vous avez rempli les zones, cliquez sur **Appliquer**, puis cliquez sur **Sauvegarder**.

8. Redémarrez le serveur.

Résultats

Les utilisateurs de la sous-arborescence de l'annuaire LDAP sont répliqués dans le domaine. Une fois que vous redémarrez le serveur, les utilisateurs de l'annuaire LDAP sont visibles sur la page Gérer les utilisateurs de la console d'administration. Le nom distinctif de l'utilisateur se compose du préfixe et du suffixe utilisateur et du nom distinctif de l'annuaire LDAP dans le domaine, dans ce cas-ci, `o=TIVIDS`, qui représente la sous-arborescence `ou=NetworkManagementdc=myco,dc=com`. Par exemple, l'utilisateur administrateur possède le nom distinctif `uid=Administr8or,cn=users,o=TIVIDS`.

Que faire ensuite

- Si votre annuaire LDAP est OpenLDAP, exécutez la configuration supplémentaire pour OpenLDAP.
- Configurez VMM afin que les nouveaux utilisateurs et groupes créés dans la console d'administration soient écrits dans l'annuaire LDAP.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Ajout d'un référentiel OpenLDAP externe :

Instructions de configuration d'un serveur d'annuaire OpenLDAP en tant que référentiel.

Procédure

1. Suivez les instructions dans Ajout d'un référentiel LDAP externe. Dans la liste **Directory type (Type d'annuaire)**, sélectionnez`Custom (Personnaliser)`.
2. Accédez à *REP_INSTALL_JazzSM*`/config/cells/Cellule_Noeud01_JazzSM/wim/config` et effectuez une copie de sauvegarde du fichier `wimconfig.xml`.
3. Editez `wimconfig.xml`.
4. Recherchez l'élément commençant par :

   ```
   <config:repositories xsi:type="config:LdapRepositoryType"
   ```

   et se terminant par :

   ```
   </config:repositories>
   ```

5. Remplacez cet élément et ses éléments enfant par l'élément suivant :

   ```
   <config:repositories xsi:type="config:LdapRepositoryType"
           adapterClassName="com.ibm.ws.wim.adapter.ldap.LdapAdapter"
           id="identificateur_référentiel" isExtIdUnique="true"
   supportAsyncMode="false"
           supportExternalName="false" supportPaging="false"
   supportSorting="false"
           supportTransactions="false" certificateFilter=""
           certificateMapMode="exactdn" ldapServerType="CUSTOM"
   translateRDN="false">
         <config:baseEntries name="nom-distinctif_ldap"
             nameInRepository="nom-distinctif_ldap"/>
         <config:loginProperties>num_identification_utilisateur
   </config:loginProperties>
         <config:ldapServerConfiguration primaryServerQueryTimeInterval="15"
       returnToPrimaryServer="true" sslConfiguration="">
           <config:ldapServers authentication="simple"
   bindDN="nom-distinctif_liaison"
               bindPassword="bind-password" connectionPool="false"
   connectTimeout="0"
   ```

```
        derefAliases="always" referal="ignore" sslEnabled="false">
      <config:connections host="hôte_principal" port="numéro_port"/>
    </config:ldapServers>
  </config:ldapServerConfiguration>
  <config:ldapEntityTypes name="Group">
    <config:objectClasses>groupOfNames</config:objectClasses>
  </config:ldapEntityTypes>
  <config:ldapEntityTypes name="OrgContainer">
    <config:rdnAttributes name="o" objectClass="organization"/>
    <config:rdnAttributes name="ou" objectClass="organizationalUnit"/>
    <config:rdnAttributes name="dc" objectClass="domain"/>
    <config:rdnAttributes name="cn" objectClass="container"/>
    <config:objectClasses>organization</config:objectClasses>
    <config:objectClasses>organizationalUnit</config:objectClasses>
    <config:objectClasses>domain</config:objectClasses>
    <config:objectClasses>container</config:objectClasses>
  </config:ldapEntityTypes>
  <config:ldapEntityTypes name="PersonAccount">
    <config:objectClasses>inetOrgPerson</config:objectClasses>
  </config:ldapEntityTypes>
  <config:groupConfiguration>
    <config:memberAttributes dummyMember="uid=dummy" name="member"
objectClass="groupOfNames"
        scope="direct"/>
  </config:groupConfiguration>
  <config:cacheConfiguration>
    <config:attributesCache/>
    <config:searchResultsCache/>
  </config:cacheConfiguration>
</config:repositories>
```

Remplacez les éléments suivants dans les éléments :

identificateur_référentiel
: Par un identificateur unique pour le référentiel. L'identificateur ne peut pas contenir d'espace.

nom-distinctif_ldap
: Par le nom distinctif du serveur OpenLDAP.

nom-distinctif_liaison
: Par le nom distinctif de liaison.

mdp_liaison
: Par le mot de passe de la liaison.

hôte_principal
: Par le nom qualifié complet ou l'adresse TCP-IP de l'hôte OpenLDAP.

numéro_port
: Par le port du serveur d'annuaire OpenLDAP.

6. Sauvegardez `wimconfig.xml`.
7. Redémarrez le serveur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Configuration de VMM pour écrire dans l'annuaire LDAP

Une fois que vous avez ajouté l'annuaire LDAP au domaine, définissez cet annuaire comme le référentiel dans lequel les nouveaux utilisateurs et groupes sont écrits. Le composant Virtual Member Manager (VMM) peut lire dans plusieurs référentiels, mais il peut écrire dans un seul référentiel. Vous pouvez ensuite utiliser les fonctions de gestion utilisateur dans la console d'administration pour créer des utilisateurs et des groupes qui sont écrits dans l'annuaire LDAP.

Vous devez configurer le mappage entre les objets LDAP, tels que des utilisateurs et des groupes, et les types d'entité de VMM qui représentent ces objets. Les types d'entité sont utilisés pour mapper les objets dans différents annuaires LDAP sur un modèle d'objet commun dans VMM.

Avant de commencer

Contactez votre administrateur LDAP pour obtenir les entrées de base dans la sous-arborescence LDAP pour les utilisateurs et les groupes. Ces entrées de base sont les emplacements dans la sous-arborescence LDAP où les utilisateurs et les groupes sont créés lorsque les utilisateurs et les groupes sont créés via la page Gérer les utilisateurs ou la page Gérer les groupes dans la console d'administration.

Vérifiez que l'ID de liaison LDAP dispose des droits d'écriture dans l'annuaire LDAP.

Pourquoi et quand exécuter cette tâche

Les types d'entité pris en charge VMM sont Group, OrgContainer et PersonAccount. Une entité Group représente une collection simple d'entités pouvant n'avoir aucun contexte relationnel. Une entité OrgContainer représente une organisation, telle qu'une compagnie ou une entreprise, une filiale ou une unité organisationnelle telle qu'une division, un emplacement ou un département. Une entité PersonAccount représente un être humain. Vous ne pouvez pas ajouter ni supprimer de types d'entité pris en charge car ces types sont prédéfinis.

Les étapes de configuration présentées dans cette tâche utilisent l'annuaire LDAP exemple décrit dans «Exemple de données LDAP», à la page 503. Remplacez les valeurs de cet exemple par les vôtres.

Procédure

Pour mapper les types d'objet LDAP sur les types d'entité dans VMM :

1. Connectez-vous en tant qu'utilisateur tipadmin.
2. Ouvrez la console d'administration :
   a. Dans le menu de gauche, cliquez sur **Paramètres** > **Console d'administration WebSphere**.
   b. Cliquez sur **Lancer la console d'administration WebSphere**.
3. Cliquez sur **Sécurité** > **Sécurité globale**
4. Sous Référentiel de comptes utilisateur, sélectionnez `Référentiels fédérés` dans la liste **Définitions de domaines disponibles**, puis cliquez sur **Configurer**. Ensuite, cliquez sur **Prendre en charge les types d'entité**.
5. Cliquez sur chaque type d'entité et entrez l'entrée de base de l'annuaire LDAP dans l'**Entrée de base pour le parent par défaut** , comme suit, en remplaçant les exemples d'entrées de base par les entrées de votre annuaire LDAP.

Type d'entité	Exemple d'entrée de base
Groupe	`cn=groups,ou=NetworkManagement, dc=myco,dc=com`
OrgContainer	`ou=NetworkManagement,dc=myco,dc=com`
PersonAccount	`cn=users,ou=NetworkManagement, dc=myco,dc=com`

6. Sauvegardez la configuration pour chaque type d'entité.
7. Redémarrez le serveur.

Résultats

Les utilisateurs et les groupes qui sont créés dans le console d'administration sont désormais écrits dans l'annuaire LDAP. Il est maintenant recommandé de créer des utilisateurs et des groupes uniquement dans la console d'administration ou à l'aide de l'utilitaire de ligne de commande **tipcli**.

Que faire ensuite

Affectez des rôles de l'Interface graphique Web pour les utilisateurs LDAP afin qu'ils puissent accéder aux fonctions de l'Interface graphique Web et afin qu'ils puissent être synchronisés avec le serveur ObjectServer.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Affectation de rôles d'Interface graphique Web à des utilisateurs et des groupes LDAP

Affecter des rôles d'Interface graphique Web aux utilisateurs LDAP afin qu'ils aient le droit d'utiliser les fonctions Interface graphique Web .

Pourquoi et quand exécuter cette tâche

Si vous attribuez les rôles à des groupes, les autorisations qui sont associées aux rôles sont attribuées à tous les utilisateurs qui sont membres de ces groupes.

Les rôles Interface graphique Web n'accordent pas aux utilisateurs le droit d'écrire sur le serveur ObjectServer. Ce droit d'accès est requis pour certaines fonctions Interface graphique Web, par exemple, la liste d'événements actifs (AEL) et les outils d'Interface graphique Web. Vous pouvez configurer cette autorisation après que vous avez affecté les rôles Interface graphique Web.

Les droit d'accès en écriture sur le serveur ObjectServer peuvent être accordés uniquement aux utilisateurs de l'Interface graphique Web ayant le rôle ncw_admin ou ncw_user. Affectez ces rôles aux utilisateurs que vous souhaitez synchroniser sur le serveur ObjectServer.

Procédure

Pour affecter des rôles d'Interface graphique Web :

1. Pour attribuer des rôles aux groupes d'utilisateurs :
   a. Cliquez sur **Paramètres de la console** > **Rôles de groupes**.

b. Renseignez les combinaisons des zones de recherche pour faciliter la localisation des groupes.
c. Sélectionnez le nombre de groupes à afficher et cliquez sur **Rechercher.** Une liste de groupes s'affiche dans la grille.
d. Cliquez sur le nom du groupe auquel vous souhaitez affecter un rôle.
e. Dans la liste **Rôle(s)**, sélectionnez les rôles à affecter au groupe d'utilisateurs.
f. Cliquez sur **Enregistrer**.

2. Pour attribuer des rôles aux utilisateurs :
   a. Cliquez sur **Paramètres de la console** > **Rôles utilisateur**.
   b. Renseignez les combinaisons des zones de recherche pour faciliter la localisation des utilisateurs.
   c. Sélectionnez le nombre d'utilisateurs à afficher et cliquez sur **Rechercher.** Une liste d'utilisateurs correspondant s'affiche dans la grille.
   d. Cliquez sur l'ID de l'utilisateur auquel vous souhaitez affecter un rôle.
   e. Dans la liste **Rôle(s)**, sélectionnez les rôles à affecter à l'utilisateur.
   f. Cliquez sur **Enregistrer**.

Que faire ensuite

Créez les utilisateurs LDAP dans le serveur ObjectServer par l'activation de la fonction de synchronisation d'utilisateur.

Synchronisation des utilisateurs LDAP avec le serveur ObjectServer

Une fois que vous avez défini l'annuaire LDAP et affecté des rôles de l'Interface graphique Web aux utilisateurs LDAP, activez la fonction de synchronisation des utilisateurs. Cette fonction crée les utilisateurs LDAP dans le serveur ObjectServer, afin qu'ils puissent utiliser toutes les fonctions qui permettent d'écrire sur le serveur ObjectServer. Ces fonctions incluent la Liste d'événements actifs (AEL) et les outils de l'Interface graphique Web.

Avant de commencer

Vérifiez que l'annuaire LDAP est en cours d'exécution. Si un serveur ObjectServer a déjà été ajouté au domaine en tant que référentiel d'utilisateurs, il doit être supprimé. Voir «Suppression de référentiels d'utilisateurs», à la page 517.

Seuls les utilisateurs de l'Interface graphique Web ayant le rôle ncw_admin ou ncw_user peuvent être synchronisés. Vérifiez que vous avez attribué ces rôles aux utilisateur requis.

Procédure

Pour activer la synchronisation des utilisateurs :

1. Modifiez le fichier *REP_INSTALL_WEBGUI*/etc/server.init en définissant la propriété **users.credentials.sync** sur TRUE.
2. Pour modifier le nom du groupe d'utilisateurs vmmusers, attribuez la valeur requise à la propriété **users.credentials.sync.groupname**.
3. Indiquez la fréquence de synchronisation :
   a. Editez le fichier ncwDataSourceDefinitions.xml.

b. Définissez l'attribut maxAge de la propriété **config** sur la durée en seconde requise. Par exemple :

```
<config maxAge="durée"/>
```

La valeur par défaut est 3600 secondes.

4. Redémarrez le serveur.
5. Si votre environnement est à équilibrage de charge, pour activer la synchronisation des utilisateurs sur les autres noeuds du cluster, répétez les étapes 1, à la page 510 à 4. Sur chaque noeud supplémentaire où vous activez la synchronisation des utilisateurs, modifiez le nom du groupe d'utilisateurs, comme décrit à l'étape 2, à la page 510. Sur chaque noeud d'un environnement à équilibrage de charge, le nom du groupe d'utilisateurs qui contient les utilisateurs synchronisés doit être unique.

Résultats

Les utilisateurs et les groupes LDAP sont synchronisés avec les serveurs ObjectServer qui sont configurés dans le fichier `ncwDataSourceDefinitions.xml`. Dans un serveur ObjectServer, tous les utilisateurs synchronisés sont attribués au groupe vmmusers (ou, selon le nom spécifié par la propriété **users.credentials.sync.groupname**). Si ce groupe d'utilisateurs ne figure pas déjà sur un serveur ObjectServer, il est créé automatiquement. Toutes les 3600 secondes (ou selon l'intervalle de régénération indiqué par l'attribut maxAge), le groupe vmmusers est resynchronisé avec le serveur ObjectServer.

Que faire ensuite

Exécutez les tâches suivantes :

- Pour permettre aux utilisateurs synchronisés de se connecter au serveur ObjectServer et de modifier les données du serveur ObjectServer, par exemple à l'aide de l'interface interactive SQL ou en exécutant les outils Interface graphique Web, affectez les groupes d'utilisateurs ObjectServer suivants :
  - ISQL
  - ISQLWrite
- Pour sécuriser votre réseau à l'aide du chiffrement SSL (Secure Socket Layer), activez les communications SSL avec l'annuaire LDAP.
- Utilisez l'outil *REP_INSTALL_WEBGUI*/bin/**webtop_osresynch** pour déclencher manuellement une demande de synchronisation. Avant d'utiliser cet outil, configurez le client WAAPI. L'attribut **methodName** requis est osresync.refreshOSCache.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

«Configuration d'une connexion SSL sur un serveur LDAP», à la page 522
Si votre implémentation de Interface graphique Web utilise un référentiel d'utilisateurs LDAP externe, tel que Microsoft Active Directory, vous pouvez la configurer pour communiquer via un canal SSL sécurisé.

Référence associée:

Annexe C, «Propriétés server.init», à la page 687
Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*/etc/server.init. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité

directement et lu au démarrage du serveur.

Configuration de l'authentification d'utilisateurs sur un serveur ObjectServer

Si vous avez spécifié un serveur ObjectServer en tant que référentiel d'utilisateurs lors du processus d'installation, aucune configuration supplémentaire n'est requise. Toutefois, si vous souhaitez définir le serveur ObjectServer comme source d'authentification en dehors du processus d'installation, vous pouvez exécuter des scripts pour configurer le composant Virtual Member Manager (VMM). Si vous le souhaitez, vous pouvez ensuite permettre aux utilisateurs d'ObjectServer d'être authentifiés auprès d'un annuaire LDAP.

Définition d'un serveur ObjectServer en tant que référentiel d'utilisateurs

Pour ajouter un ObjectServer au domaine comme un référentiel d'utilisateurs, utilisez le script **confvmm4ncos** qui reconfigure le composant Virtual Member Manager (VMM).

Avant de commencer

- Obtenez les informations suivantes à propos du serveur ObjectServer :
  - Nom d'utilisateur
  - Password
  - Adresse IP
  - Numéro de port

  Si le référentiel d'utilisateurs précédent était le référentiel de fichiers par défaut, supprimez les utilisateurs par défaut qui ont été créés lorsque le référentiel de fichiers a été ajouté. Vous devez supprimer ces utilisateurs pour éviter les noms en double dans les référentiels du domaine.
- Si vous avez un deuxième ObjectServer, obtenez les mêmes informations sur cet ObjectServer.

Pourquoi et quand exécuter cette tâche

Le script fait les hypothèses suivantes sur les répertoires :

- Le répertoire d'installation WebSphere Application Server est le répertoire parent
- `JazzSM_Home` est le profil
- `Cellule_Noeud01_JazzSM` est la cellule

Procédure

1. Accédez au répertoire *REP_INSTALL_WAS*`/bin` et entrez la commande suivante :
   `confvmm4ncos` *rép_profils utilisateur mot_passe adresse port* [*adresse2 port2*]

   Où :
   - *rép_profils* est le répertoire des profils de Jazz for Service Management. Par exemple, `/opt/IBM/JazzSM/profile`.
   - *utilisateur* désigne l'ID utilisateur d'un utilisateur possédant des droits d'administration pour cet ObjectServer.
   - *mot_passe* représente le mot de passe correspondant à l'ID utilisateur.
   - *adresse* désigne l'adresse IP du serveur ObjectServer.
   - *port* désigne le numéro de port utilisé par l'ObjectServer.

- Si un serveur ObjectServer de reprise en ligne est utilisé, *adresse2* et *port2* désignent l'adresse IP et le numéro de port de ce serveur ObjectServer.

Conseil : Exécutez **confvmm4ncos** sans option de ligne de commande pour la commande help, y compris des exemples d'utilisation de la commande.

2. Redémarrez le serveur.
3. Répétez les étapes sur chaque hôte Interface graphique Web.

Résultats

Le composant VMM est configuré pour le serveur ObjectServer et le serveur ObjectServer est ajouté au domaine en tant que référentiel d'utilisateurs. Le répertoire *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/wim/config/wimconfig.xml contient maintenant un élément <config:repositories> pour l'ObjectServer.

Conseil : Recherchez le fichier wimconfig.xml pour <config:repositories adapterClassName="com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter" afin de localiser cet élément.

Que faire ensuite

- Ajoutez l'ObjectServer en tant que référentiel d'écriture dans lequel les nouveaux utilisateurs et groupes sont écrits.
- Si vous souhaitez que le serveur ObjectServer soit authentifié par rapport à un annuaire LDAP, configurez le serveur ObjectServer.

Tâches associées:

«Configuration d'une connexion SSL au serveur ObjectServer», à la page 523
Pour les environnements intégrant un registre d'utilisateurs Tivoli Netcool/OMNIbus ObjectServer, vous devez configurer des communications chiffrées sur le Jazz for Service Management.

«Modification du registre d'utilisateurs dans lequel les droits d'utilisateur sont écrits», à la page 518
Vous pouvez modifier le registre d'utilisateurs dans lequel les droits des nouveaux utilisateurs et groupes d'utilisateurs sont écrits. Effectuez cette tâche après avoir supprimé un registre d'utilisateurs du domaine, par exemple, si vous supprimez un ObjectServer pour le remplacer par un annuaire LDAP. Si vous n'effectuez pas cette tâche, les utilisateurs et les groupes sont écrits dans le référentiel de fichiers par défaut.

«Activation de l'authentification LDAP des utilisateurs du serveur ObjectServer», à la page 514
Vous pouvez activer les utilisateurs stockés dans un référentiel ObjectServer afin de les authentifier par rapport à un registre LDAP.

Activation de l'authentification LDAP des utilisateurs du serveur ObjectServer

Vous pouvez activer les utilisateurs stockés dans un référentiel ObjectServer afin de les authentifier par rapport à un registre LDAP.

Avant de commencer

- Définissez l'ObjectServer dans le référentiel fédéré en tant que référentiel d'utilisateurs.
- Effectuez une copie de sauvegarde du fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/wim/config/wimconfig.xml.

Procédure

1. Ouvrez le fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/wim/config/wimconfig.xml pour édition.
2. Recherchez l'élément <config:repositories> qui possède un attribut id portant la valeur netcoolObjectServerRepository. Par exemple :

```
<config:repositories
    adapterClassName="com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdaptor"
    id="netcoolObjectServer" supportPaging="False">
    <config:baseEntries name="o=netcoolObjectServerRepository" />
    <config:CustomProperties name="password"
        value="{AES}F3A75EB49DC87013C11C6B021BA6B33" />
    <config:CustomProperties name="username" value="root" />
    <config:CustomProperties name="host1" value="localhost" />
    <config:CustomProperties name="port1" value="4100" />
</config:repositories>
```

3. Ajoutez les éléments <config:CustomProperties> suivants à cet élément :

```
<config:CustomProperties name="LDAP.host" value="hôte_ldap" />
<config:CustomProperties name="LDAP.port" value="port_ldap" />
<config:CustomProperties name="LDAP.distinguishedName"
    value="format_nom-distinctif_utilisateur" />
<config:CustomProperties name="LDAP.sslEnabled" value="activation_ssl" />
```

   a. Remplacez *hôte_ldap* par le nom complet du serveur hôte LDAP.
   b. Remplacez *port_ldap* par le numéro de port que le serveur LDAP utilise. Si la connexion avec le serveur LDAP utilise SSL, indiquez le port SSL du serveur LDAP (par exemple, 636).
   c. Remplacez *format_nom-distinctif_utilisateur* par les attributs LDAP qui composent une entrée d'utilisateur dans le serveur LDAP. En fonction de l'implémentation LDAP, une entrée d'utilisateur comprend la chaîne `uid=%username,` ou la chaîne `gid=%username,` suivie par les attributs LDAP qui identifient l'utilisateur. Par exemple :

```
<config:CustomProperties name="LDAP.distinguishedName"
    value="uid=%username,cn=u50000g3000,cn=test,cn=ncw,o=ibm,c=uk" />

<config:CustomProperties name="LDAP.distinguishedName"
    value="gid=%username,cn=u50000g3000,cn=test,cn=ncw,o=ibm,c=uk" />
```

   Important : Veuillez à utiliser la syntaxe `%username`. Lorsqu'un utilisateur se connecte à l'Interface graphique Web, cette syntaxe est remplacée par le nom d'utilisateur réel se trouvant dans la demande d'authentification envoyée au serveur LDAP.
   Par exemple :

```
<config:repositories
    adapterClassName="com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdaptor"
    id="netcoolObjectServer" supportPaging="False">
    <config:baseEntries name="o=netcoolObjectServerRepository" />
    <config:CustomProperties name="password"
```

```
            value="{AES}F3A75EB49DC87013C11C6B021BA6B33" />
        <config:CustomProperties name="username" value="root" />
        <config:CustomProperties name="host1" value="localhost" />
        <config:CustomProperties name="port1" value="4100" />
        <config:CustomProperties name="LDAP.host" value="ldapserver.host.com" />
        <config:CustomProperties name="LDAP.port" value= "636" />
        <config:CustomProperties name="LDAP.distinguishedName"
            value="uid=%username,cn=u50000g3000,cn=test,cn=ncw,o=ibm,c=uk" />
        <config:CustomProperties name="LDAP.sslEnabled" value="true" />
    </config:repositories>
```

d. Remplacez *activation_ssl* par `true` si la connexion au serveur LDAP utilise SSL ; sinon, utilisez `false`.

4. Vérifiez soigneusement la syntaxe de tous les éléments que vous avez édités.

   Important : Si la syntaxe du fichier `wimconfig.xml` est incorrecte, vous ne pourrez peut-être pas vous connecter à l'Interface graphique Web ni arrêter le serveur à l'aide de la commande **stopServer**. Dans ce cas, vous devez arrêter manuellement le processus Concentrateur des services d'application du tableau de bord.

5. Redémarrez le serveur.

Résultats

Les utilisateurs peuvent se connecter à l'aide de leur ID utilisateur ObjectServer et de leur mot de passe LDAP. Ils ne peuvent plus utiliser leurs mots de passe ObjectServer.

Que faire ensuite

Si la connexion au serveur LDAP utilise SSL, configurez cette connexion.

Tâches associées:

«Définition d'un serveur ObjectServer en tant que référentiel d'utilisateurs», à la page 512
Pour ajouter un ObjectServer au domaine comme un référentiel d'utilisateurs, utilisez le script **confvmm4ncos** qui reconfigure le composant Virtual Member Manager (VMM).

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

«Modification du registre d'utilisateurs dans lequel les droits d'utilisateur sont écrits», à la page 518
Vous pouvez modifier le registre d'utilisateurs dans lequel les droits des nouveaux utilisateurs et groupes d'utilisateurs sont écrits. Effectuez cette tâche après avoir supprimé un registre d'utilisateurs du domaine, par exemple, si vous supprimez un ObjectServer pour le remplacer par un annuaire LDAP. Si vous n'effectuez pas cette tâche, les utilisateurs et les groupes sont écrits dans le référentiel de fichiers par défaut.

«Configuration d'une connexion SSL sur un serveur LDAP», à la page 522
Si votre implémentation de Interface graphique Web utilise un référentiel d'utilisateurs LDAP externe, tel que Microsoft Active Directory, vous pouvez la configurer pour communiquer via un canal SSL sécurisé.

Identification et résolution des problèmes concernant les registres d'utilisateur

Si vous ne pouvez pas vous connecter par l'intermédiaire du registre d'utilisateurs spécifié, désactivez la fonction de connexion, puis modifiez les paramètres de configuration de du registre.

Procédure

1. Sauvegardez le fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/security.xml.
2. Editez le fichier existant security.xml et non la copie de sauvegarde, en définissant le premier attribut enabled sur false. Par exemple :

```
<security:Security xmi:version="2.0" xmlns:xmi="http://www.omg.org/XMI"
xmlns:orb.securityprotocol=
"http://www.ibm.com/websphere/appserver/schemas/5.0/
orb.securityprotocol.xmi"
xmlns:security="http://www.ibm.com/websphere/appserver/schemas/5.0/
security.xmi"
xmi:id="Security_1" useLocalSecurityServer="true"
useDomainQualifiedUserNames="false"
enabled="false" cacheTimeout="600" issuePermissionWarning="true"
activeProtocol="BOTH"
enforceJava2Security="false" enforceFineGrainedJCASecurity="false"
appEnabled="true"
dynamicallyUpdateSSLConfig="true" activeAuthMechanism="LTPA_1"
activeUserRegistry="WIMUserRegistry_1"
defaultSSLSettings="SSLConfig_TIPNode_1">
```

3. Redémarrez le serveur.

Que faire ensuite

Vérifiez et, si nécessaire, modifiez les paramètres pour votre registre d'utilisateurs. Le cas échéant, modifiez le registre d'utilisateurs.

Tâches associées:

«Configuration de l'authentification des utilisateurs», à la page 501
Les utilisateurs peuvent s'authentifier auprès d'un ObjectServer, un référentiel externe, tel qu'un annuaire LDAP, ou le référentiel de fichiers par défaut. Un ObjectServer ou le référentiel de fichiers peut être sélectionné pendant l'installation. Si l'option que vous avez sélectionnée pendant l'installation est la source d'authentification que vous souhaitez utiliser, aucune configuration supplémentaire n'est nécessaire. Si vous souhaitez utiliser LDAP ou modifier la sélection que vous avez effectuée, les étapes sont décrites ici.

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Suppression de référentiels d'utilisateurs

Supprimez du domaine tous les référentiels d'utilisateurs dont vous n'avez plus besoin. Par exemple, si vous souhaitez ajouter un annuaire LDAP au domaine, supprimez d'abord tous les serveurs ObjectServer du domaine. Si vous ne supprimez pas les serveurs ObjectServer, les utilisateurs ne peuvent pas se connecter une fois que vous avez ajouté l'annuaire LDAP.

Procédure

1. Lancez la console d'administration et cliquez sur **Sécurité** > **Sécurité globale**.
2. Dans la liste des **Available realms definition** (Définitions des domaines disponibles), sélectionnez **Federated repositories** (Référentiels fédérés) et cliquez sur **Configurer**.
3. Dans la fenêtre Federated (Fédéré), sélectionnez l'entrée requise dans **Repositories in the realm:** (Référentiels du domaine :) et cliquez sur **Supprimer**.
4. Cliquez sur **OK** puis sur **Save directly to the master configuration** (Sauvegarder directement dans la configuration maître) en haut de la page.
5. Cliquez sur **Manage Repositories** (Gérer les référentiels) en dessous de **Related items** (Eléments associés).
6. Dans la table, sélectionnez la ligne représentant le référentiel que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer). Par exemple, un serveur ObjectServer sera défini en tant que **NetcoolObjectServer**.
7. Cliquez sur **OK** puis sur **Save directly to the master configuration** (Sauvegarder directement dans la configuration maître) en haut de la page.
8. Redémarrez le serveur.

Que faire ensuite

Si vous remplacez un serveur ObjectServer par un annuaire LDAP :

- Dans le fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/wim/wimconfig.xml, vérifiez que le serveur ObjectServer a été supprimé, par exemple en recherchant le fragment com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter. Si le serveur a été supprimé, ce fragment n'apparaîtra plus dans le fichier.
- Ajoutez l'annuaire LDAP au domaine.
- Définissez l'annuaire LDAP ou tout autre registre d'utilisateurs en tant que référentiel en écriture dans lequel les nouveaux utilisateurs ou groupes seront enregistrés. Lorsque vous supprimez un référentiel, les nouveaux utilisateurs et groupes sont sauvegardés dans le référentiel de fichiers par défaut.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

«Ajout de l'annuaire LDAP au domaine», à la page 504
Pour authentifier les utilisateurs à partir d'un annuaire LDAP, l'Interface graphique Web a besoin de lire les données utilisateur LDAP. Pour ce faire, ajoutez l'annuaire LDAP au domaine Virtual Member Manager (VMM) en tant que référentiel.

«Modification du registre d'utilisateurs dans lequel les droits d'utilisateur sont écrits»
Vous pouvez modifier le registre d'utilisateurs dans lequel les droits des nouveaux utilisateurs et groupes d'utilisateurs sont écrits. Effectuez cette tâche après avoir supprimé un registre d'utilisateurs du domaine, par exemple, si vous supprimez un ObjectServer pour le remplacer par un annuaire LDAP. Si vous n'effectuez pas cette tâche, les utilisateurs et les groupes sont écrits dans le référentiel de fichiers par défaut.

Modification du registre d'utilisateurs dans lequel les droits d'utilisateur sont écrits

Vous pouvez modifier le registre d'utilisateurs dans lequel les droits des nouveaux utilisateurs et groupes d'utilisateurs sont écrits. Effectuez cette tâche après avoir supprimé un registre d'utilisateurs du domaine, par exemple, si vous supprimez un ObjectServer pour le remplacer par un annuaire LDAP. Si vous n'effectuez pas cette tâche, les utilisateurs et les groupes sont écrits dans le référentiel de fichiers par défaut.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez sélectionner qu'un seul registre d'utilisateurs dans lequel les utilisateurs et les groupes sont écrits lors de leur création.

Procédure

Pour accéder à un autre registre d'écriture :

1. Cliquez sur **Paramètres** > **Console d'administration WebSphere**. Cliquez ensuite sur **Lancer la console d'administration WebSphere**.
2. Cliquez sur **Sécurité** > **Sécurité globale**.
3. Dans la liste des **Définitions de domaine disponibles**, sélectionnez **Référentiels fédérés** et cliquez sur **Configurer**.
4. Sous **Propriétés supplémentaires**, cliquez sur **Types d'entité pris en charge**.
5. Dans la table, cliquez sur le type d'entité **Groupe** et remplacez les propriétés des zones **Entrée de base du parent par défaut** et **Propriétés du nom distinctif relatif**.
6. Cliquez sur **OK** puis sur **Save directly to the master configuration (Sauvegarder directement dans la configuration maître)** au début de la page.
7. Répétez les étapes 5 et 6 pour les types d'entité **OrgContainer** et **PersonAccount** et tous les autres types d'entité qui sont définis.

Que faire ensuite

Si vous avez remplacé un ObjectServer par un serveur LDAP, activez la synchronisation des droits d'utilisateur entre le serveur LDAP et l'ObjectServer.

Tâches associées:

«Définition d'un serveur ObjectServer en tant que référentiel d'utilisateurs», à la page 512
Pour ajouter un ObjectServer au domaine comme un référentiel d'utilisateurs, utilisez le script **confvmm4ncos** qui reconfigure le composant Virtual Member Manager (VMM).

«Synchronisation des utilisateurs LDAP avec le serveur ObjectServer», à la page 510
Une fois que vous avez défini l'annuaire LDAP et affecté des rôles de l'Interface graphique Web aux utilisateurs LDAP, activez la fonction de synchronisation des utilisateurs. Cette fonction crée les utilisateurs LDAP dans le serveur ObjectServer, afin qu'ils puissent utiliser toutes les fonctions qui permettent d'écrire sur le serveur ObjectServer. Ces fonctions incluent la Liste d'événements actifs (AEL) et les outils de l'Interface graphique Web.

Sécurisation de l'environnement de l'Interface graphique Web

Déterminez le niveau de sécurité dont vous avez besoin et effectuez les tâches de configuration qui sont nécessaires pour ce niveau de sécurité. Certaines tâches de configuration sont obligatoires alors que d'autres sont obligatoires uniquement pour des niveaux spécifiques de protection.

Les tâches obligatoires sont les suivantes :

- Chiffrez le mot de passe de l'utilisateur de l'ObjectServer se trouvant dans le fichier de définitions de la source de données.
- Chiffrez le mot de passe du fichier de clés certifiées de Concentrateur des services d'application du tableau de bord se trouvant dans le fichier d'initialisation de l'Interface graphique Web.

La méthode de chiffrement de ces mots de passe varie en fonction du niveau de sécurité. Utilisez une méthode pour les communications SSL et non SSL et une autre méthode pour FIPS 140-2 et les niveaux de chiffrement plus élevés.

Les tâches facultatives sont les suivantes :

- Autoriser l'accès à Concentrateur des services d'application du tableau de bord à partir de connexions HTTP, outre les connexions HTTPS par défaut.
- Sécuriser les communications avec le serveur de l'Interface graphique Web à l'aide de la communication SSL (Secure Socket Layer). Les connexions SSL peuvent être configurées pour le registre d'utilisateurs et pour les ObjectServers qui sont définis en tant que sources de données pour le fil d'événement. Si vous le souhaitez, vous pouvez remplacer le certificat SSL par défaut utilisé pour l'authentification de client auprès du serveur de l'Interface graphique Web.
- Augmentez le niveau de sécurité à partir de SSL à l'une des normes suivantes :
  - FIPS 140-2 : requiert que le protocole SSL soit Transport Layer Security (TLS) 1.0 ou une version supérieure. FIPS 140-2 autorise uniquement les tailles de clé et les algorithmes de signature conformes à la norme de sécurité FIPS 140-2.
  - NIST SP800-131a : requiert un chiffrement plus fort que FIPS 140-2 et est destiné à remplacer FIPS 140-2. SP800-131a requiert que le protocole SSL soit TLS 1.2 ou une version supérieure et autorise uniquement les tailles de clé et les algorithmes de signature conformes à la norme SP800-131a. Pour migrer à partir de FIPS 140-2, vous pouvez exécuter l'Interface graphique Web en mode transition SP800-131a, ce qui permet de continuer à utiliser TLS 1.0. Toutefois, la conformité à SP800-131a requiert de migrer vers TLS 1.2 par un passage au mode strict SP800-131a.
- Configurez Concentrateur des services d'application du tableau de bord pour utiliser Tivoli Access Manager WebSEAL Version 6.1 afin de gérer l'authentification. Tivoli Access Manager est inclus dans Jazz for Service

Management. Pour plus d'informations, voir le centre de documentation Jazz for Service Management à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

Configuration de l'accès HTTP et HTTPS

Par défaut, serveur d'applications nécessite l'accès HTTPS (Hypertext Transfer Protocol Secure). Si vous voulez que certains utilisateurs puissent se connecter à la console et l'utiliser sans chiffrement ni transfert de données - ce qui inclut l'ID utilisateur et le mot de passe -, configurez l'environnement de façon à assurer la prise en charge conjointe des deux modes HTTP et HTTPS.

Avant de commencer

Après installation de Interface graphique Web et avant d'entreprendre la présente procédure, connectez-vous à la portail afin de vous assurer de la connectivité et des bonnes conditions de démarrage.

Pourquoi et quand exécuter cette tâche

La configuration des accès HTTP et HTTPS à la console implique l'édition du fichier de composants Web `web.xml`. Pour identifier et éditer les fichiers web.xml appropriés, procédez comme suit :

Procédure

1. Accédez au répertoire : `/opt/IBM/JazzSM/profile/config/cells/applications`.
2. A partir de cet emplacement, recherchez les fichiers `web.xml` dans les répertoires suivants :
   - Pour l'archive des applications Web Integrated Solutions Console : `isc.ear/deployments/isc/isclite.war/WEB-INF`
   - Pour l'archive des applications Web Tivoli Integrated Portal Change Password : `isc.ear/deployments/isc/TIPChangePasswd.war/WEB-INF`
3. Ouvrez l'un des fichiers `web.xml` à l'aide d'un éditeur de texte.
4. Recherchez l'élément `<transport-guarantee>`. La valeur initiale de tous les éléments `<transport-guarantee>` est `CONFIDENTIAL`, ce qui signifie qu'un accès sécurisé est toujours nécessaire.
5. Passez le paramétrage à `NONE` afin d'autoriser à la fois les demandes HTTP et HTTPS. L'élément doit maintenant se présenter comme suit : `<transport-guarantee>NONE</transport-guarantee>`.
6. Sauvegardez le fichier, et répétez ces étapes pour les autres fichiers de déploiement `web.xml`.
7. Connectez-vous à Interface graphique Web.
8. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** puis sur **Lancer la console d'administration Websphere**.
9. Dans la console d'administration WebSphere Application Server, sélectionnez **Sécurité** > **Sécurité globale** et cliquez sur le lien **External authorization providers (Fournisseurs d'autorisations externes)**.
10. Dans la page External authorization providers (Fournisseurs d'autorisations externes), sélectionnez l'option **Update with application names listed (Mettre à jour avec les noms d'application listés)**.
11. Dans le panneau du texte, saisissez `isc` et cliquez sur **Appliquer**.

12. Dans la zone de messages située en haut de la page, cliquez sur le lien **Sauvegarder** pour valider les modifications dans la configuration principale.
13. Redémarrez Jazz for Service Management :
    a. Dans le répertoire `/opt/IBM/JazzSM/profile/bin` en fonction de votre système d'exploitation, entrez une des commandes suivantes :
       - Windows `stopServer.bat server1`
       - UNIX Linux `stopServer.sh server1`

       Remarque : Sur les systèmes UNIX et Linux, vous êtes invité à fournir un nom d'utilisateur et un mot de passe administrateur.
    b. Dans le répertoire `/opt/IBM/JazzSM/profile/bin` en fonction de votre système d'exploitation, entrez une des commandes suivantes :
       - Windows `startServer.bat server1`
       - UNIX Linux `startServer.sh server1`

Exemple

L'exemple suivant présente une section du fichier `web.xml` pour `TIPChangePasswd` où le paramètre transport-guarantee est défini sur `NONE`:

```
<security-constraint>
 <display-name>
 ChangePasswdControllerServletConstraint</display-name>
 <web-resource-collection>
  <web-resource-name>ChangePasswdControllerServlet</web-resource-name>
  <url-pattern>/*</url-pattern>
 </web-resource-collection>
 <auth-constraint>
     <description>Roles</description>
  <role-name>administrator</role-name>
           <role-name>operator</role-name>
           <role-name>configurator</role-name>
           <role-name>monitor</role-name>
           <role-name>iscadmins</role-name>
 </auth-constraint>
 <user-data-constraint>
  <transport-guarantee>NONE</transport-guarantee>
 </user-data-constraint>
</security-constraint>
```

Que faire ensuite

Les utilisateurs doivent maintenant spécifier un port différent, en fonction du mode d'accès. Les numéros de port par défaut sont les suivants :

http://<*nom_hôte*>**:16310/ibm/console**
Utilisez le port HTTP pour vous connecter à Jazz for Service Management sur le port HTTP.

https://<*nom_hôte*>**:16311/ibm/console**
Utilisez le port sécurisé HTTPS pour vous connecter à Jazz for Service Management.

Remarque : Si vous souhaitez utiliser une connexion unique (SSO), vous devez utiliser le nom de domaine qualifié complet de l'hôte Jazz for Service Management.

Configuration d'une connexion SSL sur un serveur LDAP

Si votre implémentation de Interface graphique Web utilise un référentiel d'utilisateurs LDAP externe, tel que Microsoft Active Directory, vous pouvez la configurer pour communiquer via un canal SSL sécurisé.

Avant de commencer

Cette tâche suppose qu'une connexion vers un serveur LDAP a déjà été configurée.

Votre serveur LDAP (par exemple, un serveur IBM Tivoli Directory Server Version 6 ou Microsoft Active Directory) doit être configuré pour accepter les connexions SSL et être exécuté sur un numéro de port sécurisé (636). Consultez la documentation de votre serveur LDAP si vous devez créer un certificat de signataire qui, dans le cadre de cette tâche, doit être importé depuis votre serveur LDAP dans le fichier de clés certifiées de Jazz for Service Management.

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour configurer Jazz for Service Management afin qu'il communique via un canal sécurisé (SSL) avec un référentiel LDAP externe. Toutes les instances de serveur d'applications doivent être configurées pour le serveur LDAP.

Procédure

1. Connectez-vous à la portail.
2. Procédez comme suit pour importer le certificat de signataire de votre serveur LDAP dans le fichier de clés certifiées du serveur d'applications.
   a. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
   b. Dans le panneau de navigation de la console d'administration WebSphere Application Server, cliquez sur **Sécurité** > **Gestion de clés et du certificat SSL**.
   c. Dans la zone Articles liés, cliquez sur le lien **Magasins de clés et certificats** et dans le tableau, cliquez sur le lien **NodeDefaultTrustStore**.
   d. Dans la zone Propriétés supplémentaires, cliquez sur le lien **Certificats de signataires** puis sur le bouton **Extraire d'un port**.
   e. Dans les zones concernées, indiquez le nom d'hôte, le port (généralement 636 pour les connexions SSL), les détails de configuration SSL et l'alias du certificat pour votre serveur LDAP et cliquez sur le bouton **Récupérer les informations du signataire** puis sur **OK**.
3. Procédez comme suit pour activer les communications SSL sur votre serveur LDAP :
   a. Dans le panneau de navigation, cliquez sur **Sécurité** > **Administration, applications et infrastructure sécurisées**.
   b. Sélectionnez **Référentiels fédérés** dans la liste **Définitions de domaines disponibles** puis cliquez sur **Configurer**.
   c. Sélectionnez votre serveur LDAP dans la liste déroulante **Référentiel**.
   d. Cochez la case **Communications SSL obligatoires** et sélectionnez l'option **Gestion centralisée**.
   e. Cliquez sur **OK**.

4. Pour que les modifications soient prises en compte, enregistrez celles-ci puis arrêtez et redémarrez toutes les instances de Jazz for Service Management.

Que faire ensuite

Si vous souhaitez activer la fonction d'authentification unique de sorte que les utilisateurs n'aient à se connecter qu'une seule fois et puissent ensuite passer sur d'autres applications sans devoir s'authentifier à nouveau, configurez cette fonction.

Tâches associées:

«Synchronisation des utilisateurs LDAP avec le serveur ObjectServer», à la page 510

Une fois que vous avez défini l'annuaire LDAP et affecté des rôles de l'Interface graphique Web aux utilisateurs LDAP, activez la fonction de synchronisation des utilisateurs. Cette fonction crée les utilisateurs LDAP dans le serveur ObjectServer, afin qu'ils puissent utiliser toutes les fonctions qui permettent d'écrire sur le serveur ObjectServer. Ces fonctions incluent la Liste d'événements actifs (AEL) et les outils de l'Interface graphique Web.

Configuration d'une connexion SSL au serveur ObjectServer

Pour les environnements intégrant un registre d'utilisateurs Tivoli Netcool/OMNIbus ObjectServer, vous devez configurer des communications chiffrées sur le Jazz for Service Management.

Avant de commencer

Vérifiez que SSL est configuré pour les composants serveur de Tivoli Netcool/OMNIbus. Vous pouvez vérifier le port SSL sur lequel les composants serveur, tels que le serveur ObjectServer, sont en cours d'exécution, dans le fichier de données de connexions `$NCHOME/etc/omni.dat`. Assurez-vous de définir le serveur ObjectServer en tant que référentiel d'utilisateurs dans le domaine du gestionnaire de membre virtuel (VMM) en exécutant le script **`confvmm4ncos`** sur le port SSL.

Procédure

Pour établir un canal sécurisé pour les communications entre Jazz for Service Management et le serveur ObjectServer.

1. Ouvrez `/opt/IBM/JazzSM/profile/etc/com.sybase.jdbc3.SybDriver.props` dans un éditeur de texte et modifiez les paramètres suivants :
   a. Activation de la couche SSL pour l'hôte ObjectServer principal : `USESSLPRIMARY=TRUE`
   b. Activation de la couche SSL pour l'hôte ObjectServer de sauvegarde : `USESSLBACKUP=TRUE`
2. Définissez les informations du certificat ObjectServer comme suit :
   a. Dans le panneau de navigation de Jazz for Service Management, cliquez sur **Paramètres** > **Console d'administration WebSphere**, et cliquez sur **Lancer la console d'administration WebSphere**.
   b. Cliquez sur **Sécurité** > **Certificat SSL et gestion des clés**.
   c. Sur la page Certificat SSL et gestion des clés, cliquez sur **Magasins de clés et certificats** et, sur la page affichée, cliquez sur **NodeDefaultTrustStore**.
   d. Sur la page NodeDefaultTrustStore page, cliquez sur **Certificats de signataires** et, sur la page qui s'affiche, cliquez sur**Extraire d'un port**.

e. Dans les zones correspondantes, entrez les valeurs d'**Hôte**, de **Port** et d'**Alias** pour le serveur ObjectServer et cliquez sur **Récupérer les informations du signataire**.

Les informations de signataires sont extraites et stockées. A des fins de référence, les détails suivants sont affichés lorsque les informations de signataire sont extraites :

Numéro de série
Indique le numéro de série du certificat, généré par l'émetteur de ce dernier.

Emis à
Indique le nom distinctif de l'entité à laquelle le certificat a été émis.

Emis par
Indique le nom distinctif de l'entité qui a émis le certificat. Il s'agit du même nom que le nom distinctif émis à si le certificat est auto-signé.

(Empreinte digitale (SHA digest)
Indique l'algorithme de hachage sécurisé (hachage SHA) du certificat, pouvant être utilisé pour vérifier le hachage du certificat sur un autre site, comme le côté client de la connexion.

Période de validité
Indique la date d'expiration du certificat de signataire extrait à des fins de validation.

3. Redémarrez le serveur Jazz for Service Management :
   a. Dans le répertoire `/opt/IBM/JazzSM/profile/bin` en fonction de votre système d'exploitation, entrez une des commandes suivantes :
      - Windows `stopServer.bat server1`
      - UNIX Linux `stopServer.sh server1`

      Remarque : Sur les systèmes UNIX et Linux, vous êtes invité à fournir un nom d'utilisateur et un mot de passe administrateur.
   b. Dans le répertoire `/opt/IBM/JazzSM/profile/bin` en fonction de votre système d'exploitation, entrez une des commandes suivantes :
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`

Résultats

Si vous pouvez ouvrir une session sur le serveur, cela signifie qu'il existe un canal sécurisé entre le serveur Jazz for Service Management et le serveur ObjectServer.

Concepts associés:

«Instructions de configuration de SSL rapide», à la page 372
Si vous êtes déjà habitué à utiliser la communication SSL dans Tivoli Netcool/OMNIbus, utilisez ces informations comme des instructions rapides relatives aux tâches que vous devez exécuter.

Tâches associées:

«Définition d'un serveur ObjectServer en tant que référentiel d'utilisateurs», à la page 512
Pour ajouter un ObjectServer au domaine comme un référentiel d'utilisateurs, utilisez le script **confvmm4ncos** qui reconfigure le composant Virtual Member

Manager (VMM).

«Configuration d'un réseau protégé SSL», à la page 380
Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **nco_igen** pour générer le fichier d'interfaces.

Référence associée:

«Obtention de correctifs», à la page 682
Un correctif du produit peut être disponible pour résoudre les problèmes que vous rencontrez.

Configuration des connexions SSL pour le flux d'événements à partir du serveur ObjectServer

Utilisez une connexion Secure Socket Layer (SSL) pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers l'Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez SSL dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

Conseil : Comme solution de rechange, vous pouvez utiliser l'utilitaire graphique iKeyman qui est fourni avec IBM pour configurer les certificats Interface graphique Web.

Avant de commencer

- Configurez SSL sur les composants serveur de l'Tivoli Netcool/OMNIbus.
- Créez un certificat public ou faites-le migrer si vous avez mis à niveau à partir d'une version antérieure.
- Vérifiez les ports sur lesquels les composants serveur sont en cours d'exécution.

  Conseil : Recherchez les numéros de port dans le fichier `$NCHOME/etc/omni.dat` ou `%NCHOME%\ini\sql.ini`.
- Concentrateur des services d'application du tableau de bord peut déjà contenir le certificat de signataire de l'autorité de certification qui a signé le certificat public Tivoli Netcool/OMNIbus. Si tel est le cas, vous pouvez ignorer l'étape 1.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser un fichier de clés certifiées JKS ou PKCS12. Dans Concentrateur des services d'application du tableau de bord, la valeur par défaut est PKCS12. Le fichier de clés certifiées par défaut est *REP_INSTALL_JazzSM*`/profile/config/cells/Cellule_Noeud01_JazzSM/nodes/Noeud01_JazzSM/trust.p12`. Le mot de passe du fichier de clés certifiées par défaut est WebAS.. Les étapes suivantes décrivent ces valeurs par défaut. Remplacez les valeurs par défaut par vos propres valeurs.

Procédure

1. Ajoutez le certificat public Tivoli Netcool/OMNIbus au fichier de clés certifiées de Concentrateur des services d'application du tableau de bord :

a. Lancez la console d'administration et cliquez sur **Sécurité** > **Certificat SSL et gestion de clés** > **Fichiers de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataire**. Cliquez ensuite sur **Ajouter**.
b. Dans la zone **Nom d'alias**, entrez un alias pour le certificat.
c. Dans la zone **Nom de fichier**, entrez le chemin du certificat.
d. Dans la liste **Type de données**, sélectionnez **Données ASCII codées en Base64** et cliquez sur **OK**.

2. Modifiez le fichier *REP_INSTALL_WEBGUI*/etc/server.init comme suit :
   a. Définissez la propriété **webtop.password.encryption** sur None ou AES.
   b. Définissez la propriété **webtop.fips** sur Off.
   c. Pour utiliser l'emplacement du fichier de clés certifiées par défaut Concentrateur des services d'application du tableau de bord, laissez la propriété **webtop.ssl.trustStore** vide.
   d. Pour utiliser le mot de passe du fichier de clés certifiées par défaut, conservez la propriété **webtop.ssl.trustStorePassword** telle quelle.

      A faire : Si vous modifiez le mot de passe dans Concentrateur des services d'application du tableau de bord, modifiez également le fichier server.init pour répercuter ce changement.
   e. Laissez le type de gestionnaire d'accréditations de l'Interface graphique Web par défaut, à savoir IbmX509, et le type de fichier de clés certifiées par défaut, à savoir PKCS12.
3. Définissez le port du serveur ObjectServer pour la connexion SSL dans le fichier de définition de source de données :
   a. Ouvrez le fichier *WEBGUI_HOME*/etc/datasources/ncwDataSourceDefinitions.xml en édition.
   b. Définissez la propriété **ncwPrimaryServer** comme indiqué dans l'exemple suivant :

      ```
      <ncwPrimaryServer>
      <ncwOSConnection host="hôte_ObjectServer" port="port_ObjectServer"
       ssl="true"/></ncwPrimaryServer>
      ```
4. Redémarrez le serveur.

Concepts associés:

«Instructions de configuration de SSL rapide», à la page 372
Si vous êtes déjà habitué à utiliser la communication SSL dans Tivoli Netcool/OMNIbus, utilisez ces informations comme des instructions rapides relatives aux tâches que vous devez exécuter.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

«Configuration d'un réseau protégé SSL», à la page 380
Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données omni.dat, puis exécutez l'utilitaire **nco_igen** pour générer le fichier d'interfaces.

Référence associée:

Annexe C, «Propriétés server.init», à la page 687
Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*/etc/server.init. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité directement et lu au démarrage du serveur.

Remplacement du certificat SSL par défaut pour les connexions aux clients d'interface graphique Web

Concentrateur des services d'application du tableau de bord contient un certificat à utiliser pour l'authentification des connexions SSL aux clients d'Interface graphique Web. Vous pouvez remplacer ce certificat par l'un des vôtres, par un certificat créé par une autorité de certification ou par un certificat autosigné.

Remplacement du certificat SSL par défaut par un certificat signé par une autorité de certification

Utilisez cette procédure pour remplacer le certificat par défaut par un certificat signé par une autorité de certification (CA).

Procédure

La procédure comprend les étapes suivantes :

1. Création d'une demande pour le certificat.
2. Obtention du certificat de l'autorité de certification.
3. Réception du certificat.
4. Ajout du certificat au fichier.
5. Activation du certificat.

Création d'une demande de certificat :

La première étape du remplacement du certificat SSL par défaut consiste à créer une demande de certificat provenant de l'autorité de certification (CA) afin qu'il puisse être envoyé à l'autorité de certification.

Procédure

1. Lancez la console d'administration et cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Gestion de clés et du certificat SSL)**.
2. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Fichiers de clés et certificats)**, puis cliquez sur **NodeDefaultKeyStore**.
3. Sur la page "NodeDefaultKeyStore", cliquez sur **Demandes de certificat personnel**, puis, sur la page qui apparaît, cliquez sur **Nouveau**.
4. Dans la zone **Fichier de demande de certificat**, entrez le chemin d'accès au fichier contenant la demande de certificat. Utilisez le formulaire suivant : *REP_INSTALL_JazzSM*/profile/config/cells/Cellule_Noeud01_JazzSM/nodes/*nom_fichier_demande*.p12. Remplacez *nom_fichier_demande* par un nom approprié pour la demande. Par exemple : demande-cert-ac.
5. Renseignez les zones du panneau "Informations de certificat" comme suit :

   Intitulé de clé
   Entrez un nom d'alias pour la demande de certificat dans le fichier de clés. Veillez à ce que ce nom soit unique parmi les autres entrées du fichier de clés.

   Nom usuel
   Entrez le nom de l'entité représentée par le certificat. Par exemple, le

nom de domaine complet où se trouve l'Interface graphique Web, comme `UI_WEb.serveur.mon_entreprise.com`.

Organization (Organisation)
Entrez le nom de votre organisation pour identifier la partie du nom distinctif (DN), comme `Mon Entreprise`, correspondant à l'organisation.

Unité organisationnelle
Entrez le nom de l'unité au sein de l'organisation pour identifier la partie du nom distinctif qui correspond à l'unité organisationnelle, par exemple `Opérations`.

Locality (Localité)
Entrez l'emplacement de l'unité organisationnelle pour identifier la partie d'emplacement du DN, comme `Région parisienne`.

Département ou province
Entrez le département ou la province de la localité pour identifier la partie du nom distinctif qui correspond au département ou à la province, par exemple : `Paris`.

Code postal
Entrez le code postal de la localité pour identifier la partie du nom distinctif qui correspond au code postal, par exemple : `75000`.

Pays Sélectionnez le code de votre pays dans la liste pour identifier la partie du nom distinctif qui correspond au pays, par exemple`France`.

6. Cliquez sur **Appliquer**.
7. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Retour**.
8. Cochez la case de l'entrée contenant le nouvel intitulé de clé, puis cliquez sur **Extraire**.
9. Sur la page "Extraire la demande de certificat", entrez le chemin du fichier où est conservé la demande de certificat que vous pouvez envoyer à l'autorité de certification. Utilisez le formulaire suivant : *REP_INSTALL_JazzSM*`/profile/config/cells/Cellule_Noeud01_JazzSM/nodes/`*nom_fichier_demande_ac*`.p12`. Remplacez *nom_fichier_demande_ac* par un nom approprié pour la demande. Par exemple : `demandecert-envoyer-ac`.
10. Cliquez sur **OK**.

Résultats

Le fichier qui contient la demande à envoyer à l'AC est créé.

Obtention du certificat de l'autorité de certification :

Faites votre demande de certificat auprès de l'autorité de certification de votre choix, généralement via leur site Web. Lorsqu'il vous est demandé de fournir la demande, utilisez le contenu entier du fichier de demande de certificat. Il s'agit du fichier *REP_INSTALL_JazzSM*`/profile/config/cells/Cellule_Noeud01_JazzSM/nodes/`*nom_fichier_demande_ac*`.p12`. Remplacez *nom_fichier_demande_ac* par le nom du fichier contenant la demande de certificat.

Lorsque vous recevez le certificat de l'autorité de certification, copiez-le dans un fichier nommé de manière appropriée, avec comme extension de nom de fichier `.p12`, dans *REP_INSTALL_JazzSM*`/profile/config/cells/Cellule_Noeud01_JazzSM/nodes`.

Réception du certificat :

Recevez le certificat que vous avez obtenu de l'autorité de certification :

Procédure

1. Lancez la console d'administration et cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Gestion de clés et du certificat SSL)**.
2. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Configuration des paramètres de sécurité de gestion des noeuds finaux**.
3. Sur la page "Configuration des paramètres de sécurité de gestion des noeuds finaux", développez le noeud **Entrant**, si nécessaire, puis cliquez sur **TIPNode(NodeDefaultSSLSettings)** sous ce noeud.
4. Sur la page "TIPNode", cliquez sur **Fichiers de clés et certificats**. Sur la page qui apparaît, cliquez sur **NodeDefaultKeyStore** dans la table au milieu de la page.
5. Sur la page "NodeDefaultKeyStore", cliquez sur **Certificats personnels**. Sur la page qui apparaît, cliquez sur **Recevoir un certificat d'une autorité de certification**.
6. Au format affiché, entrez le chemin d'accès au fichier contenant le certificat de l'autorité de certification, puis cliquez sur **Appliquer**. Par exemple, `/opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/cert-from-ca.p12`.
7. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Retour**.
8. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Résultats

Le nouveau certificat apparaît dans la liste des certificats sur la page "Certificats personnels".

En cas de problème lié au nouveau certificat SSL, vous ne pourrez pas vous connecter au serveur Concentrateur des services d'application du tableau de bord.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Ajout du certificat de signataire au fichier :

Ajoutez le certificat de signataire au fichier de clés afin qu'il soit reconnu comme un certificat valide.

Procédure

1. Sur la page "Gestion des certificats personnels", cliquez sur **TIPNode** dans la série de liens figurant en haut de page.
2. Sur la page "TipNode", cliquez sur **Fichiers de clés et certificats**. Sur la page qui apparaît, cliquez sur **NodeDefaultTrustStore** dans la table au milieu de la page.
3. Cliquez sur **Certificats de signataire**. Sur la page qui apparaît, cliquez sur **Suivant**.
4. Renseignez les zones du panneau "Configuration" comme suit :

Alias Entrez un nom d'alias pour le certificat en veillant à ce qu'il soit unique parmi les certificats de signataire du fichier de clé.

Nom de fichier
Entrez le chemin d'accès au fichier où vous avez conservé le certificat reçu de l'autorité de certification. Par exemple *:REP_INSTALL_JazzSM/*`profile/config/cells/Cellule_Noeud01_JazzSM/nodes/`*nom_fichier_demande_ac*`.p12`

5. Cliquez sur **Appliquer**.
6. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Enregistrer**.

Résultats

Le certificat apparaît dans la liste des certificats sur la page "Certificats de signataire".

Activation du certificat SSL :

Activer le certificat avant de pouvoir l'utiliser pour l'authentification.

Procédure

Pour activer le certificat :

1. Sur la page "Certificats de signataire", cliquez sur **Configuration des paramètres de sécurité de gestion des noeuds finaux** dans la série de liens figurant en haut de la page.
2. Sur la page "Configuration des paramètres de sécurité de gestion des noeuds finaux", développez le noeud **Entrant**, si nécessaire, puis cliquez sur **TIPNode(NodeDefaultSSLSettings)** sous ce noeud.
3. Sur la page "TIPNode", choisissez le nom d'alias du certificat dans la liste déroulante de la section **Alias des certificats dans le fichier de clés**, puis cliquez sur **Appliquer**.
4. Sur la page "TIPNode", cliquez sur **Enregistrer**.

Certificat autosigné

Utilisez cette procédure pour remplacer le certificat par défaut par un certificat autosigné.

Procédure

La procédure comprend les étapes suivantes :

1. Génération du certificat.
2. Affectation du certificat.

Génération du certificat :

Générez le certificat autosigné afin qu'il puisse être ajouté au fichier de clés.

Avant de commencer

Vérifiez que vous disposez de toutes les données dont vous avez besoin pour le certificat. Si vous générez et attribuez le certificat et qu'il existe un problème lié à ce certificat, vous ne pouvez pas vous connecter.

Procédure

1. Dans le panneau de navigation de Concentrateur des services d'application du tableau de bord, cliquez sur **Paramètres** > **WebSphere Administrative Console**, puis cliquez sur **Lancer la console d'administration WebSphere**.
2. Cliquez sur **Sécurité** > **Certificat SSL et gestion des clés**.
3. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Configuration des paramètres de sécurité de gestion des noeuds finaux**.
4. Sur la page "Configuration des paramètres de sécurité de gestion des noeuds finaux", développez le noeud **Entrant**, si nécessaire, puis cliquez sur **TIPNode(NodeDefaultSSLSettings)** sous ce noeud.
5. Sur la page "TIPNode", cliquez sur **Fichiers de clés et certificats**, puis sur la page qui apparaît, cliquez sur **NodeDefaultKeyStore** dans la table au milieu de la page.
6. Sur la page "NodeDefaultKeyStore", cliquez sur **Certificats personnels**, puis sur la page qui apparaît, cliquez sur **Créer** > **Certificat autosigné**.
7. Renseignez les zones du panneau "Propriétés générales" comme suit :

   Alias Entrez un nom d'alias pour la demande de certificat dans le fichier de clés. Veillez à ce que ce nom soit unique parmi les autres entrées du fichier de clés.

   Nom usuel
   Entrez le nom de l'entité représentée par le certificat, comme le nom de domaine qualifié complet où se trouve l'Interface graphique Web. Par exemple : `interfaceg.serveur.masociete.com`.

   Organization (Organisation)
   Entrez le nom de votre organisation pour identifier la partie du nom distinctif correspondant à l'organisation. Par exemple : `Ma société`.

   Unité organisationnelle
   Entrez le nom de l'unité au sein de l'organisation pour identifier la partie du nom distinctif qui correspond à l'unité organisationnelle. Par exemple : `Opérations`.

   Locality (Localité)
   Entrez l'emplacement de l'unité organisationnelle pour identifier la partie du nom distinctif qui correspond à la localité. Par exemple : `Armonk`.

   State/Province (Etat/Province)
   Entrez l'Etat ou la province de la localité pour identifier la partie du nom distinctif qui correspond à l'Etat. Par exemple : `NY`.

   Code postal
   Entrez le code postal de la localité pour identifier la partie du nom distinctif qui correspond au code postal. Par exemple : `75000`.

Pays Sélectionnez le code de votre pays dans la liste déroulante pour identifier la partie du nom distinctif qui correspond au pays. Par exemple : FR.

8. Cliquez sur **Appliquer**.
9. Sur la page "Gestion des clés et des certificats SSL", cliquez sur **Retour**.
10. Redémarrez le serveur TIP.

Résultats

Le nouveau certificat apparaît dans la liste des certificats sur la page "Gestion des certificats personnels".

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Affectation du certificat :

Une fois que vous avez généré le certificat autosigné, vous pouvez l'ajouter au fichier de clés.

Procédure

1. Sur la page "Certificats personnels", cliquez sur le lien **TIPNode** dans la série de liens figurant en haut de la page.
2. Choisissez un nom d'alias pour le certificat dans la liste déroulante de la section **Alias des certificats dans le fichier de clés**, puis cliquez sur **Appliquer**.
3. Sur la page "TIPNode", cliquez sur **Enregistrer**.
4. Cliquez sur le lien **Gestion des considérations de sécurité des noeuds finaux** dans la série de liens figurant en haut de la page.

   Le nom d'alias du certificat apparaît entre parenthèses (<>) après l'entrée pour **TIPNodeNodeDefaultSSLSettings** sous **Inbound**.

Chiffrement des mots de passe de l'Interface graphique Web

Pour chiffrer les mots de passe de l'Interface graphique Web pour des connexions SSL et non SSL, utilisez l'outil **ncw_aes_crypt**.

Avant de commencer

Le chiffrement AES peut être utilisé uniquement si le mode FIPS 140–2 n'est pas activé.

Pourquoi et quand exécuter cette tâche

Vous devez chiffrer les mots de passe ObjectServer stockés dans le fichier ncwDataSourceDefinitions.xml, ainsi que le mot de passe du fichier de clés certifiées Concentrateur des services d'application du tableau de bord stocké dans le fichier server.init.Le mot de passe du fichier de clés certifiées par défaut est WebAS. Après avoir édité le fichier server.init, redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Pour chiffrer les mots de passe de l'Interface graphique Web, procédez comme suit :

Procédure

1. Activez le chiffrement AES dans le serveur ObjectServer utilisé comme source de données :
   a. Editez le fichier de propriétés du serveur ObjectServer et définissez la valeur de la propriété **PasswordEncryption** sur AES.

      Le chemin d'accès au fichier de propriétés du serveur ObjectServer est le suivant :

      - UNIX Linux `$NCHOME/omnibus/etc/nom_serveur.props`
      - Windows `%NCHOME%\omnibus\etc\nom_serveur.props`

      Remplacez *nom_serveur* par le nom du serveur ObjectServer.
   b. Réinitialisez tous les mots de passe des comptes utilisateurs du serveur ObjectServer.
   c. Redémarrez le serveur ObjectServer.
2. Chiffrez le mot de passe ObjectServer :
   a. Exécutez *REP_INSTALL_WEBGUI*/bin/ncw_aes_crypt.
   b. Entrez le mot de passe ObjectServer.
      Le mot de passe ObjectServer chiffré est généré.
   c. Copiez le mot de passe chiffré.
3. Ajoutez le mot de passe ObjectServer chiffré au fichier de configuration de source de données :
   a. Ouvrez le fichier ncwDataSourceDefinitions.xml.
   b. Modifiez la propriété **ncwDataSourceCredentials** comme indiqué dans l'exemple suivant :
      ```
      <ncwDataSourceCredentials
      userName="root" password="encryptedObjectServerpassword"
      encrypted="true"
      algorithm="AES"/>
      ```
      Remplacez *mdp_chiffré_ObjectServer* par le mot de passe chiffré que vous avez copié dans l'étape 1
4. Chiffrez le mot de passe de fichier de clés certifiées de Concentrateur des services d'application du tableau de bord :
   a. Exécutez *REP_INSTALL_WEBGUI*/bin/ncw_aes_crypt.
   b. Entrez le mot de passe par défaut du fichier de clés certifiées de Concentrateur des services d'application du tableau de bord, WebAS.
      Un mot de passe chiffré est généré.
   c. Copiez le mot de passe chiffré.
5. Ajoutez le mot de passe de fichier de clés certifiées chiffré au fichier d'initialisation :
   a. Ouvrez le fichier *REP_INSTALL_WEBGUI*/etc/server.init.
   b. Définissez la propriété **webtop.password.encryption** sur aes.
   c. Définissez la propriété **webtop.ssl.trustStorePassword** sur le mot de passe chiffré à l'étape 4b.
   d. Pour vérifier que le fichier de clés certifiées par défaut de Concentrateur des services d'application du tableau de bord est utilisé, laissez le paramètre **webtop.ssl.trustStore** vierge.
   e. Définissez **webtop.fips** sur off.
6. Redémarrez le serveur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Référence associée:

Annexe C, «Propriétés server.init», à la page 687
Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*`/etc/server.init`. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité directement et lu au démarrage du serveur.

Activation du mode FIPS 140-2 pour l'Interface graphique Web

Pour activer l'Interface graphique Web en mode FIPS 140–2, vous devez effectuer plusieurs étapes de configuration manuelle.

Activation de FIPS sur serveur d'applications

Vous pouvez configurer le serveur d'applications pour qu'il utilise un fournisseur cryptographique approuvé par FIPS (Federal Information Processing Standard).

Pourquoi et quand exécuter cette tâche

Les algorithmes de chiffrement de mot de passe de Interface graphique Web sur serveur d'applications utilisent les fournisseurs cryptographiques approuvés FIPS indépendamment du fait que FIPS est activé pour l'ensemble de serveur d'applications. Cependant, l'activation de FIPS sur le serveur d'applications garantit que le chiffrement utilisé pour prendre en charge les communications SSL, ainsi que l'authentification unique, utilise un fournisseur cryptographique agréé FIPS.

Pour activer la norme FIPS 140–2 pour le serveur d'applications, procédez comme suit :

Procédure

1. Configurez le serveur d'applications pour l'utilisation de la norme FIPS.
   a. Connectez vous à Interface graphique Web.
   b. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** puis sur **Lancer la console d'administration Websphere**.
   c. Dans le panneau de navigation de la console d'administration WebSphere Application Server, cliquez sur **Sécurité** > **Gestion de clés et du certificat SSL**.
   d. Sélectionnez l'option **Utiliser les algorithmes de la norme FIPS (Federal Information Processing Standard)** puis cliquez sur **Appliquer**. Avec cette option, IBMJSSE2 et IBMJCEFIPS sont les fournisseurs actifs.
   e. Dans la zone Messages située en haut de la page, cliquez sur le lien **Save** et déconnectez-vous de la console WebSphere Application Server.
2. Configurez le serveur d'applications de façon à utiliser les algorithmes FIPS pour les clients Java devant accéder aux beans enterprise :
   a. Ouvrez le fichier `/opt/IBM/JazzSM/profiles/properties/ssl.client.props` dans un éditeur de texte.
   b. Pour la propriété `com.ibm.security.useFIPS`, remplacez la valeur `false` par la valeur `true`.
3. Configurez le serveur d'applications de façon à utiliser les algorithmes FIPS pour les clients d'administration basés SOAP devant accéder aux beans enterprise :

a. Ouvrez le fichier `/opt/IBM/JazzSM/profiles/properties/soap.client.props` dans un éditeur de texte.
b. Ajoutez la ligne suivante : `com.ibm.ssl.contextProvider=IBMJSSEFIPS`.

4. Configurez le fichier `java.security` afin d'activer IBMJCEFIPS :
   a. Ouvrez le fichier `./WebSphere/AppServer/java/jre/lib/security/java.security` dans un éditeur de texte.
   b. Insérez le fournisseur IBMJCEFIPS (`com.ibm.crypto.fips.provider.IBMJCEFIPS`) devant le fournisseur IBMJCE et attribuez de nouveaux numéros aux autres fournisseurs dans la liste de fournisseurs. Le fournisseur IBMJCEFIPS doit apparaître dans la liste de fournisseurs du fichier `java.security`. Reportez-vous à l'exemple en fin de rubrique.
5. Configurez votre navigateur pour qu'il utilise protocole TLS (Transport Layer Security) (TLS) 1.0 :
   a. Microsoft Internet Explorer : démarrez le navigateur et cliquez sur **Outils > Options Internet**. Dans l'onglet **Avancés**, sélectionnez l'option **TLS 1.0**.
   b. Firefox : démarrez Firefox et cliquez sur **Outils > Options**. Dans la barre d'outils, cliquez sur l'icône **Avancé** et sélectionnez l'onglet **Chiffrement**. Dans le cadre Protocoles, sélectionnez l'option **Utiliser TLS 1.0**.
6. Exportez les clés authentification LTPA (Lightweight Third Party Authentication) afin que les applications utilisant ces clés puissent être reconfigurées.
   a. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
   b. Dans la console d'administration WebSphere Application Server, sélectionnez **Security** > **Global security**.
   c. Dans la zone Authentification de la page Sécurité globale, cliquez sur le lien **LTPA**.
   d. Sous **Ouverture d'une session intercellulaire**, indiquez un fichier de clés ainsi qu'un nom et un mot de passe pour le fichier qui contiendra les clés LTPA exportées.
   e. Cliquez sur **Exporter les clés**. Par défaut, le fichier exporté est sauvegardé dans `/opt/IBM/JazzSM/profiles`.
7. Reconfigurez toute application utilisant les clés LTPAserveur d'applications : pour reconfigurer le service d'authentification unique Tivoli avec les clés LTPA mises à jour, exécutez ce script : `/opt/IBM/JazzSM/profiles/bin/setAuthnSvcLTPAKeys.jacl`.
   a. Modifiez le répertoire en `/opt/IBM/JazzSM/profiles/bin/`
   b. Si le serveur d'applications n'est pas en cours d'exécution, démarrez-le en exécutant la commande suivante :
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`
   c. Exécutez la commande suivante :

      `wsadmin -username` *`smadmin`* `-password` *`motdepasse_smadmin`* `-f setAuthnSvcLTPAKeys.jacl` *`chemin_clé_exportée motdepasse_clé`*

      Où :

      `chemin_clé_exportée` est le nom et le chemin complet du fichier de clés qui a été exporté.

      `motdepasse_clé` est le mot de passe utilisé pour exporter la clé.

8. Pour l'authentification unique, activez la norme FIPS pour toutes les autres instances de serveur d'applications, puis importez les clés LTPA mises à jour depuis le premier serveur vers chacun des autres serveurs :
   a. Copiez le fichier de clés LTPA configuré à l'étape 6, à la page 535 vers un autre ordinateur de serveur d'applications.
   b. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
   c. Dans la console d'administration WebSphere Application Server, sélectionnez **Security** > **Global security**.
   d. Dans la zone Authentification de la page Sécurité globale, cliquez sur le lien **LTPA**.
   e. Sous **Ouverture d'une session intercellulaire**, indiquez le nom et le mot de passe précédemment définis pour le fichier contenant les clés LTPA exportées .
   f. Cliquez sur **Import keys (Importer les clés)**.
9. Accédez au répertoire contenant l'utilitaire `JazzSM_HOME/ui/bin` et exécutez la commande **`ConfigureCLI`** :

   Linux UNIX `./consolecli.sh ConfigureCLI --useFIPS true`

   Windows `consolecli.bat ConfigureCLI --useFIPS true`

Exemple

Une fois IBMJCEFIPS activé, le fichier IBM SDK `/opt/IBM/JazzSM/java/jre/lib/security/java.security` se présente comme suit.

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

Configuration du client d'Interface graphique Web pour le mode FIPS

Pour utiliser le client d'Interface graphique Web en mode FIPS 140-2, assurez-vous que le client est correctement configuré.

Pourquoi et quand exécuter cette tâche

Pour configurer le client d'Interface graphique Web pour le mode FIPS 140-2 :

Procédure

- Assurez-vous que le protocole TLS (Transport Layer Security) est activé sur les navigateurs.
- Si le navigateur côté client utilise IBM JRE 1.5, ajoutez le paramètre d'exécution Java **`–Dhttps.protocols=TLSv1`** pour imposer l'utilisation du protocole TLS. Pour ce faire :
  1. Cliquez sur **Java Control Panel** > **Java** > **Vue**

2. Dans la fenêtre Java Runtime Parameter (Paramètre d'exécution Java), cliquez deux fois sur la zone IBM JRE 1.5 sous **Java Runtime Parameter** (Paramètre d'exécution Java) et entrez :

   ```
   –Dhttps.protocols=TLSv1
   ```

Chiffrement des mots de passe à l'aide du mode FIPS 140–2

Pour chiffrer les mots de passe de l'Interface graphique Web pour les connexions SSL et non SSL en mode FIPS 140–2 , utilisez l'outil de chiffrement FIPS 140–2 **ncw_fips_crypt** .

Avant de commencer

Pour utiliser l'outil de chiffrement FIPS 140–2, IBM JRE doit être installé.

Pourquoi et quand exécuter cette tâche

La clé de coffre par défaut de l'Interface graphique Web se trouve dans *REP_INSTALL_WEBGUI*/etc/encrypt/vault.key. Cette clé est utilisée pour chiffrer le mot de passe ObjectServer stocké dans le fichier ncwDataSourceDefinitions.xml, et le mot de passe de fichier de clés certifiées de Concentrateur des services d'application du tableau de bord stocké dans le fichier server.init. Le mot de passe du fichier de clés certifiées par défaut est WebAS. Après avoir édité le fichier server.init, redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Procédure

1. Pour chiffrer le mot de passe ObjectServer, entrez la commande suivante : *REP_INSTALL_WEBGUI*/bin/ncw_fips_crypt -password *netcool* -key *REP_INSTALL_WEBGUI*/etc/encrypt/vault.key
   Si vous utilisez la clé du coffre par défaut, omettez le paramètre **key**.
   Un mot de passe chiffré est généré.
2. Copiez le mot de passe chiffré.
3. Ajoutez le mot de passe ObjectServer chiffré :
   a. Ouvrez le fichier ncwDataSourceDefinitions.xml.
   b. Modifiez l'élément <ncwDataSourceCredentials>, comme indiqué dans l'exemple suivant :

      ```
      <ncwDataSourceCredentials
      userName="root" password="mdp_chiffré_ObjectServer" encrypted="true"
      algorithm="FIPS"/>
      ```

4. Pour chiffrer le mode de passe de fichier de clés certifiées de Concentrateur des services d'application du tableau de bord, entrez la commande suivante : *REP_INSTALL_WEBGUI*/bin/ncw_fips_crypt -password WebAS -key *REP_INSTALL_WEBGUI*/etc/encrypt/vault.key
   Si vous utilisez la clé du coffre par défaut, omettez le paramètre **key**.
   Un mot de passe chiffré est généré.
5. Copiez le mot de passe chiffré.
6. Ajoutez le mot de passe de fichier de clés certifiées Concentrateur des services d'application du tableau de bord chiffré au fichier d'initialisation :
   a. Ouvrez le fichier *REP_INSTALL_WEBGUI*/etc/server.init.
   b. Définissez la propriété **webtop.password.encryption** sur fips.
   c. Définissez la propriété **webtop.ssl.trustStorePassword** sur la valeur chiffrée définie à l'étape 4.

d. Pour vous assurer que le fichier de clés certifiées par défaut de Concentrateur des services d'application du tableau de bord est utilisé, laissez la propriété **webtop.ssl.trustStore** vide.
e. Définissez la propriété **webtop.fips** sur on.

7. Redémarrez le serveur.

Référence associée:

Annexe C, «Propriétés server.init», à la page 687
Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*/etc/server.init. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité directement et lu au démarrage du serveur.

Configuration des connexions SSL en mode FIPS 140–2 pour le flux d'événements à partir du serveur ObjectServer

Pour plus de sécurité, utilisez une connexion Secure Socket Layer (SSL) avec le chiffrement FIPS 140-2 pour sécuriser l'alimentation de données d'événements de l'ObjectServer vers Interface graphique Web. Ajoutez le certificat public Tivoli Netcool/OMNIbus qui comprend la clé publique àConcentrateur des services d'application du tableau de bord et activez le chiffrement FIPS 140-2 dans le fichier d'initialisation du serveur. Puis, définissez le port utilisé pour la connexion SSL dans le fichier de définitions de source de données.

Conseil : Comme solution de rechange, vous pouvez utiliser l'utilitaire graphique iKeyman qui est fourni avec IBM pour configurer les certificats Interface graphique Web.

Avant de commencer

- Configurez SSL sur les composants serveur de l'Tivoli Netcool/OMNIbus.
- Créez un certificat public ou faites-le migrer si vous avez mis à niveau à partir d'une version antérieure.
- Vérifiez les ports sur lesquels les composants serveur sont en cours d'exécution.

  Conseil : Recherchez les numéros de port dans le fichier $NCHOME/etc/omni.dat ou %NCHOME%\ini\sql.ini.
- Concentrateur des services d'application du tableau de bord peut déjà contenir le certificat de signataire de l'autorité de certification qui a signé le certificat public Tivoli Netcool/OMNIbus. Si tel est le cas, vous pouvez ignorer l'étape 1.
- Activez le chiffrement FIPS 140-2 sur le serveur Concentrateur des services d'application du tableau de bord.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser un fichier de clés certifiées JKS ou PKCS12. Dans Concentrateur des services d'application du tableau de bord, la valeur par défaut est PKCS12. Le fichier de clés certifiées par défaut est *REP_INSTALL_JazzSM*/profile/config/cells/Cellule_Noeud01_JazzSM/nodes/Noeud01_JazzSM/trust.p12. Le mot de passe du fichier de clés certifiées par défaut est WebAS.. Les étapes suivantes décrivent ces valeurs par défaut. Remplacez les valeurs par défaut par vos propres valeurs.

Procédure

1. Ajoutez le certificat public Tivoli Netcool/OMNIbus au fichier de clés certifiées de Concentrateur des services d'application du tableau de bord :

a. Lancez la console d'administration et cliquez sur **Sécurité** > **Certificat SSL et gestion de clés** > **Fichiers de clés et certificats** > **NodeDefaultTrustStore** > **Certificats de signataire**. Cliquez ensuite sur **Ajouter**.
b. Dans la zone **Nom d'alias**, entrez un alias pour le certificat.
c. Dans la zone **Nom de fichier**, entrez le chemin du certificat.
d. Dans la liste **Type de données**, sélectionnez **Données ASCII codées en Base64** et cliquez sur **OK**.

2. Modifiez le fichier *REP_INSTALL_WEBGUI*/etc/server.init comme suit :
   a. Définissez la propriété **webtop.fips** sur On.
   b. Définissez **webtop.password.encryption** pour chiffrer ou non les mots de passe :
      - Pour un chiffrement FIPS 140-2, définissez la propriété sur FIPS.
      - Pour aucun chiffrement, définissez la propriété sur NONE.
   c. Pour utiliser l'emplacement du fichier de clés certifiées par défaut Concentrateur des services d'application du tableau de bord, laissez la propriété **webtop.ssl.trustStore** vide.
   d. Pour utiliser le mot de passe du fichier de clés certifiées par défaut, conservez la propriété **webtop.ssl.trustStorePassword** telle quelle.

      A faire : Si vous modifiez le mot de passe dans Concentrateur des services d'application du tableau de bord, modifiez également le fichier server.init pour répercuter ce changement.
   e. Laissez le type de gestionnaire d'accréditations de l'Interface graphique Web par défaut, à savoir IbmX509, et le type de fichier de clés certifiées par défaut, à savoir PKCS12.
3. Définissez le port du serveur ObjectServer pour la connexion SSL dans le fichier de définition de source de données :
   a. Ouvrez le fichier *WEBGUI_HOME*/etc/datasources/ncwDataSourceDefinitions.xml en édition.
   b. Définissez la propriété **ncwPrimaryServer** comme indiqué dans l'exemple suivant :

      ```
      <ncwPrimaryServer>
      <ncwOSConnection host="hôte_ObjectServer" port="port_ObjectServer"
       ssl="true"/></ncwPrimaryServer>
      ```
4. Redémarrez le serveur.

Que faire ensuite

Si vous avez spécifié la norme FIPS 1400-2 de chiffrement des mots de passe, chiffrez les mots de passe.

Concepts associés:

«Instructions de configuration de SSL rapide», à la page 372
Si vous êtes déjà habitué à utiliser la communication SSL dans Tivoli Netcool/OMNIbus, utilisez ces informations comme des instructions rapides relatives aux tâches que vous devez exécuter.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

«Configuration d'un réseau protégé SSL», à la page 380
Pour configurer des connexions SSL entre vos clients et serveurs, vous avez besoin d'un certificat de signataire certifié et d'un certificat serveur signé par le signataire certifié. Utilisez l'utilitaire de ligne de commande **nc_gskcmd** ou l'outil graphique IBM Key Management (iKeyman) pour gérer ces clés et ces certificats numériques.

«UNIX : génération du fichier d'interfaces pour SSL», à la page 376
Pour les connexions SSL, spécifiez les ports SSL dans le fichier de connexions de données `omni.dat`, puis exécutez l'utilitaire **nco_igen** pour générer le fichier d'interfaces.

Activation du chiffrement NIST SP800-131a

Vous pouvez configurer l'Interface graphique Web pour qu'elle prenne en charge la norme de sécurité National Institute of Standards and Technology (NIST) SP800-131a. SP800-131a nécessite des clés plus longues et une cryptographie plus puissante que les autres normes telles que FIPS 140-2. SP800-131a requiert Transport Layer Security (TLS) V1.2.

Vous pouvez exécuter SP800-131a en deux modes : transition et strict. Utilisez le mode transition pour vous déplacer graduellement vers une application stricte de la norme SP800-131a. Le mode transition permet d'utiliser des clés et des algorithmes plus faibles que l'application stricte. Le mode transition permet également d'utiliser le protocole TLS v1.0 et v1.1. Par conséquent, le mode transition est utile pour mettre à niveau les paramètres de sécurité à partir de FIPS 140-2, car vous pouvez continuer à utiliser les certificats conformes à FIPS 140-2 existants.

Avant de commencer

- Vérifiez que votre environnement, à savoir, les composants de l'Tivoli Netcool/OMNIbus et les ordinateurs hôte, est configuré comme suit :
  - Vérifiez que vos clients Java prennent en charge TLS V1.2 pour la communication SSL. Ce support est actuellement fourni dans IBM Java 7 Plugin (1.7.0 SR3) et Oracle Java 7 u11.
  - Pour le client WAAPI, vérifiez que l'ordinateur hôte dispose du support IBM JRE with NIST 800-131, à savoir IBM Java JDK 6.0 SR10 ou version supérieure, Java JDK 6.26 SR1 ou version supérieure, ou IBM Java JDK 7.0 SR1 ou version supérieure.
  - Vérifiez que tous les clients qui se connectent à l'Interface graphique Web disposent d'un navigateur qui prend en charge TLS 1.0 pour le mode transition ou TLS 1.2 pour le mode strict. Actuellement, Mozilla Firefox prend uniquement en charge TLS 1.0, il n'est donc pas adapté au mode strict.
- Réalisez une copie de sauvegarde de votre installation de l'Interface graphique Web.
- Pour le mode strict, appliquez TLS 1.2 dans l'ObjectServer et recréez les certificats, afin que les certificats soient conformes.

Tâches associées:

«Configuration de l'authentification d'utilisateurs sur un serveur ObjectServer», à la page 512
Si vous avez spécifié un serveur ObjectServer en tant que référentiel d'utilisateurs lors du processus d'installation, aucune configuration supplémentaire n'est requise. Toutefois, si vous souhaitez définir le serveur ObjectServer comme source d'authentification en dehors du processus d'installation, vous pouvez exécuter des scripts pour configurer le composant Virtual Member Manager (VMM). Si vous le souhaitez, vous pouvez ensuite permettre aux utilisateurs d'ObjectServer d'être

authentifiés auprès d'un annuaire LDAP.

Définition du mode transition SP800-131a

Utilisez le mode transition pour vous déplacer graduellement vers une application stricte de la norme SP800-131a. Le mode transition permet d'utiliser des clés et des algorithmes plus faibles que l'application stricte. Un scénario typique consiste à utiliser le mode transition pour la migration à partir de FIPS 140-2 vers le mode strict SP 800-131.

Vous pouvez appliquer les protocoles TLS 1.2 et recréer les certificats pour le mode transition, mais ces configurations sont uniquement facultatives. Pour une conformité complète à SP800-131a, les protocoles TLS 1.2 doivent être appliqués, les certificats doivent être recréés et le mode strict doit être activé.

Une configuration distincte est requise pour définir le mode transition sur le client d'API d'administration de l'Interface graphique Web(WAAPI).

Configuration du mode transition SP800-131 sur le serveur d'applications :

Pour le mode de transition, une configuration minimale est requise sur l'instance du serveur d'applications qui héberge l'Interface graphique Web. Si vous le souhaitez, vous pouvez effectuer des configurations supplémentaires telles que l'application de TLS 1.2 et la création des certificats. Si ces configurations sont requises pour le mode strict, elles ne sont pas nécessaires pour le mode transition.

Procédure

1. Connectez-vous à la console d'administration et cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Gestion de clés et du certificat SSL)**, puis sous **Configuration settings (Paramètres de configuration)**, cliquez sur **Manage FIPS (Gérer FIPS)**.
2. Sélectionnez **Enable SP800-131 (Activer SP800-131)**, puis **Transition**. Cliquez ensuite sur **OK** pour enregistrer vos modifications.
3. Modifiez le fichier `/opt/IBM/JazzSM/profile/properties/ssl.client.props` :
   a. Ajoutez la ligne suivante :
      ```
      com.ibm.websphere.security.FIPSLevel=transition
      ```
   b. Si votre environnement n'utilise pas encore les niveaux de chiffrement FIPS 140-2, définissez la propriété **`com.ibm.security.useFIPS`** sur `true`.
   c. Définissez la propriété **`com.ibm.ssl.enableSignerExchangePrompt`** sur `true`.
4. Redémarrez le serveur.

Que faire ensuite

1. Si votre environnement utilise le client WAAPI, définissez le mode transition sur le client WAAPI.
2. Si vous souhaitez appliquer les certificats conformes à TLS 1.2 et SP800-131 pendant que l'Interface graphique Web s'exécute en mode transition :
   a. Activez TLS 1.2 sur les clients, dans les navigateurs et les plug-ins Java.
   b. Configurez le serveur d'applications pour appliquer TLS 1.2 et recréer les certificats afin qu'ils soient conformes.
   c. Configurez le flux d'événements à partir de l'ObjectServer afin que la norme TLS2 1.2 soit appliquée. Cette tâche implique le remplacement du certificat qui établit la confiance avec l'ObjectServer avec le nouveau certificat conforme à SP800-131 et l'application de TLS 1.2 dans le fichier

d'initialisation `server.init`. En fonction de votre environnement, vous devrez peut-être également modifier la définition de source de données et chiffrer les mots de passe utilisateur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Configuration de la conformité SP800-131 pour le flux d'événements à partir du serveur ObjectServer :

Pour garantir que le flux d'événements à partir de l'ObjectServer vers l'Interface graphique Web est conforme à SP800-131, deux configurations sont requises. Ajoutez d'abord un certificat conforme à SP800-131 pour l'ObjectServer au fichier de clés certifiées Concentrateur des services d'application du tableau de bord. Configurez ensuite la conformité SP800-131 sur le serveur de l'Interface graphique Web. Ces étapes sont obligatoires pour le mode strict et facultatives pour le mode transition.

Avant de commencer

Appliquez TLS 1.2 dans l'ObjectServer et recréez les certificats.

Procédure

Pour remplacer le certificat :

1. Sur l'hôte de l'ObjectServer, effectuez une copie du fichier `etc/security/certificate.arm` et placez-la sur l'hôte de l'Interface graphique Web.
2. Connectez-vous à la console d'administration et cliquez sur **Sécurité** > **Gestion de clés et du certificat SSL**. Puis, sous **Eléments associés**, cliquez sur **Fichiers de clés et certificats**.
3. Cliquez sur **NodeDefaultTrustStore**, puis sur **Certificats de signataire**. Notez le nom d'alias pour le certificat pour l'ObjectServer.
4. Supprimez le certificat existant pour l'ObjectServer, puis cliquez sur **Ajouter** pour ajouter le certificat conforme à SP800-131. Dans la zone **Alias**, entrez le même alias que pour le certificat que vous avez supprimé et dans la zone **Nom de fichier**, entrez l'emplacement dans lequel vous avez copié le certificat sur l'hôte Interface graphique Web. Vérifiez que le type de données est défini sur **Données ASCII codées en Base64**.
5. Enregistrez les modifications.

Pour configurer la conformité SP800-131 sur le serveur Interface graphique Web :

6. Ouvrez le fichier *REP_INSTALL_WEBGUI*`/etc/server.init` pour édition.
7. Effectuez les changements suivants :
   - Définissez le paramètre **`webtop.fips.level`** sur `sp800-131`.
   - Définissez le paramètre **`webtop.password.encryption`** sur `none` ou `fips`.
   - Définissez le paramètre **`webtop.fips`** sur `on`.

Si vous configurez SP800-131 à partir de zéro, effectuez l'étape suivante pour configurer la connexion à la source de données. Si vous utilisez déjà des communications sécurisées SSL, y compris FIPS 140-2, vous pouvez passer cette étape. Les paramètres de configuration dans le fichier `ncwDataSourceDefinitions.xml` pour SP800-131 sont identiques à ceux pour SSL et FIPS 140-2

8. Définissez le port du serveur ObjectServer à utiliser pour la connexion SSL :
   a. Ouvrez le fichier `ncwDataSourceDefinitions.xml`.
   b. Définissez la propriété **ncwPrimaryServer** comme indiqué dans l'exemple suivant :
      ```
      <ncwPrimaryServer>
      <ncwOSConnection host="hôte_ObjectServer" port="port_ObjectServer"
       ssl="true"/></ncwPrimaryServer>
      ```
   c. Si l'ObjectServer est configuré pour utiliser SSL, ouvrez le fichier `/opt/BM/JazzSM/profile/etccom.sybase.jdbc3.SybDriver.props` et définissez la propriété **USESSLPRIMARY** sur `true`.
9. Si les mots de passe ne sont pas encore chiffrés aux niveaux de chiffrement FIPS 140-2, chiffrez les mots de passe. Pour plus d'informations, voir «Chiffrement des mots de passe à l'aide du mode FIPS 140–2», à la page 537.
10. Redémarrez le serveur.

Résultats

La connexion de données de flux d'événements entre l'ObjectServer et l'Interface graphique Web est à présent conforme à SP800-131. Si vous utilisez également l'ObjectServer en tant que référentiel d'utilisateurs, la connexion pour la gestion des utilisateurs est à présent également conforme.

Configuration du mode transition SP800-131a sur le client WAAPI :

Si votre environnement utilise l'API d'administration de l'Interface graphique Web pour administrer à distance le serveur de l'Interface graphique Web, une configuration supplémentaire est nécessaire pour activer le mode transition sur le client WAAPI. Le niveau de configuration varie selon que vous passez du niveau de chiffrement FIPS 140-2 au niveau SP800-131.

Si vous évoluez à partir des niveaux de chiffrement FIPS 140-2 et, par conséquent, disposez d'un fichier de clés certifiées WAAPI, la seule configuration requise est d'appliquer SP800-131 dans le fichier d'initialisation WAAPI. Si vous n'avez pas encore de fichier de clés certifiées WAAPI, par exemple si vous n'utilisez pas les niveaux de chiffrement FIPS 140-2, vous devez mettre à jour les certificats. Créez ensuite un fichier de clés certifiées WAAPI et mettez-la à jour avec le nouveau certificat.

Procédure

Si vous disposez d'un fichier de clés certifiées WAAPI avec le certificat existant, effectuez uniquement l'étape suivante. Ignorez les étapes restantes.

1. Sur l'hôte WAAPI, éditez le fichier `waapi.init` comme suit :
   a. Remplacez la propriété **waapi.secure** par `"transition"`.
   b. Vérifiez que la propriété **waapi.host** a la même valeur que l'attribut CN à l'étape 5g.

Si vous devez créer des certificats mis à jour, créez un fichier de clés certifiées WAAPI et mettez à jour le fichier de clés certifiées, puis effectuez les étapes suivantes :

2. Connectez-vous à la console d'administration et cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Gestion de clés et du certificat SSL)**. Puis, sous **Related items (Eléments associés)**, cliquez sur **Key stores and certificates (Fichiers de clés et certificats)**.

3. Cliquez sur **NodeDefaultKeyStore** et sur **Personal certificates (Certificats personnels)** et sélectionnez **default (valeur par défaut)**.
4. Cliquez sur **Extract (Extraire)**. Dans la page Extract certificate (Extraire le certificat), entrez *accueil_interface_graphique_web*/etc/encrypt/tipcert.arm dans la zone **Certificate file name (Nom du fichier certificat)**. Sauvegardez ensuite vos modifications et déconnectez-vous de Concentrateur des services d'application du tableau de bord.
5. Supprimez le fichier de clés certifiées WAAPI qui a été précédemment utilisé pour le chiffrement FIPS 140-2. Par exemple, *accueil_interface_graphique_web*/etc/encrypt/waapiTruststore.p12.
6. Accédez au répertoire *JazzSM_HOME*/bin, exécutez la commande **ikeyman** correspondant à votre système d'exploitation. Créez un fichier de clés certifiées et chargez le certificat de signataire à partir de Concentrateur des services d'application du tableau de bord, afin que le client WAAPI fasse confiance aux certificats Concentrateur des services d'application du tableau de bord.
   a. Cliquez sur **KeyDatabaseFile** > **New (Nouveau)** et sélectionnez **PKSC12** comme type de base de données de clés.
   b. Entrez le nom de fichier *accueil_interface_graphique_web*/etc/encrypt/waapiTruststore.p12.
   c. Entrez un mot de passe.
   d. Cliquez sur **Signer certificates (Certificats de signataire)** puis sur **Add (Ajouter)**.
   e. Entrez le chemin d'accès *accueil_interface_graphique_web*/etc/encrypt et le fichier tipcert.arm.
   f. Entrez tipcert en tant que libellé.
   g. Affichez le certificat et vérifiez que l'attribut CN est identique au certificat de signataire extrait.

Que faire ensuite

Pour tester que le client WAAPI s'exécute, accédez au répertoire bin de WAAPI et exécutez un exemple de commande, tel que :

```
runwaapi -props ../etc/waapi.init -file ../etc/samples/list_filter.xml
```

Vérifiez que la commande s'exécute et renvoie la sortie attendue.

Définition du mode strict SP800-131a

Si votre environnement n'utilise pas encore le chiffrement FIPS 140-2, vous pouvez appliquer les normes SP800-131 sans effectuer les étapes de transition de FIPS 140-2.

Avant de commencer

- Vérifiez que le serveur ObjectServer est configuré pour le chiffrement de la sécurité TLS 1.2.
- Vérifiez que les certificats d'ObjectServer sont recréés en conformité à la norme SP800-131.

Tâches associées:

«Configuration des composants serveur pour le chiffrement étendu SP800-131», à la page 286
Vous pouvez configurer le chiffrement étendu SP800-131 dans le fichier de configuration FIPS pour appliquer le chiffrement TLS 1.2 aux composants serveur prenant en charge le mode FIPS 140-2.

Activation de TLS 1.2 sur les clients :

Sur tous les clients, vérifiez que TLS 1.2 est activé dans les paramètres de navigateur et dans le plug-in Java. Dans les paramètres de navigateur et du plug-in Java, TLS 1.2 est requis en plus de TLS 1.0.

Configuration du mode strict SP800-131 sur le serveur d'applications :

Sur le serveur d'applications, activez le mode strict SP800-131. Puis, dans le fichier de propriétés client SSL, spécifiez la norme de sécurité SP800-131.

Procédure

1. Connectez-vous à la console d'administration et cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Gestion de clés et du certificat SSL)**. Cliquez ensuite sur **Manage FIPS (Gérer FIPS**.
2. Sélectionnez **Enable SP800-131 (Activer SP800-131)**, puis **Strict**. Sauvegardez ensuite les modifications et déconnectez-vous de la console.
3. Sur l'hôte Interface graphique Web, éditez le fichier `/opt/IBM/JazzSM/profile/properties/ssl.client.props`. Ajoutez la ligne suivante :

   ```
   com.ibm.websphere.security.FIPSLevel=SP800-131
   ```
4. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.
5. Vérifiez que les modifications ont été appliquées. Par exemple, cliquez sur **Users and groups (Utilisateurs et groupes)** > **Manage users (Gérer les utilisateurs)** et vérifiez que les utilisateurs attendus sont répertoriés. Ouvrez également une liste d'événements et vérifiez que les données d'événement sont affichées sans erreur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Configuration du mode strict SP800-131 sur le client WAAPI :

Pour appliquer le chiffrement SP800-131 sur le client WAAPI, éditez le fichier `waapi.init` et remplacez la valeur de la propriété **`waapi.secure`** par `"sp800-131"`.

Procédure

1. Connectez-vous à la console d'administration et cliquez sur **Sécurité** > **Gestion de clés et du certificat SSL**. Puis, sous **Eléments associés**, cliquez sur **Fichiers de clés et certificats**.
2. Cliquez sur **NodeDefaultKeyStore** et sur **Personal certificates (Certificats personnels)** et sélectionnez **default (valeur par défaut)**.
3. Cliquez sur **Extract (Extraire)**. Dans la page Extract certificate (Extraire le certificat), entrez *`accueil_interface_graphique_web`*`/etc/encrypt/tipcert.arm` dans la zone **Certificate file name (Nom du fichier certificat)**. Sauvegardez ensuite vos modifications et déconnectez-vous de Concentrateur des services d'application du tableau de bord.
4. Supprimez le fichier de clés certifiées WAAPI qui a été précédemment utilisé pour le chiffrement FIPS 140-2. Par exemple, *`accueil_interface_graphique_web`*`/etc/encrypt/waapiTruststore.p12`.
5. Accédez au répertoire *`JazzSM_HOME`*`/bin`, exécutez la commande **`ikeyman`** correspondant à votre système d'exploitation. Créez un fichier de clés certifiées

et chargez le certificat de signataire à partir de Concentrateur des services d'application du tableau de bord, afin que le client WAAPI fasse confiance aux certificats Concentrateur des services d'application du tableau de bord.

a. Cliquez sur **KeyDatabaseFile** > **New (Nouveau)** et sélectionnez **PKSC12** comme type de base de données de clés.
b. Entrez le nom de fichier *accueil_interface_graphique_web*/etc/encrypt/waapiTruststore.p12.
c. Entrez un mot de passe.
d. Cliquez sur **Signer certificates (Certificats de signataire)** puis sur **Add (Ajouter)**.
e. Entrez le chemin d'accès *accueil_interface_graphique_web*/etc/encrypt et le fichier tipcert.arm.
f. Entrez tipcert en tant que libellé.
g. Affichez le certificat et vérifiez que l'attribut CN est identique au certificat de signataire extrait.

6. Sur l'hôte WAAPI, éditez le fichier waapi.init comme suit :
   a. Remplacez la propriété **waapi.secure** par "sp800-131".
   b. Vérifiez que la propriété **waapi.host** a la même valeur que l'attribut CN à l'étape 5g.

Configuration de l'interface graphique Web pour une utilisation en production

Après avoir facultativement configuré l'authentification utilisateur pour votre installation d'interface graphique Web ainsi que vos paramètres de chiffrement, vous pouvez configurer l'interface graphique Web pour l'utiliser dans votre environnement, par exemple en définissant des sources de données supplémentaires, en configurant un environnement d'équilibrage de charge ou en créant des intégrations de lancement en contexte avec d'autres produits Tivoli.

Configuration des sources de données

Définissez les sources de données à partir desquelles l'Interface graphique Web extrait des événements. Le terme "source de données" désigne toute source de données à partir de laquelle l'Interface graphique Web peut obtenir des informations sur les événements, mais le flux d'événements est généralement fourni par des serveurs ObjectServer. Plusieurs configurations sont possibles, avec des sources de données uniques ou multiples, des paires de reprise en ligne et des environnements de bureau à deux serveurs (DSD).

Le tableau ci-dessous décrit les configurations. Les configurations DSD et à un seul serveur peuvent cohabiter.

Tableau 86. Configurations de source de données

Configuration	Description
Serveur unique	Comporte une source de données unique. La source de données peut être un serveur ObjectServer unique. Elle peut également correspondre à une paire de reprise en ligne de serveurs ObjectServer, qui se compose d'un serveur ObjectServer principal et d'un serveur ObjectServer de reprise en ligne (également appelé ObjectServer secondaire). Vous pouvez configurer plusieurs sources de données à serveur unique ou des paires de reprise en ligne à serveur unique.
DSD	Comprend un serveur ObjectServer principal et un serveur ObjectServer de reprise en ligne facultatif, ainsi qu'un ou plusieurs serveurs ObjectServer d'affichage, dans un «read-cloud». Dans une configuration DSD, l'Interface graphique Web lit les données d'événement à partir des serveurs ObjectServer de la couche d'affichage dans le read-cloud. Les utilisateurs peuvent être affectés à des serveurs ObjectServer d'affichage différents.

Les configurations de source de données sont stockées dans le fichier *REP_INSTALL_WEBGUI*/etc/datasources/ncwDataSourceDefinitions.xml. Dans ce fichier, chaque source de données est définie avec son propre nom. La fonctionnalité de surveillance automatique est également contrôlée dans ce fichier.

Conseil : A titre de référence, les fichiers XML qui spécifient plusieurs sources de données, un environnement DSD, ainsi que la surveillance automatique, se trouvent dans *REP_INSTALL_WEBGUI*/etc/datasource/samples.

Si un serveur ObjectServer est défini dans une source de données et qu'il est également utilisé comme registre d'utilisateurs, les informations relatives à ce serveur ObjectServer sont conservées dans 2 emplacements : dans le fichier ncwDataSourceDefinitions.xml et également dans le plug-in VMM.

Tâches associées:

«Activation de la surveillance automatique», à la page 579
Vous pouvez configurer l'Interface graphique Web pour enregistrer les statistiques relatives à la réactivité de la source de données, l'efficacité de la mémoire cache qui stocke des données d'événement et l'utilisation de la mémoire virtuelle Java (JVM). Pour activer cette fonctionnalité de surveillance automatique, apportez des modifications aux définitions de source de données dans le fichier ncwDataSourceDefinitions.xml.

Création ou modification de sources de données

Vous pouvez utiliser la page Sources de données pour créer une nouvelle source de données ou modifier une source de données existante.

Avant de commencer

- La haute disponibilité de définition de source de données n'est pas prise en charge.
- La page Sources de données répertorie les sources de données par défaut en premier lieu, suivies des sources de données non par défaut. Créez des sources de données de la plus importante à la moins importante, car il s'agit de l'ordre reflété dans le fichier de définitions de source de données.
- Vous pouvez modifier manuellement l'ordre des sources de données dans le fichier de définitions de source de données. Redémarrez le serveur Concentrateur des services d'application du tableau de bord pour que les modifications de configuration prennent effet.

Pourquoi et quand exécuter cette tâche

Pour créer une source de données pour l'Interface graphique Web :

Procédure

1. Cliquez sur l'icône d'administration et sélectionnez **Sources de données**.
2. Un tableau contenant une liste de sources de données s'affiche. Si aucune source de données n'existe, la table est vide. Cliquez sur l'icône **Créer une source de données**.
3. Dans l'onglet **Général**, définissez les propriétés de configuration suivantes :

   Name Nom de la source de données défini par l'utilisateur.

   Sélectionnez **Activé** pour activer la source de données maintenant.

   Sélectionner **Par défaut** pour ajouter la source de données au groupe de sources de données par défaut.

   ObjectServer principal
   Le nom d'hôte et le numéro de port de l'ObjectServer principal.

   Le bouton **Tester la connexion au serveur** vous permet de tester si une connexion peut être établie avec le serveur ObjectServer en utilisant l'hôte, le port et les données d'identification entrées dans la section **Authentification** de cette page.

   Remarque : Le bouton Tester la connexion au serveur est désactivé automatiquement si les zones **Hôte** et **Port** sont vides ou contiennent des valeurs non valides.

   Authentification
   ID utilisateur et mot de passe de l'ObjectServer principal.

   Délais de connexion
   Délai d'attente (en secondes) pour l'envoi d'une instruction de requête vers la source de données. En cas de dépassement de délai, l'Interface graphique Web tente de se reconnecter à la source de données.
4. Dans l'onglet (facultatif) **Reprise en ligne**, définissez les propriétés suivantes :

   ObjectServer de secours
   Le nom d'hôte et le numéro de port de l'ObjectServer de secours.

Le bouton **Tester la connexion au serveur** vous permet de tester si une connexion peut être établie avec le serveur ObjectServer en utilisant l'hôte, le port et les données d'identification entrées dans la section **Authentification** de cette page.

Remarque : Le bouton Tester la connexion au serveur est désactivé automatiquement si les zones **Hôte** et **Port** sont vides ou contiennent des valeurs non valides.

Signal de présence actif
Interrogation de la source de données active. A essentiellement pour but de détecter une défaillance de source de données. Il s'agit de l'intervalle de temps (en secondes) entre deux interrogations d'une source de données active.

Signal de présence de reprise
Interrogation de source de données lors du basculement. A essentiellement pour but de détecter une reprise de source de données après une défaillance. Il s'agit de l'intervalle de temps (en secondes) entre deux interrogations de la source de données dans l'éventualité d'un basculement.

Multiplicateur de temporisation de reprise
Multiplicateur de temporisation d'interrogation si la source de données reste indisponible après la dernière interrogation.

5. Dans l'onglet **Serveur d'affichage**, vous pouvez configurer un environnement de bureau à deux serveurs. Le bureau à deux serveurs (DSD) est une architecture de traitement d'événement tierce. Les installations d'Interface graphique Web utilisant une architecture DSD écrivent simultanément dans un ou plusieurs serveurs d'affichage et un seul serveur maître ObjectServer. Ils lisent uniquement les données d'événement provenant des serveurs d'affichage. Vous pouvez ajouter, supprimer ou modifier le serveur d'affichage.

   Cliquez sur **Ajouter** pour configurer les propriétés du serveur d'affichage suivants :

   Hôte Définissez l'hôte du serveur d'affichage.

   Port Définissez le port du serveur d'affichage.

   Tester la connexion au serveur
   Vous permet de tester si une connexion peut être établie avec le serveur ObjectServer en utilisant l'hôte et le port.

   Remarque : Le bouton Tester la connexion au serveur est désactivé automatiquement si les zones **Hôte** et **Port** sont vides ou contiennent des valeurs non valides.

   Pool de connexions
   Définissez la taille du pool de connexions par ObjectServer d'affichage.

6. Dans l'onglet **Mise en cache**, définissez les propriétés de configuration suivantes :

   Configuration de la cache
   Délai d'expiration de la mémoire cache (en secondes). Configure les options de mise en cache pour les données de configuration de la source de données, telles que les couleurs et les conversions de zone des événements. La valeur par défaut est 3600 secondes.

Activer la mémoire cache de la liste d'événements

Expiration de la mémoire cache (en secondes) : Délai d'expiration de la mémoire cache (en secondes). Par défaut, la valeur est 60 secondes.

Nettoyage du cache toutes les (seconds) : Fréquence (en secondes) de recherche et de suppression des anciennes entrées de la mémoire cache. La valeur par défaut est 120 secondes.

Activer la mémoire cache de récapitulatif d'événements

Expiration de la mémoire cache (en secondes) : Délai d'expiration de la mémoire cache (en secondes). La valeur par défaut est de 10 secondes.

Nettoyage du cache toutes les (seconds) : Fréquence (en secondes) de recherche et de suppression des anciennes entrées de la mémoire cache. La valeur par défaut est 20 secondes.

Activer la mémoire cache de métrique

Expiration de la mémoire cache (en secondes) : Délai d'expiration de la mémoire cache (en secondes). La valeur par défaut est de 10 secondes.

Nettoyage du cache toutes les (seconds) : Fréquence (en secondes) de recherche et de suppression des anciennes entrées de la mémoire cache. La valeur par défaut est 20 secondes.

7. Dans l'onglet **Pools de connexions**, vous pouvez configurer la taille minimale et maximale du pool de connexions pour les ObjectServers principaux et de secours.
8. L'onglet **Autosurveillance** contient une liste des services qui peuvent être contrôlés par la fonctionnalité de surveillance automatique. Chaque service a un ou plusieurs seuils. Lorsque des seuils sont atteints, des événements de problème associés à des niveaux de gravité spécifiques sont émis. Le tableau ci-dessous décrit chaque service ainsi que les seuils par défaut.

Tableau 87. Services qui peuvent être contrôlés par la fonctionnalité de surveillance automatique

Nom du service	Description	Remarques
DataSourceCommand	Surveille les temps de réponse, en secondes, de la source de données à toutes les requêtes.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
ResultsCache	Surveille l'efficacité de la mémoire cache en mesurant le nombre de requêtes auxquelles les données mises en cache ont répondu. Plus les pourcentages de requêtes pouvant être répondues par la mémoire cache sont faibles, moins la mémoire cache est efficace.	Par défaut, un événement majeur est émis lorsque le pourcentage baisse au-dessous de 10 %. Un événement mineur est émis lorsque le pourcentage baisse au-dessous de 20 %.

Tableau 87. Services qui peuvent être contrôlés par la fonctionnalité de surveillance automatique (suite)

Nom du service	Description	Remarques
EventData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données d'événement, par exemple pour les afficheurs d'événements et les listes d'événements actifs.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
EventSummaryData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données récapitulatives d'événement, par exemple les cartes et les tableaux de bord d'événement.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
MetricData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données de métriques, servant à alimenter les jauges.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
SecurityRepository	Surveille le temps de réponse, en secondes, du référentiel de sécurité. Le référentiel de sécurité est définie en tant que serveur ObjectServer utilisé comme registre d'utilisateurs, ou en tant que référentiel de fichiers ou annulaire LDAP.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
JVM	Surveille l'utilisation de la mémoire virtuelle Java (JVM). Les événements sont émis lorsque l'utilisation atteint des seuils spécifiques.	Par défaut, un événement critique est émis lorsque l'utilisation atteint 95 %. Un événement majeur est émis lorsque l'utilisation dépasse 90 %. Un événement mineur est émis lorsque l'utilisation atteint 85 %.

Tableau 87. Services qui peuvent être contrôlés par la fonctionnalité de surveillance automatique (suite)

Nom du service	Description	Remarques
VMM	Surveille les événements insérés sur le serveur ObjectServer principal actif de la source de données configurée, d'après des seuils configurés pour le service VMM (Virtual Member Manager).	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes. **Remarque :** Le moniteur VMM n'insère aucun événement de surveillance si la synchronisation VMM est désactivée (`users.credentials.sync =false`) dans le fichier `server.init`.

Configurez les options suivantes dans l'onglet Autosurveillance :

Activer l'autosurveillance
Active ou désactive la surveillance automatique. Par défaut, elle est désactivée.

Fréquence (en secondes)
Indique la fréquence (en secondes) à laquelle les événements d'autosurveillance sont insérés sur le serveur ObjectServer. La valeur par défaut est de 300 secondes.

Activer
Active la surveillance pour le service. Chaque service est activé ou désactivé séparément. Par défaut, la surveillance des services est activée.

Evénements d'information
Lorsque cette option est activée, les événements d'information supplémentaires sont insérés dans l'ObjectServer à la fréquence spécifiée dans le paramètre Granularité. Par défaut, elle est désactivée.

Dédoublonner
Lorsque cette option est activée, les événements d'information sont dédoublonnés. Par défaut, elle est activée.

Tâches associées:

«Configuration d'un environnement de bureau à deux serveurs», à la page 563
Le bureau à deux serveurs (DSD) est une architecture de traitement d'événement tierce. Les installations d'Interface graphique Web utilisant une architecture DSD écrivent simultanément dans un ou plusieurs serveurs d'affichage et un seul serveur maître ObjectServer. Ils lisent uniquement les données d'événement provenant des serveurs d'affichage. Pour configurer un environnement DSD, modifiez le fichier de configuration de source de données.

Copie ou suppression de sources de données :

Vous pouvez copier les informations de source de données à partir d'un enregistrement de source de données existant, par exemple, lorsque la plupart des informations sont nécessaires dans la nouvelle définition de source de données. Vous pouvez également supprimer un enregistrement de source de données qui n'est plus nécessaire.

Procédure

1. Cliquez sur l'icône d'administration et sélectionnez **Sources de données**. Un tableau contenant une liste de sources de données s'affiche.
2. Pour copier une source de données, procédez comme suit :
   a. Sélectionnez un enregistrement dans la liste et cliquez sur **Copier la source de données**.
   b. Une boîte de dialogue est ouverte qui contient les informations copiées à partir de la source de données sélectionnée. Entrez un nouveau nom pour la source de données et modifiez les données requises.
   c. Cliquez sur **Sauvegarder**.
3. Pour supprimer une source de données :
   a. Sélectionnez un enregistrement dans la liste et cliquez sur **Supprimer la source de données**.
   b. Un message de confirmation s'affiche. Confirmez que vous souhaitez supprimer la source de données pour la retirer de la liste.

Présentation du fichier de configuration de la source de données

Le fichier `ncwDataSourceDefinitions.xml` contrôle les définitions de source de données, les connexions, la reprise en ligne, la surveillance automatique et le nettoyage de la mémoire cache. A la suite d'une nouvelle installation et de la configuration initiale, ce fichier contient uniquement les informations que vous avez spécifiées dans l'Outil de configuration de l'interface graphique Web OMNIbus. A la suite d'une mise à niveau, les éléments sont migrés afin d'être compatibles avec la version en cours du produit.

- « Exemple de fichier de configuration de source de données»
- «Explication des éléments XML», à la page 555
- «Code supplémentaire pour la configuration DSD», à la page 561

Exemple de fichier de configuration de source de données

L'exemple suivant présente un fichier de configuration de source de données pour une seule paire de reprise en ligne.

Conseil : Pour plus d'exemples, reportez-vous aux fichiers du répertoire *REP_INSTALL_WEBGUI*/etc/default/datasources/.

```
[1] <ncwDataSourceDefinitions>
[2] <ncwDefaultDataSourceList>
[3]      <ncwDataSourceEntry name="NCOMS"/>
[4] </ncwDefaultDataSourceList>
[5]   <ncwDataSourceDefinition type="singleServerOSDataSource" name="NCOMS">
[6] <results-cache>
[7]  <chart maxAge="60" enabled="false" cleantime="120"/>
[8]  <config maxAge="3600"/>
[9]  <eventList maxAge="60" enabled="false" cleantime="120"/>
[10]  <eventSummary maxAge="10" enabled="true" cleantime="20"/>
[11]      <metric maxAge="10" enabled="true" cleantime="20"/>
[12] </results-cache>
```

```
[13] <ncwDataSourcePollingParameters>
[14]         <ncwFailOverPollingParameters backOffMultiplier="2"
basePollingTime="10"/>
[14]         <ncwHeartBeatParameters basePollingTime="15"/>
[15] </ncwDataSourcePollingParameters>
[16] <ncwConnectionParameters
[17]  <ncwStatementParameters
[18]   <ncwQueryTimeout baseTime="60"/>
[19]  </ncwStatementParameters>
[20] </ncwConnectionParameters>
[21]      <ncwDataSourceCredentials password="" userName="root"
encrypted="false"/>
[22] <self-monitor enabled="false" granularity="300">
[23] <service name="DataSourceCommand" monitor="true" info="false"
deduplicateinfo="true">
[24]   <threshold value="5" severity="3"/>
[25]   <threshold value="15" severity="4"/>
[26]   <threshold value="30" severity="5"/>
[27]  </service>
[28]  <service name="ResultsCache" monitor="true" info="false"
deduplicateinfo="true">
[29]   <threshold value="20" severity="3"/>
[30]   <threshold value="10" severity="4"/>
[31]  </service>
[32]  <service name="EventData" monitor="true" info="false"
deduplicateinfo="true">
[33]   <threshold value="5" severity="3"/>
[34]   <threshold value="15" severity="4"/>
[35]   <threshold value="30" severity="5"/>
[36]  </service>
[37]  <service name="EventSummaryData" monitor="true" info="false"
deduplicateinfo="true">
[38]   <threshold value="5" severity="3"/>
[39]   <threshold value="15" severity="4"/>
[40]   <threshold value="30" severity="5"/>
[41]  </service>
[42]  <service name="MetricData" monitor="true" info="false"
deduplicateinfo="true">
[43]   <threshold value="5" severity="3"/>
[44]   <threshold value="15" severity="4"/>
[45]   <threshold value="30" severity="5"/>
[46]  </service>
[47]  <service name="SecurityRepository" monitor="true" info="false"
deduplicateinfo="true">
[48]   <threshold value="5" severity="3"/>
[49]   <threshold value="15" severity="4"/>
[50]   <threshold value="30" severity="5"/>
[51]  </service>
[52]  <service name="JVM" monitor="true" info="false"
deduplicateinfo="true">
[53]   <threshold value="85" severity="3"/>
[54]   <threshold value="90" severity="4"/>
[55]   <threshold value="95" severity="5"/>
[56]  </service>
[57]            <service name="VMM" monitor="true" info ="true"
deduplicateinfo="true">
[58]                    <threshold value="5" severity="3"/>
[59]                    <threshold value="15" severity="4"/>
[60]                    <threshold value="30" severity="5"/>
[61]            </service>
[62] </self-monitor>
[63] <ncwFailOverPairDefinition>
[64]  <ncwPrimaryServer>
[65]   <ncwOSConnection host="192.168.0.1" port="4100"/>
```

```
[66]  </ncwPrimaryServer>
[67]  </ncwFailOverPairDefinition>
[68] </ncwDataSourceDefinition>
[69]</ncwDataSourceDefinitions>
```

Explication des éléments XML

Les explications ci-dessous décrivent le fonctionnement du code ligne par ligne.

«Ligne 1 : <ncwDataSourceDefinitions>»
«Lignes 2 à 4 : <ncwDefaultDataSourceList>»
«Ligne 5 : <ncwDataSourceDefinition>»
«Lignes 6-12 : <results-cache>», à la page 556
«Lignes 13-15 : <ncwDataSourcePollingParameters>», à la page 557
«Lignes 16-20 : <ncwConnectionParameters>», à la page 557
«Ligne 21 : <ncwDataSourceCredentials>», à la page 557
«Lignes 63-67 : <ncwFailOverPairDefinition>», à la page 560
«Ligne 68 </ncwDataSourceDefinition>», à la page 561
«Ligne 69 : </ncwDataSourceDefinitions>», à la page 561

Ligne 1 : <ncwDataSourceDefinitions>

Cette ligne ouvre la balise <ncwDataSourceDefinitions> de niveau supérieur et initie le fichier.

Lignes 2 à 4 : <ncwDefaultDataSourceList>

L'élément <ncwDefaultDataSourceList> contient une liste d'un ou de plusieurs éléments <ncwDataSourceEntry>. Le premier <ncwDataSourceEntry> correspond à la source de données par défaut. Le fichier de configuration doit contenir au moins un élément <ncwDataSourceEntry>. La source de données qui est nommée dans l'élément <ncwDefaultDataSourceList> doit également être définie dans un élément <ncwDataSourceDefinition>. Pour plus d'informations, voir «Ligne 5 : <ncwDataSourceDefinition>».

Si la communication avec la source de données par défaut ne peut pas être établie, l'élément <ncwDataSourceEntry> suivant dans la liste, le cas échéant, est contacté. Les mots de passe utilisateur et les mots de passe administrateur peuvent différer d'une source de données à l'autre.

Ligne 5 : <ncwDataSourceDefinition>

L'élément <ncwDataSourceDefinition> contient les paramètres de configuration et de communication pour une source de données unique. Le fichier de configuration doit contenir au moins un élément <ncwDataSourceDefinition>. L'élément contient les attributs suivants :

name
Nom défini par l'utilisateur, auquel l'élément <ncwDataSourceEntry> fait également référence. Cet attribut doit être une chaîne alphanumérique unique ne contenant aucun espace ou caractère spécial.

valeur
Définit la source de données sous la forme d'un serveur ObjectServer unique accompagné d'un serveur de secours facultatif, ou d'une configuration de bureau à deux serveurs (DSD). Pour plus d'informations sur DSD, voir «Code supplémentaire pour la configuration DSD», à la page 561.

Lignes 6-12 : <results-cache>

L'élément <results-cache> spécifie si la mise en cache des données de la source de données est activée. Cet élément comporte les éléments enfant suivants :

<chart>
Définit la mise en cache des résultats de graphique. Cet élément comporte les attributs suivants :

enabled
Paramétrez cet attribut sur TRUE pour activer la mise en cache.

maxAge
Spécifie le délai d'expiration, en secondes, du cache.

cleantime
Spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<config>
Définit la mise en cache des données de configuration de source de données, par exemple, les couleurs de gravité d'événement et les conversions. Cet élément a l'attribut suivant :

maxAge
Spécifie le délai d'expiration, en secondes, du cache.

<eventList>
Définit la mise en cache des résultats de la liste d'événements. Cet élément comporte les attributs suivants :

enabled
Paramétrez cet attribut sur TRUE pour activer la mise en cache.

maxAge
Spécifie le délai d'expiration, en secondes, du cache.

cleantime
Spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<eventSummary>
Définit la mise en cache des résultats de récapitulatif d'événement, comme les cartes et les Tableaux de bord des événements. Cet élément a les attributs suivants :

enabled
Paramétrez cet attribut sur TRUE pour activer la mise en cache.

maxAge
Spécifie le délai d'expiration, en secondes, du cache.

cleantime
Spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<metric>
Définit la mise en cache des résultats de métrique, c'est à dire les jauges de métrique. Cet élément comporte les attributs suivants :

enabled
Paramétrez cet attribut sur TRUE pour activer la mise en cache.

maxAge
Spécifie le délai d'expiration, en secondes, du cache.

cleantime
Spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

Lignes 13-15 : <ncwDataSourcePollingParameters>

L'élément <ncwDataSourcePollingParameters> contient les éléments contrôlant l'interrogation de la reprise en ligne et du signal de présence de source de données. L'élément enfant <ncwFailOverPollingParameters> comporte les attributs suivants :

basePollingTime
Indique l'intervalle au bout duquel la source de données est interrogée en cas de reprise en ligne.

backOffMultiplier
Contient le multiplicateur de l'algorithme utilisé par l'Interface graphique Web pour calculer le délai de temporisation de l'interrogation au cours d'une reprise en ligne. Cet exemple n'est pas configuré pour la reprise en ligne ; cet attribut est donc ignoré.

L'élément enfant <ncwHeartBeatParameters> comporte l'attribut suivant :

basePollingTime
Indique l'intervalle de temps au bout duquel l'Interface graphique Web interroge une source de données active.

Lignes 16-20 : <ncwConnectionParameters>

L'élément <ncwConnectionParameters> spécifie les paramètres de connexion pour la source de données. L'élément enfant <ncwQueryTimeout> comporte l'attribut suivant :

baseTime
Indique la durée, en secondes, avant le dépassement du délai d'attente d'une requête envoyée à la source de données. Si une requête dépasse ce délai, l'Interface graphique Web tente de se reconnecter à la source de données.

Ligne 21 : <ncwDataSourceCredentials>

L'élément <ncwDataSourceCredentials> contient les informations de connexion requises par l'Interface graphique Web pour accéder à la source de données. Il comporte les attributs suivants :

userName
Nom d'utilisateur utilisé pour l'accès à la source de données. Par défaut, le nom d'utilisateur n'est pas chiffré.

password
Mot de passe de l'utilisateur. Par défaut, le nom d'utilisateur n'est pas chiffré.

encrypted
Permet le chiffrement du nom d'utilisateur et du mot de passe à l'aide de

l'utilitaire de chiffrement **nco_g_crypt**. Pour permettre le chiffrement, paramétrez l'attribut sur TRUE. La valeur par défaut est FALSE.

Important : Pour des raisons de sécurité, définissez les droits d'accès au fichier ncwDataSourceDefinitions.xml afin d'en restreindre l'accès aux utilisateurs requis.

Ligne 22 : <self-monitor>

Active la surveillance automatique, qui enregistre les statistiques relatives à votre environnement d'Interface graphique Web et émet des événements de surveillance automatique dans la source de données principale. Les événements de surveillance automatique sont répartis en événements de problème, qui sont émis lorsqu'un seuil spécifique est atteint (voir tableau 88, à la page 559) et des événements d'information, qui récapitulent le service surveillé. Les événements de problème sont systématiquement émis et les événements d'information sont facultatifs. Les attributs de cet élément sont les suivants :

enabled
Active ou désactive la surveillance automatique.

granularity
Indique la fréquence, en secondes, à laquelle les événements de surveillance automatique sont insérés dans la source de données.

Une fois que vous avez activé la surveillance automatique, une entrée est écrite dans le fichier ncw.0.log à cet effet.

Lignes 23-61 : <service>

La fonctionnalité de surveillance automatique mesure des services spécifiques. Un service est défini par un élément <service>. Cet élément comporte les attributs suivants :

name
Déclare quel service est en cours de surveillance. Ne modifiez pas les noms de cet attribut. Les valeurs possibles se trouvent dans le tableau 88, à la page 559.

monitor
Active la surveillance pour le service. Chaque service est activé ou désactivé séparément.

info
Si cet attribut est activé, les événements d'information sont émis dans la source de données à la fréquence définie par l'attribut granularity de l'élément <self-monitoring>. Les messages d'information contiennent un récapitulatif du service surveillé. Il comportent une gravité par défaut de 2 (Avertissement).

deduplicateInfo
Permet de dédoublonner les événements d'information, afin de réduire le nombre d'événements dans les listes d'événements.

Chaque service comporte un ou plusieurs seuils, qui sont définis par les éléments enfant <threshold>. Lorsque les valeurs de seuil sont atteintes, des événements de problème de gravité spécifique sont émis. Le tableau ci-dessous décrit chaque service ainsi que les seuils par défaut.

Tableau 88. Services pouvant être surveillés par l'élément <self-monitoring>

Nom du service	Description	Remarques
DataSourceCommand	Surveille les temps de réponse, en secondes, de la source de données à toutes les requêtes.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
ResultsCache	Surveille l'efficacité de la mémoire cache en mesurant le nombre de requêtes auxquelles les données mises en cache ont répondu. Plus les pourcentages de requêtes pouvant être répondues par la mémoire cache sont faibles, moins la mémoire cache est efficace.	Par défaut, un événement majeur est émis lorsque le pourcentage baisse au-dessous de 10 %. Un événement mineur est émis lorsque le pourcentage baisse au-dessous de 20 %.
EventData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données d'événement, par exemple pour les afficheurs d'événements et les listes d'événements actifs.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
EventSummaryData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données récapitulatives d'événement, par exemple les cartes et les tableaux de bord d'événement.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
MetricData	Surveille le temps de réponse, en secondes, de la source de données aux requêtes de données de métriques, servant à alimenter les jauges.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.

Tableau 88. Services pouvant être surveillés par l'élément <self-monitoring> (suite)

Nom du service	Description	Remarques
SecurityRepository	Surveille le temps de réponse, en secondes, du référentiel de sécurité. Le référentiel de sécurité est définie en tant que serveur ObjectServer utilisé comme registre d'utilisateurs, ou en tant que référentiel de fichiers ou annulaire LDAP.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes.
JVM	Surveille l'utilisation de la mémoire virtuelle Java (JVM). Les événements sont émis lorsque l'utilisation atteint des seuils spécifiques.	Par défaut, un événement critique est émis lorsque l'utilisation atteint 95 %. Un événement majeur est émis lorsque l'utilisation dépasse 90 %. Un événement mineur est émis lorsque l'utilisation atteint 85 %.
VMM	Surveille les événements insérés dans le serveur ObjectServer principal actif de la source de données de configuration, en fonction des seuils configurés pour le service VMM.	Par défaut, un événement critique est émis lorsque le temps de réponse atteint 30 secondes. Un événement majeur est émis lorsque le temps de réponse atteint 15 secondes. Un événement mineur est émis lorsque le temps de réponse atteint 5 secondes. **Remarque :** Le moniteur VMM n'insère aucun événement de surveillance si la synchronisation VMM est désactivée (`users.credentials.sync=false`) dans le fichier `server.init`.

Lignes 63-67 : <ncwFailOverPairDefinition>

L'élément <ncwFailOverPairDefinition> contient les informations de communication de serveur pour la source de données principale et, le cas échéant, une source de données secondaire pour la reprise en ligne.

Spécifiez les informations de communication de la source de données principale dans l'élément <ncwPrimaryServer>. Cet élément comporte un élément enfant appelé <ncwOSConnection >. Dans cet élément, indiquez l'adresse IP ou le nom d'hôte ainsi que le numéro de port de la source de données principale.

Pour configurer une paire de reprise en ligne, ajouter un élément <ncwBackUpServer> à l'élément <ncwFailOverPairDefinition>. L'élément <ncwBackUpServer> contient également un élément enfant <ncwOSConnection>. Dans cet élément, indiquez l'adresse IP ou le nom d'hôte ainsi que le numéro de port de la source de données de reprise en ligne. Par exemple :

```
<ncwBackUpServer>
          <ncwOSConnection host="hôte" port="port"/>
</ncwBackUpServer>
```

Vérifiez que les noms d'utilisateur et les noms de zones (dans les tables d'alertes) dans le serveur ObjectServer de sauvegarde sont identiques à ceux du serveur principal, et que serveur chaque ObjectServer contient un nombre égal de zones. Si ces zones ne concordent pas, la reprise en ligne ne peut pas se faire. Si les utilisateurs ne concordent pas, les utilisateurs ne peuvent pas se connecter.

Le serveur ObjectServer de sauvegarde est constamment interrogé quant à sa disponibilité, afin que l'Interface graphique Web puisse basculer sur le serveur de sauvegarde en cas de défaillance du serveur principal. Lors d'une reprise en ligne, l'Interface graphique Web est informée de sa connexion au serveur de sauvegarde et elle vérifie automatiquement la reprise du serveur principal dans la paire de reprise en ligne. Une fois qu'il est établi que le serveur principal est rétabli, l'Interface graphique Web repasse au serveur principal.

Ligne 68 </ncwDataSourceDefinition>

Cette ligne contient l'élément de fermeture de l'élément <ncwDataSourceDefinition>. Des sources de données supplémentaires sont contenues dans des éléments <ncwDataSourceDefinition> ultérieurs.

Ligne 69 : </ncwDataSourceDefinitions>

Cette ligne ferme l'élément <ncwDataSourceDefinitions> et le fichier.

Code supplémentaire pour la configuration DSD

Si un serveur ObjectServer est configuré pour un environnement DSD, le code suivant définit le ou les serveurs ObjectServer d'affichage. Ce code est inséré après l'élément </ncwFailOverPairDefinition> de fin (ligne 26).

```
<ncwReadCloudDefinition>
              <ncwOSConnection host="hôte" port="port"/>
</ncwReadCloudDefinition>
```

Utilisez un élément <ncwOSConnection> pour chaque ObjectServer d'affichage. Un serveur ObjectServer ne peut pas avoir plusieurs éléments <ncwReadCloudDefinition>.

Tâches associées:

«Configuration de plusieurs sources de données», à la page 562
Pour récupérer des événements de plusieurs sources de données ou paires de reprise en ligne, ajoutez des sources de données supplémentaires au fichier de configuration.

«Configuration d'un environnement de bureau à deux serveurs», à la page 563
Le bureau à deux serveurs (DSD) est une architecture de traitement d'événement tierce. Les installations d'Interface graphique Web utilisant une architecture DSD écrivent simultanément dans un ou plusieurs serveurs d'affichage et un seul serveur maître ObjectServer. Ils lisent uniquement les données d'événement provenant des serveurs d'affichage. Pour configurer un environnement DSD, modifiez le fichier de configuration de source de données.

Référence associée:

«Référence ncwDataSourceDefinitions.xml», à la page 565
Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration `ncwDataSourceDefinitions.xml` se trouvant dans *REP_INSTALL_WEBGUI*`/etc/datasources`. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

Configuration de plusieurs sources de données

Pour récupérer des événements de plusieurs sources de données ou paires de reprise en ligne, ajoutez des sources de données supplémentaires au fichier de configuration.

Pourquoi et quand exécuter cette tâche

Par défaut, le fichier `ncwDataSourceDefinitions.xml` contient la source de données ou paire de reprise en ligne que vous avez spécifié pendant l'installation. Après avoir édité ce fichier, redémarrez le serveur pour que les modifications prennent effet.

Si vous souhaitez utiliser plusieurs sources de données ou paires de reprise en ligne, assurez-vous que toutes les sources de données contiennent des définitions de zone et des utilisateurs, groupes et droits d'accès cohérents.

Pour configurer l'interface graphique Web pour plusieurs sources de données :

Procédure

1. Ouvrez le fichier `ncwDataSourceDefinitions.xml`.
2. Recherchez l'élément <ncwDefaultDataSourceList>.
3. Pour ajouter une source de données, ajoutez un élément <ncwDataSourceEntry> en tant qu'enfant de <ncwDefaultDataSourceList>.

   Conseil : Pour les réseaux IPv6, utilisez des noms d'hôte au lieu d'adresses littérales. La première source de données définie dans l'élément <ncwDefaultDataSourceList> est la source de données par défaut.
   Un fichier de configuration de source de données avec deux sources de données définies est illustré dans l'exemple suivant :

   ```
   <ncwDefaultDataSourceList>
     <ncwDataSourceEntry name="NCOMS"/>
     <ncwDataSourceEntry name="NILKA"/>
   </ncwDefaultDataSourceList>
   ```

   Où *NCOMS* est le nom de la source de données définie pendant l'installation et *NILKA* est le nom de la source de données supplémentaire. Les noms peuvent contenir jusqu'à 29 caractères.
4. Pour définir la source de données ajoutée à l'étape 3 :
   a. Ajoutez un nouvel élément <ncwDataSourceDefinition> ainsi que des éléments enfant.
   b. Définissez l'attribut `type` de l'élément <ncwDataSourceDefinition> sur «singleServerOSDataSource».
   c. Pour définir une source de données supplémentaire comme paire de reprise en ligne, définissez la source de données de secours en ajoutant le code suivant sous l'élément final </ncwPrimaryServer> :

```
<ncwBackUpServer>
      <ncwOSConnection host="hôte" port="port"/>
</ncwBackUpServer>
```

Où *hôte* est le nom d'hôte du serveur ObjectServer de secours et *port* est le numéro de port.

5. Enregistrez et fermez le fichier.
6. Redémarrez le serveur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Référence associée:

«Référence ncwDataSourceDefinitions.xml», à la page 565
Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration `ncwDataSourceDefinitions.xml` se trouvant dans *REP_INSTALL_WEBGUI*`/etc/datasources`. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

«Présentation du fichier de configuration de la source de données», à la page 553
Le fichier `ncwDataSourceDefinitions.xml` contrôle les définitions de source de données, les connexions, la reprise en ligne, la surveillance automatique et le nettoyage de la mémoire cache. A la suite d'une nouvelle installation et de la configuration initiale, ce fichier contient uniquement les informations que vous avez spécifiées dans l'Outil de configuration de l'interface graphique Web OMNIbus. A la suite d'une mise à niveau, les éléments sont migrés afin d'être compatibles avec la version en cours du produit.

Configuration d'un environnement de bureau à deux serveurs

Le bureau à deux serveurs (DSD) est une architecture de traitement d'événement tierce. Les installations d'Interface graphique Web utilisant une architecture DSD écrivent simultanément dans un ou plusieurs serveurs d'affichage et un seul serveur maître ObjectServer. Ils lisent uniquement les données d'événement provenant des serveurs d'affichage. Pour configurer un environnement DSD, modifiez le fichier de configuration de source de données.

Pourquoi et quand exécuter cette tâche

L'architecture DSD améliore les performances d'un serveur ObjectServer qui est soumis fréquemment à de lourdes charges. De lourdes charges peuvent se produire si plusieurs serveurs ObjectServer envoient des alertes à un serveur ObjectServer central via des passerelles unidirectionnelles ou si plusieurs utilisateurs se connectent directement au serveur ObjectServer central via l'Interface graphique Web ou les lises d'événements de bureau. Une configuration du serveur ObjectServer DSD réduit la charge de travail du serveur ObjectServer central en transférant la charge à des serveurs ObjectServer d'affichage. Les clients d'Interface graphique Web ne voient aucune différence entre le fait d'être connecté au serveur ObjectServer central ou à un serveur ObjectServer d'affichage. Les actions utilisateur sur l'Interface graphique Web sont envoyées simultanément aux serveurs ObjectServer central et d'affichage.

Le serveur d'affichage des pages contenant des listes d'événements ou des cartes est statique pendant toute la durée de la session et est sélectionné lorsqu'un utilisateur se connecte.

Restriction : L'harmonisation absolue des données entre deux ou plusieurs serveurs d'affichage est impossible. Plus la granularité et l'échelle des charges entre les serveurs d'affichage sont élevées, plus la probabilité de disparité des événements au cours du cycle d'équilibrage de charges est grande, même s'il y a peu de chances que les disparités se produisent. Cette remarque ne s'applique pas aux AEL et aux LEL, car un seul serveur d'affichage est utilisé au cours d'une session d'AEL ou de LEL.

Pour configurer un environnement DSD :

Procédure

1. Ouvrez le fichier *WEBGUI_HOME*/etc/datasources/ncwDataSourceDefinitions.xml et recherchez l'élément <ncwDefaultDataSourceList>.
2. Ajoutez toutes les sources de données requises comme éléments <ncwDataSourceEntry> en tant qu'enfant de <ncwDefaultDataSourceList>.

   Conseil : Pour les réseaux IPv6, utilisez des noms d'hôte au lieu d'adresses littérales. La première source de données définie dans l'élément <ncwDefaultDataSourceList> est la source de données par défaut.
   Par exemple :

   ```
   <ncwDefaultDataSourceList>
        <ncwDataSourceEntry name="source_données_défaut_1"/>
        <ncwDataSourceEntry name="source_données2"/>
        <ncwDataSourceEntry name="source_données3"/>
   </ncwDefaultDataSourceList>
   ```
3. Définissez les sources de données ajoutées à l'étape 2 en ajoutant des éléments <ncwDataSourceDefinition> et des éléments enfant pour chaque source de données.
4. Définissez la source de données de sauvegarde en ajoutant le code suivant sous l'élément de fermeture </ncwPrimaryServer> :

   ```
   <ncwBackUpServer>
         <ncwOSConnection host="hôte" port="port"/>
   </ncwBackUpServer>
   ```

   Où *hôte* est le nom d'hôte du serveur ObjectServer de secours et *port* est le numéro de port.
5. Pour configurer une source de données pour DSD, procédez comme suit :
   a. Définissez l'attribut type de l'élément <ncwDataSourceDefinition> sur «multipleServerOSDataSource».
   b. Définissez les serveurs d'affichage en ajoutant l'élément <ncwReadCloudDefinition> sous l'élément </ncwFailOverPairDefinition> de fermeture. Vous y définissez l'hôte et le port des serveurs d'affichage. Dans l'élément <ncwReadCloudDefinition>, définissez chaque serveur d'affichage dans un élément <ncwOSConnection>. Par exemple :

      ```
      <ncwReadCloudDefinition>
                    <ncwOSConnection host="192.168.0.9" port="4747"/>
                    <ncwOSConnection host="192.168.0.10" port="4848"/>
                    <ncwOSConnection host="192.168.0.11" port="4949"/>
      </ncwReadCloudDefinition>
      ```

      Un élément <ncwReadCloudDefinition> est autorisé par source de données. Plusieurs nuages de serveurs d'affichage ne peuvent pas communiquer avec un même serveur maître ObjectServer.
6. Enregistrez et fermez le fichier.
7. Redémarrez le serveur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Référence associée:

«Référence ncwDataSourceDefinitions.xml»
Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration `ncwDataSourceDefinitions.xml` se trouvant dans *REP_INSTALL_WEBGUI*`/etc/datasources`. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

«Présentation du fichier de configuration de la source de données», à la page 553
Le fichier `ncwDataSourceDefinitions.xml` contrôle les définitions de source de données, les connexions, la reprise en ligne, la surveillance automatique et le nettoyage de la mémoire cache. A la suite d'une nouvelle installation et de la configuration initiale, ce fichier contient uniquement les informations que vous avez spécifiées dans l'Outil de configuration de l'interface graphique Web OMNIbus. A la suite d'une mise à niveau, les éléments sont migrés afin d'être compatibles avec la version en cours du produit.

Référence ncwDataSourceDefinitions.xml

Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration `ncwDataSourceDefinitions.xml` se trouvant dans *REP_INSTALL_WEBGUI*`/etc/datasources`. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

Le terme *source de données* désigne toute source de données à partir de laquelle l'Interface graphique Web peut obtenir des informations sur les événements. Il inclut, sans s'y limiter, les serveurs ObjectServer.

Types de données et légendes

Les types de données et les légendes qui accompagnent les éléments et attributs de DTD de l'interface graphique Web sont les suivants :

NM Indique que les types d'attribut sont des noms composés de caractères XML NMTOKEN (lettres, points, nombres, traits de soulignement, tirets et deux-points). NM indique généralement que l'attribut contient une liste de sélections prédéfinies.

CDATA
Indique que l'attribut contient des données de type caractères non analysées.

IMP Indique que la présence de l'attribut est implicite (facultative).

REQ Indique que la présence de l'attribut est obligatoire.

Eléments de la DTD de configuration de l'Interface graphique Web :

Eléments spécifiés dans la DTD de configuration de l'Interface graphique Web.

Les éléments définis dans la DTD de configuration sont les suivants.

<chart>
Elément enfant de l'élément <results-cache>. Cet élément définit les options de mise en cache pour les résultats de graphique. Si la mise en cache est activée, l'attribut maxAge spécifie le délai d'expiration, en secondes, du cache. L'attribut cleantime spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<config>
Elément enfant de l'élément <results-cache>. Cet élément spécifie si la mise en cache des données est activée. Si la mise en cache est activée, l'attribut maxAge spécifie le délai d'expiration, en secondes, du cache. Par exemple :

```
<config maxAge="60" enabled="true">
```

<eventList>
Elément enfant de l'élément <results-cache>. Cet élément définit la mise en cache des résultats de la liste d'événements. Si la mise en cache est activée, l'attribut maxAge spécifie le délai d'expiration, en secondes, du cache. L'attribut cleantime spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<eventSummary>
Elément enfant de l'élément <results-cache>. Cet élément spécifie la mise en cache des résultats de récapitulatif d'événement, comme les cartes et les Tableaux de bord des événements. Si la mise en cache est activée, l'attribut maxAge spécifie le délai d'expiration, en secondes, du cache. L'attribut cleantime spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<metric>
Elément enfant de l'élément <results-cache>. Cet élément définit la mise en cache des résultats dans les pages Jauges. Si la mise en cache est activée, l'attribut maxAge spécifie le délai d'expiration, en secondes, du cache. L'attribut cleantime spécifie l'intervalle, en secondes, de vérification et de suppression des entrées en cache. Les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées.

<ncwBackUpServer>

Cet élément est un élément enfant de <ncwDefaultDataSourceList> et contient l'élément ncwOSConnection qui spécifie l'hôte et le port du serveur ObjectServer de reprise en ligne. Par exemple :

```
<ncwBackUpServer>
   <ncwOSConnection
    host="192.168.0.3"
    port="4141"
   />
</ncwBackUpServer>
```

<ncwConnectionParameters>
Cet élément est un élément enfant de <ncwDataSourceDefinition> et contient des éléments contrôlant la connexion à une source de données.

<ncwDataSourceCredentials>
Cet élément est un élément enfant de <ncwDataSourceDefinition> et contient les informations de connexion requises par l'Interface graphique Web pour accéder à la source de données. Si l'attribut "encrypted" est défini sur `true`, un mot de passe chiffré à l'aide de l'utilitaire de chiffrement **nco_g_crypt** de Tivoli Netcool/OMNIbus peut être utilisé. Par exemple :

```
<ncwDataSourceCredentials
 password=""
 userName="root"
 encrypted="false"
/>
```

<ncwDataSourceDefinition>
Cet élément est un élément enfant de <ncwDataSourceDefinitions> qui contient les balises qui définissent les paramètres de configuration et de communication pour une source de données individuelle.

<ncwDataSourceDefinitions>
Il s'agit de l'élément root de la DTD.

<ncwDataSourceEntry>
Cet élément est un élément enfant de <ncwDefaultDataSourceList> qui contient les noms des sources de données par défaut qui communiquent avec l'Interface graphique Web. Ces entrées sont définies ultérieurement dans le fichier de configuration à l'aide des balises <ncwDataSourceDefinition> correspondantes. La première entrée de la liste est la source de données par défaut utilisée par l'Interface graphique Web pour l'authentification client. Si cette source de données n'est pas présente, la prochaine entrée de la liste sera utilisée comme source par défaut. Par exemple :

```
<ncwDefaultDataSourceList>
   <ncwDataSourceEntry name="NCOMS"/>
   <ncwDataSourceEntry name="NILKA"/>
</ncwDefaultDataSourceList>
```

Remarque : Le nom de chaque source de données peut contenir jusqu'à 29 caractères.

<ncwDataSourcePollingParameters>
Cet élément est un élément enfant de <ncwDataSourceDefinition> qui contient les éléments qui contrôlent l'interrogation de la reprise en ligne et du signal de présence de source de données.

<ncwDefaultDataSourceList>
Voir <ncwDataSourceEntry>.

<ncwFailOverPairDefinition>
Cet élément est un élément enfant de <ncwDataSourceDefinition> qui contient les balises qui spécifient les serveurs ObjectServer principal et de sauvegarde. L'inclusion d'un serveur ObjectServer de sauvegarde est facultative (toutefois un seul serveur de sauvegarde est autorisé par source de données). Par exemple :

```
<ncwFailOverPairDefinition>
   <ncwPrimaryServer>
      <ncwOSConnection
       host="192.168.0.7"
       port="4545"
      />
   </ncwPrimaryServer>
   <ncwBackUpServer>
      <ncwOSConnection
       host="192.168.0.8"
```

```
        port="4646"
       />
    </ncwBackUpServer>
</ncwFailOverPairDefinition>
```

<ncwFailOverPollingParameters>

Cet élément spécifie l'intervalle au bout duquel la source de données est interrogée en cas de reprise en ligne. Cet élément est uniquement utilisé lorsqu'un serveur de reprise en ligne est disponible, comme défini par l'élément <ncwBackUpServer>. Par exemple :

```
<ncwFailOverPollingParameters
backOffMultiplier="2" basePollingTime="10"/>
```

<ncwHeartBeatParameters>

Cet élément est un élément enfant de <ncwDataSourcePollingParameters> qui spécifie l'intervalle de temps, en secondes, au bout duquel l'Interface graphique Web interroge une source de données active. Par exemple :

```
<ncwHeartBeatParameters basePollingTime="15"/>
```

<ncwOSConnection>

Cet élément est un élément enfant de <ncwPrimaryServer> et de <ncwBackUpServer> qui spécifie les critères de communication pour une source de données principale ou de reprise en ligne. Par exemple :

```
<ncwOSConnection host="192.168.0.3" port="4141"/>
```

<ncwPrimaryServer>

Cet élément est un élément enfant de <ncwDefaultDataSourceList> et contient l'élément ncwOSConnection qui spécifie l'hôte et le port du serveur ObjectServer principal. Par exemple :

```
<ncwPrimaryServer>
   <ncwOSConnection
    host="192.168.0.3"
    port="4141"
   />
</ncwPrimaryServer>
```

<ncwQueryTimeout>

Cet élément est un élément enfant de <ncwStatementParameters> et définit la période de dépassement de délai, en secondes, des instructions SQL envoyées à une source de données. Par exemple :

```
<ncwQueryTimeout baseTime="60" />
```

<ncwReadCloudDefinition>

Cet élément est l'élément enfant de <ncwDataSourceDefinition> qui contient les adresses de tous les serveurs d'affichage que vous souhaitez utiliser avec cet ObjectServer maître. Un élément <ncwReadCloudDefinition> est autorisé par source de données. Plusieurs serveurs d'affichage ne peuvent communiquer avec un même ObjectServer maître. Par exemple :

```
<ncwReadCloudDefinition>
   <ncwOSConnection
    host="192.168.0.9"
    port="4747"
   />
   <ncwOSConnection
    host="192.168.0.10"
    port="4848"
   />
   <ncwOSConnection
   host="192.168.0.11"
   port="4949"
   />
</ncwReadCloudDefinition>
```

<ncwStatementParameters>
Cet élément est un élément enfant de <ncwConnectionParameters> et contient des élément contrôlant l'échange d'instructions SQL avec une source de données.

<results-cache>

L'élément <results-cache> est un élément enfant de l'élément <ncwDataSourceDefinition>. Il contient les éléments enfant <chart>, <config>, <eventList>, <eventSummary> et <metric>.

<self-monitoring>
Elément enfant de <ncwDataSourceDefinition>. Il active la fonctionnalité de surveillance automatique. La surveillance automatique enregistre les statistiques relatives à votre environnement d'Interface graphique Web et émet des événements de surveillance automatique dans la source de données principale.

<service>
Cet élément est un enfant de l'élément <self-monitoring>. Un élément <self-monitoring> peut comporter plusieurs éléments enfant <service>. Cet élément active la surveillance automatique pour un service et indique le nom du service surveillé. Les noms des services ne peuvent pas être modifiés. Pour les noms des services, voir «Présentation du fichier de configuration de la source de données», à la page 553. Cet élément indique également si les événements d'information de surveillance, qui fournissent un récapitulatif du service surveillé, sont émis et si ces événements sont dédoublonnés.

<threshold>
Cet élément est un enfant de l'élément <service>. Un élément <service> peut comporter plusieurs éléments enfant <threshold>. Cet élément définit la valeur d'un seuil qui doit être atteinte avant qu'un événement soit émis pour le service. Il définit également la gravité de l'événement.

Attributs de la DTD de configuration de l'Interface graphique Web :

Attributs utilisés dans la DTD de configuration de l'Interface graphique Web. Certains attributs sont énumérés et les valeurs de ces attributs sont limitées à une liste de chaînes de texte prédéfinies. Lorsque des attributs énumérés sont utilisés dans le fichier de commandes XML, les attributs doivent utiliser l'une de ces valeurs.

Le tableau ci-dessous décrit chaque attribut défini dans la DTD de configuration ainsi que les valeurs par défaut, le cas échéant.

Tableau 89. Définitions des attributs de la DTD de configuration

Attribut	Valeurs contraintes	Description
algorithm	AES | FIPS	Indique si un algorithme AES ou FIPS 140-2 est utilisé.
backOffMultiplier	Aucun	Multiplicateur de l'algorithme backoff utilisé pour calculer le délai de temporisation de l'interrogation au cours d'une reprise en ligne. Default 1

Tableau 89. Définitions des attributs de la DTD de configuration (suite)

Attribut	Valeurs contraintes	Description
basePollingTime	Aucun	Délai de démarrage, en secondes, de l'algorithme utilisé pour calculer le délai de temporisation de l'interrogation au cours d'une reprise en ligne. Default `20` pour l'élément <ncwFailoverPollingParameters> et `15` pour l'élément <ncwHeartbeatParameters>.
baseTime	Aucun	Délai d'attente, en secondes, pour l'envoi d'une instruction de requête envoyée à la source de données. Si aucune réponse n'est reçue dans ce délai, l'Interface graphique Web tente de se reconnecter. Default `30`
cleantime	Aucun	Intervalle de temps, en secondes, au cours duquel l'Interface graphique Web attend avant de vérifier la durée pendant laquelle chaque session utilisateur a été inactive. Lorsque cette vérification a lieu, les données du cache qui dépassent la durée imposée par l'attribut maxAge sont supprimées. Default `120` pour les éléments <chart> et <eventList> et `20` pour les éléments <eventSummary> et <metric>.
deduplicateInfo	`true|false`	Indique si les messages d'information, qui sont contrôlés par l'attribut info pour un service, sont dédoublonnés. Default `false`
enabled	`true|false`	Pour la mise en cache, spécifie si la mise en cache de page est activée ou désactivée. Default `TRUE` pour les éléments <ncwDataSourceDefinition>, <eventSummary> et <metric>, et `FALSE` pour les éléments <chart> et <eventList>. Pour la surveillance automatique, indique si un service est activé. Default `FALSE`

Tableau 89. Définitions des attributs de la DTD de configuration (suite)

Attribut	Valeurs contraintes	Description
encrypted	`true|false`	Spécifie si le mot de passe de l'utilisateur est chiffré. Default `false`
granularity	Aucun	Indique la fréquence, en secondes, à laquelle les événements de surveillance automatique sont émis dans la source de données. Default `60`
host	Aucun	Nom d'hôte ou adresse IP d'une source de données.
info	`true|false`	Indique si les messages d'information, qui contiennent un récapitulatif du service surveillé, sont émis si la surveillance automatique est activée pour ce service. Default `false`
maxAge	Aucun	Heure d'expiration de la mémoire cache en secondes. Default `10` pour les éléments <eventSummary> et <metric>, `60` pour les éléments <chart> et <eventList> et `3600` pour l'élément <config>.
maxPoolSize	Valeur maximale : `1024`	Nombre maximal des connexions en pool vers une source de données pouvant exister simultanément. Default `10`
moniteur	Aucun	Indique si la surveillance automatique est activée pour un service. Default `false`
minPoolSize	Aucun	Nombre minimal des connexions en pool à conserver vers une source de données. Default `5`

Tableau 89. Définitions des attributs de la DTD de configuration (suite)

Attribut	Valeurs contraintes	Description
name	Aucun	• Nom d'une source de données. Si la source de données est un serveur ObjectServer, il n'est pas nécessaire que le nom soit identique au nom d'un serveur ObjectServer figurant dans le fichier de connexions de données `omni.dat`. Ce nom peut contenir un maximum de 29 caractères. Cette valeur lie chaque définition de source de données répertoriée au début du fichier de configuration à sa définition sous-jacente. • Cet attribut peut également spécifier le nom d'un service pour la surveillance automatique. Ne modifiez pas la valeur de cet attribut.
mot de passe	Aucun	Mot de passe utilisé pour se connecter au serveur ObjectServer. Default Mot de passe à blanc
port	Aucun	Numéro de port d'une source de données spécifiée. Default `8080`
gravité	Aucun	Gravité de l'événement qui est émis lorsqu'une valeur de seuil est atteinte, si la surveillance automatique est activée.
ssl	`true|false`	Indique si la communication SSL est utilisée pour la connexion à la source de données. Default `false`
type	`singleServerOS DataSource| multipleServerOS DataSource`	Type de la configuration de source de données. • `singleServerOSDataSource` : pour une configuration de source de données principale unique ou pour une configuration de source de données de secours. • `multipleServerOSDataSource` : Pour une configuration de bureau à deux serveurs. Default `singleServerOSDataSource`
userName	Aucun	Nom d'utilisateur de l'utilisateur qui se connecte au serveur ObjectServer. L'utilisateur doit disposer des droits d'accès root au serveur ObjectServer. Default `root`

Tableau 89. Définitions des attributs de la DTD de configuration (suite)

Attribut	Valeurs contraintes	Description
value	Aucun	Valeur d'un seuil qui doit être atteinte avant qu'un événement soit émis, si la surveillance automatique est activée.

Configuration de variables d'environnement pour les graphiques

Sous les systèmes d'exploitation AIX et HP-UX, définissez la variable d'environnement de façon à ce que les graphiques de l'Interface graphique Web s'affichent correctement.

Procédure

Pour vous assurer que les graphiques s'affichent correctement, définissez la variable d'environnement DISPLAY sur l'hôte exécutant le serveur X Windows.

Configuration et gestion de l'authentification unique

Comment configurer et gérer la fonction d'authentification unique entre l'Interface graphique Web et les autres produits Tivoli.

Authentification unique

L'authentification unique (SSO) est prise en charge par les produits Tivoli. Lorsque les utilisateurs se connectent à une application dans un environnement SSO, les informations d'identification utilisateur sont autorisées dans un référentiel central des utilisateurs. Ce référentiel peut être Tivoli Netcool/OMNIbus ObjectServer ou un répertoire LDAP. Après autorisation des informations d'identification utilisateur, les utilisateurs peuvent lancer des applications. L'authentification unique est prise en charge dans des environnements qui sont hébergés dans des serveurs Jazz for Service Management sur plusieurs hôtes, ou un seul hôte.

Pour participer à un environnement d'authentification unique, vérifiez que les produits utilisent authentification LTPA (Lightweight Third Party Authentication) (LTPA) comme mécanisme d'authentification. Après l'activation de l'authentification unique, un cookie est créé, qui contient le jeton LTPA. Le cookie est inséré dans la réponse HTTP. Lorsque les utilisateurs accèdent aux ressources, telles que des portlets ou widgets, dans d'autres applications qui sont dans le même domaine Domain Name Service (DNS), le cookie est envoyé avec la demande. Le jeton LTPA est alors extrait du cookie puis validé. Si la demande est effectuée entre différentes cellules de serveurs d'applications, partagez les clés LTPA et le registre d'utilisateurs entre ces cellules pour que l'authentification unique fonctionne. Les noms de domaine sur chaque système dans le domaine SSO sont sensibles à la casse et doivent rigoureusement correspondre. Pour plus d'informations, voir *Authentification LTPA (Lightweight Third Party Authentication)* et *Gestion des clés LTPA à partir de plusieurs cellules WebSphere Application Serve* dans le centre de documentation de WebSphere Application Server.

Concepts associés:

Authentification LTPA (Lightweight Third Party Authentication)

«Intégration à d'autres produits Tivoli», à la page 62
Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

Authentification LTPA (Lightweight Third Party Authentication)

Tâches associées:

«Configuration de l'authentification unique (SSO)», à la page 576
Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

Gestion des clés LTPA à partir de plusieurs cellules WebSphere Application Server

«Configuration d'intégrations de lancement en contexte dans les produits Tivoli», à la page 591
Vous pouvez configurer l'Interface graphique Web pour qu'elle démarre dans des produits Tivoli compatibles.

Configuration de l'authentification unique à l'aide du sous-système de sécurité avancée entre plusieurs serveurs

Comment configurer l'authentification unique entre plusieurs serveurs.

Avant de commencer

Avant de configurer l'authentification unique entre un certain nombre de serveurs, tous doivent pointer vers un registre d'utilisateurs central, par exemple, le serveur LDAP.

Procédure

Pour configurer l'authentification unique entre un certain nombre de serveurs, procédez comme suit :

1. Sur le serveur exécutant l'Interface graphique Web :
   a. Configurez l'authentification unique.
   b. Redémarrez le serveur.
   c. Exportez les clés LPTA à partir de WebSphere.
2. Sur chacun des autres serveurs :
   a. Copiez le fichier de clés exportées à partir du serveur de l'Interface graphique Web.
   b. Configurez l'authentification unique.
   c. Importez les clés LTPA dans WebSphere Application Server et dans le sous-système de sécurité avancée. Puis, redémarrez le serveur.

Tâches associées:

«Configuration de l'authentification unique (SSO)», à la page 576
Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

«Exportation des clés LTPA», à la page 577
Comment exporter les clés LTPA à partir de WebSphere Application Server.

«Importation des clés LTPA», à la page 577
Comment importer les clés LTPA dans WebSphere Application Server et ESS. Chaque composant conserve sa propre copie des clés et doit être synchronisé.

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Gestion des clés LTPA

Si les clés LTPA changent pour WebSphere sur le serveur de l'Interface graphique Web, exportez les clés et chargez-les dans le sous-système de sécurité avancée local. En outre, chargez-les dans WebSphere et dans le sous-système de sécurité avancée sur tous les autres serveurs participants.

Pourquoi et quand exécuter cette tâche

Etant donné que WebSphere et le sous-système de sécurité avancée possèdent leur propre copie des clés LTPA, ils doivent rester synchronisés. Si les clés changent sur le serveur de l'Interface graphique Web, vous devez les importer vers le sous-système de sécurité avancée de ce serveur. En outre, importez-les dans WebSphere et dans le sous-système de sécurité avancée sur tous les autres serveurs qui coopèrent dans le domaine d'authentification unique.

Procédure

Lorsque les clés LTPA pour WebSphere sur l'Interface graphique Web changent, procédez comme suit :

1. Sur le serveur exécutant l'Interface graphique Web :
   a. Exportez les clés LTPA à partir de WebSphere.
   b. Importez les clés dans le sous-système de sécurité avancée.
   c. Redémarrez le serveur.
2. Sur chacun des autres serveurs dans le domaine d'authentification unique :
   a. Copiez les fichiers des clés exportées depuis l'Interface graphique Web.
   b. Importez les clés LTPA dans WebSphere Application Server et dans le sous-système de sécurité avancée.
   c. Redémarrez le serveur.

Tâches associées:

«Exportation des clés LTPA», à la page 577
Comment exporter les clés LTPA à partir de WebSphere Application Server.

«Importation des clés LTPA», à la page 577
Comment importer les clés LTPA dans WebSphere Application Server et ESS. Chaque composant conserve sa propre copie des clés et doit être synchronisé.

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Prise en charge des procédures d'authentification unique

Procédures utilisées pour configurer et gérer l'authentification unique et les clés LTPA entre un certain nombre de serveurs.

Configuration de l'authentification unique (SSO) :

Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

Avant de commencer

La configuration de l'authentification unique est nécessaire avant intégration de produits déployés sur plusieurs serveurs. Toutes les instances du Jazz for Service Management doivent pointer sur le registre d'utilisateurs central (serveur protocole LDAP (Lightweight Directory Access Protocol), par exemple).

Avertissement : La prise en charge d'ITM Single Sign On (SSO) est uniquement disponible avec ITM Version 6.2 Fix Pack 1 ou supérieur.

Pourquoi et quand exécuter cette tâche

Pour configurer les fonctionnalités du référentiel fédéré WebSphere pour le serveur LDAP :

Procédure

1. Connectez vous à Jazz for Service Management.
2. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
3. Dans le panneau de navigation de la console d'administration WebSphere Application Server, cliquez sur **Security** > **Global security**.
4. Dans la zone **Authentification**, développez **Web Security (Sécurité Web)** et cliquez sur **Single sign-on (Authentification unique)**.
5. Si l'authentification unique est désactivée, cliquez sur l'option **Activée**.
6. S'il est prévu que toutes les demandes utilisent HTTPS, cliquez sur **Requires SSL (Nécessite SSL)**.
7. Dans la zone Nom de domaine, entrez les noms qualifiés complets des domaines pour lesquels l'authentification unique est effective. Si le nom de domaine n'est pas qualifié complet, Jazz for Service Management ne définit pas de valeur de nom de domaine pour le cookie **LtpaToken** et l'authentification unique n'est valide que pour le serveur qui a créé le cookie. Pour que l'authentification unique fonctionne entre différentes applications Tivoli, les serveurs de ces applications doivent être installés dans le même domaine (utilisez le même nom de domaine).
8. Facultatif : Activez l'option **Interoperability Mode (Mode d'interopérabilité)** si vous souhaitez que les connexions uniques aux versions 5.2.1 et supérieures de WebSphere Application Server interopèrent avec les précédentes versions du serveur.
9. Facultatif : Activez l'option **Web inbound security attribute (Propagation de l'attribut de sécurité des communications entrantes Web)** si vous voulez que les informations ajoutées lors de la connexion à un serveur Tivoli Enterprise Portal donné se propagent vers d'autres instances serveur d'applications.

10. Cliquez sur **OK** pour enregistrer vos modifications, puis arrêtez et redémarrez toutes les instances Jazz for Service Management.

Que faire ensuite

Remarque : Lorsque vous lancez Interface graphique Web, vous devez utiliser une adresse URL au format protocole://hôte.domaine:port /*. Si vous n'utilisez pas de nom de domaine qualifié complet, Interface graphique Web ne peut pas utiliser l'authentification unique entre les produits Tivoli.

Concepts associés:

«Authentification unique», à la page 573
L'authentification unique (SSO) est prise en charge par les produits Tivoli. Lorsque les utilisateurs se connectent à une application dans un environnement SSO, les informations d'identification utilisateur sont autorisées dans un référentiel central des utilisateurs. Ce référentiel peut être Tivoli Netcool/OMNIbus ObjectServer ou un répertoire LDAP. Après autorisation des informations d'identification utilisateur, les utilisateurs peuvent lancer des applications. L'authentification unique est prise en charge dans des environnements qui sont hébergés dans des serveurs Jazz for Service Management sur plusieurs hôtes, ou un seul hôte.

Tâches associées:

«Configuration d'intégrations de lancement en contexte dans les produits Tivoli», à la page 591
Vous pouvez configurer l'Interface graphique Web pour qu'elle démarre dans des produits Tivoli compatibles.

Exportation des clés LTPA :

Comment exporter les clés LTPA à partir de WebSphere Application Server.

Procédure

1. Lancez la console d'administration et cliquez sur **Sécurité** > **Sécurité globale**.
2. Dans la zone **Authentification**, cliquez sur **LTPA**.
3. Dans la zone **Authentification unique inter-cellules**, saisissez un mot de passe pour le fichier de clés dans **Mot de passe** et **Confirmer le mot de passe**.
4. Saisissez un nom pour le fichier de clés dans la zone **Nom de fichier de clés qualifié complet** et cliquez sur **Exporter les clés**. Le fichier de clés est créé dans *REP_INSTALL_JazzSM*. Un message de confirmation est affiché en haut de la console d'administration.

Importation des clés LTPA :

Comment importer les clés LTPA dans WebSphere Application Server et ESS. Chaque composant conserve sa propre copie des clés et doit être synchronisé.

Avant de commencer

Copiez le fichier de clés vers le serveur de destination. Placez le fichier dans *REP_INSTALL_JazzSM*.

Procédure

1. Pour importer les clés dans WebSphere Application Server :
   a. Lancez la console d'administration et cliquez sur **Sécurité** > **Sécurité globale**.

b. Dans la zone **Authentification**, cliquez sur **LTPA**.
c. Dans la zone **Authentification unique inter-cellules**, saisissez le mot de passe pour le fichier de clés dans **Mot de passe** et **Confirmer le mot de passe**.
d. Saisissez un nom pour le fichier de clés dans la zone **Nom de fichier de clés qualifié complet** et cliquez sur **Importer les clés**.

Le fichier de clés est importé dans WebSphere Application Server. Un message de confirmation est affiché en haut de la console d'administration Windows.

2. Pour importer les clés LTPA dans le sous-système de sécurité avancée, procédez comme suit :
   a. Dans l'interface de ligne de commande, accédez à *REP_INSTALL_JazzSM*/bin et exécutez l'utilitaire **wsadmin** pour votre système d'exploitation :
      - UNIX Linux `./wsadmin.sh`
      - Windows `wsadmin.bat`
   b. Lorsque vous y êtes invité, indiquez le nom d'utilisateur et le mot de passe de l'administrateur Concentrateur des services d'application du tableau de bord.
   c. Dans l'invite wsadmin>, saisissez la commande suivante :

```
$AdminTask importESSLTPAKeys
{-pathname /opt/IBM/JazzSM/profile/nom_fichier_clés
 -password mdp_fichier_clés}
```

   Remplacez :

   nom_fichier_clés
   Par le nom du fichier de clés LTPA.

   mdp_fichier_clés
   Par le mot de passe du fichier de clés LTPA.

   d. Quittez **wsadmin** en saisissant quit.
   a. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Surveillance automatique

La surveillance automatique de l'Interface graphique Web enregistre les statistiques relatives à la réactivité de la source de données, l'efficacité de la mémoire cache qui stocke des données d'événement et l'utilisation de la mémoire virtuelle Java (JVM).

Lorsque la surveillance automatique est activée, les statistiques du système sont périodiquement vérifiées. Si une violation de seuil est détectée, un événement est envoyé au serveur ObjectServer principal actuel qui est défini dans la source de données.

Tâches associées:

«Activation de la surveillance automatique», à la page 579
Vous pouvez configurer l'Interface graphique Web pour enregistrer les statistiques relatives à la réactivité de la source de données, l'efficacité de la mémoire cache qui stocke des données d'événement et l'utilisation de la mémoire virtuelle Java (JVM). Pour activer cette fonctionnalité de surveillance automatique, apportez des modifications aux définitions de source de données dans le fichier ncwDataSourceDefinitions.xml.

Activation de la surveillance automatique

Vous pouvez configurer l'Interface graphique Web pour enregistrer les statistiques relatives à la réactivité de la source de données, l'efficacité de la mémoire cache qui stocke des données d'événement et l'utilisation de la mémoire virtuelle Java (JVM). Pour activer cette fonctionnalité de surveillance automatique, apportez des modifications aux définitions de source de données dans le fichier `ncwDataSourceDefinitions.xml`.

Lorsque la surveillance automatique est activée, les statistiques du système sont périodiquement vérifiées. Si une violation de seuil est détectée, un événement est envoyé au serveur ObjectServer principal actuel qui est défini dans la source de données. Si des événements d'information sont configurées, un événement est émis dans la source de données pour chaque période de granularité. L'événement contient les statistiques qui ont été collectées pour le service système surveillé. Les services suivants sont surveillés :

- Commande de source de données
- Service de données d'événement
- Service de données récapitulatives d'événement
- Service de données métriques
- Référentiel d'utilisateurs et de sécurité
- Statistiques de la mémoire cache des résultats
- Utilisation de la mémoire virtuelle Java
- Virtual Member Manager

Lorsque les seuils de ces services sont dépassés, des événements de problème gravité dont la gravité est définie sont émis dans la source de données. Des seuils par défaut sont fournis. Le cas échéant, un événement d'information peut également être émis. Les événements sont systématiquement émis dans le serveur ObjectServer principal de la source de données. L'événement d'information contient un récapitulatif du service surveillé. Il comporte une gravité par défaut de 2 (Avertissement). La fréquence à laquelle les événements de problème et les événements d'information sont émis est contrôlée par un paramètre de période de granularité. Les événements d'information possèdent une valeur d'expiration configurable. Par défaut, cette période d'expiration correspond à la période de granularité, plus 30 secondes. La surveillance automatique est configurée séparément pour chaque service surveillé et pour chaque source de données.

Un exemple de fichier`ncwDataSourceDefinitions.xml` est disponible dans *REP_INSTALL_WEBGUI*`/dataources/samples`. Pour une explication des éléments contrôlant la surveillance automatique, voir «Présentation du fichier de configuration de la source de données», à la page 553.

Avant de commencer

Pour générer des événements d'autosurveillance, vous devez appliquer la personnalisation SQL avant de configurer l'autosurveillance. Cette configuration doit être effectuée pour un environnement autonome ou un environnement multiniveau. Pour plus d'informations à ce sujet et sur la création ou la modification des sources de données, allez à «Création ou modification de sources de données», à la page 548.

Procédure

- Faites une copie de sauvegarde de votre fichier `ncwDataSourceDefinitions.xml` actuel.

- Pour apporter les modifications à l'aide de de l'interface graphique, procédez comme suit :
  1. Dans la console Interface graphique Web, cliquez sur l'icône **Administration** et sélectionnez **Sources de données**.
  2. Cliquez sur **Modifier la source de données existante** ou **Créer une nouvelle source de données**.
  3. Dans l'onglet **Autosurveillance**, cochez la case **Activer l'autosurveillance** et modifiez les seuils et les gravités du service selon les besoins en utilisant les boutons de configuration de seuil appropriés.
  4. Cliquez sur **Sauvegarder la source de données**.
- Pour modifier manuellement le fichier xml, effectuez les étapes suivantes :
  1. Fusionnez les éléments <self-monitoring> à partir d'un des exemples de fichiers XML fournis avec votre fichier `ncwDataSourceDefinitions.xml`.
  2. Activez la surveillance automatique en définissant l'élément <self-monitoring> comme suit :
     ```
     <self-monitor enabled="false" granularity="300">
     ```
  3. Apportez les modifications nécessaires aux seuils et gravités du service. Ne modifiez pas les noms des services.
  4. Redémarrez le serveur.

Que faire ensuite

Les opérateurs peuvent désormais utiliser le tableau de bord Netcool Health. Les jauges situées dans la partie supérieure du tableau de bord représentent les services surveillés. Les événements émis lorsque les seuils sont atteints apparaissent dans l'afficheur d'événements situé dans la partie inférieure.

Référence associée:

«Présentation du fichier de configuration de la source de données», à la page 553
Le fichier `ncwDataSourceDefinitions.xml` contrôle les définitions de source de données, les connexions, la reprise en ligne, la surveillance automatique et le nettoyage de la mémoire cache. A la suite d'une nouvelle installation et de la configuration initiale, ce fichier contient uniquement les informations que vous avez spécifiées dans l'Outil de configuration de l'interface graphique Web OMNIbus. A la suite d'une mise à niveau, les éléments sont migrés afin d'être compatibles avec la version en cours du produit.

«Référence ncwDataSourceDefinitions.xml», à la page 565
Pour modifier les configurations contrôlant comment l'Interface graphique Web reçoit des événements des sources de données, modifiez le fichier de configuration `ncwDataSourceDefinitions.xml` se trouvant dans *`REP_INSTALL_WEBGUI`*`/etc/datasources`. La structure de fichier doit respecter le contenu de la DTD (définition de type de document) de configuration de l'interface graphique Web. Les éléments et les attributs se trouvant dans la DTD sont décrits ici.

tableau de bord Netcool Health

Le tableau de bord Netcool Health est un tableau de bord d'Interface graphique Web qui affiche des données de surveillance automatique Tivoli Netcool/OMNIbus.

Le tableau de bord est divisé en trois panneaux affichant des jauges d'état de santé de serveur ObjectServer, des jauges d'état de santé d'application et de client et des détails d'événement de surveillance automatique. Lorsqu'une jauge est sélectionnée dans les panneaux Netcool/OMNIbus ObjectServer Health ou Etat de santé des clients et applications Netcool, les événements de surveillance automatique associés s'affichent dans le panneau Evénements d'état.

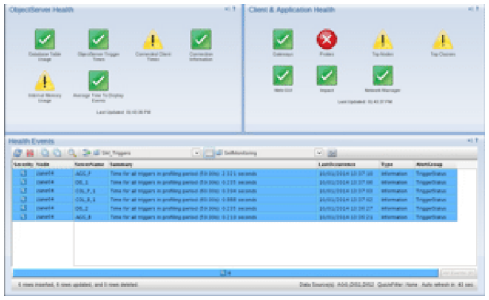

Figure 17. Tableau de bord Netcool Health

Les jauges d'état organisent les événements de surveillance automatique dans des groupes logiques. L'état de chaque jauge reflète l'événement dont la gravité est la plus élevée parmi tous les événements de ce groupe. Par exemple, si l'événement dont la gravité est la plus élevée dans le groupe est 2 (Avertissement), l'état de la jauge est Correct (vert). Si l'événement dont la gravité est la plus élevée dans le groupe est 5 (Critique), l'état de la jauge est Incorrect (rouge).

Les événements d'information sont générés à l'aide d'une gravité de 2 (Avertissement). Les événements d'alerte sont générés avec une gravité de 3 (Mineure), 4 (Majeure) ou 5 (Critique), en fonction de la valeur métrique surveillée.

Le tableau ci-dessous montre comment la gravité des événements de surveillance automatique est mappée vers les états de jauge d'état du tableau de bord.

Tableau 90. Mappages de jauge d'état de gravité d'événement

Etats de la jauge d'état	Gravité d'événement
Correct (vert)	0 (Aucune), 1 (Indéterminée) ou 2 (Avertissement)
Marginal (jaune)	3 (Mineure) ou 4 (Majeure)
Incorrect (rouge)	5 (Critique)

Référence associée:

«Etat de santé d'ObjectServer», à la page 582
Le panneau Netcool/OMNIbus ObjectServer Health dans le tableau de bord Netcool Health contient des jauges indiquant l'état de santé des composants ObjectServer.

«Etat de santé des clients et des applications», à la page 584
Le panneau Etat de santé des clients et applications Netcool du tableau de bord Netcool Health contient des jauges indiquant l'état de santé des clients et applications connectés au serveur ObjectServer.

Etat de santé d'ObjectServer :

Le panneau Netcool/OMNIbus ObjectServer Health dans le tableau de bord Netcool Health contient des jauges indiquant l'état de santé des composants ObjectServer.

Remarque : Dans un environnement multiniveau, définissez les jauges du panneau Netcool/OMNIbus ObjectServer Health de sorte qu'elles incluent la paire ObjectServer d'agrégation sous la forme d'une source de données et chaque ObjectServer de la couche d'affichage (s'il est présent) sous la forme d'une source de données distincte.

Les jauges d'état suivantes indiquent l'état de santé du serveur ObjectServer.

Utilisation de la table de base de données
Cette jauge affiche l'état du groupe d'événements `DBStatus`, qui fournit des informations sur les métriques de tables de base de données alerts.status, alerts.journal et alerts.details. Les événements `DBStatus` sont générés toutes les 5 minutes.

Les événements d'information signalent le nombre de lignes en cours de chaque table et le nombre d'insertions au cours des 5 dernières minutes. Pour chaque événement d'information, il existe une entrée correspondante dans la table master.sm_thresholds qui définit les seuils de métrique. Un événement d'alerte distinct est généré pour chaque métrique dépassée.

Remarque : Pour la table alerts.status, les réinsertions (également appelées «dédoublonnages») sont incluses dans le nombre d'insertions.

Si les nombres de lignes sont trop élevés, les performances peuvent être compromises. Si le nombre d'événements nouveaux, de journaux ou de détails créés au cours des 5 dernières minutes est élevé, il peut y avoir un problème de performances dans l'environnement surveillé.

Temps de déclencheur ObjectServer
Cette jauge affiche l'état du groupe d'événements `TriggerStatus`, qui fournit des informations relatives au temps total consommé par tous les déclencheurs ObjectServer. Le temps total est la même valeur que la ligne récapitulative dans le fichier journal des statistiques du déclencheur. A l'instar du fichier journal des statistiques du déclencheur, le déclencheur qui génère les événements `TriggerStatus` est activé lors du déclenchement du signal `profiler_report` (c-à-d toutes les 60 secondes par défaut).

L'événement d'information généré signale le temps consommé par l'exécution du déclencheur dans le serveur ObjectServer, ainsi que la durée de la période de profilage.

Un événement d'alerte est généré lorsque le temps total de tous les déclencheurs dépasse le seuil `sm_triggers_total` défini dans la table master.sm_thresholds. Un événement d'alerte distinct est également généré pour chaque déclencheur individuel dépassant le seuil `sm_triggers_individual`. Un troisième événement d'alerte est généré lorsque la période de profilage dépasse le seuil de profilage `sm_triggers_reporting_period`.

La période de profilage est généralement à moins d'une seconde de 60 secondes exactement. Une période de profilage plus longue indique clairement que le serveur ObjectServer est surchargé. Cette surcharge peut avoir plusieurs causes, notamment des déclencheurs à performances

médiocres, un nombre excessif d'événements dans le serveur ObjectServer et une surcharge créée par des clients externes. Etant donné que les opérations de lecture peuvent s'exécuter simultanément, les processus qui écrivent des opérations sont plus susceptibles de provoquer des charges élevées sur le serveur ObjectServer. Les déclencheurs du serveur ObjectServer s'exécutent à l'aide d'une seule unité d'exécution sur le serveur ObjectServer et sont souvent responsables des périodes de profilage prolongées.

Temps d'état des clients

Cette jauge affiche l'état du groupe d'événements `ClientStatus`, qui fournit des informations relatives au temps total consommé par tous les clients ObjectServer externes. Les clients externes sont notamment les sondes, les passerelles et les applications telles qu'IBM Tivoli Netcool/Impact et IBM Tivoli Network Manager. Tous les processus externes qui se connectent au serveur ObjectServer contribuent potentiellement à cette valeur de métrique.

Le déclencheur qui génère les événements `ClientStatus` est activé lors du déclenchement du signal `profiler_report` (c-à-d toutes les 60 secondes par défaut).

L'événement d'information généré signale le temps ObjectServer consommé par l'interaction des clients externes et indique également la période de granularité.

Un événement d'alerte est généré lorsque le temps total de tous les clients dépasse le seuil `sm_client_time_total` défini dans la table master.sm_thresholds. Un événement d'alerte distinct est généré pour chaque client dépassant le seuil `sm_client_time_individual` pour les temps de clients individuels.

Informations de connexion

Cette jauge affiche l'état du groupe d'événements `ConnectionStatus`, qui fournit des informations relatives aux sondes et passerelles connectées à chaque serveur ObjectServer. Elle fournit également des informations sur le nombre de connexions libres disponibles.

Les événements d'information de sonde et de passerelle sont réactualisés toutes les 60 secondes. Les événements de connexions libres sont réactualisés toutes les 5 minutes car la métrique est mise à jour dans la table master.stats une seule fois toutes les 5 minutes.

Un événement d'alerte est généré lorsque le nombre de connexions libres baisse sous le seuil `sm_connections_nodes` défini dans la table master.sm_thresholds.

Utilisation de la mémoire interne

Cette jauge affiche l'état du groupe d'événements `MemstoreStatus`, qui fournit des informations relatives à l'espace mémoire interne utilisé par le serveur ObjectServer. Le magasin de mémoire (memstore) du serveur ObjectServer correspond à l'espace mémoire utilisé pour stocker toutes les tables ObjectServer. La valeur par défaut est une limite souple de 450 Mo et une limite absolue de 500 Mo.

Les événements d'information sont réactualisés toutes les 60 secondes. Un événement d'alerte est généré lorsque le pourcentage de la limite souple du magasin de mémoire utilisé dépasse le seuil `sm_memstore` défini dans la table master.sm_thresholds.

Remarque : La taille totale du processus ObjectServer (**nco_objserv**) inclut le magasin de mémoire et toute autre mémoire allouée (par exemple, mémoire utilisée par le processus IDUC). Les valeurs de magasin de mémoire ne concordent généralement pas avec la taille de processus ObjectServer réelle et sont toujours inférieures.

Evénements de temps moyen d'affichage
Cette jauge affiche l'état des événements de temps d'affichage synthétiques générés sur les serveurs ObjectServer de la couche d'affichage. Les serveurs ObjectServer de la couche d'affichage génèrent automatiquement ces événements afin de permettre aux administrateurs de surveiller le temps moyen mis par les événements pour atteindre la couche d'affichage dans un environnement multiniveau.

Les événements de temps d'affichage sont réactualisés toutes les 60 secondes. La gravité des événements est mise à jour en fonction des seuils définis dans la table master.sm_thresholds.

Si une couche d'affichage n'est pas présente dans l'environnement, aucun événement n'est généré et l'état de la jauge est Correct (vert).

Référence associée:

«tableau de bord Netcool Health», à la page 581
Le tableau de bord Netcool Health est un tableau de bord d'Interface graphique Web qui affiche des données de surveillance automatique Tivoli Netcool/OMNIbus.

Etat de santé des clients et des applications :

Le panneau Etat de santé des clients et applications Netcool du tableau de bord Netcool Health contient des jauges indiquant l'état de santé des clients et applications connectés au serveur ObjectServer.

Les jauges d'état suivantes indiquent l'état de santé des clients et des applications qui sont connectés au serveur ObjectServer.

Etat de la sonde
Cette jauge affiche l'état du groupe d'événements `ProbeStatus`, qui fournit des informations relatives au nombre d'événements envoyés par chaque sonde déployée dans l'environnement.

Les événements d'information indiquent le nombre d'événements provenant de chaque sonde et générés toutes les 5 minutes.

Un événement d'alerte est généré lorsque le nombre d'événements provenant d'une sonde dépasse le seuil `sm_top_probes` défini dans la table master.sm_thresholds. Un nombre élevé d'événements provenant d'une sonde unique peut indiquer un problème et doit être signalé à votre équipe opérationnelle.

Si la propriété **ProbeWatchHeartbeatInterval** est activée dans un fichier de propriétés de sonde, les événements de pulsation sont inclus dans le groupe d'événements. La fréquence de pulsation par défaut (et recommandée) est de 60 secondes. Les événements de pulsation non mis à jour depuis plus de 3 minutes sont transférés au niveau de gravité 3 (Mineure). La zone Récapitulatif des événements est également mise à jour pour afficher le nombre de minutes écoulé depuis la réception du dernier événement de pulsation à partir de cette sonde spécifique, pour cet ID processus (PID).

Remarque : Si une sonde est redémarrée, un nouveau PID lui est probablement affecté par le système d'exploitation. Cette action entraîne la génération d'un événement d'alerte de pulsation pour l'ID processus de sonde d'origine. Après avoir vérifié que la sonde est en cours d'exécution, un administrateur peut effacer ces événements en toute sécurité.

Noeuds supérieurs

Cette jauge affiche l'état du groupe d'événements `TopNodes`. Ce groupe fournit des informations sur le nombre d'événements reçus de chaque nœud dans l'environnement surveillé au cours des 5 dernières minutes.

Les événements d'information indiquent le nombre d'événements provenant de chaque nœud et générés toutes les 5 minutes.

Un événement d'alerte est généré lorsque le nombre d'événements provenant d'un nœud dépasse le seuil `sm_top_nodes` défini dans la table master.sm_thresholds. Un nombre élevé d'événements provenant d'un nœud unique peut indiquer un problème et doit être signalé à votre équipe opérationnelle.

Classes supérieures

Cette jauge affiche l'état du groupe d'événements `TopClasses`. Ce groupe fournit des informations sur le nombre d'événements reçus de chaque classe dans l'environnement surveillé au cours des 5 dernières minutes.

Les événements d'information indiquent le nombre d'événements provenant de chaque classe et générés toutes les 5 minutes.

Un événement d'alerte est généré lorsque le nombre d'événements provenant d'une classe dépasse le seuil `sm_top_classes` défini dans la table master.sm_thresholds.

Pour la plupart des sondes, la classe est synonyme de la sonde, de sorte que l'état signalé par cette jauge est identique aux informations signalées par la jauge Etat de la sonde. Cependant, pour les sondes génériques telles que la sonde SNMP (**`nco_p_mttrapd`**), des événements de nombreuses classes différentes peuvent être reçus via la même sonde. En outre, il se peut que plusieurs sondes générant des événements de la même classe soient présentes dans l'environnement. Un aperçu rapide du total collectif par classe peut fournir des informations précieuses sur les problèmes potentiels.

Remarque : Les événements d'information de Classe supérieure provenant de la couche Collection ne peuvent pas être visualisés à l'aide d'un filtre de valeur Classe de 99999.

Etat de la passerelle

Cette jauge affiche l'état des passerelles ObjectServer dans l'environnement. Ce groupe d'événements contient des événements ConnectionWatch qui sont générés lorsque les passerelles se connectent au serveur ObjectServer et se déconnectent de celui-ci. Il contient également des événements générés chaque fois qu'une passerelle termine son processus de resynchronisation.

Remarque : Un événement de resynchronisation de passerelle est utile pour un administrateur car il informe qu'une passerelle a perdu sa connexion et qu'elle s'est ensuite reconnectée. Il confirme également que la passerelle s'est reconnectée correctement, a été resynchronisée avec succès et est de nouveau en service.

Les événements ConnectionWatch de la passerelle sont conservés indéfiniment mais sont effacés lorsque la passerelle se reconnecte avec succès. Les événements de resynchronisation de passerelle sont conservés pendant 24 heures afin de permettre à un administrateur de vérifier si, par exemple, une passerelle a rencontré des problèmes au milieu de la nuit.

Etat de l'interface graphique Web

Cette jauge affiche l'état des instances d'Interface graphique Web déployées dans l'environnement. Les événements sont filtrés sur `AlertGroup = 'WebGUI Status'`. Les serveurs d'Interface graphique Web peuvent être configurés de sorte qu'ils envoient des événements de surveillance automatique à une ou plusieurs sources de données. Ce paramètre est configuré dans le fichier de définition de source de données de l'Interface graphique Web.

Les événements de surveillance automatique de l'Interface graphique Web sont générés par défaut toutes les 60 secondes. Cette valeur peut être personnalisée dans le fichier de définition de source de données.

La surveillance automatique d'Interface graphique Web couvre plusieurs indicateurs clés de performances qui intéressent les administrateurs Netcool, y compris l'état de la source de données, le temps de réponse de la source de données et l'utilisation de la mémoire de la machine JVM de l'Interface graphique Web.

Les événements de surveillance automatique de l'Interface graphique Web sont générés de manière cohérente avec les événements de surveillance automatique Netcool/OMNIbus, en ce sens que les événements d'information ont une gravité de 2 (Avertissement) et les événements d'alerte sont générés en sus des événements d'information. Les deux types d'événement sont dédoublonnés par défaut, mais le dédoublonnage peut être désactivé pour les événements d'information. A l'instar des événements de surveillance automatique Netcool/OMNIbus, la valeur de métrique est stockée dans la zone Grade.

Les événements d'information arrivent à expiration après la fréquence à laquelle ils sont générés plus 30 secondes. Les événements d'alerte sont conservés pendant 24 heures.

Netcool/Impact

Si IBM Tivoli Netcool/Impact est présent dans l'environnement et que la surveillance automatique est activée, cette jauge affiche l'état de Netcool/Impact. Les événements sont filtrés sur `Class = 10500`.

Si Netcool/Impact n'est pas présent dans l'environnement, aucun événement n'est généré et l'état de la jauge est Correct (vert).

Network Manager

Si IBM Tivoli Network Manager est présent dans l'environnement et que la surveillance automatique est activée, cette jauge affiche l'état de Network Manager. Les événements sont filtrés sur `AlertGroup = 'ITNM Status'`.

Si Network Manager n'est pas présent dans l'environnement, aucun événement n'est généré et l'état de la jauge est Correct (vert).

Référence associée:

«tableau de bord Netcool Health», à la page 581
Le tableau de bord Netcool Health est un tableau de bord d'Interface graphique Web qui affiche des données de surveillance automatique Tivoli Netcool/OMNIbus.

Extension de la fonctionnalité de l'Interface graphique Web

Tivoli Netcool/OMNIbus inclut des ressources pouvant être utilisées pour étendre la fonctionnalité de l'Interface graphique Web lorsque Tivoli Netcool/OMNIbus est intégré avec d'autres produits.

Concepts associés:

«Intégration à d'autres produits Tivoli», à la page 62
Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

Activation des événements prévisibles dans l'Interface graphique Web

Vous exécuterez un fichier de commandes WAAPI, fourni avec le composant serveur, sur le serveur Interface graphique Web afin de créer les configurations nécessaires pour afficher les événements prévisibles qui sont générés par IBM Tivoli Monitoring dans les listes d'événements.

Le fichier de commandes WAAPI (Interface graphique Web Administration API) est nommé `predictive_events_web_gui.xml`. Ce fichier crée les ressources suivantes pour utilisation avec les événements prévisibles :

- Filtre global par défaut
- Vue globale par défaut
- Outils. L'outil ShowDetailsInTEP a besoin du nom d'hôte et du numéro de port de l'hôte Tivoli Enterprise Portal. Si le numéro de port n'est pas le numéro par défaut, vous devez le changer manuellement dans l'outil. Voir étape 5, à la page 588.
- Sous-menu des listes d'événements contenant les outils. Ce sous-menu doit être ajouté à un menu de façon à être accessible par clic droit sur un événement prévisible.
- Invites
- Fichier `.jsp`, images et feuille de style

Avant de commencer

- Configurez les composants serveur pour la gestion des événements prévisibles. Voir «Configuration des événements prévisibles dans votre environnement intégré», à la page 448.
- Activez et configurez le client WAAPI. Familiarisez-vous avec le fonctionnement du client WAAPI. Voir Gestion à distance du serveur de l'Interface graphique Web. Pour tout détail concernant le client WAAPI, reportez-vous au *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .
- Activez une connexion unique entre le serveur de l'Interface graphique Web et le serveur Tivoli Enterprise Portal. Dès lors que cette connexion est activée, les utilisateurs n'ont plus à se connecter à Tivoli Enterprise Portal après un clic sur un événement prévisible. Voir «Configuration et gestion de l'authentification unique», à la page 573.

Procédure

1. Sur le serveur Tivoli Netcool/OMNIbus, copiez le contenu du répertoire `$NCHOME/omnibus/extensions/itmpredictive` vers le répertoire *WEBGUI_HOME*`/waapi/bin` du serveur de l'Interface graphique Web :
2. Sur le serveur de l'Interface graphique Web, accédez au répertoire *REP_INSTALL_WEBGUI*`/waapi/bin`.
3. Pour exécuter le fichier de commandes, entrez la commande suivante :

   ```
   ./runwaapi -file predictive_events_web_gui.xml
   ```
4. Ajoutez le sous-menu à un menu de telle sorte que les outils de gestion des événements prévisibles puissent être exécutés depuis une liste d'événements :
   a. Cliquez sur **Administration** > **Outils de gestion d'événements**, puis sur **Configuration de menu**.
   b. Dans la liste **Menus disponibles**, sélectionnez **alertes** et cliquez sur **Modifier**.
   c. Dans la fenêtre Editeur de menus, sélectionnez **Menu** dans la liste **Eléments disponibles**.
   d. Sélectionnez le sous-menu **Evénements prévisibles** et cliquez sur **Ajouter un élément sélectionné**.

      Le sous-menu est ajouté à la liste dans le panneau **Eléments en cours** à droite de la page.
5. Configurez l'outil ShowDetailsInTEP de façon à ce qu'il ouvre Tivoli Enterprise Portal :
   a. Cliquez sur **Administration** > **Outils de gestion d'événements** > **Création d'outils**.
   b. Sélectionnez **ShowDetailsInTEP**.

      L'outil est affiché avec l'entrée suivante dans la zone **URL** : `http://`*hôte_teps*`:15200/LICServletWeb/LICServlet`.
   c. Remplacez `teps_host` par le nom de l'hôte sur lequel Tivoli Enterprise Portal est installé. Si le numéro de port n'est pas le numéro par défaut, changez-le.

Résultats

Les opérateurs peuvent maintenant utiliser l'outil de gestion des événements prévisibles pour démarrer Tivoli Enterprise Portal à partir des listes d'événements.Pour tout détail concernant l'utilisation des outils de gestion des événements prévisibles, reportez-vous au *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Concepts associés:

«Authentification unique», à la page 573
L'authentification unique (SSO) est prise en charge par les produits Tivoli. Lorsque les utilisateurs se connectent à une application dans un environnement SSO, les informations d'identification utilisateur sont autorisées dans un référentiel central des utilisateurs. Ce référentiel peut être Tivoli Netcool/OMNIbus ObjectServer ou un répertoire LDAP. Après autorisation des informations d'identification utilisateur, les utilisateurs peuvent lancer des applications. L'authentification unique est prise en charge dans des environnements qui sont hébergés dans des serveurs Jazz for Service Management sur plusieurs hôtes, ou un seul hôte.

«L'Interface graphique Web dans un environnement d'équilibrage de charge», à la page 604
Informations relatives au fonctionnement de l'Interface graphique Web dans un environnement d'équilibrage de charge et les implications de gestion et d'utilisation du produit.

Tâches associées:

«Configuration du client WAAPI», à la page 186
Pour configurer l'utilisation des événements prévisibles et la surveillance des événements IBM Tivoli Application Dependency Discovery Manager (TADDM), vous devez effectuer une configuration minimale du client WAAPI en spécifiant un utilisateur et un mot de passe.

«Configuration de l'authentification unique (SSO)», à la page 576
Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

Activation de la corrélation d'événements de gestion virtuels dans l'Interface graphique Web

Vous pouvez configurer l'Interface graphique Web pour gérer des événements qui sont issus d'un environnement virtuel. Copiez un fichier de commandes WAAPI de l'hôte Tivoli Netcool/OMNIbus vers l'hôte de l'Interface graphique Web et exécutez le client WAAPI sur le fichier. Des colonnes sont ajoutées à l'Afficheur d'événements pour définir la relation entre les événements de cause première et les événements symptôme qui sont issus d'un environnement virtuel

Avant de commencer

Vérifiez que vous respectez les conditions préalables suivantes :

- Vous avez configuré l'environnement requis pour la gestion virtuelle. La configuration varie en fonction des produits qui sont déployés dans votre environnement. Pour plus d'informations, consultez les rubriques suivantes :
  - «Configuration de la gestion d'événements dans un environnement virtuelà l'aide d'une sonde pour SNMP et IBM Tivoli Netcool/OMNIbus Knowledge Library», à la page 465
  - «Configuration de la gestion d'événements dans un environnement virtuel à l'aide de IBM Tivoli Monitoring», à la page 469
- Vous avez effectué au moins la configuration minimale du client WAAPI (Administration Application Program Interface) de l'Interface graphique Web et vous êtes familiarisé avec le fonctionnement du client WAAPI.

Procédure

Pour définir cette relation d'événement dans l'Interface graphique Web :

1. Sur l'ordinateur hôte de l'Tivoli Netcool/OMNIbus, accédez au répertoire `$NCHOME/omnibus/extensions/virtualization/common` et copiez le fichier `virtualization_webgui_config.xml`.
2. Ajoutez ce fichier à l'emplacement suivant sur l'ordinateur hôte de l'Interface graphique Web : *`rép_principal_interface_Web`*`/waapi/bin`.
3. Pour exécuter le fichier de commandes, lancez la commande suivante :
   ```
   ./runwaapi -file virtualization_webgui_config.xml
   ```
4. Définissez la relation d'événement dans l'Afficheur d'événements :
   a. Démarrez le Générateur de vues.
   b. Dans la liste **Available views (Vues disponibles)**, sélectionnez la vue à appliquer à la relation.

c. Cliquez sur l'onglet **Relationships (Relations)** et, dans la liste, sélectionnez **IBM Tivoli Netcool/OMNIbus Root Cause/Symptom (IBM Tivoli Netcool/OMNIbus - cause première/symptôme)**

d. Cliquez sur **Save and Close (Sauvegarder et fermer)** pour sauvegarder et fermer le Générateur de vues.

e. Lancez l'Afficheur d'événements et éditez les préférences de widget ou, en tant qu'administrateur, éditez les valeurs par défaut du widget.

f. Dans les **General Settings (Paramètres généraux)**, sélectionnez la vue qui était préalablement définie.

g. Cliquez sur **OK**.

Tâches associées:

«Configuration de la gestion d'événements dans un environnement virtuelà l'aide d'une sonde pour SNMP et IBM Tivoli Netcool/OMNIbus Knowledge Library», à la page 465
Vous pouvez exécuter Tivoli Netcool/OMNIbus avec IBM Tivoli Netcool/OMNIbus Knowledge Library et avec une sonde personnalisée pour SNMP afin de surveiller et de gérer un environnement virtuel VMware vSphere utilisant des hyperviseurs ESXi.

Activation de la prise en charge des événements TADDM dans l'Interface graphique Web

Vous pouvez ajouter un menu, des outils et un filtre pour les événements TADDM sur le serveur de l'Interface graphique Web pour vous permettre d'afficher des détails supplémentaires sur ces événements lorsqu'ils sont affichés dans la liste des événements actifs.

Avant de commencer

Les critères de configuration sont les suivants :

- Vous devez avoir configuré l'intégration entre Tivoli Netcool/OMNIbus et TADDM, comme décrit dans «Configuration du support pour les événements TADDM dans votre environnement intégré», à la page 459.
- Vous devez avoir configuré le client WAAPI (Web GUI Administration Application Program Interface) avec les paramètres de propriété corrects dans le fichier de propriétés *REP_INSTALL_WEBGUI*`/waapi/etc/waapi.init` comme décrit dans «Configuration du client WAAPI», à la page 186.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter le menu, les outils et le filtre en exécutant un fichier de commande WAAPI, fourni dans l'installation de Tivoli Netcool/OMNIbus. Après avoir exécuté le fichier de commande, vous devez ajouter le menu en tant que sous-menu du menu **Alertes** de la liste des événements actifs.

Pour plus d'informations sur le client WAAPI, consultez le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Pour ajouter le menu et les outils pour les événements TADDM au serveur de l'Interface graphique Web, procédez comme suit :

Procédure

1. A partir d'un hôte Tivoli Netcool/OMNIbus, copiez le contenu du répertoire `$NCHOME/omnibus/extensions/taddm` dans l'emplacement d'installation du serveur de l'Interface graphique Web :

REP_INSTALL_WEBGUI/waapi/bin

2. Sur le serveur de l'Interface graphique Web, ouvrez une fenêtre de commande et entrez la commande WAAPI suivante pour ajouter le menu et les outils pour les événements TADDM :

   REP_INSTALL_WEBGUI/waapi/bin/runwaapi -file taddm_menutools_web_gui.xml

   Vous pouvez maintenant ajouter le nouveau menu comme sous-menu du menu **Alertes** utilisé dans la liste des événements actifs.
3. Dans l'Interface graphique Web, ajoutez un sous-menu TADDM dans le menu **Alertes** comme suit :
   a. Cliquez sur **Administration** > **Outils de gestion d'événements** > **Configuration de menu**.
   b. Sélectionnez **alertes** dans la liste des menus et cliquez sur **Modifier**.
   c. Dans la zone **Eléments disponibles**, sélectionnez **menu** dans la liste déroulante. La liste de tous les éléments de menu qui peuvent être ajoutés au menu **Alertes** est affichée.
   d. Sélectionnez l'élément **TADDM** et cliquez sur **Ajouter un élément sélectionné** pour déplacer l'élément dans la zone **Eléments en cours**. Utilisez les touches de déplacement pour déplacer l'élément **TADDM**, le cas échéant.
   e. Cliquez sur **Enregistrer** puis sur **OK** pour confirmer.

Résultats

Le menu, les outils et le filtre sont désormais disponibles dans la liste des événements actifs pour être utilisés avec les événements TADDM. Pour plus d'informations sur la surveillance des événements TADDM, voir *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Concepts associés:

«L'Interface graphique Web dans un environnement d'équilibrage de charge», à la page 604
Informations relatives au fonctionnement de l'Interface graphique Web dans un environnement d'équilibrage de charge et les implications de gestion et d'utilisation du produit.

Tâches associées:

«Configuration du client WAAPI», à la page 186
Pour configurer l'utilisation des événements prévisibles et la surveillance des événements IBM Tivoli Application Dependency Discovery Manager (TADDM), vous devez effectuer une configuration minimale du client WAAPI en spécifiant un utilisateur et un mot de passe.

Configuration d'intégrations de lancement en contexte dans les produits Tivoli

Vous pouvez configurer l'Interface graphique Web pour qu'elle démarre dans des produits Tivoli compatibles.

Des intégrations de lancement en contexte sont prises en charge entre l'Interface graphique Web et les produits compatibles Tivoli. Une intégration de lancement externe décrit le démarrage d'un autre produit à partir d'un widget de l'Interface graphique Web. Une intégration de lancement interne décrit le démarrage de l'Interface graphique Web à partir d'un autre produit.

Avant de commencer

- Veillez à ce que l'intégration entre l'Interface graphique Web et l'autre produit et la version est prise en charge.
- Assurez-vous que vous maîtrisez le fonctionnement du produit d'intégration. Seules les configurations Interface graphique Web sont décrites ici. Consultez la documentation de l'autre produit.
- Configurez un annuaire LDAP comme référentiel d'authentification des utilisateurs. Assurez-vous que l'annuaire LDAP est le référentiel d'utilisateurs commun à tous les produits qui se trouvent dans la même instance de Concentrateur des services d'application du tableau de bord que l'Interface graphique Web.
- Configurez l'authentification unique (SSO), de sorte que les utilisateurs n'aient pas à entrer à nouveau leurs informations d'identification lorsqu'ils cliquent sur les produits. Assurez-vous que tous les hôtes font partie du même domaine d'authentification unique Websphere Application Server.
- Créez les utilisateurs dans tous les produits et attribuez les rôles d'utilisateur requis. Certains rôles dans IBM Tivoli Network Manager IP Edition correspondent à des rôle de l'Interface graphique Web. Cette mise en correspondance est décrite dans le tableau suivant.

Tableau 91. Mise en correspondance des rôlesNetwork Manager IP Edition avec des rôles Interface graphique Web

Rôle Network Manager IP Edition	**Correspond à ce rôle Interface graphique Web**
ncp_networkview	ncw_user
ncp_hopview	ncw_user
ncp_mibbrowser	ncw_user
ncp_structurebrowser	ncw_user

Concepts associés:

«Intégration à d'autres produits Tivoli», à la page 62
Vous pouvez étendre les fonctionnalités de Tivoli Netcool/OMNIbus via l'intégration à d'autres produits et composants IBM. Cette intégration étend la fonction de gestion des événements de Tivoli Netcool/OMNIbus car elle prend en charge l'échange de données entre les produits. L'Interface graphique Web prend en charge la navigation par lancement en contexte à partir de Tivoli Netcool/OMNIbus vers les produits compatibles. Ces intégrations ne sont pas configurées dans le produit tel qu'il est fourni. Chaque intégration doit être configurée séparément.

«Authentification unique», à la page 573
L'authentification unique (SSO) est prise en charge par les produits Tivoli. Lorsque les utilisateurs se connectent à une application dans un environnement SSO, les informations d'identification utilisateur sont autorisées dans un référentiel central des utilisateurs. Ce référentiel peut être Tivoli Netcool/OMNIbus ObjectServer ou un répertoire LDAP. Après autorisation des informations d'identification utilisateur, les utilisateurs peuvent lancer des applications. L'authentification unique est prise en charge dans des environnements qui sont hébergés dans des serveurs Jazz for Service Management sur plusieurs hôtes, ou un seul hôte.

Tâches associées:

«Configuration de l'authentification unique (SSO)», à la page 576
Suivez les instructions ci-après pour la prise en charge de l'authentification unique et pour la configuration d'un référentiel fédéré.

Configuration d'intégrations de lancement externe de l'Interface graphique Web :

Vous pouvez effectuer des lancements externes de l'Interface graphique Web vers une autre application de diverses manières. Vous pouvez écrire un script qui lance l'URL de l'application et définir le script comme un outil qui sera lancé à partir d'une liste d'événements. De la même manière, vous pouvez définir une action de clic visant à lancer une URL à partir de tableaux de bord d'événements. Pour les produits qui sont basés sur Concentrateur des services d'application du tableau de bord, vous pouvez utiliser le cadre d'action pour définir et vous abonner à des événements.

Configuration des intégrations de lancement externe de l'Interface graphique Web pour la liste des événements actifs :

Pour effectuer un lancement externe à la liste des événements actifs (AEL), vous pouvez créer un outil qui, lors de son exécution, lance l'adresse URL d'un autre produit Tivoli. Pour les intégrations avec des produits basés sur Concentrateur des services d'application du tableau de bord, vous pouvez utiliser l'infrastructure d'action de Concentrateur des services d'application du tableau de bord pour diffuser des événements entre des widgets.

Définition d'outils pour les intégrations de lancement externe :

Les outils sont le principal mécanisme pour lancer d'autres produits de l'Interface graphique Web. Vous pouvez écrire un outil de script qui diffuse des événements définis dans l'infrastructure d'actions, ou écrire l'URL pour lancer l'outil directement dans la définition de l'outil.

Avant de commencer

Vous devez connaître l'adresse URL du produit Tivoli que vous voulez lancer depuis l'AEL. Pour plus d'informations sur la création de cette adresse URL, consultez le centre de documentation du produit. Pour les Knowledge Centers des produits Tivoli, voir *IBM Knowledge Center* à l'adresse http://www-01.ibm.com/support/knowledgecenter.

Pourquoi et quand exécuter cette tâche

Cette méthode permet d'effectuer des lancements dans les produits pris en charge, déployés avec l'infrastructure Concentrateur des services d'application du tableau de bord et ceux utilisant d'autres infrastructures d'interface graphique, telles que TPAe, ou Java Swing. Une fois l'outil créé, vous devez l'ajouter au menu AEL.

Pour créer un outil qui effectue des lancements depuis l'AEL dans d'autres produits Tivoli :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Outils de gestion d'événements**.
2. Dans la page Création d'outils, cliquez sur **Créer un outil**.
3. Sélectionnez **CGI/URL** dans la liste **Type**.
4. Entrez un nom d'outil dans la zone **Nom**.

Par défaut, les caractères suivants ne peuvent pas être utilisés dans les noms d'outils :
`$ ! £ % ^ & * ( ) + = ¬ ` ~ # @ ' : ; < > { } [ ] ? / \ \ | , "`

Par défaut, les caractères suivants ne peuvent pas être utilisés comme caractère initial dans les noms d'outils :
`/ \ \ * ? " < > | & .`

Ces caractères non valides sont définis dans le fichier suivant :
REP_INSTALL_WEBGUI`/etc/illegalChar.prop`

5. Dans la zone **URL**, entrez l'adresse URL qualifiée complète de l'application, en respectant le format suivant :

   protocole`://`*nom_hôte*`:`*port*`/`*chemin*`/?`*paramètres*

   Où les valeurs valides pour chaque variable de l'adresse URL sont les suivantes :

   protocole
   Protocole Web à utiliser. Les valeurs valides sont `http` et `https`.

   Hostname
   Nom d'hôte du produit Tivoli vers lequel vous effectuez le lancement.

   port
   Numéro de port du produit Tivoli vers lequel vous effectuez le lancement.

   path
   Emplacement de la ressource demandée.

   paramètres
   Paramètres de l'adresse URL.

6. Complétez les autres zones comme suit :

   Méthode
   Sélectionnez **GET**.

   Ouvrir dans
   Sélectionnez **Nouvelle fenêtre**.

   Exécuter pour chaque ligne sélectionnée
   Cochez cette case pour exécuter l'outil sur toutes les lignes sélectionnées individuellement dans l'AEL. Décochez la case si vous voulez que l'outil s'exécute uniquement sur la première ligne de la sélection.

   Fenêtre pour chaque ligne sélectionnée
   Cochez cette case pour ouvrir une fenêtre distincte pour chaque ligne sélectionnée dans la liste d'événements actifs (AEL).

7. Définissez un accès pour les outils selon les groupes auxquels un utilisateur appartient et la classe d'un événement sur laquelle l'outil est déployé :

   Groupe
   Sélectionnez le groupe d'utilisateurs qui doit accéder à l'outil et cliquez sur **>.** Pour que l'ensemble des groupes puissent accéder à l'outil sélectionné, cliquez sur **>>**. Les utilisateurs doivent être membres d'un groupe sélectionné pour utiliser l'outil.

   Classe Sélectionnez la classe d'événement (définie par la zone Classe du serveur ObjectServer) qui doit accéder à l'outil et cliquez sur **>.** Pour que l'ensemble des classes puissent accéder à l'outil sélectionné, cliquez sur **>>**.

8. Cliquez sur **Enregistrer**.

9. Ajoutez l'outil à un menu AEL :
   a. Cliquez sur **Administration** > **Outils de gestion d'événements** > **Configuration de menu**.
   b. Dans la liste **Menus disponibles**, sélectionnez le menu dans lequel vous voulez ajouter l'outil et cliquez sur **Modifier**.
   c. Sélectionnez **outil** dans la liste **Eléments disponibles**.
   d. Sélectionnez le nouvel outil et cliquez sur **Ajouter un élément sélectionné**.
   e. Cliquez sur **Enregistrer**.

Résultats

L'outil est ajouté au menu AEL.

Que faire ensuite

Assurez-vous que l'adresse URL est correctement générée et qu'elle lance le produit Tivoli indiqué dans l'outil en la testant sur un événement de l'AEL. Pour ouvrir l'applet AEL par défaut, cliquez sur **Disponibilité** > **Evénements** > **Liste d'événements actifs (AEL)**. Vous disposez des options suivantes :

- Afficher l'outil en cliquant sur **Outil** sur la barre de menu.
- Exécuter l'outil sur un événement, en cliquant avec le bouton droit sur une ligne de l'AEL et en sélectionnant l'outil dans la liste.

Si l'Interface graphique Web et le produit démarré ne sont pas configurés pour une connexion unique, une fenêtre de connexion s'ouvre. Avant d'afficher les données sur l'événement, vous devez fournir un nom d'utilisateur et un mot de passe.

Configuration de l'infrastructure d'actions :

L'infrastructure d'actions de Concentrateur des services d'application du tableau de bord définit les communications entre les widgets. Dans le produit d'intégration, définissez un événement qui peut être utilisé par l'Interface graphique Web dans un outil lancé à partir d'une liste d'événements.

Procédure

1. Sur le serveur de l'Interface graphique Web, définissez l'événement de diffusion dans le fichier *REP_INSTALL_JazzSM*/installedApps/TIPCell/isc.ear/OMNIbusWebGUI.war/WEB-INF/ibm-portal-event.xml. Par exemple :

```
<!--  Event Definition -->
<events:event-definition>
      <events:name xmlns:x="http://ibm.com/espace-noms">

x:nom_événement
      </events:name>
</events:event-definition>
```

   Où *nom_événement* est le nom de l'événement de diffusion et *espace-noms* est l'espace de nom abrégé de l'Interface graphique Web.

   Conseil : La combinaison de *espace-noms* et de *nom_événement* doit être unique.
2. Dans le fichier ibm-portal-event.xml du produit d'intégration, définissez un abonnement à l'événement dans le widget que vous souhaitez lancer à partir de l'Interface graphique Web :

a. Recherchez la section qui appartient au widget qui doit s'abonner à l'événement.
b. Définissez l'abonnement.

Par exemple :

```
<!--  Portlet Subscriptions -->
<events:widget-definition-ref widgetDefinitionRef="définition_widget">
        <events:supported-subscribed-event>
                <events:name xmlns:x="http://ibm.com/espace-noms">
x:nom_événement
                </events:name>
        </events:supported-subscribed-event>
</events:widget-definition-ref>
```

Où :

nom_événement
Est le nom de l'événement défini dans l'étape 1, à la page 595

espace-noms
Est le raccourci d'espace de nom pour l'Interface graphique Web

définition_widget
Est la définition du widget de la page vers laquelle vous souhaitez lancer à partir de la liste des événements.

3. Créez un outil qui diffuse l'événement qui a été créé dans les étapes 1, à la page 595 et 2, à la page 595 à partir de la liste des événements Dans la zone **Commandes de script**, entrez la commande JavaScript qui diffuse l'événement. Par exemple :

```
{$param.widgetNamespace}sendPortletEvent
({'name':'http//ibm.com/espace-noms#nom_événement',
'paramètre':{valeur_paramètre}'});
```

Où *espace-noms* est le nom de l'événement de diffusion et *nom_événement* est l'espace de nom abrégé de l'Interface graphique Web.

Que faire ensuite

- Pour un lancement externe à partir d'une liste d'événements, définissez l'outil qui diffuse l'événement que vous avez créé dans les étapes 1, à la page 595 et 2, à la page 595.
- Pour un lancement externe à partir d'une action de clic, définissez l'action de clic qui crée l'événement. Les actions de clic sont définies dans les préférences d'un widget ou dans un widget.

Configuration d'intégrations de lancement externe pour le Tableau de bord des événements :

Vous pouvez configurer le Tableau de bord des événements pour exécuter un script qui lance un autre produit. Le script est exécuté lorsqu'un utilisateur clique sur un écran de surveillance. Pour les intégrations entre les produits de Jazz for Service Management, vous pouvez utiliser l'infrastructure d'actions Concentrateur des services d'application du tableau de bord pour définir des événements pouvant être lancés par le script ou indiquer une URL ouverte dans le navigateur. Pour les produits qui ne sont pas dans Jazz for Service Management, vous pouvez uniquement utiliser une URL.

Avant de commencer

Si vous voulez que le script lance une URL, obtenez l'URL que vous souhaitez lancer à partir du tableau de bord d'événements. Pour plus d'informations sur la façon de construire l'URL, consultez la documentation du produit lancé. Pour les Knowledge Centers des produits Tivoli, voir *IBM Knowledge Center* à l'adresse http://www-01.ibm.com/support/knowledgecenter.

Procédure

Pour utiliser l'infrastructure d'actions Concentrateur des services d'application du tableau de bord, suivez les étapes 1 et 2. Sinon, passez ces étapes.

1. Sur le serveur de l'Interface graphique Web, définissez l'événement de diffusion dans le fichier *REP_INSTALL_JazzSM*/installedApps/Cellule_Noeud01_JazzSM/isc.ear/OMNIbusWebGUI.war/WEB-INF/ibm-portal-event.xml. Par exemple :

   ```
   <!--  Event Definition -->
   <events:event-definition>
         <events:name xmlns:x="http://ibm.com/espace_nom">

   x:nom_événement
         </events:name>
   </events:event-definition>
   ```

   Où *nom_événement* est le nom de l'événement de diffusion et *espace_nom* est l'espace de nom abrégé pour l'Interface graphique Web.

   Important : La combinaison de *espace_nom* et *nom_événement* doit être unique.

2. Dans le fichier ibm-portal-event.xml du produit d'intégration, définissez un abonnement à l'événement dans le widget que vous souhaitez lancer à partir du tableau de bord d'événements :
   a. Recherchez la section qui définit le widget que vous souhaitez abonner à l'événement.
   b. Définissez l'abonnement. Par exemple :

      ```
      <!--  Portlet Subscriptions -->
      <events:widget-definition-ref widgetDefinitionRef="widgetdefinition">
              <events:supported-subscribed-event>
                      <events:name xmlns:x="http://ibm.com/espace_noms">
      x:nom_événement
                      </events:name>
              </events:supported-subscribed-event>
      </events:widget-definition-ref>
      ```

      Où :

      nom_événement
      Est le nom de l'événement défini dans l'étape 1

      espace de nom
      Est le raccourci d'espace de nom pour l'Interface graphique Web

      définition de widget
      Est la définition du widget de la page vers laquelle vous souhaitez lancer à partir du tableau de bord d'événements..

3. Editez les préférences du widget pour un tableau de bord d'événements ou définissez les valeurs par défaut pour tous les utilisateurs. Dans la fenêtre Edit Event Dashboard Portlet Preferences (Editer les préférences de portlet du tableau de bord des événements), dans la liste **Single Click** (Clic unique),

sélectionnez **Script**. Dans la zone de texte, écrivez le code JavaScript requis. Voir «Exemples de scripts» pour plus d'informations.

4. Cliquez sur **OK**.

Exemples de scripts

Les exemples de scripts suivants vous aident à écrire un script pour le Tableau de bord des événements à l'étape 3, à la page 597.

L'exemple suivant vous montre comment écrire un script qui diffuse un événement dans l'infrastructure d'action Concentrateur des services d'application du tableau de bord, comme défini aux étapes 1, à la page 597 et 2, à la page 597:

```
{$param.widgetNamespace}sendPortletEvent
({'name':'http//ibm.com/espace_nom#nom_événement',
'paramètre':{valeur_paramètre}'});
```

Où *espace_nom* est le nom de l'événement de diffusion et *nom_événement* est l'espace de nom abrégé pour l'Interface graphique Web.

L'exemple suivant vous explique comment écrire un script qui lance une adresse URL statique ; par exemple pour lancer un produit Tivoli qui n'est pas basé sur Concentrateur des services d'application du tableau de bord :

```
window.open("protocole://nom_hôte:numéro_port/racine_contexte/?chaîne_requête");
```

Où les valeurs valides pour chaque variable de l'adresse URL sont les suivantes :

protocole
Protocole Web à utiliser. Les valeurs valides sont `http` et `https`.

Hostname
Nom d'hôte du produit Tivoli vers lequel vous effectuez le lancement.

port
Numéro de port du produit Tivoli vers lequel vous effectuez le lancement.

chemin
Emplacement de la ressource demandée.

paramètres
Paramètres de l'adresse URL.

Que faire ensuite

Testez le script en cliquant sur l'écran de surveillance du Tableau de bord des événements. Si l'authentification unique n'est pas configurée, assurez-vous que vous disposez des données d'identification de connexion pour le produit lancé.

Configuration d'intégrations de lancement interne de l'Interface graphique Web :

Vous pouvez effectuer un lancement dans l'Interface graphique Web à partir d'un autre produit Tivoli des manières suivantes : en créant une adresse URL qui ouvre une application de l'Interface graphique Web ou, pour les produits basés sur Concentrateur des services d'application du tableau de bord, en utilisant Concentrateur des services d'application du tableau de bord pour définir des événements et s'y abonner.

Configuration d'intégrations de lancement interne de l'Interface graphique Web pour des produits Concentrateur des services d'application du tableau de bord :

Pour les produits basés sur Concentrateur des services d'application du tableau de bord, utilisez l'infrastructure d'actions Concentrateur des services d'application du tableau de bord pour définir un événement dans l'Interface graphique Web et pour définir un outil dans le produit de lancement qui diffuse l'événement.

Procédure

1. Dans le fichier `ibm-portal-event.xml` du produit de lancement, définissez l'événement. Par exemple :

```
<!-- Event Definition -->
<events:event-definition>
        <events:name xmlns:x="http://ibm.com/espace_nom">
                              x:nom_événement
        </events:name>
</events:event-definition>
```

   Où *espace_nom* est l'espace de nom abrégé du produit de lancement et *nom_événement* est le nom de l'événement.

   Important : La combinaison de *espace_nom* et de *nom_événement* doit être unique.

2. Sur le serveur de l'Interface graphique Web, ouvrez le fichier *REP_INSTALL_JazzSM*`/installedApps/Cellule_Noeud01_JazzSM/isc.ear/OMNIbusWebGUI.war/WEB-INF/ibm-portal-event.xml`.

3. Abonnez-vous à l'événement créé à l'étape 1. Par exemple :

```
<!-- Portlet Subscriptions -->
<events:portlet-definition-ref portletDefinitionRef="définition_portlet">
         <events:supported-subscribed-event>
                 <events:name xmlns:x="http://ibm.com/espace_nom">
                         x:nom_événement
         </events:supported-subscribed-event>
                 </events:name>
 </events:portlet-definition-ref>
```

   Où :

   portletdefinition
   : Définition de portlet pour l'application de l'Interface graphique Web que vous voulez abonner à l'événement.

   espace_nom
   : Est l'espace de nom abrégé du produit de lancement.

   nom_événement
   : Est le nom de l'événement créé à l'étape 1.

   Conseil : La définition de portlet de l'AEL est `item.portletDef.AEL`.

Que faire ensuite

Dans le produit de lancement :

1. Définissez un outil pour diffuser les événements.
2. Configurez une action de clic pour lancer l'outil.

Lancement d'afficheurs d'événements à partir de Concentrateur des services d'application du tableau de bord :

Vous pouvez utiliser l'événement de page de lancement de portlet Concentrateur des services d'application du tableau de bord pour lancer l'Afficheur d'événements à partir des produits qui s'exécutent dans l'application Concentrateur des services d'application du tableau de bord.

Avant de commencer

Utilisez l'événement de page de lancement de portlet Concentrateur des services d'application du tableau de bord pour lancer l'Afficheur d'événements de l'Interface graphique Web à partir d'une autre application Concentrateur des services d'application du tableau de bord.

Utilisez les valeurs suivantes pour les attributs de base :

Tableau 92. Valeurs d'attributs de base

Attribut	Valeur
NavigationNode	`item.desktop.navigationElement.EventViewer`
switchPages	`true`
PageInstanceRef	Cet attribut n'est pas obligatoire.

Utilisez les attributs personnalisés suivants pour définir les caractéristiques de l'Afficheur d'événements lancé :

Tableau 93. Attributs personnalisés utilisés pour définir les caractéristiques de l'Afficheur d'événements lancé

Attribut	Obligatoire ou facultatif	Description
filterName	Oui (Yes)	Indique le nom du filtre utilisé dans l'afficheur d'événements.
registerFilter	Non	Spécifie si un filtre transitoire est créé. Valeurs : `true` (il s'agit d'un filtre transitoire) ou `false` (il ne s'agit pas d'un filtre transitoire). Default `false`
forceOverwrite	Non	Indique si un filtre transitoire existant portant le même nom doit être écrasé. Valeurs: `true` (le nom du filtre transitoire existant est remplacé) ou `false` (le nom du filtre transitoire existant n'est pas remplacé). Valeur par défaut : `false`
sql	Cette valeur dépend d'autres valeurs.	Indique la clause `Where` SQL pour un filtre transitoire. Cet attribut est obligatoire si l'attribut registerFilter a la valeur`true`. Dans la négative, cet attribut n'est pas obligatoire.
viewName	Non	Indique le nom de la vue à appliquer à l'Afficheur d'événements. Si cet attribut n'est pas spécifié, une vue par défaut est appliquée.

Tableau 93. Attributs personnalisés utilisés pour définir les caractéristiques de l'Afficheur d'événements lancé (suite)

Attribut	Obligatoire ou facultatif	Description
viewType	Oui, si viewName est spécifié. Si tel n'est pas le cas, non.	Indique le type de la vue à appliquer à l'Afficheur d'événements. Il peut s'agir de l'un des types suivants : • `user` • `global` • `system` Valeur par défaut : `user`
filterType	Oui, si registerFilter est défini sur `false`	Indique le type de filtre à appliquer à l'Afficheur d'événements. Il peut s'agir de l'un des types suivants : • `user` • `global` • `system` • `user transient` Valeur par défaut : `user transient`
dataSource	Non	Indique une liste séparée par des virgules de noms de sources de données à partir desquelles l'Afficheur d'événements obtient sa source de données par défaut, par exemple NCOMS.
filterCollection	Non	Indique la collection de filtres à laquelle est affecté un filtre transitoire. Valeur par défaut : `default`
métrique Condition	Non	Indique la condition métrique. Il peut s'agir de l'une des conditions suivantes : • `Moyenne` • `Nombre` • `Somme` • `Maximum` • `Minimum` Valeur par défaut : `Moyenne`
metricField	Non	Indique la zone métrique. Valeur par défaut : `severity`

Lancement dans l'Interface graphique Web à partir d'autres interfaces graphiques :

Pour se lancer dans l'Interface graphique Web à partir d'un produit qui ne s'exécute pas dans Concentrateur des services d'application du tableau de bord, créez l'URL d'un widget de l'Interface graphique Web qui peut être lancé à partir de votre produit.

Pourquoi et quand exécuter cette tâche

Si vous voulez lancer une page Concentrateur des services d'application du tableau de bord, utilisez l'URL Concentrateur des services d'application du tableau de bord.

Procédure

Les URL Concentrateur des services d'application du tableau de bord utilisent le format suivant :

```
nom_protocole://<nom_hôte>:<port>/ibm/action/launch?pageID=
<dash-page-id>&<paramètres>
```

Vous pouvez obtenir *pageID* de la console d'administration de la page, dans Concentrateur des services d'application du tableau de bord. Les paramètres pour différents widgets de l'Interface graphique Web intégrés dans les pages peuvent être trouvés dans les *URL d'ouverture des widgets de l'interface graphique Web*, référencées à la fin de cette rubrique.

Lancement de contenu direct :

Les liens directs sont des URL qui pointent vers des pages HTML personnalisées, des SmartPages, des scripts CGI, des JSP de l'Interface graphique Web. Ces liens se lancent habituellement dans une nouvelle fenêtre ou un onglet de navigateur.

Procédure

- Utilisez les paramètres d'URL de n'importe quel widget d'interface graphique Web. Pour plus d'informations, consultez les modèles d'URL pour les widgets de l'Interface graphique Web.

  ```
  protocole://serveur.domaine:port/ibm/console/webtop/path?querystring
  ```

- Utilisez l'URL d'un fichier HTML qui a été créé par une commande SmartPage. Ces URL ont un format spécifique. Exemple :

  ```
  https://localhost:16133/ibm/console/webtop/filename.html
  ```

Lancement de contenu direct dans une page Concentrateur des services d'application du tableau de bord :

Pour intégrer du contenu directement de sorte qu'il apparaisse dans une page Concentrateur des services d'application du tableau de bord, générez une URL d'un format spécifique.

Procédure

Utilisez une URL qui lance une page Concentrateur des services d'application du tableau de bord de l'extérieur de la console. L'application externe ou une page doit fournir une URL de requête en utilisant le format suivant :

nom_protocole://*<nom_hôte>*:*<port>*/ibm/action/launch?*pageID*
=item.desktop.navigationElement.LaunchWebGUIURL&URL=*<encoded-direct-url>*

L'exemple suivant montre l'URL directe vers l'afficheur d'événements Interface graphique Web :

```
https://<nom_hôte>:<port>/ibm/console/webtop/eventviewer/eventViewer.jsp?
filtername=Default&filtertype=global
```

La forme codée de cette URL est :

```
https%3A%2F%2F<nom_hôte>%3A<port>%2Fibm%2Fconsole%2Fwebtop%2Feventviewer
%2FeventViewer.jsp%3Ffiltername%3DDefault%26filtertype%3Dglobal
```

Ainsi, l'URL de lancement finale est :

```
nom_protocole://<nom_hôte>:<port>/ibm/action/launch?pageID=
item.desktop.navigationElement.LaunchWebGUIURL&URL=https%3A%2F%2F<nom_hôte>
%3A<port>%2Fibm%2Fconsole%2Fwebtop%2Feventviewer%2FEventViewer.jsp
%3Ffiltername%3DDefault%26filtertype%3Dgloba
```

Que faire ensuite

Utilisez les fonctions dans l'autre produit pour lancer l'URL de l'Interface graphique Web. Si l'Interface graphique Web et le produit qui est en cours de lancement ne sont pas configurés pour l'authentification unique, les utilisateurs doivent entrer des informations de connexion à l'invite.

Pour plus d'informations sur les URL pour les widgets et les pages de commande Interface graphique Web, voir le *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Configuration d'un environnement d'équilibrage de charge

Vous pouvez configurer un cluster d'équilibrage de charge composé de noeuds de portail ayant des configurations identiques pour répartir uniformément les sessions utilisateur. L'équilibrage de charge est idéal pour les environnements avec un grand nombre d'utilisateurs. En cas d'échec d'un noeud dans un cluster, les nouvelles sessions utilisateur sont dirigées vers les autres noeuds actifs. L'équilibrage de charge est fourni dans Concentrateur des services d'application du tableau de bord.

La charge de travail est répartie par session et non par requête. En cas de défaillance d'un noeud dans un cluster, les utilisateurs ayant une session sur ce noeud doivent se reconnecter pour accéder à Interface graphique Web. Tout travail non sauvegardé n'est pas récupéré.

Pour plus d'informations sur l'installation et la configuration d'un environnement de l'équilibrage de charge, recherchez *Load balancing for Dashboard Application Services Hub* dans le centre de documentation Jazz for Service Management à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

En plus de la configuration de l'équilibrage de charge sur Concentrateur des services d'application du tableau de bord, vous devez effectuer des réglages dans le fichier Interface graphique Web `server.init` chaque fois que vous ajoutez un nœud à un cluster d'équilibrage de charge, ou chaque fois que vous supprimez un nœud d'un cluster. La configuration pour `server.init` est décrite ci-dessous.

Procédure

- Pour démarrer les opérations d'équilibrage de charge de l'Interface graphique Web sur un noeud, procédez comme suit :
  1. Ouvrez le fichier *REP_INSTALL_WEBGUI*`/etc/server.init` dans un éditeur de texte et recherchez les propriétés qui commencent par la propriété **`cluster.mode`**.
  2. Définissez les valeurs des propriétés de la manière suivante :

Tableau 94. Configuration des propriétés d'équilibrage de charge

Propriété	Valeur
`cluster.mode`	`on`
`cluster.hostname`	Nom ou adresse TCP/IP de l'hôte qui exécute le nouveau noeud. Par exemple, `server1`.

Tableau 94. Configuration des propriétés d'équilibrage de charge (suite)

Propriété	Valeur
cluster.port	Numéro de port SSL utilisé par le serveur de l'Interface graphique Web. Par exemple 16311.

3. Définissez **timedtasks.enabled** sur true.
4. Configurez les plannings des tâches temporisées le cas échéant. Définissez le même ensemble de tâches temporisées avec des plannings identiques sur tous les noeuds du cluster.
5. Redémarrez le serveur.

Le noeud est relié au cluster et lit les données de configuration à partir de la base de données.

- Pour supprimer un nœud d'un cluster :
  1. Assurez-vous qu'aucun des utilisateurs n'est connecté au noeud.
  2. Pour supprimer les informations d'équilibrage de charge pour le nœud à partir de la base de données de configuration du cluster, exécutez la commande d'API d'administration (WAAPI) de l'Interface graphique Web suivante à partir du noeud :

     ```
     WEBGUI_HOME/waapi/etc/samples/cluster_removenode.xml
     ```
  3. Ouvrez server.init et définissez la propriété **cluster.mode** sur off. Les propriétés se trouvent dans tableau 94, à la page 603. Vous pouvez éventuellement réinitialiser les autres propriétés.
  4. Redémarrez le serveur.

  Le nœud est restauré en tant que système autonome.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Référence associée:

Annexe C, «Propriétés server.init», à la page 687
Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*/etc/server.init. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité directement et lu au démarrage du serveur.

L'Interface graphique Web dans un environnement d'équilibrage de charge

Informations relatives au fonctionnement de l'Interface graphique Web dans un environnement d'équilibrage de charge et les implications de gestion et d'utilisation du produit.

Un environnement d'équilibrage de charge est composé d'un groupe de serveurs d'Interface graphique Web liés entre eux et qui fonctionnent comme un seul serveur. Le groupe de de serveurs est nommé *cluster* et chaque serveur est appelé *nœud*.

Les avantages principaux d'un cluster sont les suivants :

- Equilibrage de charge – où la charge de travail liée aux demandes de service des utilisateurs est répartie entre les nœuds. Cette fonction améliore la performance globale du système.

- Disponibilité – maintenir la disponibilité de la surveillance réseau même si certains nœuds de cluster sont indisponibles pour une raison quelconque (par exemple, ils sont éteints à des fins de maintenance).

Les sections ci-après contiennent de plus amples informations sur les clusters, leur gestion et leur utilisation :

- «Structure d'un cluster»
- «Données de configuration»
- «Mise à jour des données de configuration», à la page 606
- «Conditions nécessaires à la modification des données de configuration», à la page 607
- «Administration d'un cluster d'équilibrage de charge», à la page 608
- «Utilisation d'un cluster d'équilibrage de charge», à la page 609

Structure d'un cluster :

Un cluster est composé d'un groupe de serveurs d'Interface graphique Web, d'un serveur HTTP et d'une base de données DB2.

- Les serveurs exécutent les demandes de service des utilisateurs. Chaque serveur est également configuré pour faire confiance aux autres serveurs du cluster et peut communiquer avec les autres membres du cluster. Ceci leur permet de fonctionner comme une seule unité.
- Le serveur HTTP répartit les sessions HTTP des utilisateurs entre les serveurs. Il attribue les demandes aux serveurs de manière aléatoire ou par permutation circulaire. La méthode utilisée par le serveur HTTP dépend de sa configuration lors de l'installation.
- La base de données DB2 conserve les données de configuration du cluster.

Données de configuration :

Les données de configuration définissent le fonctionnement d'un serveur d'Interface graphique Web. Il est organisé différemment dans un cluster que dans un serveur autonome.

Un serveur d'Interface graphique Web autonome conserve ses données de configuration dans un système de fichiers local. Dans un cluster, la base de données DB2 conserve les données de configuration de l'intégralité du cluster. Il s'agit d'une copie maître des données partagée par tous les nœuds du cluster. Un ensemble de données de configuration unique signifie que chaque nœud est configuré de la même manière. Aucune donnée de configuration n'est spécifique à un nœud de cluster.

Bien que la base de données conserve la copie maître, chaque nœud possède une copie dans son système de fichiers local, pour des raisons de tolérance aux pannes. Ceci permet au cluster de continuer à fonctionner si la base de données de configuration devient indisponible au cours du fonctionnement. Lorsqu'un nœud démarre, il lit un ensemble complet de données de configuration à partir de la base de données dans le système de fichiers local et le charge en mémoire pour améliorer les performances.

Les données de configuration conservées dans la base de données sont les suivantes :

- Sources de données

- Utilisateurs, groupes et rôles
- Mises en page, informations sur la page personnalisée et descripteurs de widget
- Descripteurs de déploiement
- Filtres et vues
- Tous les éléments du magasin de configuration :
  - Menus AEL et données de configuration des menus
  - Métriques des jauges
  - Invites
  - Outils
  - Préférences utilisateur
- Préférences AEL comme par exemple le délai d'actualisation et le nombre de lignes à afficher
- Propriétés de l'Interface graphique Web comme le fuseau horaire par défaut et le délai d'attente
- Cartes et ressources, ainsi que leurs propriétés
- Jauges et leurs propriétés
- Graphiques et leurs propriétés
- Informations d'événements prévisibles
- Evénements TADDM
- Informations d'accès au widget Cadre incorporé

Mise à jour des données de configuration :

Les modifications apportées aux données de configuration doivent être coordonnées dans l'intégralité du cluster, sans tenir compte du nœud à l'origine des modifications.

Les données de configuration peuvent être modifiées de trois façons :

- Via les fonctions de l'Interface graphique Web elle-même (par exemple, définition d'un ensemble de préférences pour un widget)
- En modifiant directement les fichiers de configuration (par exemple, définition des métriques d'une jauge)
- A l'aide des commandes WAAPI (par exemple, activation des événements prévisibles)

Une modification peut provenir de n'importe quel nœud du cluster. Cependant, cette modification doit être propagée dans l'intégralité du cluster pour maintenir l'homogénéité de la configuration du cluster.

Mise à jour de la base de données

Le processus de modification des données de configuration est le suivant :

1. L'utilisateur d'un nœud modifie un élément de la configuration et demande au nœud d'enregistrer la modification.
2. Le nœud écrit les nouvelles informations (par exemple, un fichier de configuration) dans la base de données.
3. Le nœud signale à tous les autres nœuds du cluster que des informations de configuration ont été modifiées.
4. Le nœud met à jour sa copie locale des données de configuration pour répercuter la modification.

5. Les autres nœuds du cluster lisent les nouvelles informations dans la base de données et mettent à jour les copies dans leurs systèmes de fichiers locaux.
6. Le cluster continue de fonctionner avec les nouveaux paramètres de configuration.

Détection des modifications dans les fichiers de configuration

Il n'est pas toujours nécessaire de redémarrer le cluster ou ses nœuds pour collecter les nouvelles informations de configuration. Au lieu de cela, les modifications des données de configuration sont automatiquement appliquées le cas échéant. Cette opération est réalisée via :

- La fonction des tâches temporisées de l'Interface graphique Web
- Un fichier répertoriant les fichiers à surveiller et un ensemble de processus de surveillance associé

Les tâches temporisées déterminent lorsqu'un nœud charge des fichiers modifiés de la base de données.

Le fichier se nomme *REP_INSTALL_WEBGUI*`/etc/system/stores.lst` et comprend une liste de tous les fichiers de configuration conservés dans la base de données. Lorsqu'un nœud démarre ou se joint à un cluster, il crée un ensemble de processus qui surveille tous les fichiers répertoriés dans `stores.list`. Lorsqu'une modification se produit dans l'un de ces fichiers, le processus correspondant propage le fichier modifié dans la base de données DB2 et signale la modification aux autres nœuds.

Cette fonction de surveillance de fichier signifie qu'il n'est pas nécessaire pour un composant individuel de l'Interface graphique Web (comme par exemple un widget) de savoir si les informations de configuration sont conservées dans une base de données ou dans un système de fichiers local. Au lieu de cela, le composant écrit toujours les modifications apportées à sa configuration directement dans le système de fichiers local. Les processus de surveillance se chargent de mettre à jour la base de données.

Il existe des exceptions pour lesquelles un redémarrage du nœud, et généralement du cluster, est nécessaire. La modification des fichiers suivants nécessite un redémarrage du serveur :

- `server.init`
- `ncwDataSourceDefinitions.xml`

Conditions nécessaires à la modification des données de configuration :

Pour pouvoir fonctionner correctement, certaines conditions doivent être réunies pour que le cluster autorise la modification de ses données de configuration.

Pour que le cluster fonctionne correctement, la base de données DB2 doit être disponible. La base de données est le point de coordination clé du cluster car elle contient les données de configuration.

Si la base de données n'est pas disponible une fois le cluster démarré, les opérations se poursuivent, chaque nœud utilisant sa copie locale des données de configuration. Cependant, les nœuds empêchent toute modification des données de configuration. Cette situation se poursuit jusqu'à ce que la base de données DB2 soit à nouveau disponible. Les nœuds du cluster actualisent alors leur configuration stockée localement à partir de la base de données et autorisent à

nouveau la modification des données de configuration. La règle autorisant les modifications uniquement lorsque la base de données est disponible permet de garantir la synchronisation permanente du cluster et un comportement homogène dans le cluster.

Lorsqu'un nœud démarre et se joint au cluster, il lit les données de configuration dans la base de données, même s'il possède des données dans son système de fichiers local. Les nœuds effectuent cette action pour s'assurer qu'ils possèdent les données de configuration les plus récentes. Si la base de données n'est pas disponible lorsqu'un nœud démarre, il ne peut pas poursuivre car il ne peut pas vérifier que sa copie locale des données de configuration est à jour.

Outre les données de configuration, les nœuds d'un cluster doivent s'exécuter avec la même version de l'Interface graphique Web, avec le même ensemble de fonctions, et configuré de manière identique. Comme pour les données, il s'agit du seul moyen pour fournir un service commun aux utilisateurs de l'Interface graphique Web.

Administration d'un cluster d'équilibrage de charge : La gestion d'un cluster d'équilibrage de charge présente deux aspects que vous devez connaître :

- «Gestion quotidienne»
- «Gestion de cluster»

Gestion quotidienne

Pour la gestion quotidienne, pensez que chaque modification effectuée s'applique toujours à l'intégralité du cluster et non uniquement au nœud sur lequel vous avez effectué la modification. Par exemple, l'ajout d'un utilisateur sur un nœud ajoute cet utilisateur sur tous les nœuds. Un léger temps de décalage peut se produire avant qu'un modification s'applique à tous les nœuds. Cela dépend de la fréquence définie pour chaque intervalle de tâche temporisée, et du délai avant la prochaine exécution de la fonction de tâches temporisées.

Un des avantages de la propagation des données de configuration est la simplification de votre travail de gestion. Vous ne devez effectuer chaque modification qu'une seule fois, et le cluster s'assure que tous les nœuds la reçoive. Si la base de données n'est pas disponible, vous ne pouvez effectuer aucune modification dans les données de configuration. Lorsque vous utilisez directement l'Interface graphique Web, le système vous empêche d'enregistrer toute modification de données. Lorsque vous modifiez des fichiers ou utilisez WAAPI, le nœud que vous utilisez ne propage pas les informations modifiées tant que la base de données n'est pas à nouveau disponible.

Gestion de cluster

Une fois configuré, un cluster ne nécessite que peu d'administration en dehors de la gestion quotidienne que requiert toute installation de l'Interface graphique Web. Cependant, l'Interface graphique Web vous fournit un ensemble complet d'outils pour administrer le cluster. Ces outils vous permettent d'effectuer les actions suivantes :

- Activer l'équilibrage de charge après l'installation
- Administrer la fonction de tâches temporisées
- Ajouter et supprimer des nœuds
- Resynchroniser un nœud de cluster

- Exporter des informations de configuration d'un environnement de test dans une production
- Gérer la liste des fichiers à surveiller et à propager dans la base de données lorsqu'ils sont modifiés

Utilisation d'un cluster d'équilibrage de charge : Pour les utilisateurs, l'Interface graphique Web se comporte quasiment de la même manière dans un environnement groupé qu'avec un serveur autonome. La seule différence qu'ont pu noter les utilisateurs après avoir intégré un environnement groupé, est une amélioration de la réactivité du produit. Ceci est du à l'amélioration globale de la performance fournie par le cluster.

Définition de l'accès utilisateur au widget Cadre incorporé

Si vous prévoyez de créer un contenu, par exemple des cartes sur des widgets Cadre incorporé, vous devez permettre à tous les utilisateurs non administrateurs d'accéder au widget.

Pourquoi et quand exécuter cette tâche

Par défaut, les utilisateurs en lecture-écriture et les utilisateurs en lecture seule ne peuvent pas accéder au widget Cadre incorporé. Seuls les utilisateurs administrateurs, c'est-à-dire ceux ayant le rôle ncw_admin, peuvent y accéder.

Pour octroyer aux utilisateurs en lecture-écriture et en lecture seule l'accès au widget Cadre incorporé :

Procédure

1. Dans le panneau de navigation, cliquez sur **Settings** > **Portlet Management**.
2. Dans la page Portlet Management (Gestion des portlets), cliquez sur **Uncategorized Portlets** > **Cadre incorporé**.
3. Cliquez sur **Roles with access to this portlet (Rôles ayant accès à ce portlet)** puis sur **Ajouter**.
4. Dans la liste, sélectionnez les rôles auxquels vous voulez octroyer l'accès au widget :
   - Pour les utilisateurs en lecture-écriture, sélectionnez **ncw_user** et **netcool_rw**.
   - Pour les utilisateurs en lecture seule, sélectionnez **ncw_user** et **netcool_ro**.
5. Cliquez sur **Ajouter** puis sur **Enregistrer**.

Concepts associés:

«L'Interface graphique Web dans un environnement d'équilibrage de charge», à la page 604
Informations relatives au fonctionnement de l'Interface graphique Web dans un environnement d'équilibrage de charge et les implications de gestion et d'utilisation du produit.

Activation des connexions multiples

Configurez Concentrateur des services d'application du tableau de bord de sorte à autoriser plusieurs utilisateurs à se connecter à l'aide du même ID utilisateur et du même mot de passe.

Procédure

1. Connectez-vous en tant qu'administrateur et ouvrez le fichier *REP_INSTALL_JazzSM*/config/cells/Cellule_Noeud01_JazzSM/applications/isc.ear/deployments/isc/isclite.war/WEB-INF/consoleProperties.xml pour édition.
2. Recherchez la propriété portant l'attribut **id** de ENABLE.CONCURRENT.LOGIN et définissez sa valeur sur true.
3. Redémarrez le serveur.

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Installation et configuration de Tivoli Common Reporting

Tivoli Common Reporting V2.1.1 est fourni en tant que composant facultatif du module d'installation de Tivoli Netcool/OMNIbus. Tivoli Common Reporting est distribué sous forme de fichier compressé disponible sur CD ou que vous pouvez télécharger à partir du site Web en ligne IBM Passport Advantage.

Pour plus d'informations sur l'installation et la configuration de Tivoli Common Reporting, consultez le Tivoli Common Reporting à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp?topic=/com.ibm.tivoli.tcr.doc_211/ctcr_prodoverview.html.

Tâches associées:

«Obtention du module d'installation», à la page 31
Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

Fournisseur de données de l'Interface graphique Web

Les données sont poussées dans le Concentrateur des services d'application du tableau de bord à partir de l'Interface graphique Web par le fournisseur de données de l'Interface graphique Web. Le fournisseur de données définit les données de l'Interface graphique Web qu'il est possible d'interroger à partir du Concentrateur des services d'application du tableau de bord. Le fournisseur de données expose des données d'événement dans plusieurs sources de données qui sont des groupes de fichiers. Les fichiers comportent des paramètres qui contrôlent quelles données d'événement sont exposées et la vue de ces données d'événement.

Remarque : Les sources de données dans le contexte du Concentrateur des services d'application du tableau de bord sont différentes de celles qui sont définies pour le fil d'événements dans l'Interface graphique Web. Un source de données dans le Concentrateur des services d'application du tableau de bord ne peut pas être un ObjectServer. Une source de données dans l'Interface graphique Web est généralement un ObjectServer.

Fichiers

Le tableau suivant décrit les fichiers qui sont inclus dans le fournisseur de données et les paramètres pour contrôler l'affichage des données d'événement dans le Concentrateur des services d'application du tableau de bord. Outre les paramètres du tableau, vous pouvez spécifier des paramètres d'affichage lorsque vous créez les widgets dans le Concentrateur des services d'application du tableau de bord.

Tableau 95. Fichiers dans le fournisseur de données d'événement

Name	Paramètres obligatoires	Description
Détail d'événement	Série Source de données	Renvoie les détails de l'événement dont la série est spécifiée dans la source de données sélectionnée. Le fichier est identique à l'ensemble d'informations affiché dans l'onglet **Détails** de la fenêtre Informations sur l'événement d'un afficheur d'événements. Généralement, ces données proviennent de la table alerts.details de l'ObjectServer.
Zones d'événement	Série Source de données	Renvoie les informations sur l'événement dont la série est spécifiée dans la source de données sélectionnée. Le fichier est identique à l'ensemble d'informations affiché dans l'onglet **Zones** de la fenêtre Informations sur l'événement d'un afficheur d'événements. Généralement, ces données proviennent de la table alerts.status de l'ObjectServer.
Regroupement d'événements	Filter View	Ce fichier fonctionne uniquement si le regroupement d'événements est activé dans l'Interface graphique Web. Etant donné que le jeu de données est hiérarchique, utilisez un widget d'arborescence de tableau dans le Concentrateur des services d'application du tableau de bord pour visualiser les données.
Evénements : *nom_vue* (*type_vue*)	Filter	Renvoie un fichier pour chaque vue.
Récapitulatif des événements	Filter	Renvoie une ligne pour chaque gravité correspondante dans le filtre sélectionné, avec le nombre d'événements de chaque gravité.

Tableau 95. Fichiers dans le fournisseur de données d'événement (suite)

Name	Paramètres obligatoires	Description
Récapitulatif du filtre	Filter	Renvoie une ligne unique pour le filtre sélectionné avec chaque gravité correspondante dans une colonne différente. Le résumé Filtre contient des informations telles que le nombre total d'événements, la métrique des filtres et la gravité maximale.
Entrées de journal	Série Source de données	Renvoie les entrées de journal de l'événement dont la série est spécifiée dans la source de données sélectionnée. Le fichier est identique à l'ensemble d'informations affiché dans l'onglet **Journal** de la fenêtre Informations sur l'événement d'un afficheur d'événements. Généralement, ces données proviennent de la table alerts.journal de l'ObjectServer.
Métriques	Métriques	Renvoie la valeur de courant d'une ou plusieurs métriques.

Si vous utilisez un Concentrateur des services d'application du tableau de bord à connexion à utilisateur unique, les fichiers de filtre, vues et préférences utilisateur affichent uniquement les filtres, les vues ou les préférences qui sont associés à cet utilisateur.

Sources de données

Les sources de données du fournisseur de données sont les suivantes :

- «Données d'agrégation»
- «Toutes les données», à la page 613
- «Informations sur un événement», à la page 613
- «Evénements», à la page 613

Données d'agrégation

Cette source de données contient les fichiers suivants :

- Regroupement d'événements
- Récapitulatif des événements
- Récapitulatif du filtre
- Metrics

Toutes les données

Toutes les données provenant de toutes les autres sources de données du fournisseur de données d'événement. Cette source de données contient les fichiers suivants :

- Détail d'événement
- Zones d'événement
- Regroupement d'événements
- Evénements : Par défaut : (global)
- Récapitulatif des événements
- Récapitulatif du filtre
- Filtres
- Entrées de journal

Informations sur un événement

Données provenant d'un événement unique. Pour afficher ces données, spécifiez la source de données (à savoir l'ObjectServer ou une autre source du fil d'événement) et la série de l'événement. Cette source de données contient les fichiers suivants :

- Détail d'événement
- Zones d'événement
- Entrées de journal

Evénements

Cette source de données contient un fichier pour chaque vue à laquelle peut accéder chaque utilisateur. Par exemple, pour un utilisateur non administrateur, un fichier pour chaque vue utilisateur et chaque vue globale est renvoyé. Au minimum, cette source de données contient le fichier suivant pour la vue globale par défaut.

- Evénements : Par défaut : (global)

Visualisation de données d'événement dans le Concentrateur des services d'application du tableau de bord

Vous pouvez créer des tableaux de bord dans le Concentrateur des services d'application du tableau de bord et ajoutez les widgets permettant d'afficher les données d'événement. Le flux d'événements pour les widgets Interface graphique Web est fourni par la source de données ou les sources de données. Les widgets de la bibliothèque Tivoli Widgets Library (TWL) recueillent des données d'événement à partir du fournisseur de données Interface graphique Web.

Pour plus d'informations sur chaque widget TWL qui se trouve dans Concentrateur des services d'application du tableau de bord, recherchez *Tivoli Widgets Library* dans le centre de documentation Jazz for Service Management à l'adresse http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html

Conseil : Pour spécifier le fichier qui alimente un widget, dans la fenêtre du widget, cliquez sur **Options d'édition** > **Editer**. Dans la page Sélectionner un fichier, cliquez sur **Afficher tout** pour visualiser une liste des fichiers possibles. Les

fichiers de l'Interface graphique Web provenant du fournisseur de données de l'Interface graphique Web sont intitulés **Provider: Netcool/OMNIbus Interface graphique Web**.

Procédure

- Pour intégrer des données d'événement dans un widget TWL, modifiez le widget et sélectionnez un ensemble de données dans l'Interface graphique Web. Pour des informations sur les sources de données, les fichiers et les paramètres du fournisseur de données de l'Interface graphique Web, consultez la description du fournisseur de données dans l'interface utilisateur. Par exemple, vous pouvez définir les paramètres de l'interface graphique Interface graphique Web Métriques, puis utiliser ceux-ci pour alimenter une jauge d'état TWL ou jauge d'état de la valeur. Lorsque vous sélectionnez le jeu de données de métriques du fournisseur de donnée de l'Interface graphique Web, toutes les métriques définies sont disponibles pour la sélection.
- Vous pouvez effectuer des intégrations de lancement en contexte à partir de widgets hotspot et web TWL en spécifiant une URL qui lance un widget d'Interface graphique Web dans la zone **URL cible**.
- Vous pouvez créer des connexions entre des widgets de sorte qu'un widget cible soit mis à jour dans le contexte du widget source.

Comment insérer dans Tivoli Widget Library des données d'événement provenant du fournisseur de données de l'Interface graphique Web

Vous pouvez utiliser le fournisseur de données de l'Interface graphique Web pour insérer des widgets provenant de Tivoli Widget Library. Ces widgets comprennent des tableaux, des listes, des graphiques, des barres de volume et des jauges. La compatibilité de ces widgets avec les sources de données et les ensembles de données du fournisseur de données de l'Interface graphique Web est décrit dans cette section.

Pour plus d'informations sur les widgets de Tivoli Widget Library, recherchez *Tivoli Widget Library* dans le centre de documentation Jazz for Service Management à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome.

Les données d'événement de l'Interface graphique Web sont intégralement prises en charge dans les widgets de tableau. Les widgets de liste et de graphique peuvent ne pas s'afficher correctement. Une prise en charge limitée est fournie pour les widgets de jauge.

Restriction : Pour les widgets de jauge et de table, seule 1 métrique peut être sélectionnée. Plusieurs métriques peuvent être sélectionnées pour les widgets de graphiques.

Le lancement en contexte à partir du Concentrateur des services d'application du tableau de bord vers l'Interface graphique Web est pris en charge dans les widgets Web et les widgets de macro directe. Vous pouvez effectuer le lancement à partir du Concentrateur des services d'application du tableau de bord vers une liste d'événements actifs (AEL) ou une carte. Pour configurer le lancement, entrez l'adresse URL dans la zone **URL cible** du widget. Les widgets Web peuvent également être hébergés sur des pages d'Interface graphique Web hôte dans le Concentrateur des services d'application du tableau de bord. Cette fonctionnalité est prise en charge par les listes AEL, les afficheurs d'événements et les cartes.

Pour plus d'informations sur le déploiement de l'Interface graphique Web dans le Concentrateur des services d'application du tableau de bord, consultez le document *Netcool/OMNIbus Web GUI Integration Features for JazzSM UI (DASH)* sur le wiki Tivoli Netcool/OMNIbus sur Service Management Connect à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Netcool%20OMNIbus/page/V7.4%20FP2%2C%20Setting%20up%20Netcool%20OMNIbus%20Web%20GUI%20integration%20features%20in%20Jazz%20for%20Service%20Management.

Le tableau ci-dessous décrit les ensembles de données du fournisseur de données d'Interface graphique Web qui peuvent être utilisés dans les widgets de Tivoli Widget Library, ainsi que d'autres aspects de la visualisation des données d'événement à partir de l'Interface graphique Web.

Tableau 96. Utilisation des données d'événement de l'Interface graphique Web dans les widgets de Tivoli Widget Library

Widget	**Utilisez ces ensembles de données pour le flux de données d'événement à partir de l'Interface graphique Web**	**Remarques**
Jauge analogique	Métriques	Une seule métrique peut être sélectionnée pour chaque instance du widget sur une page.
Graphique		
Macro directe		
Liste	Récapitulatif des événements, Récapitulatif du filtre, Evénements (pour n'importe quelle vue), Métriques	
Compteur d'actualisation		
Status		
Jauge d'état	Métriques	Une seule métrique peut être sélectionnée pour chaque instance du widget sur une page.
Table	Tous les ensembles de données	
Texte		
Sélecteur de temps		
Topologie		
Tableau arborescent		
Jauge d'état avec valeur	Métriques	Une seule métrique peut être sélectionnée pour chaque instance du widget sur une page.

Tableau 96. Utilisation des données d'événement de l'Interface graphique Web dans les widgets de Tivoli Widget Library (suite)

Widget	Utilisez ces ensembles de données pour le flux de données d'événement à partir de l'Interface graphique Web	Remarques
Barre de volume	Métriques et Récapitulatif du filtre	Les données les plus utiles à afficher sur la barre de volume sont la valeur métrique issue de l'ensemble de données Métriques, ou le nombre total d'événements, la métrique de filtre, ainsi que la gravité maximale de l'ensemble de données Récapitulatif du filtre.
Web		

Concepts associés:

«Fournisseur de données de l'Interface graphique Web», à la page 610
Les données sont poussées dans le Concentrateur des services d'application du tableau de bord à partir de l'Interface graphique Web par le fournisseur de données de l'Interface graphique Web. Le fournisseur de données définit les données de l'Interface graphique Web qu'il est possible d'interroger à partir du Concentrateur des services d'application du tableau de bord. Le fournisseur de données expose des données d'événement dans plusieurs sources de données qui sont des groupes de fichiers. Les fichiers comportent des paramètres qui contrôlent quelles données d'événement sont exposées et la vue de ces données d'événement.

Ensembles de données source et cible pour la connexion de widgets

Vous pouvez créer des connexions entre des widgets de sorte qu'un widget cible soit mis à jour dans le contexte du widget source à la suite d'un événement nodeClickedOn.

Le tableau ci-dessous décrit les ensembles de données du fournisseur de données d'interface graphique Web qui peuvent être utilisés comme ensembles de données source et cible pour la connexion de widgets, ainsi que d'autres aspects de la visualisation des données d'événement à partir de l'interface graphique Web.

Tableau 97. Ensembles de données source et cible pour la connexion de widgets

Ensemble de données source	Ensemble de données cible	Transformation nécessaire	Remarques
Récapitulatif du filtre	Récapitulatif des événements	Aucun	L'ensemble de données cible sera mis à jour pour afficher la distribution de la gravité pour le même filtre en tant qu'ensemble de données source.

Tableau 97. Ensembles de données source et cible pour la connexion de widgets (suite)

Ensemble de données source	Ensemble de données cible	Transformation nécessaire	Remarques
Récapitulatif du filtre	Evénements	Aucun	L'ensemble de données cible sera mis à jour pour afficher des événements pour le même filtre en tant qu'ensemble de données source.
Récapitulatif des événements	Evénements	Aucun	L'ensemble de données cible sera mis à jour pour afficher des événements pour le même filtre et le niveau de gravité en tant que ligne d'ensemble de données source.
Récapitulatif des événements	Récapitulatif du filtre	Aucun	L'ensemble de données cible sera mis à jour pour afficher des informations relatives au même filtre en tant qu'ensemble de données source.
Métriques	Evénements	ShowGaugeEvents	L'ensemble de données cible sera mis à jour pour afficher des événements pour le filtre qui est associé à l'ensemble de données source, le cas échéant.
Métriques	Récapitulatif des événements	ShowGaugeEvents	L'ensemble de données cible sera mis à jour pour afficher la distribution de la gravité pour le filtre qui est associé à l'ensemble de données source, le cas échéant.
Métriques	Récapitulatif du filtre	ShowGaugeEvents	L'ensemble de données cible sera mis à jour pour afficher des informations relatives au filtre qui est associé à l'ensemble de données source, le cas échéant.

Tableau 97. Ensembles de données source et cible pour la connexion de widgets (suite)

Ensemble de données source	Ensemble de données cible	Transformation nécessaire	Remarques
Evénements	Zones événement	Aucun	L'ensemble de données cible sera mis à jour pour afficher des valeurs de zone pour le même événement en tant que ligne d'ensemble de données source.
Evénements	Détails d'événement	Aucun	L'ensemble de données cible sera mis à jour pour afficher des valeurs de détails d'événement pour le même événement en tant que ligne d'ensemble de données source.
Evénements	Entrées de journal	Aucun	L'ensemble de données cible sera mis à jour pour afficher des entrées de journal pour le même événement en tant que ligne d'ensemble de données source.

Concepts associés:

«Fournisseur de données de l'Interface graphique Web», à la page 610
Les données sont poussées dans le Concentrateur des services d'application du tableau de bord à partir de l'Interface graphique Web par le fournisseur de données de l'Interface graphique Web. Le fournisseur de données définit les données de l'Interface graphique Web qu'il est possible d'interroger à partir du Concentrateur des services d'application du tableau de bord. Le fournisseur de données expose des données d'événement dans plusieurs sources de données qui sont des groupes de fichiers. Les fichiers comportent des paramètres qui contrôlent quelles données d'événement sont exposées et la vue de ces données d'événement.

Redémarrage du serveur

Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Pourquoi et quand exécuter cette tâche

Redémarrez le serveur pendant ou après les actions suivantes sur votre serveur d'Interface graphique Web :

- Modification d'un des fichiers suivants :
  - `server.init`
  - `ncwDataSourceDefinitions.xml`

  - `virtualhosts.xml`
  - `deployment.xml`
  - `security.xml`
  - `winconfig.xml`
  - N'importe quel fichier de propriétés dans le répertoire *REP_INSTALL_JazzSM*`/properties`.
- Définition d'un cluster d'équilibrage de charges
- Ajout d'un noeud à un cluster d'équilibrage de charge
- Ajout ou modification de registres d'utilisateurs
- Sauvegarde et restauration de l'Interface graphique Web
- Copie des configurations d'un autre serveur d'Interface graphique Web
- Configuration du chiffrement
- Configuration de l'authentification unique (SSO)
- Configuration de LDAP ou d'Active Directory et de leurs connexions

Si vous n'utilisez pas la fonction de tâches temporisées dans le fichier `server.init`, vous devez également redémarrer le serveur après modification de tout fichier dans les répertoires suivants de *REP_INSTALL_WEBGUI*`/etc` :

- `configstore`
- `cgi-bin`
- `graphiques`
- `charts/definitions`
- `templates` et tous les répertoires qu'il contient

Procédure

Pour redémarrer le serveur :

1. Accédez à *REP_INSTALL_JazzSM*`/bin`.
2. Arrêtez le serveur :
   - Linux UNIX `stopServer.sh server1`

     Avertissement : Les systèmes Linux et Unix vous invitent à entrer le nom d'utilisateur et le mot de passe de l'administrateur.
   - Windows `stopServer.bat server1`

   Remarque : Spécifiez le nom d'utilisateur du système d'exploitation correct.
3. Attendez quelques instants pour que le serveur soit complètement arrêté puis vérifiez que tous les processus Java ont cessé de s'exécuter. Ceci est particulièrement important lorsque vous installez un groupe de correctifs. Les messages suivants confirment que le serveur est arrêté :

   ```
   ADMU3201I: Server stop request issued
   (Une demande d'arrêt du serveur a été émise).
   Waiting for stop status (Attente de l'état d'arrêt).
   ADMU4000I: Server server1 stop completed (Arrêt du serveur serveur1 terminé).
   ```
4. Démarrez le serveur :
   - Linux UNIX `startServer.sh server1`
   - Windows `startServer.bat server1`

Tâches associées:

«Configuration du mode transition SP800-131 sur le serveur d'applications», à la page 541
Pour le mode de transition, une configuration minimale est requise sur l'instance du serveur d'applications qui héberge l'Interface graphique Web. Si vous le souhaitez, vous pouvez effectuer des configurations supplémentaires telles que l'application de TLS 1.2 et la création des certificats. Si ces configurations sont requises pour le mode strict, elles ne sont pas nécessaires pour le mode transition.

«Configuration du mode strict SP800-131 sur le serveur d'applications», à la page 545
Sur le serveur d'applications, activez le mode strict SP800-131. Puis, dans le fichier de propriétés client SSL, spécifiez la norme de sécurité SP800-131.

Chapitre 19. Exemples de scénarios d'installation de Tivoli Netcool/OMNIbus (architectures de base, de reprise en ligne et de bureau)

Certains exemples de scénarios d'installation de Tivoli Netcool/OMNIbus des architectures de base, de reprise en ligne et de bureau sont décrits ici. Chaque exemple d'architecture est construit sur le précédent.

Exemple d'architecture de base de Tivoli Netcool/OMNIbus

L'exemple d'architecture de base de Tivoli Netcool/OMNIbus utilise une seule sonde Syslog pour surveiller une application qui écrit des messages de débogage dans le démon syslog sur son ordinateur hôte.

La sonde Syslog réachemine des événements vers le serveur ObjectServer s'exécutant sur un deuxième ordinateur hôte. Les utilisateurs affichent les événements à l'aide d'un bureau Windows sur un troisième hôte. Le serveur ObjectServer et la sonde s'exécutent sous contrôle de processus.

Cet exemple ajoute certaines zones à la table alerts.status une fois que le système fonctionne.

Déploiement de l'architecture de base

L'architecture de base de Tivoli Netcool/OMNIbus comprend les composants suivants : le serveur ObjectServer, l'agent de processus, la sonde Syslog et la liste d'événements.

Le serveur ObjectServer (AGG_P) et l'agent de processus s'exécutent sur un ordinateur Solaris portant le nom d'hôte nchost01. La liste d'événements s'exécute sur un ordinateur Windows portant le nom d'hôte ncdesktop. L'installation surveille une application qui écrit des messages de débogage dans le démon syslog sur un ordinateur Solaris portant le nom d'hôte targethost.

L'architecture de base de Tivoli Netcool/OMNIbus est présentée dans l'illustration suivante.

Remarque : L'intitulé **ObjectServer NETCOOLPRI** doit être remplacé par **ObjectServer principal AGG_P**.

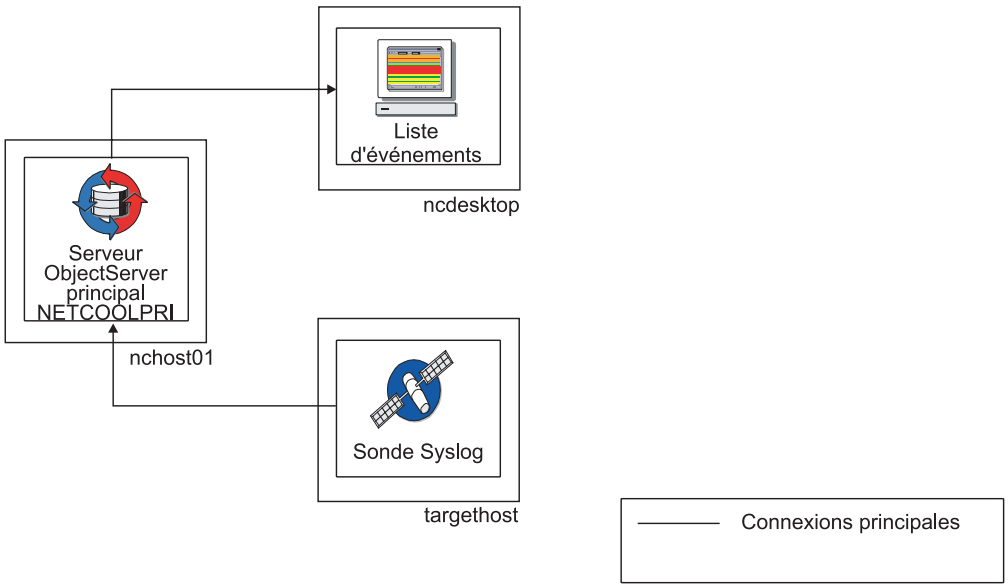

Figure 18. Exemple d'architecture de base de Tivoli Netcool/OMNIbus

Prérequis de l'architecture de base

Un compte utilisateur UNIX appelé netcool doit exister sur chaque hôte. Cet utilisateur doit être membre du groupe UNIX ncoadmin afin d'utiliser les utilitaires de contrôle de processus (**nco_pa_***).

Les variables d'environnement suivantes doivent être définies pour l'utilisateur netcool :

- $NCHOME - /opt/IBM/tivoli/netcool
- $PATH - $NCHOME/omnibus/bin:$PATH

Ce déploiement suppose que les répertoires par défaut sont utilisés.

Etape 1 : Installation du serveur ObjectServer et de l'agent de processus

Cette étape vous permet d'installer le serveur ObjectServer et l'agent de processus.

Sur l'ordinateur nchost01, procédez de la manière suivante :

1. Téléchargez le bundle d'installation de Tivoli Netcool/OMNIbus pour Solaris à partir de Passport Advantage et extrayez les fichiers.
2. Exécutez le programme d'installation `./install_gui.sh` ou `./install_console.sh`.
3. Acceptez les termes du contrat de licence ainsi que l'emplacement d'installation par défaut.
4. Sélectionnez et installez **Interface graphique d'administration**, **Outils d'administration**, **Interface graphique de l'opérateur**, **ObjectServer**, **Agent de processus**, **Support de sonde** et **extensions**.

Le serveur ObjectServer et l'agent de processus sont installés sur le même ordinateur Solaris dans l'emplacement `$NCHOME`. Des fonctions supplémentaires requises pour la configuration du système sont également installées.

Etape 2 : Installation de sondes

Pour installer les sondes sur l'ordinateur nchost01, téléchargez les sondes pertinentes à partir de Passport Advantage. Le fichier `install.txt` attenant, qui est disponible pour chaque sonde, décrit comment installer la sonde. A des fins de test, utilisez la sonde Simnet, nco_p_simnet, qui est incluse dans le module d'installation Tivoli Netcool/OMNIbus.

Etape 3 : Installation de la liste d'événements

Cette étape vous permet d'installer la liste d'événements.

Sur l'ordinateur Windows (ncdesktop), procédez comme suit :

1. Téléchargez le bundle d'installation de Tivoli Netcool/OMNIbus pour Windows à partir de Passport Advantage et extrayez les fichiers.
2. Cliquez deux fois sur le fichier `install.exe` pour démarrer l'installation.
3. Acceptez les termes du contrat de licence ainsi que l'emplacement d'installation par défaut.
4. Sélectionnez **Bureau** en tant que seule fonction installable.

Lorsque vous avez terminé l'installation, les outils de bureau, notamment la liste d'événements, sont installés sur l'ordinateur Windows.

Etape 4 : Configuration des communications

Cette étape vous permet de configurer les communications entre les composants Tivoli Netcool/OMNIbus.

Sur l'ordinateur exécutant le serveur ObjectServer (nchost01), procédez comme suit :

1. Exécutez la commande suivante pour ouvrir la fenêtre de l'éditeur de serveur :
   `$NCHOME/omnibus/bin/nco_xigen`
2. Configurez le serveur ObjectServer et les paramètres de communication de l'agent de processus en indiquant par exemple les paramètres de l'éditeur de serveur, comme indiqué dans la table suivante. Cliquez sur **Ajouter** après chaque jeu d'entrées. (La valeur SSL de 0 est disponible par défaut et est indiquée comme valeur vide dans la zone d'affichage de l'éditeur de serveur.)

Tableau 98. Paramètre de l'éditeur de serveur - architecture de base

Serveur	Nom d'hôte	Port	SSL
NCOOS_PA	nchost01	4200	0
NCOPR_PA	targethost	4300	0
AGG_P	nchost01	4100	0

3. Appliquez vos modifications et fermez l'éditeur de serveur. Cela crée le fichier `$NCHOME/etc/interfaces.solaris2`, contenant vos informations de communication.

Etape 5 : Création du serveur ObjectServer

Cette étape vous permet de créer et de démarrer un serveur ObjectServer appelé AGG_P.

Sur l'ordinateur nchost01, procédez comme suit :

1. Initialisez le serveur ObjectServer AGG_P et incluez le fichier SQL d'importation à appliquer à cet ObjectServer en exécutant la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_P -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

2. Démarrez le serveur ObjectServer en exécutant la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name AGG_P
   ```

Vous possédez maintenant un serveur ObjectServer en cours d'exécution appelé AGG_P.

Etape 6 : Test du système

Cette étape vous permet de tester le serveur ObjectServer et la liste d'événements en exécutant une sonde Simnet. La sonde Simnet envoie des événements simulés au serveur ObjectServer.

Procédez de la manière suivante :

1. Sur l'ordinateur nchost01, démarrez la sonde Simnet en exécutant la commande suivante :

   ```
   $NCHOME/omnibus/probes/nco_p_simnet -server AGG_P
   ```

2. Démarrez la liste d'événements sur l'ordinateur Windows ncdesktop :

   ```
   %NCHOME%\omnibus\desktop\NCOEvent.exe
   ```

   Connectez-vous au serveur AGG_P en tant qu'utilisateur `root` avec le mot de passe correspondant. Les événements simulés s'affichent dans la liste d'événements.

   Remarque : Le mot de passe par défaut de l'utilisateur `root` est une chaîne vide. Il ne s'agit pas de l'utilisateur et du mot de passe `root` système.

Vous avez maintenant vu que le serveur ObjectServer peut traiter des événements et les envoyer à la liste d'événements.

Etape 7 : Installation et configuration de la sonde Syslog et du démon Syslog

Cette étape comprend un certain nombre de sous-étapes, que vous devez exécuter sur l'ordinateur targethost.

1. «Configuration du démon Syslog»
2. «Installation et configuration de la sonde Syslog», à la page 625
3. «Test de la sonde Syslog», à la page 626

Configuration du démon Syslog

Cette étape vous permet de configurer le démon Syslog pour consigner les messages de débogage de l'application cible. Procédez de la manière suivante :

1. Sur l'ordinateur targethost, entrez la commande suivante :

   ```
   touch /var/log/ncolog
   ```

2. Editez le fichier /etc/syslog.conf. Ajoutez la ligne suivante :

   ```
   *.debug /var/log/ncolog
   ```

   Le séparateur entre le sélecteur et l'action *doit* être un caractère de tabulation pour que l'entrée soit acceptée par syslog.

   Remarque : Cette ligne ne doit pas être la première ligne du fichier `/etc/syslog.conf`. Si c'est le cas, cela active un bogue dans le démon syslog, où une tentative de vérification est lancée dans le premier fichier de la première entrée de `/etc/syslog.conf`. Le système syslog sera alors instable. Notez également que certaines implémentations de syslog sont limitées à 20 entrées valides dans le fichier `/etc/syslog.conf`.

3. Redémarrez le démon syslog. Recherchez l'identificateur de processus du démon syslog et émettez une commande `kill -HUP` pour ce processus. Par exemple :

   ```
   targethost# ps-ef | grep syslogd
    root 169 1 0 Dec 12 ?  0:47 /usr/sbin/syslogd
    root 26429 25748 0 16:13:13 pts/13  0:00 grep syslogd
   targethost# kill -HUP 169
   ```

   Cela force le démon Syslog à lire une nouvelle fois le fichier `/etc/syslog.conf`.

4. Vérifiez que le démon syslog envoie des messages au fichier `/var/log/ncolog` à l'aide de la commande :

   ```
   logger -p debug testing
   more /var/log/ncolog
   ```

   Le message suivant s'affiche à la fin du fichier journal :

   ```
   horodatage targethost netcool: testing
   ```

Le démon syslog est maintenant configuré pour consigner des messages de débogage provenant de l'application cible.

Installation et configuration de la sonde Syslog

Pour installer et configurer la sonde Syslog :

1. Sur l'ordinateur targethost, téléchargez le bundle d'installation de Tivoli Netcool/OMNIbus et de la sonde Syslog (nco_p_syslog) pour Solaris à partir de Passport Advantage.
2. Installez Tivoli Netcool/OMNIbus et sélectionnez **Interface graphique d'administration**, **Outils d'administration**, **Agent de processus** et **Support de sonde** comme fonctions installables.
3. Installez la sonde comme indiqué dans le fichier `install.txt`, qui est fourni pour chaque sonde. Ce fichier décrit comment installer la sonde dans les différents modes d'installation.
4. Copiez `$NCHOME/etc/omni.dat` de l'ordinateur exécutant le serveur ObjectServer (nchost01) vers le répertoire `$NCHOME/etc` sur l'ordinateur hôte cible.
5. Exécutez `$NCHOME/bin/nco_igen` sur l'ordinateur hôte cibler pour créer le fichier `interfaces.solaris2`.
6. Editez le fichier `$NCHOME/omnibus/probes/solaris2/syslog.props`. Copiez et collez les propriétés **`Manager`**, **`Server`**, et **`LogFile`** à la fin du fichier. Cela vous permet de conserver une configuration par défaut commentée dans ce fichier.
7. Supprimez la mise en commentaire et éditez les propriétés **`Manager`**, **`Server`** et **`LogFile`** collées. Utilisez les valeurs suivantes :

   ```
   Manager   :  'Syslog@targethost'
   Server    :  'AGG_P'
   LogFile   :  '/var/log/ncolog'
   ```

8. Démarrez la sonde à l'aide de la commande :`$NCHOME/omnibus/probes/nco_p_syslog &`

Vous avez terminé d'installer et de configurer la sonde Syslog.

Test de la sonde Syslog

Pour vérifier que la sonde Syslog fonctionne correctement :

1. Sur l'ordinateur targethost, vérifiez que la sonde Syslog lit les messages du fichier `/var/log/ncolog` à l'aide de la commande suivante :

   ```
   logger -p debug "testing the probe"
   ```

2. Connectez-vous au serveur ObjectServer à l'aide de l'interface SQL interactive, **nco_sql**. Utilisez la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_sql -server AGG_P -user root
   ```

3. Entrez le mot de passe `root` du serveur ObjectServer dans l'invite.
4. Déterminez si une alerte contenant un récapitulatif de `testing the probe` est présente dans la table alerts.status. Pour ce faire, entrez la commande suivante :

   ```
   1> select * from alerts.status where Summary like 'testing the probe';
   2> go
   ```

5. Si la sonde Syslog a lu l'événement et l'a réacheminé vers le serveur ObjectServer, la dernière ligne de la sortie texte est :

   ```
   (1 row affected)
   ```

6. Vous pouvez également confirmer cela en vérifiant la liste d'événements.

Vous avez terminé de tester la sonde Syslog.

Etape 8 : Configuration du contrôle de processus

Configurez le contrôle de processus sur les ordinateurs exécutant le serveur ObjectServer maître (nchost01) et la sonde Syslog (targethost).

Ordinateur exécutant le serveur ObjectServer

Cette procédure vous permet de configurer un agent de processus appelé NCOOS_PA sur nchost01. Procédez de la manière suivante :

1. Sur nchost01, éditez le fichier de configuration de l'agent de processus, `$NCHOME/omnibus/etc/nco_pa.conf`. Le fichier de configuration complet de l'agent de processus NCOOS_PA est le suivant :

   ```
   nco_process 'ObjectServer'
   {
   Command '$NCHOME/omnibus/bin/nco_objserv -name AGG_P -pa NCOOS_PA' run as 0
   Host='nchost01'
   Managed=true
   RestartMsg='The ObjectServer has been restarted'
   AlertMsg='The ObjectServer has gone down'
   RetryCount=0
   ProcessType=PaPA_AWARE
   }
   nco_service 'Omnibus'
   {
   ServiceType=Master
   ServiceStart=Auto
   process 'ObjectServer' NONE
   }
   ```

```
nco_routing
{
host 'nchost01' 'NCOOS_PA'
}
```

Pour le processus de serveur `ObjectServer` défini dans la première section du fichier `nco_pa.conf`, les premières lignes définissent la ligne de commande utilisée pour démarrer le processus et l'hôte sur lequel il s'exécute. L'élément `Managed` est défini sur `true` afin que le contrôle de processus redémarre le serveur ObjectServer s'il s'arrête pour quelque raison que ce soit.

Le service `Omnibus` contient le processus du serveur ObjectServer. L'entrée `ServiceType Master` indique que le service `Omnibus` doit être le premier à démarrer. L'entrée `ServiceStart Auto` indique que le service `Omnibus` doit démarrer automatiquement après le démarrage du démon de contrôle de processus.

La section `nco_routing` indique à chaque agent de processus l'emplacement des autres agents de processus.

2. Arrêtez le serveur ObjectServer. Vous devez également arrêter la sonde qui s'exécute sur l'ordinateur targethost.
3. Démarrez le démon de contrôle de processus à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pad -name NCOOS_PA
   ```

4. Pour vérifier que le serveur ObjectServer est en cours d'exécution, entrez la commande suivante :

   ```
   ps -ef | grep nco_objserv
   ```

Le serveur ObjectServer est maintenant en cours d'exécution sous contrôle de processus.

Ordinateur exécutant la sonde Syslog

Pour configurer un agent de processus appelé NCOPR_PA sur targethost :

1. Sur targethost, éditez le fichier `$NCHOME/omnibus/etc/nco_pa.conf`. Le fichier de configuration complet de l'agent de processus NCOPR_PA est présenté ci-dessous.

   ```
   nco_process 'SyslogProbe'
   {
   Command '$NCHOME/omnibus/probes/nco_p_syslog' run as 0
   Host='targethost'
   Managed=true
   RestartMsg='The Syslog Probe has been restarted'
   AlertMsg='The Syslog Probe has gone down'
   RetryCount=0
   ProcessType=PaPA_AWARE
   }
   nco_service 'Probes'
   {
   ServiceType=Master
   ServiceStart=Auto
   process 'SyslogProbe' NONE
   }
   nco_routing
   {
   host 'targethost' 'NCOPR_PA'
   }
   ```

   Pour le processus `SyslogProbe` défini dans la première section du fichier ci-dessus, les premières lignes définissent la ligne de commande utilisée pour

démarrer le processus et l'hôte sur lequel il se trouve. L'élément `Managed` est défini sur `true` afin que le contrôle de processus redémarre le processus s'il s'arrête pour quelque raison que ce soit.

Le service `Probes` contient le processus `SyslogProbe`. L'entrée `ServiceType Master` indique que le service `SyslogProbe` doit être le premier à démarrer. L'entrée `ServiceStart Auto` indique que le service `SyslogProbe` doit démarrer automatiquement après le démarrage du démon de contrôle de processus.

La section `nco_routing` indique à chaque agent de processus l'emplacement des autres agents de processus.

2. Démarrez le démon de contrôle de processus à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pad -name NCOPR_PA
   ```

3. Pour vérifier que la sonde est en cours d'exécution, entrez la commande suivante :

   ```
   ps -ef | grep nco_p_syslog
   ```

La sonde Syslog est maintenant en cours d'exécution sous contrôle de processus.

Etape 9 : Ajout de colonnes au serveur ObjectServer

Cette étape vous permet d'ajouter des colonnes au serveur ObjectServer AGG_P.

Procédez de la manière suivante :

1. Sur l'ordinateur targethost, arrêtez la sonde à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_stop -server NCOPR_PA -service Probes
   ```

2. A l'aide de Netcool/OMNIbus Administrator ou de la commande **`nco_sql`**, ajoutez les zones suivantes à la table alerts.status :

   ```
   CustomerID int,
   CustomerContact varchar(1024),
   ReferenceCode varchar(128),
   ```

   Si vous utilisez la commande **`nco_sql`** pour ajouter les zones, utilisez la commande ALTER TABLE. Pour de plus amples informations sur l'utilisation de Netcool/OMNIbus Administrator et de la commande ALTER TABLE, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

3. Sur l'ordinateur targethost, redémarrez la sonde à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_start -server NCOPR_PA -service Probes
   ```

   La sonde utilise un fichier de récupération qui enregistre la dernière entrée de journal lue. Elle lit cela, puis lit le fichier `/var/log/ncolog` à partir de l'entrée suivante.

4. Vérifiez que la sonde s'exécute correctement sous contrôle de processus à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_status -server NCOPR_PA -user netcool
   ```

5. Vérifiez que la sonde Syslog lit les messages à partir du fichier `/var/log/ncolog` à l'aide de la commande suivante :

   ```
   logger -p debug "testing the new tables"
   ```

6. Redémarrez la liste d'événements sur l'ordinateur Windows ncdesktop et connectez-vous à AGG_P. La liste d'événements contient un événement accompagné du récapitulatif de `testing the new tables`.

La configuration de l'architecture de base de Tivoli Netcool/OMNIbus est terminée.

Etapes suivantes

Après avoir terminé les étapes de déploiement de l'architecture de base, vous pouvez installer en option l'Interface graphique Web.

Important : Si vous souhaitez déployer l'architecture de reprise en ligne de base, n'installez pas l'Interface graphique Web à ce moment. Installez plutôt l'Interface graphique Web après avoir terminé les étapes de déploiement de l'architecture de reprise en ligne de base.

Procédez de la manière suivante :

1. Vous pouvez installer l'Interface graphique Web avec l'interface graphique ou la console ou vous pouvez effectuer une installation en mode silencieux. Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145 décrit les options disponibles pour l'installation de l'Interface graphique Web avec IBM Installation Manager.
2. Un fois l'Interface graphique Web installée, vous pouvez lancer un outil qui effectue une configuration de post-installation. Vous pouvez également configurer l'Interface graphique Web en mode silencieux. Si vous n'avez pas exécuté l'utilitaire de configuration de post-installation, vous pouvez effectuer toutes les tâches manuellement.

   L'outil crée une source de données unique qui est appelée « OMNIBUS ». Vous devez spécifier l'hôte et le numéro de port et le nom d'utilisateur et mot de passe pour cet ObjectServer. L'outil utilise l'ObjectServer pour l'authentification des utilisateurs et crée des utilisateurs et groupes par défaut Interface graphique Web dans cet ObjectServer. Lorsque l'outil termine la configuration du produit, le serveur redémarre automatiquement.

   Le mot de passe initial pour les comptes d'utilisateur par défaut, par exemple ncoadmin et ncouser, est netcool. Vous devez modifier ce mot de passe dans un environnement de production.

Exemple d'architecture de reprise en ligne de base Tivoli Netcool/OMNIbus

Vous pouvez ajouter un serveur ObjectServer de reprise en ligne (sauvegarde) à l'exemple d'architecture de base. Les données d'alerte du serveur ObjectServer maître sont répliquées dans le serveur ObjectServer de sauvegarde via une passerelle bidirectionnelle du serveur ObjectServer. Si une connexion au serveur ObjectServer maître échoue, les clients tentent de se connecter au serveur ObjectServer de sauvegarde.

Les instructions figurant dans cet exemple supposent que vous disposez d'une architecture Tivoli Netcool/OMNIbus de base existante.

Déploiement de l'architecture de reprise en ligne de base

L'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus comprend tous les composants de l'architecture de base et les composants supplémentaires suivants : le serveur ObjectServer de sauvegarde et la passerelle bidirectionnelle du serveur ObjectServer.

Le serveur ObjectServer de sauvegarde et la passerelle bidirectionnelle du serveur ObjectServer s'exécutent sur un seul ordinateur Solaris portant le nom d'hôte nchost02.

L'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus est présentée dans la figure suivante.

Remarque : Les intitulés **ObjectServer principal NETCOOLPRI** et **ObjectServer de sauvegarde NETCOOLBAK** doivent être remplacés par **ObjectServer principal AGG_P** et **ObjectServer de sauvegarde AGG_B**.

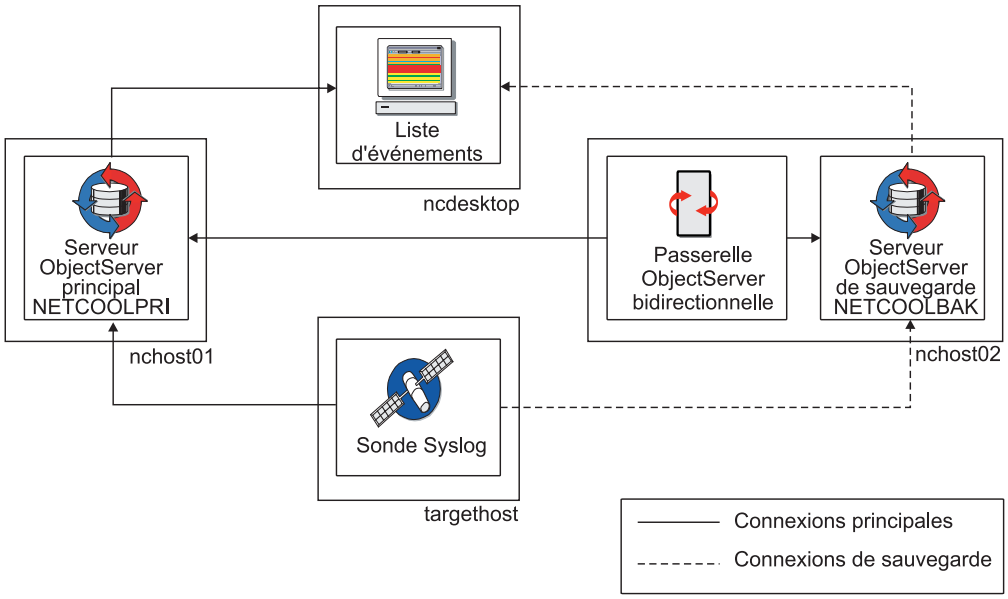

Figure 19. Exemple d'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus

Référence associée:

«Déploiement de l'architecture de base», à la page 621
L'architecture de base de Tivoli Netcool/OMNIbus comprend les composants suivants : le serveur ObjectServer, l'agent de processus, la sonde Syslog et la liste d'événements.

Prérequis de l'architecture de reprise en ligne de base

Un compte utilisateur UNIX appelé netcool doit exister sur chaque hôte. Cet utilisateur doit être membre du groupe UNIX ncoadmin afin d'utiliser les utilitaires de contrôle de processus (**nco_pa_***).

Les variables d'environnement suivantes doivent être définies pour l'utilisateur netcool :

- $NCHOME - /opt/IBM/tivoli/netcool
- $PATH - $NCHOME/omnibus/bin:$PATH

Ce déploiement suppose que les répertoires par défaut sont utilisés.

Etape 1 : Installation de l'architecture de base

Avant de pouvoir installer des composants de reprise en ligne à votre installation, vous devez d'abord installer l'architecture de base de Tivoli Netcool/OMNIbus.

Référence associée:

«Exemple d'architecture de base de Tivoli Netcool/OMNIbus», à la page 621
L'exemple d'architecture de base de Tivoli Netcool/OMNIbus utilise une seule sonde Syslog pour surveiller une application qui écrit des messages de débogage dans le démon syslog sur son ordinateur hôte.

Etape 2 : Installation du serveur ObjectServer de sauvegarde et de la passerelle du serveur ObjectServer

Cette étape permet d'installer le serveur ObjectServer de sauvegarde et la passerelle du serveur ObjectServer.

Sur l'ordinateur de sauvegarde (nchost02), procédez comme suit :

1. Téléchargez le bundle d'installation de Tivoli Netcool/OMNIbus pour Solaris à partir de Passport Advantage et extrayez les fichiers. Sinon, copiez les fichiers extraits de l'ordinateur exécutant le serveur ObjectServer maître (nchost01).
2. Exécutez le programme d'installation `./install_gui.sh` ou `./install_console.sh`. Sélectionnez et installez **Interface graphique d'administration**, **Outils d'administration**, **Interface graphique de l'opérateur**, **ObjectServer**, **Passerelles ObjectServer**, **Agent de processus**, **Support de sonde** et **extensions**.

Lorsque le processus est terminé, le serveur ObjectServer, la passerelle du serveur ObjectServer et les autres fonctions obligatoires sont installées sur nchost02.

Etape 3 : Configuration des communications

Cette étape vous permet de configurer les communications entre les composants Tivoli Netcool/OMNIbus.

Procédez de la manière suivante :

1. Sur l'ordinateur sur lequel le serveur ObjectServer *principal* s'exécute (nchost01), exécutez la commande suivante pour ouvrir la fenêtre de l'éditeur de serveur :
   ```
   $NCHOME/omnibus/bin/nco_xigen
   ```
2. Configurez les paramètres de communication supplémentaires. L'ensemble complet d'entrées de l'éditeur de serveur est présenté dans le tableau suivant.

Tableau 99. Paramètres de l'éditeur de serveur - architecture de reprise en ligne de base

Serveur	Hostname (Nom d'hôte)	Port	SSL
AGG_GATE	nchost02	4500	0
NCOBK_PA	nchost02	4600	0
NCOOS_PA	nchost01	4200	0
NCOPR_PA	targethost	4300	0
AGG_B	nchost02	4400	0
AGG_P	nchost01	4100	0
AGG_V	nchost01	4100	0
Sauvegarde 1 :	nchost02	4400	0

3. Appliquez vos modification et fermez l'éditeur de serveur. Cela crée le fichier $NCHOME/etc/interfaces.solaris2, contenant vos informations de communication.
4. Copiez le fichier $NCHOME/etc/omni.dat vers le répertoire $NCHOME/etc sur l'ordinateur de sauvegarde (nchost02) et l'ordinateur exécutant la sonde Syslog (targethost).
5. Exécutez $NCHOME/bin/nco_igen sur les ordinateurs nchost02 et targethost pour créer le fichier interfaces.solaris2.
6. Pour l'ordinateur Windows (ncdesktop), utilisez l'éditeur de serveur pour entrer des informations de communication supplémentaires.

Les ordinateurs principal, de sauvegarde, de sonde et de bureau ont maintenant les mêmes informations de communication.

Etape 4 : Création et configuration du serveur ObjectServer de sauvegarde

Cette étape vous permet de créer un serveur ObjectServer appelé AGG_B et de copier les colonnes personnalisées dans alerts.status.

Procédez de la manière suivante :

1. Créez le serveur ObjectServer AGG_B sur nchost02 :
   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_B -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```
2. Sur l'ObjectServer primaire, utilisez la commande suivante **nco_confpack** pour extraire la définition de alerts.status de AGG_P :
   ```
   $NCHOME/omnibus/bin/nco_confpack -list -server AGG_P -user root | grep
   alerts.status | $NCHOME/omnibus/bin/nco_confpack -export -user root
   -package alerts_status.jar
   ```
3. Copiez alerts_status.jar dans nchost02.
4. Démarrez le serveur ObjectServer de sauvegarde :
   ```
   $NCHOME/omnibus/bin/nco_objserv -name AGG_B &
   ```
5. Importez les colonnes alerts.status personnalisées dans AGG_B :
   ```
   $NCHOME/omnibus/bin/nco_confpack -import -package alerts_status.jar
   -from AGG_P -server AGG_B -user root
   ```
6. Utilisez l'interface interactive SQL pour vous connecter à AGG_B :
   ```
   $NCHOME/omnibus/bin/nco_sql -user root -server AGG_B
   ```
7. Utilisez l'interface interactive SQL pour vérifier que les trois nouvelles colonnes sont à la fin de la définition de la table :
   ```
   1> select ColumnName from catalog.columns where DatabaseName = 'alerts' and
    TableName = 'status' order by OrdinalPosition;
   2> go
   ```
8. Arrêtez l'ObjectServer :
   ```
   1> alter system shutdown;
   2> go
   ```

Le serveur ObjectServer AGG_B est maintenant configuré en tant que serveur ObjectServer de sauvegarde. Il est démarré ultérieurement à l'aide du contrôle de processus.

Concepts associés:

Chapitre 11, «Importation et exportation de configurations du serveur ObjectServer», à la page 293
Tivoli Netcool/OMNIbus fournit deux utilitaires, nommés **nco_confpack** et **nco_osreport** ; vous pouvez les utiliser pour importer et exporter les configurations d'un serveur ObjectServer.

Etape 5 : Configuration de la passerelle bidirectionnelle du serveur ObjectServer

Cette étape vous permet de configurer le mappage de la passerelle bidirectionnelle du serveur ObjectServer.

Sur l'ordinateur de sauvegarde (nchost02), procédez comme suit :

1. Copiez `AGG_GATE.props`, `AGG_GATE.map`, et `AGG_GATE.tblrep.def` du répertoire `$NCHOME/omnibus/extensions/multitier/gateway` vers le répertoire `$NCHOME/omnibus/etc`.
2. Editez le fichier `AGG_GATE.map`.

   Un mappage par défaut de passerelle bidirectionnelle du serveur ObjectServer est présenté ci-dessous, avec certaines zones personnalisées supplémentaires (en gras) que vous devez ajouter pour correspondre aux serveurs ObjectServer AGG_P et AGG_B :

```
CREATE MAPPING StatusMap
(
'Identifier'  = '@Identifier'  ON INSERT ONLY,
'Node'   = '@Node'   ON INSERT ONLY,
'NodeAlias'  = '@NodeAlias'   ON INSERT ONLY,
...
...
'CustomerID'  = '@CustomerID'  ON INSERT ONLY,
'CustomerContact' = '@CustomerContact'  ON INSERT ONLY,
'ReferenceCode' = '@ReferenceCode'  ON INSERT ONLY,
'ServerName'  = '@ServerName'  ON INSERT ONLY,
'ServerSerial'  = '@ServerSerial'  ON INSERT ONLY
);
```

La passerelle bidirectionnelle du serveur ObjectServer est maintenant configurée pour échanger des données d'alerte entre AGG_P et AGG_B.

Etape 6 : Configuration de la sonde Syslog

Cette étape vous permet de configurer la sonde Syslog pour la reprise en ligne sur le serveur ObjectServer de sauvegarde.

Procédez de la manière suivante :

1. Connectez-vous à l'ordinateur sur lequel la sonde Syslog est en cours d'exécution (targethost).
2. Arrêtez la sonde Syslog à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_stop -server NCOPR_PA -service Probes
   ```
3. Editez le fichier `$NCHOME/omnibus/probes/solaris2/syslog.props`.
4. Remplacez les propriétés Server et NetworkTimeout par les valeurs suivantes :

   ```
   Server   : 'AGG_V'
   NetworkTimeout   : 30
   ```

   Remarque : Si vous définissez la propriété **NetworkTimeout** sur 30 secondes, cette valeur devrait être appropriée pour la plupart des réseaux. Cependant, vous devez augmenter cette valeur si la sonde se déconnecte en permanence du

serveur ObjectServer. Cette propriété ignore le délai d'attente TCP standard du système d'exploitation, qui est compris entre 7 et 12 minutes sous Solaris).

5. Redémarrez la sonde à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_start -server NCOPR_PA -service Probes
   ```

La sonde Syslog s'exécute maintenant à nouveau sous contrôle de processus et utilise les propriétés mises à jour.

Etape 7 : Configuration du contrôle de processus sur l'ordinateur de sauvegarde

Cette étape vous permet de configurer un agent de processus appelé NCOBK_PA sur nchost02.

Pour de plus amples informations sur le contrôle de processus, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.

Procédez de la manière suivante :

1. Connectez-vous à l'ordinateur exécutant le serveur ObjectServer de sauvegarde (nchost02).
2. Editez le fichier `$NCHOME/omnibus/etc/nco_pa.conf`.
3. Ajoutez les informations de processus, de service et de routage pour le serveur ObjectServer de sauvegarde, comme indiqué ci-dessous :

   ```
   nco_process 'Bak_ObjectServer'
   {
   Command '$NCHOME/omnibus/bin/nco_objserv -name AGG_B -pa NCOBK_PA' run as 0
   Host='nchost02'
   Managed=true
   RestartMsg='The backup ObjectServer has been restarted'
   AlertMsg='The backup ObjectServer has gone down'
   RetryCount=0
   ProcessType=PaPA_AWARE
   }
   nco_process 'Bi_Gate'
   {
   Command '$NCHOME/omnibus/bin/nco_g_objserv_bi -name AGG_GATE' run as 0
   Host='nchost02'
   Managed=true
   RestartMsg='The bidirectional gateway has been restarted'
   AlertMsg='The bidirectional gateway has gone down'
   RetryCount=5
   ProcessType=PaPA_AWARE
   }
   nco_service 'Bak_OS'
   {
   ServiceType=Master
   ServiceStart=Auto
   process 'Bak_ObjectServer' NONE
   process 'Bi_Gate' 'Bak_ObjectServer'
   }
   nco_routing
   {
   host 'nchost02' 'NCOBK_PA'
   }
   ```

4. Démarrez le démon de contrôle de processus à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pad -name NCOBK_PA
   ```

5. Pour vérifier si le serveur ObjectServer de sauvegarde et la passerelle bidirectionnelle du serveur ObjectServer s'exécutent sous contrôle de processus, entrez la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_status -server NCOBK_PA -user netcool
   ```

6. Entrez le mot de passe dans l'invite.

Le serveur ObjectServer de sauvegarde et la passerelle bidirectionnelle du serveur ObjectServer doivent être signalés comme s'exécutant sous contrôle de processus.

La configuration de l'architecture de reprise en ligne Tivoli Netcool/OMNIbus de base est terminée.

Etapes suivantes

Après avoir terminé les étapes de déploiement de l'architecture de reprise en ligne, vous pouvez installer l'Interface graphique Web.

Procédez de la manière suivante :

1. Vous pouvez installer l'Interface graphique Web avec l'interface graphique ou la console ou vous pouvez effectuer une installation en mode silencieux. Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145 décrit les options disponibles pour l'installation de l'Interface graphique Web avec IBM Installation Manager.
2. Un fois l'Interface graphique Web installée, vous pouvez lancer un outil qui effectue une configuration de post-installation. Vous pouvez également configurer l'Interface graphique Web en mode silencieux. Si vous n'avez pas exécuté l'utilitaire de configuration de post-installation, vous pouvez effectuer toutes les tâches manuellement.

   L'outil crée une source de données unique qui est appelée « OMNIBUS ». Vous devez spécifier l'hôte et le numéro de port et le nom d'utilisateur et mot de passe pour cet ObjectServer. L'outil utilise l'ObjectServer pour l'authentification des utilisateurs et crée des utilisateurs et groupes par défaut Interface graphique Web dans cet ObjectServer. Lorsque l'outil termine la configuration du produit, le serveur redémarre automatiquement.

   Le mot de passe initial pour les comptes d'utilisateur par défaut, par exemple ncoadmin et ncouser, est netcool. Vous devez modifier ce mot de passe dans un environnement de production.

Exemple d'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus

Vous pouvez ajouter un serveur ObjectServer de bureau à l'exemple d'architecture de reprise en ligne de base. Un serveur ObjectServer de bureau accroît les performances d'un serveur ObjectServer standard, qui rencontre fréquemment de lourdes charges provenant des bureaux des utilisateurs.

Concepts associés:

Chapitre 12, «Configuration des serveurs ObjectServer de bureau», à la page 325
Vous pouvez configurer une architecture du serveur ObjectServer de bureau pour réduire la charge sur les serveurs ObjectServer qui reçoivent une grande quantité d'événements.

Référence associée:

«Exemple d'architecture de reprise en ligne de base Tivoli Netcool/OMNIbus», à la page 629
Vous pouvez ajouter un serveur ObjectServer de reprise en ligne (sauvegarde) à l'exemple d'architecture de base. Les données d'alerte du serveur ObjectServer maître sont répliquées dans le serveur ObjectServer de sauvegarde via une passerelle bidirectionnelle du serveur ObjectServer. Si une connexion au serveur ObjectServer maître échoue, les clients tentent de se connecter au serveur ObjectServer de sauvegarde.

Déploiement de l'architecture du serveur ObjectServer de bureau

L'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus comprend tous les composants de l'architecture de reprise en ligne de base et les composants supplémentaires suivants : le serveur ObjectServer de bureau et la passerelle unidirectionnelle du serveur ObjectServer.

Dans l'exemple suivant, le serveur ObjectServer de bureau et la passerelle unidirectionnelle du serveur ObjectServer sont installés sur un seul ordinateur Solaris portant le nom d'hôte ncdesk.

L'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus est présentée dans la figure suivante.

Remarque : Les intitulés **ObjectServer principal NETCOOLPRI**, **ObjectServer de bureau DESKOS** et **ObjectServer de sauvegarde NETCOOLBAK** doivent être remplacés par **ObjectServer principal AGG_P**, **ObjectServer de bureau DIS_1** et **ObjectServer de sauvegarde AGG_B**.

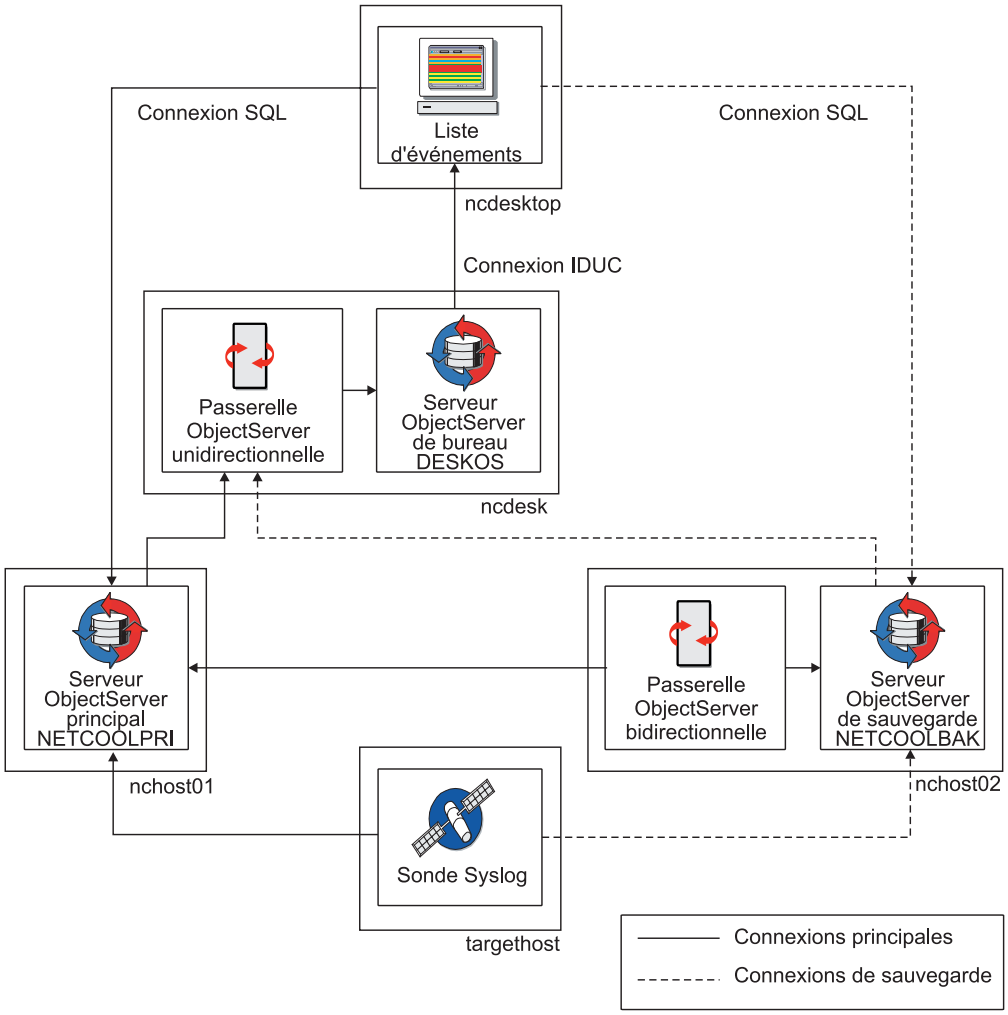

Figure 20. Exemple d'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus

Référence associée:

«Déploiement de l'architecture de reprise en ligne de base», à la page 629
L'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus comprend tous les composants de l'architecture de base et les composants supplémentaires suivants : le serveur ObjectServer de sauvegarde et la passerelle bidirectionnelle du serveur ObjectServer.

Prérequis pour l'architecture du serveur ObjectServer de bureau

Un compte utilisateur UNIX appelé netcool doit exister sur chaque hôte. Cet utilisateur doit être membre du groupe UNIX ncoadmin afin d'utiliser les utilitaires de contrôle de processus (**nco_pa_***).

Les variables d'environnement suivantes doivent être définies pour l'utilisateur netcool :

- $NCHOME - /opt/IBM/tivoli/netcool
- $PATH - $NCHOME/omnibus/bin:$PATH

Ce déploiement suppose que les répertoires par défaut sont utilisés.

Etape 1 : Installation des architectures de reprise en ligne de base

Avant de pouvoir ajouter des composants du serveur ObjectServer de bureau à votre installation, vous devez d'abord installer l'architecture de reprise en ligne de base de Tivoli Netcool/OMNIbus.

Référence associée:

«Exemple d'architecture de reprise en ligne de base Tivoli Netcool/OMNIbus», à la page 629
Vous pouvez ajouter un serveur ObjectServer de reprise en ligne (sauvegarde) à l'exemple d'architecture de base. Les données d'alerte du serveur ObjectServer maître sont répliquées dans le serveur ObjectServer de sauvegarde via une passerelle bidirectionnelle du serveur ObjectServer. Si une connexion au serveur ObjectServer maître échoue, les clients tentent de se connecter au serveur ObjectServer de sauvegarde.

Etape 2 : Installation du serveur ObjectServer de bureau et de la passerelle unidirectionnelle

Cette étape vous permet d'installer le serveur ObjectServer de bureau et la passerelle unidirectionnelle du serveur ObjectServer.

Sur l'ordinateur exécutant le serveur ObjectServer de bureau (ncdesk), procédez comme suit :

1. Téléchargez le bundle d'installation de Tivoli Netcool/OMNIbus pour Solaris à partir de Passport Advantage et extrayez les fichiers. Sinon, copiez les fichiers extraits depuis l'ordinateur exécutant le serveur ObjectServer maître (nchost01).
2. Exécutez le programme d'installation `./install_gui.sh` ou `./install_console.sh`. Sélectionnez et installez **Interface graphique d'administration**, **Outils d'administration**, **Interface graphique de l'opérateur**, **ObjectServer**, **Passerelles ObjectServer**, **Agent de processus**, **Support de sonde** et **extensions**.

   Notez l'ajout des **passerelles d'ObjectServer** sur la machine principale.

Le serveur ObjectServer, la passerelle unidirectionnelle du serveur ObjectServer et les fichiers de contrôle de processus sont installés sur le même ordinateur Solaris.

Etape 3 : Configuration des communications entre composants

Cette étape vous permet de configurer les communications entre les composants Tivoli Netcool/OMNIbus.

Procédez de la manière suivante :

1. Sur l'ordinateur *sur lequel le serveur ObjectServer principal s'exécute* (nchost01), exécutez la commande suivante pour ouvrir la fenêtre de l'éditeur de serveur :
   `$NCHOME/omnibus/bin/nco_xigen`
2. Configurez les paramètres de communication supplémentaires. L'ensemble complet d'entrées de l'éditeur de serveur est présenté dans le tableau suivant.

Tableau 100. Paramètres de l'éditeur de serveur - architecture du serveur ObjectServer de bureau

Serveur	Hostname (Nom d'hôte)	Port	SSL
DIS_1	ncdesk	4700	0
A_TO_D_GATE_1	ncdesk	4800	0
AGG_GATE	nchost02	4500	0
NCOBK_PA	nchost02	4600	0
NCOOS_PA	nchost01	4200	0
NCOPR_PA	targethost	4300	0
NCOSDESK_PA	ncdesk	4900	0
AGG_B	nchost02	4400	0
AGG_P	nchost01	4100	0
AGG_V	nchost01	4100	0
Sauvegarde 1 :	nchost02	4400	0

3. Appliquez vos modifications et fermez l'éditeur de serveur. Cela crée le fichier `interfaces.solaris2`, qui contient vos informations de communication.
4. Copiez le fichier `$NCHOME/etc/omni.dat` file dans le répertoire `$NCHOME/etc` sur nchost02, ncdesk, et targethost.
5. Exécutez `$NCHOME/bin/nco_igen` sur les ordinateurs nchost02, ncdesk et targethost pour créer le fichier `interfaces.solaris2`.
6. Pour l'ordinateur Windows (ncdesktop), utilisez l'éditeur de serveur pour entrer les informations de communication correctes.

Tous les ordinateurs de votre installation de Tivoli Netcool/OMNIbus possèdent maintenant les mêmes informations de communication.

Etape 4 : Création et configuration du serveur ObjectServer de bureau

Cette étape vous permet de créer et de configurer un serveur ObjectServer de bureau appelé DIS_1.

Procédez de la manière suivante :

1. Sur l'ordinateur exécutant le serveur ObjectServer de bureau (ncdesk), entrez la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -desktopserver -dsddualwrite -dsdprimary
   AGG_V -server DIS_1 -customconfigfile $NCHOME/omnibus/extensions/
   multitier/objectserver/display.sql
   ```

   Le serveur ObjectServer de bureau DIS_1 est créé.
2. Sur l'ObjectServer primaire, utilisez la commande suivante **nco_confpack** pour extraire la définition de alerts.status de AGG_P :

   ```
   $NCHOME/omnibus/bin/nco_confpack -list -server AGG_P -user root | grep
   alerts.status | $NCHOME/omnibus/bin/nco_confpack -export -user root
   -package alerts_status.jar
   ```
3. Copiez `alerts_status.jar` dans nchost02.
4. Démarrez le serveur ObjectServer de bureau :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name DIS_1 &
   ```
5. Importez les colonnes alerts.status personnalisées dans DIS_1 :

   ```
   $NCHOME/omnibus/bin/nco_confpack -import -package alerts_status.jar
   -from AGG_P -server DIS_1 -user root
   ```
6. Utilisez l'interface interactive SQL pour vous connecter à DIS_1 :

   ```
   $NCHOME/omnibus/bin/nco_sql -user root -server DIS_1
   ```
7. Utilisez l'interface interactive SQL pour vérifier que les trois nouvelles colonnes sont à la fin de la définition de la table :

   ```
   1> select ColumnName from catalog.columns where DatabaseName = 'alerts' and
    TableName = 'status' order by OrdinalPosition;
   2> go
   ```

Le serveur ObjectServer de bureau DIS_1 est maintenant configuré et en cours d'exécution.

Etape 5 : Configuration de la passerelle unidirectionnelle du serveur ObjectServer

Cette étape vous permet de configurer la passerelle unidirectionnelle du serveur ObjectServer.

A partir de l'ordinateur exécutant le serveur ObjectServer de bureau (ncdesk), procédez de la manière suivante :

1. Copiez les fichiers suivants de `$NCHOME/omnibus/extensions/multitier/gateway` dans `$NCHOME/omnibus/etc` :

   ```
   A_TO_D_GATE.map
   A_TO_D_GATE.tblrep.def
   A_TO_D_GATE_1.props
   ```
2. Editez le fichier `$NCHOME/omnibus/etc/A_TO_D_GATE.map`. Les zones et l'ordre des zones dans le mappage doivent correspondre *exactement* à la table alerts.status des serveurs ObjectServer principal et de sauvegarde, y compris les zones personnalisées supplémentaires.

Les nouvelles entrées doivent se trouver dans la section Zones personnalisées. Les champs personnalisés doivent être ajoutés dans la zone indiquée. Les colonnes ServerName/ServerSerial/MasterSerial sont déjà dans le fichier de mappe.

Un mappage partiel de passerelle unidirectionnelle du serveur ObjectServer est présenté ci-dessous, avec l'entrée `MasterSerial` et les zones personnalisées supplémentaires en gras :

```
CREATE MAPPING StatusMap
(
'Identifier'   = '@Identifier'  ON INSERT ONLY,
'Node'    = '@Node'   ON INSERT ONLY,
'NodeAlias'   = '@NodeAlias'   ON INSERT ONLY,
...
...
'CustomerID'   = '@CustomerID'  ON INSERT ONLY,
'CustomerContact'  = '@CustomerContact'  ON INSERT ONLY,
'ReferenceCode'  = '@ReferenceCode'  ON INSERT ONLY,
'ServerName'   = '@ServerName'  ON INSERT ONLY,
'ServerSerial'   = '@ServerSerial'  ON INSERT ONLY,
'MasterSerial'   = '@Serial'   ON INSERT ONLY
);
```

3. Ajoutez une entrée pour la passerelle dans l'éditeur de serveur.

Votre passerelle unidirectionnelle du serveur ObjectServer est maintenant configurée et peut envoyer des événements du serveur ObjectServer maître (AGG_P) au serveur ObjectServer de bureau (AGG_B).

Etape 6 : Configuration du contrôle de processus sur l'ordinateur hébergeant le serveur ObjectServer de bureau

Cette procédure vous permet de configurer un agent de processus appelé NCOSDESK_PA sur ncdesk.

Procédez de la manière suivante :

1. Connectez-vous à l'ordinateur exécutant le serveur ObjectServer de bureau (ncdesk).
2. Editez le fichier `$NCHOME/omnibus/etc/nco_pa.conf`.
3. Ajoutez les informations de processus, de service et de routage pour le serveur ObjectServer de bureau de la manière suivante :

```
nco_process 'Desk_ObjectServer'
{
Command '$NCHOME/omnibus/bin/nco_objserv -name DIS_1 -pa NCOSDESK_PA' run as 0
Host='ncdesk'
Managed=true
RestartMsg='The desktop ObjectServer has been restarted'
AlertMsg='The desktop ObjectServer has gone down'
RetryCount=0
ProcessType=PaPA_AWARE
}
nco_process 'Uni_Gate'
{
Command '$NCHOME/omnibus/bin/nco_g_objserv_uni -name A_TO_D_GATE_1' run as 0
Host='ncdesk'
Managed=true
RestartMsg='The unidirectional gateway has been restarted'
AlertMsg='The unidirectional gateway has gone down'
RetryCount=5
ProcessType=PaPA_AWARE
}
nco_service 'Desk_OS'
```

```
{
ServiceType=Master
ServiceStart=Auto
process 'Desk_ObjectServer' NONE
process 'Uni_Gate' 'Desk_ObjectServer'
}
nco_routing
{
host 'ncdesk' 'NCOSDESK_PA'
}
```

4. Arrêtez le serveur ObjectServer de bureau.
5. Démarrez le démon de contrôle de processus à l'aide de la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pad -name NCOSDESK_PA
   ```

6. Pour vérifier si le serveur ObjectServer de bureau et la passerelle unidirectionnelle du serveur ObjectServer s'exécutent sous contrôle de processus, entrez la commande suivante :

   ```
   $NCHOME/omnibus/bin/nco_pa_status -server NCOSDESK_PA -user netcool
   ```

7. Entrez le mot de passe dans l'invite.

Le serveur ObjectServer de bureau et la passerelle unidirectionnelle du serveur ObjectServer doivent être signalés comme s'exécutant sous contrôle de processus.

La configuration de l'architecture du serveur ObjectServer de bureau Tivoli Netcool/OMNIbus est terminée.

Etapes suivantes

Après avoir déployé l'architecture du serveur ObjectServer de bureau, vous pouvez configurer l'architecture de bureau à deux serveurs de l'Interface graphique Web.

Procédez de la manière suivante :

1. Sur le serveur exécutant l'Interface graphique Web, ouvrez le fichier `ncwDataSourceDefinitions.xml`.
2. Définissez le serveur ObjectServer DIS_1 en tant que serveur d'affichage du serveur ObjectServer AGG_P :
   a. Recherchez l'élément <ncwDataSourceDefinition> du serveur AGG_P.
   b. Définissez le type d'attribut de l'élément <ncwDataSourceDefinition> sur `multipleServerOSDataSource`.
   c. Ajoutez l'élément <ncwReadCloudDefinition> en dessous de l'élément de fermeture </ncwFailOverPairDefinition>, dans lequel vous définissez l'hôte et le port du serveur d'affichage DIS_1. Dans l'élément <ncwReadCloudDefinition>, définissez le serveur DIS_1 dans un élément <ncwOSConnection>. Par exemple :

      ```
      <ncwReadCloudDefinition>
                    <ncwOSConnection host="ncdesk" port="4700"/>
      </ncwReadCloudDefinition>
      ```

3. Enregistrez et fermez le fichier.
4. Arrêtez le serveur en entrant la commande suivante :
   - UNIX Linux *rép_install*/bin/stopServer.sh server1 -username *nom d'utilisateur_administrateur_SM* -password *mot de passe*
   - Windows *rép_install*/bin/stopServer.bat
5. Redémarrez le serveur en entrant la commande suivante :

- UNIX Linux *rép_install*/bin/startServer.sh server1
- Windows *rép_install*/bin/startServer.bat server1

Chapitre 20. Exemple de scénario d'installation pour les composants non Web et l'Interface graphique Web de Tivoli Netcool/OMNIbus (sous Windows)

Ce scénario d'installation décrit comment effectuer une installation et une configuration de base des composants non Web et de l'Interface graphique Web de Tivoli Netcool/OMNIbus dans un environnement de test Windows.

Tivoli Netcool/OMNIbus effectue un suivi des informations d'alerte dans une base de données du serveur ObjectServer en mémoire et à hautes performances, et présente des informations pertinentes à des utilisateurs spécifiques via des filtres et des vues pouvant être configurés individuellement. Les composants non Web de Tivoli Netcool/OMNIbus incluent les serveurs ObjectServer, les sondes, les passerelles, les outils de bureau et les outils d'administration.

L'Interface graphique Web fournit une interface Web permettant de traiter des événements de réseau provenant d'un ou plusieurs serveurs ObjectServer et utilise une interface client-serveur. Le serveur exécutant l'Interface graphique Web s'exécute dans Concentrateur des services d'application du tableau de bord, qui offre une connexion unique, une gestion consolidée des utilisateurs et un seul point d'accès pour différentes applications Tivoli. Les clients se connectent à Concentrateur des services d'application du tableau de bord pour accéder à l'Interface graphique Web.

Les informations de ce scénario agissent comme un guide d'installation et d'exécution rapide du produit. Les informations vous guident à travers les étapes nécessaires pour :

- Installer et configurer un serveur ObjectServer pour la gestion des événements
- Installer et configurer une sonde pour envoyer des événements au serveur ObjectServer
- Installer et configurer l'Interface graphique Web pour surveiller les événements sur le serveur ObjectServer

Configuration d'un environnement de test

Vous pouvez rapidement définir une configuration simple pour tester votre installation de Tivoli Netcool/OMNIbus. Les composants principaux obligatoires pour configurer l'environnement de test sont les fonctions de base nécessaires à la configuration d'un serveur ObjectServer, une sonde Simnet pour simuler des événements et l'Interface graphique Web pour surveiller les événements générés.

L'environnement de test est composé d'un ObjectServer (nommé `MYOBJ`) et d'un serveur d'Interface graphique Web, exécutés sur un serveur Windows avec le nom d'hôte `myserverhost`. La sonde Simnet s'exécute sur le même serveur et réachemine les événements vers l'ObjectServer. Les événements envoyés au serveur ObjectServer sont affichés dans la liste d'événements actifs de l'Interface graphique Web.

Les étapes à haut niveau permettant de configurer cet environnement de test sont les suivantes :

1. Installation des composants non Web de Tivoli Netcool/OMNIbus et configuration d'un serveur ObjectServer :
   a. Installez les fonctions de base pour configurer un serveur ObjectServer.
   b. Créer un serveur ObjectServer.
   c. Définissez et générez les connexions d'interface entre le serveur ObjectServer et toutes les applications s'y connectant.
   d. Configurez le serveur ObjectServer afin qu'il s'exécute comme un service Windows.
2. Configurez la sonde pour simuler des données d'événement et configurez-la pour qu'elle s'exécute en tant que service Windows.
3. Installation et configuration de l'Interface graphique Web afin de recevoir des événements du serveur ObjectServer :
   a. Installez l'Interface graphique Web et définissez les connexions d'interface avec le serveur ObjectServer.
   b. Connectez-vous au serveur exécutant l'Interface graphique Web.
   c. Créez un nouvel utilisateur et configurez les droits d'accès pour permettre à l'utilisateur d'afficher des événements dans la liste d'événements actifs.

Portée, hypothèses et prérequis d'installation

Même si Tivoli Netcool/OMNIbus est pris en charge sur divers systèmes d'exploitation, ces informations décrivent une installation et une configuration de Windows à des fins de test rapide.

Les hypothèses sont les suivantes :

- Un système d'exploitation Windows pris en charge est utilisé.
- Vous installez les composants non Web et de l'Interface graphique Web et la sonde sur le même serveur.
- Vous avez téléchargé les modules d'installation pour le système test et extrait le contenu de chaque module vers un emplacement temporaire sur le serveur Windows.
- Les répertoires d'installation par défaut sont utilisés.
- Votre système d'exploitation possède tous les modules de correction recommandés, notamment les derniers niveaux de modules de correction.
- L'ordinateur Windows n'a aucune installation existante de Tivoli Netcool/OMNIbus ou de version précédente de l'Interface graphique Web ou de Netcool/Webtop.

Les composants non Web, l'Interface graphique Web et la sonde sont répartis sous forme de modules d'installation distincts que vous pouvez télécharger à partir du site Web d'IBM Passport Advantage.

Les prérequis d'installation sont les suivants :

- Vous devez disposer de droits d'administration sur les ordinateurs Windows.
- Vous devez disposer de droits d'accès en écriture dans les répertoires d'installation.
- L'environnement d'exécution Java est installé sur les ordinateurs.

Des méthodes d'installation et de configuration alternatives sont disponibles à des fins de configuration et d'exécution de Tivoli Netcool/OMNIbus et des sondes. Pour ce scénario de test, Installation Manager est utilisé pour installer Tivoli

Netcool/OMNIbus. Les différents composants du produit sont configurés pour être exécutés en tant que services Windows.

Installation de Tivoli Netcool/OMNIbus et configuration du serveur ObjectServer

Vous devez installer les composants non Web de Tivoli Netcool/OMNIbus, configurer un serveur ObjectServer, puis le démarrer avant d'installer l'Interface graphique Web.

Pourquoi et quand exécuter cette tâche

Installation de Tivoli Netcool/OMNIbus

Pourquoi et quand exécuter cette tâche

Vous pouvez installer Tivoli Netcool/OMNIbus avec l'interface graphique d'IBM Installation Manager ou la console ou vous pouvez effectuer une installation en mode silencieux. Tivoli Netcool/OMNIbus est disponible sous forme de distribution de fichier compressé sur DVD et à partir d'IBM Passport Advantage.

Procédure

«Installation de Tivoli Netcool/OMNIbus», à la page 72 décrit les options disponibles pour l'installation de Tivoli Netcool/OMNIbus.

Résultats

L'installation de Tivoli Netcool/OMNIbus ajoute les raccourcis suivants au menu **Démarrer** de Windows :

- **Démarrer** > **Tous les programmes** > **Netcool Conductor (Netcool Conductor)**
- **Démarrer** > **Tous les programmes** > **Suite NETCOOL**

Que faire ensuite

Chaque installation Tivoli Netcool/OMNIbus peut avoir au moins un serveur ObjectServer pour stocker et gérer les informations d'alerte. Vous pouvez maintenant créer un serveur ObjectServer en créant l'utilitaire d'initialisation de la base de données (**nco_dbinit**).

Création d'un serveur ObjectServer

Pourquoi et quand exécuter cette tâche

Pour créer un serveur ObjectServer appelé `MYOBJ` pour votre environnement de test, procédez comme suit :

Procédure

1. Dans une invite de commande, accédez au répertoire `C:\IBM\Tivoli\Netcool\omnibus\bin` :

   ```
   cd C:\IBM\tivoli\netcool\omnibus\bin
   ```

2. Exécutez la commande suivante :

   ```
   nco_dbinit -server MYOBJ
   ```

   L'utilitaire **nco_dbinit** crée les objets suivants pour le serveur ObjectServer `MYOBJ` :

- Un fichier de propriétés appelé `MYOBJ.props` dans l'emplacement `C:\IBM\Tivoli\Netcool\omnibus\etc`
- Des tables et des données de base de données par défaut
- Les utilisateurs par défaut appelés `root` et `nobody`, ainsi que les groupes et rôles par défaut pour vous aider à gérer les droits

  L'utilisateur `root` est créé en tant qu'administrateur et se voit attribuer une chaîne vide en tant que mot de passe. L'utilisateur `nobody` est désactivé et ne peut pas être utilisé pour accéder au serveur ObjectServer.

Conseil : Laissez la fenêtre d'invite de commande ouverte pour une utilisation ultérieure.

Que faire ensuite

Vous devez maintenant utiliser l'éditeur de serveur pour ajouter des détails de communication pour le serveur ObjectServer sur le serveur Windows. Deux entrées de l'éditeur de serveur sont obligatoires pour le serveur ObjectServer : une entrée *programme d'écoute* qui répond aux demandes des clients et une entrée *client* que les clients locaux peuvent utiliser pour se connecter au serveur.

Tout ordinateur (notamment l'ordinateur exécutant la sonde) devant se connecter au serveur ObjectServer a également besoin de ces détails de communication.

Configuration d'informations de communication avec le serveur

Pourquoi et quand exécuter cette tâche

Pour ajouter des détails de communication au serveur ObjectServer sur le serveur Windows, procédez comme suit :

Procédure

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Suite NETCOOL** > **Utilitaires système** > **Editeur de serveurs**.

   La fenêtre Editeur de serveurs s'ouvre. La liste de serveurs dans la partie supérieure de cette fenêtre indique la liste des entrées serveur par défaut. Tous les autres paramètres de serveur que vous définissez dans cette fenêtre sont ajoutés à cette liste.
2. Complétez cette fenêtre de la manière suivante. (Les instructions sont fournies en fonction de leur pertinence pour l'environnement de test.)

   Programme d'écoute
   Laissez d'abord cette case non cochée.

   SSL Laissez cette case non cochée. A des fins de test, les connexions cryptées des clients utilisant le protocole SSL ne sont pas utilisées.

   Nom Entrez le nom du serveur ObjectServer que vous avez créé plus tôt - c'est-à-dire `MYOBJ`.

   Port Entrez `4321`. Vous pouvez entrer un numéro de port valide inutilisé dans cette zone. Il s'agit du port sur lequel le serveur ObjectServer écoute les connexions.

   Hôte Indiquez le nom d'hôte de l'ordinateur actuel sur lequel vous avez installé le serveur ObjectServer. (Ce nom doit être visible dans la liste déroulante.)

Ajouter
Cliquez sur ce bouton pour ajouter les détails sur le serveur MYOBJ à la liste de serveurs située au-dessus des zones de saisie. Ces détails correspondent à l'entrée client.

Vous devez maintenant ajouter l'entrée du programme d'écoute :

Programme d'écoute
Cochez cette case.

Ajouter
Cliquez sur ce bouton pour ajouter une sous-entrée Programmes d'écoute à l'entrée MYOBJ dans la liste de serveurs.

3. Cliquez sur **OK** pour sauvegarder vos modifications et fermer la fenêtre Editeur de serveurs.

Résultats

L'éditeur de serveurs sauvegarde les paramètres de communication dans le fichier de données de connexion, qui se trouve dans C:\IBM\Tivoli\Netcool\ini\sql.ini.

Que faire ensuite

Vous devez maintenant configurer le serveur ObjectServer à exécuter en tant que service Windows en exécutant le fichier exécutable du serveur ObjectServer avec une ou plusieurs options de ligne de commande.

Configuration du serveur ObjectServer en tant que service Windows

Pourquoi et quand exécuter cette tâche

Pour configurer le serveur ObjectServer MYOBJ en tant que service Windows, procédez comme suit :

Procédure

1. Dans la fenêtre d'invite de commande, exécutez la commande suivante pour installer le service du serveur ObjectServer :

   ```
   nco_objserv /install /cmdline "-name MYOBJ"
   ```

   Conseil : Si vous avez fermé la fenêtre de commande précédente à partir de laquelle vous aviez exécuté l'utilitaire **nco_dbinit**, vous devez accéder au répertoire C:\IBM\Tivoli\Netcool\omnibus\bin avant d'exécuter la commande **nco_objserv**.

   Un message s'affiche confirmant que le service du serveur ObjectServer a bien été installé.
2. Dans le panneau de contrôle de Windows, utilisez la fenêtre Services pour démarrer le service de l'ObjectServer. Le nom d'affichage de la sonde est **Netcool/OMNIbus ObjectServer**.

Résultats

La configuration du serveur ObjectServer est terminée.

Configuration et installation de la sonde

La sonde Simnet est fournie avec l'Tivoli Netcool/OMNIbus et peut être utilisée pour simuler des événements à des fins de test.

Procédure

1. Ouvrez le fichier de propriétés de la sonde Simnet suivant pour le modifier :

   `C:\IBM\Tivoli\Netcool\omnibus\probes\win32\simnet.props`
2. Copiez et collez la propriété **Server** à la fin du fichier. Cela vous permet de conserver une configuration par défaut commentée dans ce fichier à des fins de référence.
3. Supprimez la mise en commentaire de la propriété **Server** et remplacez la valeur par défaut par `MYOBJ`, comme suit :

   ```
   Server : 'MYOBJ'
   ```
4. Sauvegardez et fermez le fichier de propriétés.
5. Dans une invite de commande, accédez au répertoire `C:\IBM\Tivoli\Netcool\omnibus\probes\win32`.
6. Utilisez la commande suivante pour installer la sonde en tant que service Windows :

   ```
   nco_p_simnet -install
   ```

   Un message s'affiche pour confirmer que l'installation du service NCO Simnet Probe a abouti.
7. Dans le panneau de contrôle de Windows, utilisez la fenêtre Services pour démarrer le service de la sonde. Le nom d'affichage de la sonde est **NCO Simnet Probe**.

Que faire ensuite

Maintenant que la sonde fonctionne et est en cours d'exécution, vous pouvez surveiller les événements à partir de la sonde sur l'ordinateur sur lequel Tivoli Netcool/OMNIbus et l'Interface graphique Web sont installés.

Installation et configuration de l'Interface graphique Web

Un serveur ObjectServer doit être en cours d'exécution en même temps que vous installez l'Interface graphique Web. Le processus d'installation tente de se connecter au serveur ObjectServer.

Avant de commencer

Vous devez garder sous la main les informations suivantes pour établir la connexion :

- Le nom et le mot de passe de l'administrateur de Tivoli Netcool/OMNIbus - dans ce cas, `root` avec un mot de passe vide
- Le nom du serveur ObjectServer, l'hôte et le port - dans ce cas, `MYOBJ`, le nom qualifié complet de l'ordinateur et `4321`

Installation de l'Interface graphique Web

Pourquoi et quand exécuter cette tâche

Sur le même ordinateur que celui sur lequel vous avez installé les composants non Web de Tivoli Netcool/OMNIbus, procédez comme suit :

Procédure

1. Vous pouvez installer l'Interface graphique Web avec l'interface graphique ou la console ou vous pouvez effectuer une installation en mode silencieux. Chapitre 6, «Installation et mise à niveau du composantInterface graphique Web», à la page 145 décrit les options disponibles pour l'installation de l'Interface graphique Web avec IBM Installation Manager.
2. Un fois l'Interface graphique Web installée, vous pouvez lancer un outil qui effectue une configuration de post-installation. Vous pouvez également configurer l'Interface graphique Web en mode silencieux. Si vous n'avez pas exécuté l'utilitaire de configuration de post-installation, vous pouvez effectuer toutes les tâches manuellement.

   L'outil crée une source de données unique qui est appelée « OMNIBUS ». Vous devez spécifier l'hôte et le numéro de port et le nom d'utilisateur et mot de passe pour cet ObjectServer. L'outil utilise l'ObjectServer pour l'authentification des utilisateurs et crée des utilisateurs et groupes par défaut Interface graphique Web dans cet ObjectServer. Lorsque l'outil termine la configuration du produit, le serveur redémarre automatiquement.

   Le mot de passe initial pour les comptes d'utilisateur par défaut, par exemple ncoadmin et ncouser, est netcool. Vous devez modifier ce mot de passe dans un environnement de production.

Que faire ensuite

Vous pouvez maintenant vous connecter à la console Concentrateur des services d'application du tableau de bord. (Notez que le serveur Concentrateur des services d'application du tableau de bord démarre automatiquement après son installation et lors du démarrage de l'ordinateur.)

Connexion à la console Concentrateur des services d'application du tableau de bord

Pourquoi et quand exécuter cette tâche

Pour vous connecter à la console à partir de la page de connexion, procédez comme suit :

Procédure

1. Indiquez vos données d'identification de la manière suivante :

   User ID (ID utilisateur)
   Entrez `smadmin`. Il s'agit de l'ID administrateur par défaut indiqué lors de l'installation.

   Password
   Entrez le mot de passe que vous avez indiqué pour l'utilisateur `smadmin`.
2. Cliquez sur **Ouverture de session**.

Résultats

Une fois que vos données d'identification de l'utilisateur ont été vérifiées, la page Bienvenue de l'interface graphique Web de Tivoli Netcool/OMNIbus s'affiche dans la fenêtre de la console Concentrateur des services d'application du tableau de bord. Cette fenêtre dispose d'un panneau de navigation sur la gauche comprenant un ensemble de nœuds pour accéder aux fonctions que vous souhaitez exécuter. La zone de travail sur la droite affiche généralement la page actuelle sur laquelle vous travaillez et contient un ou plusieurs portlets ou applications Web, tous se trouvant dans leur propre fenêtre de portlet avec une barre de titre.

Remarque : Lorsque vous êtes connecté à la console, évitez de cliquer sur le bouton **Retour** de votre navigateur pour revenir à la page Web précédente car vous serez automatiquement déconnecté. Cliquez sur **Suivant** et vous verrez que vous êtes déconnecté et que vous devez soumettre de nouveau vos données d'identification de l'utilisateur pour vous reconnecter.

Que faire ensuite

Après l'installation, l'administrateur Concentrateur des services d'application du tableau de bord doit généralement créer un ou plusieurs utilisateurs administrateurs de l'Interface graphique Web, qui disposent de droits pour modifier les paramètres de l'Interface graphique Web. L'administrateur Concentrateur des services d'application du tableau de bord peut aussi créer des utilisateurs supplémentaires avec divers droits d'accès. Les rôles et groupes sont associés à l'utilisateur de l'Interface graphique Web. Les rôles sont utilisés pour attribuer des droits aux utilisateurs et les groupes peuvent être utilisés pour classer logiquement les utilisateurs disposant d'objectifs fonctionnels communs.

Dans votre environnement de test, vous créez un utilisateur, attribuez des rôles à l'utilisateur et vous connectez en tant que cet utilisateur pour afficher les événements générés dans la liste d'événements actifs.

Création d'utilisateurs dans la console d'administration WebSphere

Vous pouvez gérer vos utilisateurs de référentiel fédéré dans la fenêtre **Gérer les utilisateurs > Créer un utilisateur** de la console d'administration de WebSphere.

Avant de commencer

Avant d'ajouter des utilisateurs, exécutez les tâches suivantes :

- Vérifiez que vous avez correctement configuré tous les registres d'utilisateurs (par exemple LDAP ou ObjectServer) qui contiennent les utilisateurs que vous souhaitez affecter. Il est conseillé d'activer la sécurité avec le registre d'utilisateurs de votre choix avant de commencer.
- Assurez-vous que si vous modifiez quelque chose dans le référentiel fédéré, vous enregistrez la configuration et redémarrez le serveur d'applications pour que les modifications entrent en vigueur. Par exemple, ajouter et supprimer des registres d'utilisateurs.
- Dans une configuration de plusieurs référentiels, assurez-vous que vous avez identifié un registre d'utilisateurs dédié pour les opérations d'écriture. Cela peut être fait par le biais des types d'entités pris en charge dans la configuration de référentiel fédéré.

Procédure

1. Cliquez sur **Paramètres de la console** > **Console d'administration WebSphere**.
2. Sélectionnez **Utilisateurs et groupes** > **Manage Users (Gérer les utilisateurs)**.
3. Entrez les détails de l'utilisateur, par exemple l'ID utilisateur, le nom et le prénom, l'adresse électronique, le mot de passe et toute appartenance à un groupe.
4. Cliquez sur **Créer**.
5. Cliquez sur **Créer autre** pour créer un autre utilisateur comme décrit dans l'étape 3 ; sinon, cliquez sur **Fermer**.

Que faire ensuite

Maintenant que Tivoli Netcool/OMNIbus et l'Interface graphique Web fonctionnent et sont en cours d'exécution, vous pouvez installer la sonde sur un ordinateur client et la configurer pour envoyer des événements au serveur ObjectServer à des fins d'affichage dans la liste d'événements actifs.

Le processus d'installation de la sonde est en deux étapes :

1. Les sondes requièrent que la fonction **Support de sonde** de Tivoli Netcool/OMNIbus soit installée. Vous devez donc installer Tivoli Netcool/OMNIbus sur l'ordinateur conçu pour la sonde.
2. Lorsque l'installation de Tivoli Netcool/OMNIbus est terminée, vous devez installer la sonde.

Etapes suivantes

L'environnement de test décrit dans ce scénario est conçu pour vous permettre de vous familiariser avec la manière selon laquelle les composants non Web et l'Interface graphique Web de Tivoli Netcool/OMNIbus peuvent collaborer au niveau le plus simple. Les composants sont hautement configurables. Consultez la documentation en détails pour déterminer la configuration la plus adaptée à vos exigences.

Chapitre 21. Liste de contrôle de configuration pour le mode FIPS 140–2

Si vous souhaitez exécuter Tivoli Netcool/OMNIbus en mode FIPS 140–2, les étapes de configuration requises dépendent de votre environnement d'installation. Exécutez également ces étapes de configuration si vous souhaitez utiliser le chiffrement fort dans un réseau protégé par SSL.

Utilisez la liste de contrôle suivante en tant que guide pour la configuration du mode FIPS 140–2.

Tableau 101. Liste de contrôle de configuration pour le mode FIPS 140–2

	Exigence	Action pour le fonctionnement en mode FIPS 140–2
☐	Si nécessaire, effectuez une mise à niveau sur le mode FIPS 140–2.	• Si votre installation existante utilise le chiffrement DES pour les mots de passe, modifiez le schéma de chiffrement des mots de passe en AES. Exécutez cette tâche avant ou après la mise à niveau. Cela dépend de la version à partir de laquelle vous effectuez la mise à niveau. • Si votre installation existante utilise le chiffrement des valeurs de propriété ou utilise les utilitaires **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe : 1. Déchiffrez les valeurs chiffrées avant d'effectuer la mise à niveau. 2. Mettez à niveau puis configurez vos composants serveur pour le mode FIPS 140–2. 3. Chiffrez à nouveau les valeurs à l'aide de l'algorithme et du mode de fonctionnement défini sur `AES_FIPS`.
☐	Si vous souhaitez commuter votre installation Tivoli Netcool/OMNIbus en mode FIPS 140–2, reconfigurez votre chiffrement si nécessaire. (Le reste des entrées de cette liste de contrôle s'applique également.)	• Si votre installation utilise le chiffrement DES pour vos mots de passe, définissez le schéma de chiffrement de mots de passe sur AES. • Si votre installation utilise le chiffrement des valeurs de propriété AES ou utilise les utilitaires **nco_g_crypt** et **nco_pa_crypt** pour chiffrer les mots de passe : 1. Déchiffrez les valeurs chiffrées. 2. Configurez vos composants de serveur en mode FIPS 140–2. 3. Chiffrez à nouveau les valeurs à l'aide de l'algorithme et du mode de fonctionnement défini sur `AES_FIPS`.

Tableau 101. Liste de contrôle de configuration pour le mode FIPS 140–2 (suite)

	Exigence	Action pour le fonctionnement en mode FIPS 140–2
☐	Configurez l'environnement d'exécution Java de Tivoli Netcool/OMNIbus pour le mode FIPS 140–2.	Après l'installation ou la mise à niveau : • Apportez les modifications de configuration nécessaires dans le fichier de propriétés de sécurité (`java.security`). • Téléchargez et ajoutez des fichiers de règles pour utiliser les algorithmes de chiffrement étendus.
☐	Configurez la prise en charge du mode FIPS 140–2 pour vos composants serveur.	Après la configuration de votre environnement d'exécution Java : 1. Créez un fichier de configuration FIPS (`fips.conf`) pour l'initialisation du mode FIPS 140–2. 2. Configurez les serveurs ObjectServer, les agents de processus, les serveurs proxy et les passerelles du serveur ObjectServer avec les paramètres FIPS 140–2 requis.
☐	Si vous utilisez SSL, activez le mode FIPS 140–2 pour les connexions SSL.	Avant de créer la base de données de clés, qui est utilisée pour stocker des certificats numériques et des clés, activez l'utilisation de la cryptographie certifiée par la norme FIPS 140–2 en configurant les propriétés pertinentes de l'utilitaire IBM Key Management (iKeyman). Lorsque vous migrez des données manuellement ou avec IBM Installation Manager, le script de migration `UPGRADE.SH` copie les magasins clés de l'ancien répertoire `$NCHOME/etc/security/keys/` vers `$NCHOME/etc/security/keys/migrated/`. Vous pouvez déplacer les fichiers migrés jusqu'au répertoire de clés, ou vous pouvez utiliser **`nc_gskcmd`** ou **`nc_ikeyman`** pour créer un nouveau magasin de clés et transférer les certificats de l'ancien magasin de clés vers le nouveau. Les utilisateurs FIPS qui mettent à niveau à partir de Tivoli Netcool/OMNIbus version 7.3.1.2 ou versions antérieures sont invités à créer un nouveau fichier de clés et noter les restrictions suivantes : • **`nc_ikeyman`** ne doit pas être utilisé en mode FIPS. • En mode FIPS, le mot de passe du magasin de clés doit être d'au moins 14 caractères et inclure au moins une lettre minuscule, une lettre majuscule et un caractère non alphabétique. En outre, aucun caractère peut apparaître plus de trois fois, ou plus de deux fois de suite.

Tableau 101. Liste de contrôle de configuration pour le mode FIPS 140–2 (suite)

	Exigence	Action pour le fonctionnement en mode FIPS 140–2
☐	Configurez l'Interface graphique Web en mode FIPS 140-2.	Après avoir configuré Tivoli Netcool/OMNIbus : 1. Activez le mode FIPS 140-2 sur le serveur Concentrateur des services d'application du tableau de bord. 2. Activez le mode FIPS 140-2 sur les clients d'Interface graphique Web. 3. Chiffrez les mots de passe à l'aide du mode FIPS 140-2. 4. Configurez une connexion SSL (Secure Socket Layer) pour l'échange de données d'événement entre le serveur ObjectServer et l'Interface graphique Web. 5. Configurez une connexion SSL pour gérer le Interface graphique Web à l'aide de l'interface WAAPI à partir de l'hôte distant. Pour plus d'informations, voir *Guide d'administration et d'utilisation de l'interface graphique Web d'IBM Tivoli Netcool/OMNIbus* .

Utilisez les liens suivants pour obtenir de plus amples informations sur l'exécution de ces tâches.

Annexe A. Identification et résolution des problèmes

Ces informations permettent d'identifier et de résoudre les problèmes liés à Tivoli Netcool/OMNIbus.

Identification et résolution des problèmes liés à la sécurité

Ces informations vous permettent d'identifier et de résoudre les problèmes de sécurité.

Exigences d'accès root pour les processus Tivoli Netcool/OMNIbus

Tivoli Netcool/OMNIbus ne nécessite pas d'accès root pour fonctionner. Des exceptions s'appliquent à l'utilisation du contrôle de processus et du module PAM.

L'accès root est nécessaire lorsque l'agent de processus est configuré pour exécuter des processus en tant qu'utilisateur différent de celui qui a démarré l'agent de processus.

L'accès root est obligatoire lorsque le module PAM est utilisé et configuré de telle sorte qu'il accède aux objets appartenant à la racine.

La sonde SNMP (**nco_p_mttrapd**) peut être exécutée en tant que root SUID sans compromettre la sécurité du système, lorsque l'accès root aux ports est requis. Dans ce mode, la sonde supprime ses privilèges après avoir ouvert la session SNMP et avant le démarrage de la bibliothèque de sondes IBM Tivoli Netcool/OMNIbus.

Référence associée:

«Echec d'authentification d'utilisateur avec les modules PAM», à la page 658
L'authentification auprès d'un système d'authentification PAM externe peut échouer si le serveur ObjectServer, l'agent de processus ou le processus de passerelle ne s'exécute pas en tant que root.

Echec de nco_pad lors de l'authentification du module PAM sous SUSE Linux

Echec du démon agent de contrôle de processus (nco_pad) lors de l'authentification du module PAM sous SUSE Linux.

Lorsque vous exécutez le démon agent de contrôle de processus (nco_pad) à l'aide de l'authentification du module PAM sous SUSE Linux, la valeur par défaut de la taille de la pile nco_pad doit être augmentée. Pour augmenter la taille de la pile Nco_pad et permettre ainsi de prendre en compte l'authentification du module PAM, exécutez la commande `$NCHOME/omnibus/bin/nco_pad` en indiquant une des options de ligne de commande suivantes :

- `-stacksize 139248` (sous SUSE Linux version 9.0)
- `-stacksize 278496` (sous SUSE Linux version 10.0).

Echec d'authentification d'utilisateur avec les modules PAM

L'authentification auprès d'un système d'authentification PAM externe peut échouer si le serveur ObjectServer, l'agent de processus ou le processus de passerelle ne s'exécute pas en tant que root.

Il ne s'agit pas d'une limitation des processus Tivoli Netcool/OMNIbus. Cela est provoqué par la configuration sous-jacente du module PAM et du système d'exploitation. Par exemple, ce problème se produit généralement si votre système est configuré pour utiliser le module pam_unix (ou un module équivalent) et le système d'exploitation est lui configuré (à l'aide du fichier `/etc/nsswitch.conf` ou d'un fichier similaire) pour vérifier le fichier de mots de passe caché local plutôt que le protocole NIS ou LDAP. Les processus Tivoli Netcool/OMNIbus exigent un accès en lecture à tous les fichiers auxquels le module PAM accède, notamment le fichier `/etc/shadow` (ou `/etc/security/passwd` sous AIX), qui stocke les informations sécurisées sur les comptes utilisateur.

- Linux HP-UX Solaris `etc/password`, `etc/shadow` et `etc/group`
- AIX `/etc/passwd`, `/etc/security/passwd`, `/etc/security/groupet /etc/security`

Cependant, les droits du système d'exploitation sont généralement définis de sorte que les fichiers puissent uniquement être lus par l'utilisateur root. Un processus non-root ne peut par conséquent pas lire le fichier afin de valider les mots de passe des utilisateurs. Il en résulte une erreur d'authentification.

Pour résoudre cette anomalie, indiquez une liste de contrôle d'accès (ACL) pour les fichiers `etc/password`, `etc/shadow` et `etc/group`.

L'exemple suivant explique comment utiliser la commande **`setfacl`** sur les systèmes d'exploitation Solaris pour créer une liste de contrôle d'accès pour l'utilisateur netcool sur `/etc/shadow`. Vérifiez avec votre administrateur que cette commande est disponible sur votre système.

```
vi /tmp/shadow.acl
user::r--
user:netcool:r--
group::---
mask:r--
other:---

setfacl -f /tmp/shadow.acl /etc/shadow

getfacl /etc/shadow

# file: /etc/shadow
# owner: root
# group: sys
user::r--
user:netcool:r--        #effective:r--
group::---              #effective:---
mask:r--
other:---
```

Autres solutions de rechange

- Demandez à votre administrateur système de reconfigurer le système d'exploitation afin que les fichiers ne soient pas vérifiés.
- Modifiez la configuration PAM pour utiliser un module différent qui n'exige pas d'accès à des ressources protégées (par exemple, pam_krb5).

- Exécutez le serveur ObjectServer, l'agent de processus et les processus de passerelle en tant qu'utilisateur root. De cette manière, ces processus peuvent lire le fichier `/etc/shadow` et les mots de passe entrés dans Tivoli Netcool/OMNIbus peuvent être validés en comparaison avec les mots de passe codés dans le fichier `shadow`.
- Modifiez les droits sur les ressources protégées. Par exemple, accordez un accès en lecture au fichier `/etc/shadow` pour l'utilisateur pour lequel le serveur ObjectServer, l'agent de processus ou la passerelle s'exécute. (Alors que cette solution palliative peut être considérée comme inappropriée dans les environnements de production, elle peut être temporairement appliquée dans un environnement de test pour rechercher si un échec d'authentification est lié au système d'exploitation et à la configuration du module PAM.)

Remarque : AIX Le module pam_aix exige que le processus d'appel (par exemple, le serveur ObjectServer, l'agent de processus ou la passerelle) soit exécuté en tant qu'utilisateur root. Si le processus s'exécute en tant qu'utilisateur non-root, le fait d'accorder l'accès en lecture à des fichiers protégés du système d'exploitation n'est pas une solution palliative viable et des échecs d'authentification continueront à se produire.

Test de la configuration LDAP

Vous pouvez utiliser l'utilitaire **ldapsearch** pour tester la configuration LDAP de l'Tivoli Netcool/OMNIbus sans redémarrer l'ObjectServer. **ldapsearch** permet la connexion au serveur LDAP, émet une requête et obtient des résultats qui sont basés sur votre configuration. Il n'authentifie pas les utilisateurs ni ne teste les définitions utilisateur de l'ObjectServer.

ldapsearch est fourni avec des systèmes d'exploitation et des variantes sont fournies par les fournisseurs LDAP. Les options et la syntaxe dépendent de la variante de l'utilitaire que vous utilisez.

Vous avez besoin des informations suivantes pour exécuter un test avec **ldapsearch** :

- Valeurs des propriétés suivantes, telles que définies dans le fichier de propriétés LDAP (`$NCHOME/omnibus/etc/ldap.props`) :
  - **Hostname**
  - **Port**
  - **LDAPBindDN**
  - **LDAPBindPassword**
  - **LDAPSearchBase**
  - **LDAPSearchFilter**
- Nom de l'utilisateur que vous souhaitez authentifier.

Des instructions et des exemples pour le test de la configuration LDAP de l'Tivoli Netcool/OMNIbus sont fournis dans la note technique suivante :

http://www-01.ibm.com/support/docview.wss?uid=swg21579907

Exemples de fichiers journaux

L'initialisation réussie d'une authentification d'utilisateur est consignée comme suit dans le fichier journal de l'ObjectServer :

```
2013-01-02T16:12:49: Information : I-ALD-104-006:
 Liaison imminente au serveur LDAP pour l'utilisateur
 cn=Bind User,ou=Webtop,ou=Tivoli,ou=SWG,o=ibm
2013-01-02T16:12:49: Information : I-ALD-104-007:
 Liaison réussie au serveur LDAP pour l'utilisateur
 cn=Bind User,ou=Webtop,ou=Tivoli,ou=SWG,o=ibm
```

Une connexion utilisateur réussie est consignée comment suit dans le fichier journal de l'ObjectServer :

```
2013-01-02T09:07:43: Débogage : D-UNK-000-000:
 secure-login@examplehost.ibm.com: Secure [User One]
2013-01-04T16:57:34: Débogage : D-ALD-105-005:
 Recherche LDAP imminente avec le filtre 'cn=User One'
2013-01-02T09:07:43: Information : I-ALD-104-012:
 La recherche LDAP sur l'utilisateur 'User One' a renvoyé
 le nom distinctif cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm
2013-01-02T09:07:43: Information : I-ALD-104-006:
 Liaison imminente au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm
2013-01-02T09:07:43: Information : I-ALD-104-007:
 Liaison réussie au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm.
2013-01-02T09:07:43: Débogage : D-OBX-105-016:
 Connexion authentifiée pour l'utilisateur User One sur l'hôte
 testserver.ibm.com à partir de l'application GET_LOGIN_TOKEN
2013-01-02T09:07:43: Information : I-OBX-104-007:
 Connexion de l'utilisateur User One@examplehost.hursley.ibm.com
réussie (ID connexion 1)
```

Tâches associées:

«Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe», à la page 343
Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

Erreurs d'authentification LDAP communes

Erreurs d'authentification LDAP communes

Les sections suivantes contiennent des détails sur les erreurs d'authentification LDAP communes, les message de journal résultant et les réponses suggérées :

- «Un utilisateur existe dans l'ObjectServer mais pas dans LDAP», à la page 661
- «Un utilisateur existe dans LDAP mais un mot de passe incorrect est spécifié», à la page 661
- «Un nom d'utilisateur existe dans plusieurs annuaires LDAP», à la page 662
- «L'ObjectServer ne peut pas contacter le serveur LDAP», à la page 662
- «La syntaxe de recherche LDAP est incorrecte», à la page 663
- «Une recherche LDAP arrive à expiration», à la page 663
- Windows «Echec de l'authentification LDAP avec des caractères Unicode», à la page 663

Les performances LDAP sont dépendantes de l'environnement de serveur LDAP particulier que vous utilisez. Votre administrateur LDAP est votre premier point de contact pour les problèmes d'authentification et de performances.

Un utilisateur existe dans l'ObjectServer mais pas dans LDAP

Lorsqu'un utilisateur existe dans l'ObjectServer mais pas dans LDAP, des messages similaires aux messages suivants sont écrits dans le fichier journal de l'ObjectServer :

```
2013-01-02T09:34:14: Erreur : E-ALD-102-027 :
 Aucun utilisateur LDAP trouvé avec le nom distinctif de base ou=Tivoli,ou=SWG,
o=ibm et le filtre (cn=Notin Ldap)
2013-01-02T09:34:14: Erreur : E-ALD-102-027:
Aucun utilisateur LDAP trouvé avec le nom distinctif de base ou=Tivoli,ou=SWG,
o=ibm et le filtre (cn=Notin Ldap)
2013-01-02T09:34:14: Information : I-SEC-104-003:
 Impossible d'authentifier l'utilisateur "Notin Ldap" avec
 la source externe. Erreur = "Utilisateur introuvable"
2013-01-02T09:34:14: Information : I-SEC-104-002:
 Impossible d'authentifier l'utilisateur "Notin Ldap" :
 Non authentifié
2013-01-02T09:34:14: Erreur : E-OBX-102-023 :
 Echec de l'authentification de l'utilisateur Notin Ldap.
 (-3602:Not authenticated)
2013-01-02T09:34:14: Erreur : E-OBX-102-057 :
 L'utilisateur Notin Ldap@examplehost.ibm.com n'a pas pu se connecter :
 Non authentifié
```

Le message associé suivant est consigné dans le journal d'audit :

```
2013-01-02T09:31:00: Erreur : E-SEC-010-002 :
 échec d'authentification - impossible d'authentifier l'utilisateur "Notin Ldap" :
 Non authentifié
```

Pour résoudre ce problème, contactez l'administrateur LDAP et déterminez si l'utilisateur existe dans LDAP et si l'ObjectServer dispose de l'accès en recherche pour cet utilisateur. Si l'utilisateur existe dans LDAP, vérifiez que vous utilisez le nom distinctif de base et le filtre de recherche corrects. Vérifiez les valeurs qui sont spécifiées pour les propriétés **LDAPSearchBase** et **LDAPSearchFilter**.

Si les propriétés de recherche et de filtre LDAP sont correctes, vérifiez avec votre administrateur LDAP que le compte utilisateur spécifié par les propriétés **LDAPBindDn** et **LDAPBindPassword** a le droit d'exécuter des recherches dans LDAP. Si l'ObjectServer est lié anonymement à LDAP, vérifiez que le répertoire et les utilisateurs que vous souhaitez rechercher sont configurés pour permettre un accès en lecture anonyme.

Un utilisateur existe dans LDAP mais un mot de passe incorrect est spécifié

Lorsqu'un utilisateur existe dans LDAP mais un mot de passe incorrect est fourni à LDAP, des messages similaires aux messages suivants sont écrits dans le fichier journal de l'ObjectServer :

```
2013-01-02T16:13:39: Information : I-ALD-104-006:
 Liaison imminente au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm
2013-01-02T16:13:39: Erreur : E-ALD-102-016:
 Echec de la liaison au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm.
(49:Données d'identification non valides)
2013-01-02T16:13:39: Erreur : E-ALD-102-011:
 Message de serveur LDAP reçu pendant la liaison.
2013-01-02T16:13:39: Information : I-ALD-104-006:
 Liaison imminente au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm
2013-01-02T16:13:39: Erreur : E-ALD-102-016:
```

```
 Echec de la liaison au serveur LDAP pour l'utilisateur
 cn=User One,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm.
(49:Données d'identification non valides)
2013-01-02T16:13:39: Erreur : E-ALD-102-011:
 Message de serveur LDAP reçu pendant la liaison.
2013-01-02T16:13:39: Information : I-SEC-104-003:
 Impossible d'authentifier l'utilisateur "User One"
 avec la source externe. Erreur = 'Données d'identification non valides'.
```

Le message associé suivant est consigné dans le journal d'audit :

```
2013-01-02T16:13:39: Information : I-SEC-104-002:
 Impossible d'authentifier l'utilisateur "User One" : Non authentifié
```

Pour résoudre le problème, indiquez le mot de passe correct.

Un nom d'utilisateur existe dans plusieurs annuaires LDAP

Lorsqu'un nom d'utilisateur n'est pas unique et existe dans plusieurs annuaires LDAP, des messages similaires aux messages suivants sont écrits dans le fichier journal de l'ObjectServer :

```
2013-01-02T16:13:52: Erreur : E-ALD-102-028:
 Plusieurs utilisateurs LDAP avec le nom distinctif
de base 'ou=Tivoli,ou=SWG,o=ibm'
 et le filtre '(cn=User Two)'
2013-01-02T16:13:52: Erreur : E-ALD-102-028:
 Plusieurs utilisateurs LDAP avec le nom distinctif de base 'ou=Tivoli,ou=SWG,o=ibm'
 et le filtre '(cn=User Two)'
2013-01-02T16:13:52: Information : I-SEC-104-003:
 Impossible d'authentifier l'utilisateur "User Two" avec
 une source externe. Erreur = 'Utilisateur LDAP non unique'.
2013-01-02T16:13:52: Information : I-SEC-104-002:
 Impossible d'authentifier l'utilisateur "User Two" : Non authentifié
2013-01-02T16:13:52: Erreur : E-OBX-102-023 :
 Echec de l'authentification de l'utilisateur User Two.
 (-3602:Not authenticated)
2013-01-02T16:13:52: Erreur : E-OBX-102-057:
 Echec de la connexion de l'utilisateur User Two@examplehost.ibm.com
: Non authentifié
```

Le message associé suivant est consigné dans le journal d'audit :

```
2013-01-02T16:13:39: Information : I-SEC-104-002:
 Impossible d'authentifier l'utilisateur "User Two" : Non authentifié
```

Pour résoudre le problème, contactez l'administrateur LDAP.

L'ObjectServer ne peut pas contacter le serveur LDAP

Lorsque l'ObjectServer ne peut pas contacter le serveur LDAP, des messages similaires aux messages suivants sont écrits dans le fichier journal de l'ObjectServer :

```
2013-01-04T16:17:57: Erreur : E-ALD-102-026:
 Echec de l'exécution de la recherche sur le serveur LDAP
avec le nom distinctif de base
 'ou=bluepages,o=ibm.com' et le filtre '(cn=Test User)':
 81:Impossible de contacter le serveur LDAP
2013-01-04T16:17:57: Information : I-SEC-104-003:
 Impossible d'authentifier l'utilisateur "Test User" avec une source externe.
 Erreur = 'Impossible de contacter le serveur LDAP'.
```

Si vous exécutez LDAP V2, le message suivant est consigné :

```
2013-01-04T16:34:42: Erreur : E-ALD-102-012:
 Echec de ldap_open au serveur LDAP. Hôte exampleserver.ibm.com. Port 389.
 Erreur - 145:Expiration du délai de la connexion.
```

Pour résoudre ce problème, vérifiez que le serveur LDAP s'exécute, que la connexion n'est pas bloquée par un pare-feu et que le port LDAP correct est spécifié pour la propriété **Port** dans le fichier de propriétés LDAP.

Ces messages peuvent également être consignés lorsque le serveur LDAP requiert la sécurité de liaison mais l'ObjectServer est configuré pour la liaison anonyme. Si l'ObjectServer est configuré pour la liaison anonyme, contactez l'administrateur LDAP pour vérifier si la configuration LDAP requiert la sécurité de liaison.

La syntaxe de recherche LDAP est incorrecte

Lorsque la syntaxe d'un filtre de recherche LDAP est incorrecte, des messages similaires aux messages suivants sont écrits dans le fichier journal de l'ObjectServer :

```
2013-01-07T11:34:46: Débogage : D-ALD-105-005:
 Recherche LDAP imminente avec le filtre '(&(cn=User Five)(|(ou=Tivoli)(ou=Webtop))'
2013-01-07T11:34:46: Erreur : E-ALD-102-026:
 Echec de l'exécution de la recherche sur le serveur LDAP avec le
nom distinctif de base
 'ou="Tivoli",ou=SWG,o=ibm' et le filtre '(
&(cn=User Five)(|(ou=Tivoli)(ou=Webtop))' :
 87:Filtre de recherche incorrect
```

Lorsque vous testez le filtre de recherche avec l'utilitaire **ldapsearch**, vous obtenez une réponse similaire à la réponse suivante :

```
ldapsearch : ldap_search_ext : Filtre de recherche incorrect (-7)
```

Pour résoudre le problème, contactez l'administrateur LDAP pour obtenir de l'aide pour formuler la requête de recherche.

Une recherche LDAP arrive à expiration

Lorsqu'une recherche LDAP arrive à expiration, un message similaire au message suivant est écrit dans le fichier journal de l'ObjectServer :

```
2013-01-07T15:16:08: Erreur : E-AUT-102-026:
 Echec de l'exécution de la recherche sur le serveur LDAP avec le
nom distinctif de base
 'ou="Tivoli",ou=SWG,o=ibm' et le filtre '(cn=A User)':
 85:Expiration du délai
```

Pour résoudre le problème, contactez l'administrateur LDAP pour obtenir de l'aide pour améliorer les performances des requêtes.

Windows

Echec de l'authentification LDAP avec des caractères Unicode

Sur les systèmes d'exploitation Windows, vous devez sauvegarder le fichier de propriétés LDAP en codage UTF-8 lorsque l'ObjectServer est configuré pour s'exécuter avec UTF-8 activé.

Des erreurs similaires aux suivantes sont consignées lorsque vous n'utilisez pas le codage UTF-8 : Dans cet exemple, la valeur de propriété **LDAPSearchBase** contient la chaîne `plutôt`.

```
2013-05-23T10:45:27: Avertissement : W-ETC-102-003:
Caractère non valide 0xf4 trouvé lors
 de la conversion en Unicode.
2013-05-23T10:45:27: Avertissement : W-ETC-102-003:
Caractère non valide 0xf4 trouvé lors
 de la conversion en Unicode.
2013-05-23T10:45:27: Avertissement : W-ETC-102-003:
Caractère non valide 0xf4 trouvé lors
 de la conversion en Unicode.
...
...
2013-05-23T10:45:54: Débogage : D-AUT-105-005: Recherche LDAP imminente avec le
filtre '(uid=yaya)' et nom distinctif de base 'ou=plut...t,dc=HURSLEY,dc=IBM,dc=COM'
2013-05-23T10:45:54: Erreur : E-AUT-102-034: LDAPSearch a renvoyé 'NO_SUCH_OBJECT'.
 Vérifiez que LDAPSearchBase a été correctement spécifié et
 que l'objet de nom distinctif de base 'ou=plut...t,dc=HURSLEY,dc=IBM,dc=COM' existe
```

Pour coder le fichier de propriétés en UTF-8, ouvrez-le dans le Bloc-notes Windows et utilisez la commande **Enregistrer sous...** pour enregistrer une nouvelle version. Utilisez le nom de fichier existant, `ldap.props`. Vous devez ensuite redémarrer l'ObjectServer afin qu'il lise le fichier de propriétés mis à jour.

Pour plus d'informations sur les paramètres d'environnement linguistique et le codage UTF-8, voir *Guide d'installation et de déploiement d'IBM Tivoli Netcool/OMNIbus*.

Concepts associés:

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Tâches associées:

«Configuration de Tivoli Netcool/OMNIbus pour utiliser LDAP pour une authentification externe», à la page 343
Tivoli Netcool/OMNIbus prend en charge l'authentification externe d'utilisateurs du serveur ObjectServer dont les mots de passe sont stockés dans un référentiel conforme au protocole LDAP (Lightweight Directory Access Protocol), notamment Active Directory ou Tivoli Directory Services.

«Calcul des temps de recherche LDAP», à la page 665
Vous pouvez calculer le temps nécessaire à une recherche LDAP en comparant les horodatages de message de débogage dans le fichier journal de l'ObjectServer. Vous pouvez utiliser les entrées de journal pour connaître la durée des recherches individuelles et pour optimiser l'ordre des recherches dans vos requêtes.

Référence associée:

«Propriétés LDAP», à la page 348
Le fichier de propriétés `$NCHOME/omnibus/etc/ldap.props` vous permet de définir des paramètres de configuration pour se connecter à un référentiel LDAP.

Calcul des temps de recherche LDAP

Vous pouvez calculer le temps nécessaire à une recherche LDAP en comparant les horodatages de message de débogage dans le fichier journal de l'ObjectServer. Vous pouvez utiliser les entrées de journal pour connaître la durée des recherches individuelles et pour optimiser l'ordre des recherches dans vos requêtes.

Procédure

1. Définissez le niveau des messages de l'ObjectServer sur débogage.
2. Connectez-vous à l'ObjectServer. Si vous êtes déjà connecté à l'ObjectServer, déconnectez-vous et reconnectez-vous.

   Cette action est nécessaire pour démarrer le processus d'authentification LDAP.
3. Localisez les entrées de message de débogage suivantes dans le fichier journal de l'ObjectServer :

   ```
   2013-01-04T16:57:34: Débogage : D-ALD-105-005:
    Recherche LDAP imminente avec le filtre '(cn=User Three)'
   2013-01-04T16:57:34: Débogage : D-ALD-105-004:
    La recherche LDAP sur l'utilisateur 'User Three' a renvoyé le nom distinctif
    'uid=123456,c=gb,ou=someplace,o=ibm.com'
   ```

   La différence entre les horodatages indique le nombre de secondes nécessaire à l'exécution de la recherche LDAP. Dans ce cas, étant donné que les horodatages sont identiques, la recherche a pris moins d'une seconde.

Exemple

Dans l'extrait de fichier journal suivant, plusieurs noms distinctifs ont été spécifiés pour la recherche.

```
2013-02-07T09:20:25: Débogage : D-AUT-105-005:
 Recherche LDAP imminente avec le filtre '(cn=User Five)'
 et nom distinctif de base dn 'ou=Webtop,ou=Tivoli,ou=SWG,o=ibm'
2013-02-07T09:20:25: Débogage : D-AUT-102-006:
 Aucun utilisateur LDAP trouvé avec le nom distinctif de base
'ou=Webtop,ou=Tivoli,ou=SWG,o=ibm' et le filtre '(cn=User Five)'
2013-02-07T09:20:25: Débogage : D-AUT-105-005:
 Recherche LDAP imminente avec le filtre '(cn=User Five)'
 et nom distinctif de base dn 'ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm'
2013-02-07T09:20:25: Débogage : D-AUT-105-004:
 La recherche LDAP sur l'utilisateur 'User Five' a renvoyé le nom distinctif
 'cn=User Five,ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm'
```

L'ObjectServer a recherché le nom d'utilisateur `User Five`, comme indiqué par la propriété **`LDAPSearchFilter`** dans le fichier de propriétés LDAP. Le nom distinctif de base pour la recherche, comme spécifié par la propriété **`LDAPSearchBase`** était `ou=Webtop,ou=Tivoli,ou=SWG,o=ibm;;ou=OMNIbus,ou=Tivoli,ou=SWG,o=ibm`. L'ObjectServer a recherché chaque nom distinctif dans l'ordre indiqué. La recherche du nom distinctif de base `Webtop` a échoué.

Le temps de recherche total est la différence entre les horodatages de la première et de la dernière entrées de journal (dans ce cas, moins d'une seconde). La différence entre les horodatages de la première et de la deuxième entrées indique le temps pris pour la recherche `Webtop` ayant échoué.

Référence associée:

«Erreurs d'authentification LDAP communes», à la page 660
Erreurs d'authentification LDAP communes

Connexion à l'Interface graphique Web après un échec du serveur LDAP

Si l'Interface graphique Web est configurée pour s'authentifier à un serveur LDAP, aucun utilisateur ne peut se connecter à l'Interface graphique Web lorsque le serveur LDAP échoue.

Ce problème affecte également l'utilisateur tipadmin par défaut. Pour autoriser l'utilisateur tipadmin à accéder à l'installation de l'Interface graphique Web lorsque le serveur LDAP échoue :

1. Accédez au répertoire *REP_INSTALL_JazzSM*/bin et démarrez l'utilitaire **wsadmin**.
2. Utilisez la commande **updateIdMgrRealm** pour modifier le paramètre **allowOperationIfReposDown** de false à true, dans le domaine defaultWIMFileBasedRealm :

   ```
   $AdminTask updateIdMgrRealm {-name defaultWIMFileBasedRealm
   -allowOperationIfReposDown true}
   ```

3. Redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Vous pouvez désormais vous connecter à l'Interface graphique Web à l'aide de l'utilisateur et du mot de passe tipadmin.

Pour plus d'informations sur la commande **wsadmin** et sur les commandes associées, voir le centre de documentation *Websphere Application Server* à l'adresse http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.wim.doc/UnableToAuthenticateWhenRepositoryIsDown.html

Tâches associées:

«Redémarrage du serveur», à la page 618
Une fois la personnalisation et la configuration effectuées, il sera peut-être nécessaire de redémarrer le serveur de l'Interface graphique Web.

Identification et résolution des problèmes liés au support multiculturel

Lors de l'exécution du serveur ObjectServer au codage UTF-8 sous Windows, la liste d'événements de bureau sous Windows peut ne pas parvenir à afficher correctement certains caractères du serveur ObjectServer en raison de limitations de la liste d'événements.

La liste d'événements de bureau ne prend pas totalement en charge le codage UTF-8. Vous devez donc plutôt utiliser la liste d'événements actifs du composant d'Interface graphique Web pour afficher les données d'événement au codage UTF-8.

Concepts associés:

«Configuration de votre environnement local», à la page 418
Les paramètres de langue, de jeu de caractères, d'ordre de tri et de format de données utilisés au moment de l'exécution sont déterminés par vos paramètres d'environnement local. Vous pouvez utiliser les variables d'environnement de localisation sous UNIX et Linux ou le panneau de configuration sous Windows pour définir votre environnement local.

Traitement des problèmes de connexion aux listes d'événements (Windows)

Si vous rencontrez un message d'erreur `Impossible d'écrire sur le socket` lorsque vous démarrez la liste d'événements de bureau (**NCOEvent**) sur des systèmes d'exploitation Windows, utilisez les informations suivantes pour résoudre le problème.

Testez la disponibilité du serveur ObjectServer en y ouvrant une session à l'aide de Netcool/OMNIbus Administrator (**nco_config**) ou de l'éditeur de serveurs.

Si la connexion au serveur ObjectServer est disponible, la cause du problème est probablement un problème réseau, tel qu'un échec de résolution DNS ou l'existence d'un pare-feu entre le serveur ObjectServer et la liste d'événements. Le message suivant dans le journal du système d'exploitation indique un problème réseau :

```
Echec de la connexion au port IDUC pour le serveur ObjectServer :
nom_serveur_ObjectServer,
 hôte IDUC nom_hôte_local, port IDUC : numéro_port
```

Vérification de la résolution du nom d'hôte

Si vous pouvez ouvrir une session dans le serveur ObjectServer mais que le problème persiste, utilisez les étapes suivantes pour tester la connexion :

1. Sur l'ordinateur client à partir duquel vous voulez exécuter la liste d'événements, démarrez l'interface interactive SQL (**isql**) et établissez une connexion avec le serveur ObjectServer.
2. Lancez la commande SQL suivante pour trouver le nom et le port de l'hôte utilisés par la liste d'événements pour se connecter au serveur ObjectServer :

   ```
   1> bind to iduc;
   2> go
   ```

   Si la commande retourne un nom d'hôte abrégé, tel que `exemple_hôte`, au lieu d'un nom de domaine complet (FQDN), tel que `exemple_hôte.ibm.com`, il peut s'agir de la cause du problème : le nom d'hôte abrégé ne peut pas être résolu à partir de l'ordinateur client.
3. Utilisez l'utilitaire **ping** pour vérifier la connexion à l'hôte retournée par **isql**.

   Si la commande ping échoue pour le nom d'hôte abrégé mais qu'elle réussit pour le nom de domaine complet, c'est que le problème est provoqué par l'impossibilité pour l'ordinateur client de résoudre le nom d'hôte abrégé.

Si le problème est provoqué par l'utilisation par le serveur ObjectServer d'un nom d'hôte abrégé, vous pouvez ajouter le nom d'hôte abrégé au fichier des hôtes Windows ou changer votre configuration DNS pour vous assurer que l'ordinateur client résout le nom d'hôte abrégé. Vous pouvez aussi définir la propriété ObjectServer **Iduc.ListeningHostname** avec le nom de domaine complet. Utilisez ensuite **nslookup** ou un utilitaire similaire pour vérifier que les noms d'hôte se résolvent correctement sur les deux ordinateurs.

Vérification des paramètres de port

Si le problème n'est pas provoqué par la résolution du nom d'hôte, vérifiez que les ports corrects sont définis et qu'ils ne sont pas bloqués par un pare-feu.

Deux ports sont utilisés pour transmettre les données entre un serveur ObjectServer et une liste d'événements. Le port ObjectServer est utilisé par les clients pour établir une connexion au serveur the ObjectServer et il est défini dans l'éditeur de serveur (ou dans le fichier des interfaces sur les systèmes d'exploitation UNIX et Linux). Le port IDUC est utilisé par le serveur ObjectServer pour envoyer des mises à jour à la liste d'événements. Si vous ne spécifiez pas le port IDUC en définissant la propriété **Iduc.ListeningPort** (ou en définissant le port dans le fichier ObjectServer `/etc/services` sur les systèmes d'exploitation UNIX et Linux), le serveur ObjectServer sélectionne de façon aléatoire un port IDUC dans les ports inutilisés disponibles.

Définissez la propriété ObjectServer **Iduc.ListeningPort** avec le numéro de port IDUC correct et demandez à l'administrateur du pare-feu d'ouvrir ce port.

Pour plus d'informations sur les propriétés ObjectServer **Iduc.ListeningHostname** et **Iduc.ListeningPort**, voir le *Guide d'administration de Netcool OMNIbus*.

Traitement des problèmes liés aux erreurs de programme d'écoute ObjectServer (UNIX et Linux)

Si vous rencontrez une erreur d'échec du programme d'écoute lorsque vous démarrez un serveur ObjectServer, utilisez les informations suivantes pour résoudre le problème.

Lorsqu'un serveur ObjectServer échoue à démarrer en raison d'une erreur d'échec du programme d'écoute, des messages similaires à ceci sont consignés :

```
Net-Library routine net_listen failed in srv_start_net Network error:
 status = 23 - Net-Lib protocol driver call to register a listener failed

Net-Library routine sybnet_listen() failed in srv__start_net OpenServer -
 Fatal Error: numéro_erreur : Failed to start any network listeners
```

Pour résoudre le problème, vérifiez les conditions suivantes :

- Vérifiez que les paramètres d'hôte et de port dans le fichier d'interfaces (`$NCHOME/omnibus/etc/omni.dat`) sont corrects.

  Corrigez les éventuelles erreurs et utilisez l'éditeur de serveur ou l'utilitaire **nco_igen** pour générer un nouveau fichier d'interfaces.
- Vérifiez que le port spécifié pour le serveur ObjectServer n'est pas déjà utilisé par une autre application.

  Ce problème est indiqué par le message suivant dans le fichier journal :

  ```
  Error -1:Socket bind failed - errno 125 Address already in use
  ```

  Vous pouvez utiliser les commandes **netstat** et **grep** suivantes pour vérifier que le port est disponible :

  ```
  netstat -an |grep numéro_port
  ```
- Utilisez l'utilitaire **ping** pour tester la connexion à l'hôte ObjectServer spécifié dans le fichier d'interfaces.

  Si la connexion n'est pas disponible, signalez le problème à votre administrateur réseau.
- Utilisez l'utilitaire **nslookup** pour tester la résolution de nom DNS pour l'hôte ObjectServer qui est spécifié dans le fichier d'interfaces.

  Si le nom d'hôte ObjectServer ne peut pas être résolu, signalez le problème à votre administrateur réseau.
- Vérifiez que le nom d'hôte est configuré correctement dans les fichiers suivants :

- $NCHOME/omnibus/etc/resolv.conf
- $NCHOME/omnibus/etc/nsswitch.conf
- $NCHOME/omnibus/etc/hosts

Traitement des problèmes d'affichage (UNIX et Linux)

Si vous rencontrez des problèmes lors du démarrage des interfaces graphiques sur les systèmes d'exploitation UNIX et Linux, vous pouvez faire appel à l'utilitaire **nco_xcheck** pour vérifier la disponibilité du système X Window (X11).

Pour exécuter l'utilitaire **nco_xcheck**, accédez au répertoire $NCHOME/omnibus/bin et exécutez la commande suivante :

```
./nco_xcheck
```

L'utilitaire vérifie que la variable d'environnement $DISPLAY est paramétrée sur un serveur X11.

Si X11 est disponible, l'utilitaire renvoie le message suivant : `XDisplay test passed`

Si X11 n'est pas disponible, l'utilitaire renvoie le message suivant : `XDisplay test failed`

Collecte des détails d'installation

Après avoir installé les composants côté serveur de Tivoli Netcool/OMNIbus, vous pouvez exécuter l'outil d'affichage de version de serveur d'objets (**nco_id**) pour vérifier que l'installation des composants a abouti. Les informations recueillies sont également utiles pour le dépannage.

Pourquoi et quand exécuter cette tâche

L'outil d'affichage de version de serveur d'objets est un utilitaire de ligne de commande qui peut recueillir et afficher des informations de base ou détaillées sur votre installation Tivoli Netcool/OMNIbus. Il peut écrire les informations recueillies dans un fichier `.html` ou vous pouvez rediriger la sortie de ligne de commande vers un fichier.

L'ensemble d'informations de base inclut les répertoires d'installation, les produits installés, les composants et les groupes de correctifs.

L'ensemble détaillé des informations comprend l'ensemble des informations de base et les informations suivantes :

- Informations sur le système d'exploitation.
- Informations sur IBM Installation Manager collectées de Tivoli Netcool/OMNIbus ainsi que de toutes les sondes qui sont installées sur l'ordinateur hôte. Le compte d'utilisateur qui exécute **nco_id** doit avoir accès en lecture au répertoire de données Installation Manager et son contenu.
- Liste des fichiers binaires installés dans les répertoires suivants, y compris les sommes SHA1 de tous les fichiers :

  UNIX Linux 32-bit

  - $NCHOME/omnibus/*arch*/bin
  - $NCHOME/omnibus/*arch*/lib

UNIX Linux 64-bit

- $NCHOME/omnibus/*arch*/bin64
- $NCHOME/omnibus/*arch*/lib64

Windows

- %NCHOME%\omnibus\win32\bin
- %NCHOME%\omnibus\win32\lib

- Heure à laquelle les bibliothèques de produits ont été compilées.

Vous pouvez lancer l'outil d'affichage de version de serveur d'objets avec l'une des commandes suivantes :

- *NCHOME*/bin/nco_id
- *NCHOME*/omnibus/bin/nco_id

Vous pouvez spécifier les options de ligne de commande suivantes lorsque vous démarrez l'outil.

Option de ligne de commande	Description
-?	Affiche des informations d'aide sur les options disponibles.
-o *chaîne*	Indique le nom et l'emplacement d'un fichier .html dans lequel les informations recueillies sont écrites. Si vous spécifiez uniquement un nom de fichier, le fichier est créé dans le répertoire de travail.
-s	Affiche des informations de base sur l'installation. Il s'agit de l'option par défaut.
-v	Affiche des informations détaillées sur l'installation.

Procédure

1. Pour écrire les informations détaillées dans un fichier .html, utilisez la commande suivante :

   NCHOME/omnibus/bin/nco_id -o PackageTest.html -v

2. Pour rediriger les informations détaillées dans un fichier texte, utilisez la commande suivante:

   NCHOME/omnibus/bin/nco_id -v > PackageTest.txt

Que faire ensuite

Si un composant que vous avez choisi d'installer est absent des informations recueillies, cela pourrait indiquer qu'un ou plusieurs composants n'ont pas été installés avec succès. Vérifiez les fichiers journaux d'installation et relisez les messages d'installation pour identifier tout problème survenu au cours de l'installation.

Identification et résolution des problèmes d'intégration

Ces informations vous permettent d'identifier et résoudre les problèmes d'intégration d'IBM Tivoli Netcool/OMNIbus à d'autres produits.

Le changement de statut génère des valeurs d'événement Tivoli Monitoring incorrectes dans Netcool/OMNIbus

Lorsque la synchronisation des événements IBM Tivoli Monitoring et IBM Tivoli Netcool/OMNIbus est installée, les changements de statut d'événement dans Tivoli Monitoring ou Tivoli Netcool/OMNIbus peuvent entraîner des erreurs dans les zones de gravité et de récapitulatif de Tivoli Netcool/OMNIbus. La gravité d'un événement Tivoli Monitoring clos peut être définie sur une valeur différente de 0 et le récapitulatif d'un événement Tivoli Monitoring peut être abrégé pour contenir uniquement le nom de la situation.

Ce problème est causé par un conflit entre le déclencheur itm_deduplication fourni par le composant de synchronisation des événements et le déclencheur de dédoublonnage Tivoli Netcool/OMNIbus standard.

Si vous utilisez une configuration Tivoli Netcool/OMNIbus à plusieurs niveaux, les déclencheurs col_deduplication et agg_deduplication peuvent être en conflit avec le déclencheur itm_deduplication. Dans ce cas, seuls les ObjectServers qui reçoivent les données Tivoli Monitoring peuvent être mis à jour, généralement au niveau de la couche collection.

Le problème peut se produire en réponse aux changements de statut d'événement suivants :

- Un événement de situation est réceptionné dans Tivoli Monitoring.
- Un événement de situation est réinitialisé ou fermé dans Tivoli Monitoring.
- Un accusé de réception d'événement de situation arrive à expiration dans Tivoli Monitoring.
- Un événement de situation est récurrent dans Tivoli Monitoring.
- Un événement de situation est réceptionné dans Tivoli Netcool/OMNIbus.
- La gravité d'un événement de situation est définie sur effacement dans Tivoli Netcool/OMNIbus.
- La gravité d'un événement de situation passe d'effacement à une autre gravité dans Tivoli Netcool/OMNIbus.

Pour résoudre ce problème, modifiez le déclencheur de dédoublonnage standard Tivoli Netcool/OMNIbus pour ignorer les événements de situation Tivoli Monitoring. Vous pouvez utiliser Netcool/OMNIbus Administrator ou l'interface interactive SQL pour modifier le déclencheur de dédoublonnage.

Pour modifier le déclencheur de dédoublonnage avec Netcool/OMNIbus Administrator :

1. Démarrez Netcool/OMNIbus Administrator (**nco_config**).
2. Connectez-vous à l'ObjectServer dont vous modifiez le déclencheur.
3. Dans le menu, sélectionnez **Automation Triggers (Déclencheurs d'automatisation)**.
4. Démarrez l'éditeur pour le déclencheur de dédoublonnage.
5. Dans l'onglet **When**, entrez la clause suivante :

   ```
   new.Type not in (20,21)
   ```

6. Sauvegardez le déclencheur modifié et quittez Netcool/OMNIbus Administrator.

Pour modifier le déclencheur de dédoublonnage avec l'interface interactive SQL :

1. Ouvrez le fichier SQL d'automatisations suivant pour l'éditer :

   UNIX Linux `$NCHOME/omnibus/etc/automation.sql`

   Windows `%NCHOME%\omnibus\etc\automation.sql`

2. Dans le fichier d'automatisations, identifiez la commande qui crée le déclencheur de dédoublonnage. Par exemple :

```
create or replace trigger deduplication
group default_triggers
priority 1
comment 'Deduplication processing for ALERTS.STATUS'
before reinsert on alerts.status
for each row
begin
   set old.Tally = old.Tally + 1;
   set old.LastOccurrence = new.LastOccurrence;
   set old.StateChange = getdate();
   set old.InternalLast = getdate();
   set old.Summary = new.Summary;
   set old.AlertKey = new.AlertKey;
   if ((old.Severity = 0) and (new.Severity > 0))
   then
      set old.Severity = new.Severity;
   end if;
end;
go
```

3. Copiez la commande dans un fichier temporaire, par exemple `/tmp/dedup.sql` ou `C:\tmp\dedup.sql`.
4. Editez le fichier temporaire et ajoutez la ligne suivante à la clause `for each row` :

   ```
   when (new.Type not in (20,21))
   ```

   Par exemple :

```
create or replace trigger deduplication
group default_triggers
priority 1
comment 'Deduplication processing for ALERTS.STATUS'
before reinsert on alerts.status
for each row
 when (new.Type not in (20,21))
begin
   set old.Tally = old.Tally + 1;
   set old.LastOccurrence = new.LastOccurrence;
   set old.StateChange = getdate();
   set old.InternalLast = getdate();
   set old.Summary = new.Summary;
   set old.AlertKey = new.AlertKey;
   if ((old.Severity = 0) and (new.Severity > 0))
   then
      set old.Severity = new.Severity;
   end if;
end;
go
```

5. Sauvegardez le fichier temporaire.
6. Exécutez la commande suivante pour remplacer le déclencheur de dédoublonnage standard :

UNIX Linux `$NCHOME/omnibus/bin/nco_sql -user nom_utilisateur -password mot_de_passe -server nom_serveur < /tmp/dedup.sql`

Windows `%NCHOME%\omnibus\bin\isql -U nom_utilisateur -P mot_de_passe -S nom_serveur < C:\tmp\dedup.sql`

Où *nom_utilisateur* est le nom d'utilisateur de l'ObjectServer, *mot_de_passe* est le mot de passe de l'ObjectServer et *nom_serveur* est le nom de l'ObjectServer.

Informations de support

Si vous rencontrez un incident avec votre logiciel IBM, vous souhaitez le résoudre rapidement. Ces informations décrivent comment utiliser l'application IBM Support Assistant et comment obtenir des correctifs du produit et recevoir des mises à jour de support.

IBM Support Assistant

IBM Support Assistant (ISA) est un outil de maintenabilité logicielle local gratuit qui vous aide à résoudre les problèmes liés aux applications logicielles IBM. ISA permet d'accéder rapidement aux informations de support et aux outils de maintenabilité pour identifier les problèmes.

Le Plan de travail ISA utilise un composant de collecteur de données pour collecter des informations sur votre installation de Tivoli Netcool/OMNIbus. Tivoli Netcool/OMNIbus fonctionne avec ISA version 4.1.1 et ultérieures.

Remarque : Vous pouvez également exécuter le Collecteur de données ISA (ISADC) indépendamment, sans installer le Plan de travail ISA. ISADC recueille les mêmes informations de prise en charge que le Plan de travail.

Pour plus d'informations sur le téléchargement et l'exécution du Plan de travail ISA, consultez le site Web suivant :

http://www.ibm.com/software/support/isa/workbench.html

Vous devez avoir un ID IBM pour télécharger ISA. Si vous avez déjà installé une version plus ancienne de ISA, utilisez son composant de mise à jour pour mettre à jour votre installation à la version 4.1.1.

Pour plus d'informations sur l'utilisation de ISA, consultez le guide de l'utilisateur intégré. Un tutoriel en ligne IBM assistant de formation est disponible à l'adresse suivante :

http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp?topic=/com.ibm.iea.isa/isa/ISAv40_Task.html

Collecte de données avec le Plan de travail ISA

Utilisez le composant de mise à jour ISA pour installer la version la plus récente de Tivoli Netcool/OMNIbus Collector.

Les conditions suivantes s'appliquent lorsque vous utilisez ISA pour collecter des données Tivoli Netcool/OMNIbus :

- Sur les systèmes d'exploitation Windows, vous devez posséder des droits d'administrateur.

- Vous devez avoir le droit d'exécuter toutes les applications lors de l'installation de Tivoli Netcool/OMNIbus.
- Pour collecter le maximum de données sur un ObjectServer, vérifiez qu'il est en cours d'exécution avant d'exécuter le collecteur de données. Vous devez également disposer des informations d'identification pour vous connecter à l'ObjectServer lorsque vous êtes invité à le faire.

Pour collecter les données, lancez ISA, puis exécutez Tivoli Netcool/OMNIbus Collector.

Par exemple, si vous rencontrez des problèmes avec la configuration de la sonde sur un ordinateur Solaris, lancez ISA sur cet ordinateur, puis exécutez Tivoli Netcool/OMNIbus Collector. Si vous souhaitez collecter uniquement les données de la sonde, sélectionnez la catégorie de collecte de données de la sonde.

Si vous rencontrez des problèmes liés à une liste d'événements sur un client Windows qui est connecté à un ObjectServer sur un ordinateur Solaris, lancez ISA sur la machine Windows. Exécutez ensuite Tivoli Netcool/OMNIbus Collector.

Vous pouvez choisir d'envoyer automatiquement les résultats de la collecte de données au site FTP d'assistance IBM (ftp://ftp.emea.ibm.com/). Vous pouvez également envoyer les données vers d'autres serveurs de support IBM. Contactez votre représentant du support de niveau 2 pour les informations sur le serveur FTP et d'authentification.

Tâches associées:

«Exécution du Collecteur de données d'ISA», à la page 676
Vous pouvez exécuter le Collecteur de données d'ISA (ISADC) indépendamment du Plan de travail IBM Support Assistant (ISA). Vous pouvez l'exécuter comme un utilitaire de console à partir de Tivoli Netcool/OMNIbus ou de l'interface Web ISADC publique ou comme un utilitaire autonome que vous téléchargez à partir du site Web ISADC.

Référence associée:

«Collecteur de données d'ISA»
Le IBM Support Assistant Data Collector (ISADC)est un outil basé sur Java pour collecter automatiquement les données de problèmes des produits IBM.

«Analyseur de traces et de journaux ISA», à la page 678
L'analyseur de traces et de journaux vous permet de recueillir des données système et de performances à partir de vos systèmes locaux et distants. Les données peuvent vous permettre d'identifier un incident, dès lors qu'un événement système inférieur à optimal se produit.

Collecteur de données d'ISA

Le IBM Support Assistant Data Collector (ISADC)est un outil basé sur Java pour collecter automatiquement les données de problèmes des produits IBM.

Vous pouvez utiliser ISADC pour exécuter un collecteur de données Tivoli Netcool/OMNIbus qui recueille des informations sur votre système. En plus des données par défaut qui sont recueillies, vous pouvez choisir de collecter les catégories d'informations suivantes :

- Données d'installation
- Données de sonde
- Données de passerelle
- Données d'ObjectServer

Vous pouvez exécuter ISADC indépendamment du Plan de travail ISA. Vous pouvez l'exécuter comme un utilitaire de console à partir de Tivoli Netcool/OMNIbus ou de l'interface Web ISADC publique ou comme un utilitaire autonome que vous téléchargez à partir du site Web ISADC.

Le tableau suivant décrit les informations recueillies par le collecteur de données Tivoli Netcool/OMNIbus.

Remarque : *NCHOME* indique que le répertoire existe sur les systèmes d'exploitation Windows, UNIX et Linux. `$NCHOME` indique un répertoire spécifique d'UNIX ou de Linux. `%NCHOME%` indique un répertoire spécifique de Windows.

Tableau 102. Informations recueillies par ISADC

Catégorie de collection	**Fichier ou répertoire**
Par défaut	*NCHOME*`/omnibus/etc` Le contenu des sous-répertoires suivants est exclu : • `initial` • `default` • `restos/default`
Par défaut	*NCHOME*`/omnibus/log`
Par défaut	`$NCHOME/etc` Le contenu des sous-répertoires suivants est exclu : • `security` • `default`
Par défaut	*NCHOME*`/log`
Par défaut	Liste des fichiers et des tailles de fichiers dans le répertoire *NCHOME*`/omnibus/db`.
Par défaut	Liste des fichiers et des tailles de fichiers dans le répertoire *NCHOME*`/omnibus/var`.
Par défaut	*NCHOME*`/omnibus/RELEASE_ID`
Par défaut	Sortie de *NCHOME*`/omnibus/bin/nco_id -v`.
Par défaut	Configuration du système hôte. Ces informations sont collectées par les collecteurs de données ISADC My System qui est exécuté automatiquement par le collecteur de donnée Tivoli Netcool/OMNIbus.
Par défaut	`$NCHOME/omnibus/desktop` Tous les fichiers avec des extensions `.elc` et `.elv` sont inclus.
Par défaut	`%NCHOME%\omnibus\ini` Le contenu du sous-répertoire `default` est exclu.
Par défaut	*NCHOME*`/platform/`*arch*`/jre.`*version*`/jre/lib/security` Inclut le fichier `java.security`.
Par défaut	`%NCHOME%\ini` Le contenu des sous-répertoires suivants est exclu : • `security` • `default`

Tableau 102. Informations recueillies par ISADC (suite)

Catégorie de collection	Fichier ou répertoire
Installation	Sortie de `imcl exportInstallData` (données IBM Installation Manager).
Sondes	*NCHOME*`/omnibus/probes/`*arch* Tous les fichiers avec les extensions suivantes sont incluses : `.rules`, `.props`, et `.def`. Les fichiers de plus de 100 ko sont exclus.
Passerelles	*NCHOME*`/omnibus/gates/` Le contenu du sous-répertoire *passerelle*`/default` est exclu.
ObjectServer	Sortie de *NCHOME*`/omnibus/bin/nco_osreport -html -server` *nom_serveur*.

Tâches associées:

«Exécution du Collecteur de données d'ISA»
Vous pouvez exécuter le Collecteur de données d'ISA (ISADC) indépendamment du Plan de travail IBM Support Assistant (ISA). Vous pouvez l'exécuter comme un utilitaire de console à partir de Tivoli Netcool/OMNIbus ou de l'interface Web ISADC publique ou comme un utilitaire autonome que vous téléchargez à partir du site Web ISADC.

Exécution du Collecteur de données d'ISA

Vous pouvez exécuter le Collecteur de données d'ISA (ISADC) indépendamment du Plan de travail IBM Support Assistant (ISA). Vous pouvez l'exécuter comme un utilitaire de console à partir de Tivoli Netcool/OMNIbus ou de l'interface Web ISADC publique ou comme un utilitaire autonome que vous téléchargez à partir du site Web ISADC.

Avant de commencer

Pour collecter le maximum de données sur un ObjectServer, vérifiez qu'il est en cours d'exécution avant d'exécuter l'ISADC. Vous devez également disposer des informations d'identification pour vous connecter à l'ObjectServer lorsque vous êtes invité à le faire.

Le texte ISADC n'est pas actuellement traduit en arabe et en hébreu. Lorsqu'il est exécuté dans l'environnement linguistique *ar* ou *he*, le texte ISADC est affiché en anglais.

Pourquoi et quand exécuter cette tâche

Utilisez l'utilitaire de console ISADC (**nco_isadc**) fourni avec Tivoli Netcool/OMNIbus pour recueillir des données relatives à l'assistance sur votre système.

Procédure

1. Exécutez la commande suivante pour démarrer le collecteur de données :
   NCHOME`/omnibus/bin/nco_isadc`
2. Suivez les instructions à l'écran pour réaliser la collecte de données. L'utilitaire nécessite la saisie suivante à différents stades de la collecte :

- Entrez un nom fichier et de répertoire pour stocker les archives des informations collectées.
- Indiquez si vous souhaitez recueillir toutes les données disponibles ou choisissez une ou plusieurs catégories de collecte.
- Si vous y êtes invité, entrez le répertoire de Netcool.
- Si vous y êtes invité, entrez l'installation répertoire IBM Installation Manager.
- Entrez le nom et les détails d'authentification pour un ou plusieurs ObjectServers en cours d'exécution.

3. Lorsque la collecte des données est terminée, vous pouvez choisir d'envoyer le fichier archive de données au support IBM en utilisant l'une des options FTP disponibles. Assurez-vous que les pare-feu de votre réseau sont configurés pour accepter le trafic FTP.

Résultats

Les données collectées sont enregistrées dans un fichier archive dans le répertoire que vous avez spécifié.

Référence associée:

«Collecteur de données d'ISA», à la page 674
Le IBM Support Assistant Data Collector (ISADC)est un outil basé sur Java pour collecter automatiquement les données de problèmes des produits IBM.

Collecte de données avec les outils Web :
Avant de commencer

Un navigateur Web activé Java 1.6 est requis pour utiliser l'interface Web ou l'utilitaire téléchargeable.

Pour collecter le maximum de données sur un ObjectServer, vérifiez qu'il est en cours d'exécution avant d'exécuter l'ISADC. Vous devez également disposer des informations d'identification pour vous connecter à l'ObjectServer lorsque vous êtes invité à le faire.

Pourquoi et quand exécuter cette tâche

Si l'ordinateur hôte Tivoli Netcool/OMNIbus a accès à l'Internet, vous pouvez exécuter le collecteur de données à partir d'un navigateur web installé sur cet ordinateur. Si l'ordinateur hôte n'a pas accès à Internet, vous pouvez télécharger le collecteur de données à partir d'un ordinateur connecté et le transférer manuellement à l'ordinateur hôte Tivoli Netcool/OMNIbus.

Pour plus d'informations sur l'utilisation de ISADC, voir le guide suivant sur la communauté des utilisateurs du Wiki ISA :

https://w3-connections.ibm.com/wikis/home?lang=en#!/wiki/W024719f96b08_427f_92a7_19d63adb6f8a/page/User%20Guide

Procédure

1. Ouvrez un navigateur Web et accédez au site Web suivant ISADC :
   http://public.dhe.ibm.com/software/isa/isadc/2.0/isacoreweb/2.0.1/isadc/lang/en/index.html
2. Pour recueillir des données avec l'interface Web :
   a. Sélectionnez le collecteur Tivoli Netcool/OMNIbus dans la liste déroulante.

b. Sélectionnez l'option pour recueillir des données à partir du système à l'aide du navigateur actuel.
c. Lisez et acceptez les dispositions du contrat de licence et cliquez sur **Démarrer la collecte**.

3. Pour recueillir des données avec l'utilitaire téléchargeable :
   a. Sélectionnez le collecteur Tivoli Netcool/OMNIbus dans la liste déroulante.
   b. Sélectionnez l'option pour recueillir des données à l'aide de l'utilitaire téléchargeable.
   c. Lisez et acceptez les dispositions du contrat de licence et cliquez sur le bouton de téléchargement pour votre système d'exploitation.
   d. Sauvegardez le fichier archive et extrayez son contenu.

      Si vous souhaitez exécuter l'utilitaire sur un autre ordinateur, transférez-le vers l'ordinateur, puis extrayez son contenu.
   e. Dans le répertoire `isadc`, ouvrez le fichier `index.html` dans un navigateur Web.
   f. Sélectionnez **Collect All** or **Customised Collection**.
   g. Cliquez sur **Démarrer** pour lancer la collecte de données.
4. Suivez les instructions à l'écran pour réaliser la collecte de données.
5. Lorsque la collecte des données est terminée, vous pouvez choisir d'envoyer le fichier archive de données au support IBM en utilisant l'une des options FTP disponibles. Assurez-vous que les pare-feu de votre réseau sont configurés pour accepter le trafic FTP.

Résultats

Les données collectées sont enregistrées dans un fichier archive à l'emplacement suivant :

- UNIX Linux `$HOME/.isadc`
- Windows *base_utilisateur*`\isadc`

Analyseur de traces et de journaux ISA

L'analyseur de traces et de journaux vous permet de recueillir des données système et de performances à partir de vos systèmes locaux et distants. Les données peuvent vous permettre d'identifier un incident, dès lors qu'un événement système inférieur à optimal se produit.

Vous pouvez utiliser l'analyseur de traces et de journaux pour créer des ensembles de ressources. Ces ensembles de ressources regroupent des définitions qui contiennent les emplacements des chemins d'accès aux journaux dont vous avez besoin pour établir vos diagnostics et les niveaux d'informations qu'ils contiennent. Vous pouvez conserver des définitions personnalisées pour les réutiliser. Les définitions fournissent le même jeu d'instructions concernant l'emplacement où trouver un journal et le type d'informations à recueillir dans le journal, ce qui vous permet de gagner du temps lors des importations de journaux suivantes.

L'analyseur de traces et de journaux permet également de télécharger et de stocker des catalogues de bases de données de symptômes sur votre système local. Ces catalogues fournissent des solutions de diagnostic détaillées pour divers scénarios, qui peuvent vous donner la direction à suivre lors de l'identification et de la résolution des problèmes.

Pour utiliser l'analyseur de traces et de journaux, vous devez télécharger et installer ISA ainsi que le plug-in de Tivoli Netcool/OMNIbus.

Téléchargement de l'analyseur de traces et de journaux

Pour télécharger l'analyseur de traces et de journaux, procédez comme suit :

1. A l'aide du programme de mise à jour d'ISA intégré, téléchargez et installez le plug-in de l'analyseur de traces et de journaux à partir du site Web d'IBM à l'adresse http://www.ibm.com/software/support/isa/.
   a. Sélectionnez le composant additionnel Trace and Log Analyzer (Analyseur de traces et de journaux) dans la liste **JVM-based Tools (Outils basés sur JVM)** et cliquez sur **Suivant**.
   b. Lisez les termes du contrat de licence associé et acceptez-les, puis cliquez sur **Suivant**.
   c. Vérifiez la liste de composants additionnels à télécharger et à installer, puis cliquez sur **Finish (Terminer)**.
2. Après la fin de l'installation de l'analyseur de traces et de journaux :
   a. Démarrez ISA.
   b. Sélectionnez **Analyze Problem (Analyser le problème)**.
   c. Cliquez sur l'onglet **Outils**.
   d. Sélectionnez l'outil **Log Analyzer (Analyseur de journaux)** dans la liste d'outils du **Tools Catalog (Catalogue d'outils)**.
   e. Cliquez sur **Lancer**. L'analyseur de journaux démarre.

Importation des fichiers journaux de Tivoli Netcool/OMNIbus dans l'analyseur de traces et de journaux

Pour importer les fichiers journaux de Tivoli Netcool/OMNIbus dans l'analyseur de traces et de journaux, procédez comme suit :

1. Copiez les fichiers journaux pertinents depuis les serveurs Tivoli Netcool/OMNIbus vers le système sur lequel vous avez installé le plan de travail d' IBM Support Assistant. Placez les fichiers journaux de chaque serveur dans un répertoire unique. Par exemple, `C:\OMNI\logs\NCOMS1`.
2. Importez les fichiers journaux de Tivoli Netcool/OMNIbus. L'analyseur de traces et de journaux organise les fichiers journaux connexes en ensembles de journaux. Ces ensembles de journaux peuvent être utilisés pour importer et analyser un ensemble de fichiers journaux connexes. Cette fonction vous permet d'organiser et d'importer vos fichiers journaux de Tivoli Netcool/OMNIbus. Les définitions des ensembles de journaux fournissent des informations à l'analyseur de traces et de journaux qui indiquent l'emplacement des données de traces et de consignation ainsi que le type de données à recueillir à partir de vos systèmes locaux et distants. L'analyseur de traces et de journaux vous permet d'importer des ensembles de journaux prédéfinis qui contiennent les informations de chemin d'accès nécessaires à la récupération des fichiers journaux à la demande.
3. Procédez de l'une des manières suivantes :

Procédure	Etapes
Créez l'ensemble de journaux d'origine de Tivoli Netcool/OMNIbus.	1. Cliquez sur **Fichier** > **Import Log File (Importer un fichier journal)**. 2. Créez un nouvel ensemble de journaux. 3. Saisissez le nom de l'ensemble de journaux, par exemple : `Fichiers journaux de Tivoli Netcool/OMNIbus pour NCOMS1` 4. Cliquez sur **Ajouter**. 5. Répétez les étapes suivantes pour chaque fichier journal que vous souhaitez inclure dans l'ensemble de journaux : a. Dans la fenêtre Name Filter (Désigner un filtre), saisissez `Discovery (Reconnaissance)` pour limiter la liste de fichiers journaux aux fichiers journaux de Tivoli Netcool/OMNIbus. b. Sélectionnez le type de fichier journal que vous ajoutez à l'ensemble de journaux. c. Saisissez le nom du fichier journal sur votre système local. Assurez-vous que le type de fichier journal correspond à celui que vous avez indiqué. d. Entrez la version correcte du produit Tivoli Netcool/OMNIbus qui correspond au fichier journal. Pour plus d'options, voir l'aide en ligne de l'analyseur de traces et de journaux. e. Pour ajouter un fichier journal à l'ensemble de fichiers journaux, cliquez sur **OK**. **Valeurs recommandées :** La première fois que vous créez l'ensemble de journaux, vous pouvez gagner du temps en incluant chaque fichier journal à inclure à l'ensemble de journaux.
Réutilisez un ensemble de journaux de Tivoli Netcool/OMNIbus existant.	1. Cliquez sur **Fichier** > **Import Log File (Importer un fichier journal)**. 2. Sélectionnez une définition d'ensemble de journaux existante dans la liste déroulante d'ensembles de journaux définis. 3. Si nécessaire, modifiez le contenu de la définition de l'ensemble de journaux. Vous pouvez ajouter, éditer ou supprimer des fichiers de la liste des fichiers journaux dans l'ensemble de journaux.

4. Pour indiquer que le fichier doit être importé dans l'ensemble de journaux, cochez la case en regard du fichier journal.
5. Pour importer les fichiers journaux, cliquez sur **Finish (Terminer)**.

Pour réutiliser un ensemble de journaux de Tivoli Netcool/OMNIbus existant, procédez comme suit :

1. Pour indiquer que le fichier doit être importé dans l'ensemble de journaux, cochez la case en regard du fichier journal.
2. Pour importer les fichiers journaux, cliquez sur **Finish (Terminer)**.

Vous pouvez créer et réutiliser autant d'ensembles de journaux que vous le souhaitez. Par exemple, lors de l'importation de fichiers journaux à partir de

plusieurs serveurs, vous avez besoin de plusieurs ensembles de journaux.

Analyse des fichiers journaux de Tivoli Netcool/OMNIbus avec l'analyseur de traces et de journaux

A l'aide de l'analyseur de traces et de journaux, vous pouvez associer plusieurs fichiers journaux de Tivoli Netcool/OMNIbus dans une seule vue. Les fichiers journaux de Tivoli Netcool/OMNIbus peuvent être associés dans une seule vue, classés par horodatage, pour établir une corrélation entre le fonctionnement des composants Tivoli Netcool/OMNIbus. Il existe deux manières d'établir une corrélation entre des fichiers journaux :

1. Simple : pour établir une corrélation entre tous les fichiers journaux importés, procédez comme suit :
   a. Dans l'arborescence de navigation de l'analyseur de traces et de journaux, cliquez avec le bouton droit de la souris sur **Logs (Journaux)**.
   b. Cliquez sur **View All Logs (Afficher tous les journaux)**.
2. Avancé : pour établir une corrélation entre un ensemble de fichiers journaux en créant une corrélation personnalisée, procédez comme suit :
   a. Dans l'arborescence de navigation de l'analyseur de traces et de journaux, cliquez avec le bouton droit de la souris sur **Correlations (Corrélations)**.
   b. Cliquez sur **Nouveau** > **Log Correlation (Corrélation de journaux)**.
   c. Dans la fenêtre qui s'affiche, saisissez le nom de la corrélation.
   d. Ajoutez les fichiers journaux à inclure à la corrélation.
   e. Cliquez sur **Finish (Terminer)**.
   f. Actualisez l'arborescence de navigation.
   g. Dans l'arborescence de navigation, cliquez avec le bouton droit de la souris sur le nom de corrélation que vous avez saisi et cliquez sur **Open With (Ouvrir avec)** > **Log View (Vue Journaux)**.

Une fois que vous avez créé une vue des journaux, vous pouvez organiser les données consignées pour isoler les problèmes. La liste suivante identifie certaines méthodes d'organisation des données :

- Organiser les enregistrements de journaux : par exemple, vous pouvez les organiser par heure, par composant ou par nom de serveur.
- Mettre en évidence les enregistrements de journaux : par exemple, vous pouvez mettre en évidence tous les événements d'erreur en rouge ou afficher tous les événements pour un composant spécifique en bleu. La mise en évidence est similaire au filtrage, mais au lieu d'éliminer les données d'une vue, vous pouvez mettre en évidence les informations pertinentes dans une liste complète d'événements.
- Filtrage des enregistrements de journaux : vous pouvez restreindre la portée d'un incident et les données affichées en fonction de critères de filtre. Exemples de critères de filtre : horodatages, gravité, composant et serveur.
- Recherche d'enregistrements de journaux : vous pouvez rechercher des informations spécifiques dans un fichier journal. Par exemple, vous pouvez rechercher les événements connexes à l'interaction avec un serveur ou un utilisateur spécifique.

Pour de plus amples informations sur l'organisation des données, recherchez la rubrique "Analyse des fichiers journaux" dans l'aide en ligne de l'analyseur de traces et de journaux. "Filtrage, tri, recherche et mise en évidence" est l'un des sous-titres de cette rubrique.

En outre, certaines autres rubriques de l'aide en ligne peuvent également vous être utiles :

- Lors de tentatives de corrélation de fichiers journaux à partir de plusieurs serveurs, les horloges de ces serveurs peuvent ne pas être synchronisées. Cet incident de synchronisation peut être dû à quelque chose de simple, comme des fuseaux horaires différents, ou de plus subtil, comme une horloge en retard d'une milliseconde sur celle d'un autre serveur. L'analyseur de traces et de journaux intègre une fonction de synchronisation de l'heure entre plusieurs fichiers journaux, en vous permettant de régler les horodatages dans un fichier journal. Pour de plus amples informations, voir la rubrique intitulée "Synchronisation de l'heure des enregistrements de journaux pour les applications réparties" dans l'aide en ligne de l'analyseur de traces et de journaux.
- Vous pouvez utiliser les catalogues de symptômes pour déterminer rapidement les problèmes connus. L'analyseur de traces et de journaux fournit une fonctionnalité d'analyse des journaux qui permet de détecter les problèmes connus définis dans une base de données de connaissance, appelée *catalogue de symptômes*. IBM fournit un catalogue de symptômes pour les problèmes connus pour plusieurs produits. IBM vous donne également la possibilité de recueillir et de définir vos propres informations de symptômes. Pour de plus amples informations, voir la rubrique intitulée "Synchronisation de l'heure des enregistrements de journaux pour les applications réparties" dans l'aide en ligne de l'analyseur de traces et de journaux.

Obtention de correctifs

Un correctif du produit peut être disponible pour résoudre les problèmes que vous rencontrez.

Remarque : Pour empêcher la perte d'informations au cours de l'installation, de la mise à niveau, de l'application d'un groupe de correctifs ou en cas d'incident, et pour pouvoir récupérer ces informations, sauvegardez votre installation Tivoli Netcool/OMNIbus et de l'interface utilisateur Web.

Pour déterminer les correctifs disponibles pour Tivoli Netcool/OMNIbus, procédez comme suit :

1. Accédez au site Web du service de support logiciel IBM à l'adresse http://www.ibm.com/software/support.
2. Recherchez le panneau **Software Support** sur la page et cliquez sur **Download**.
3. Cliquez sur le lien hypertexte **I** dans la liste de A à Z, puis sur IBM Tivoli Netcool/OMNIbus dans la liste de progiciels.
4. Sélectionnez en option un système d'exploitation ou laissez la valeur par défaut sur `Any operating system`.
5. Si vous souhaitez restreindre votre recherche, entrez vos termes de recherche dans la zone **Enter search terms**.
6. Pour restreindre vos résultats aux groupes de correctifs, aux fichiers readme et aux modules de correction, cochez uniquement la case **Updates** dans la section **Limit and sort results** de la page.

   Conseil : Notez que le nombre de documents correspondant à vos critères est directement affiché au-dessus de l'icône et du lien **Rechercher** dans la partie inférieure de la page. Ce nombre varie en fonction des cases cochées dans la section **Limit and sort results**.
7. Cliquez sur **Rechercher**.

8. Dans la liste de résultats renvoyée par votre recherche, cliquez sur le lien pertinent pour obtenir des informations sur les problèmes résolus dans un groupe de correctifs et télécharger ce groupe de correctifs.

Pour de plus amples informations sur les types de correctifs disponibles, voir la page *IBM Software Support Handbook* à l'adresse http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

Réception de mises à jour de support

Ces informations vous permettent d'obtenir des notifications par courrier électronique sur les correctifs et les autres nouveautés en matière de support logiciel.

Pour rester à jour avec les mises à jour logicielles, procédez comme suit :

1. Accédez au site Web du service de support logiciel IBM à l'adresse http://www.ibm.com/software/support.
2. Recherchez le panneau **Additional support links** sur la page et utilisez les liens suivants pour configurer les flux RSS pour surveiller le nouveau contenu de support Tivoli Netcool/OMNIbus et pour recevoir les mises à jour par courrier électronique :
   - **RSS feeds of support content**
   - **Request e-mail updates**

Astuces de recherche

Les ressources suivantes vous permettent d'optimiser vos résultats de recherche.

- Recherche du site Web de support IBM : http://www.ibm.com/support/us/srchtips.html
- Utilisation du moteur de recherche Google : http://www.google.com/support/

Annexe B. Numéros de port par défaut utilisés par Tivoli Netcool/OMNIbus

Un certain nombre de numéros de port par défaut est défini pour Tivoli Netcool/OMNIbus. vous pouvez modifier ces valeurs par défaut.

L tableau ci-dessous répertorie les ports par défaut et indique comment les modifier.

Tableau 103. Ports par défaut

Composant et port par défaut	**Configuration du port**
Serveurs Tivoli Netcool/OMNIbus : • Serveur d'objets (NCOMS) : 4100 • Agent de processus (NCO_PA) : 4200 • Serveur de passerelle (NCO_GATE) : 4300 • Serveur proxy (NCO_PROXY) : 4400	Ces numéros de port par défaut sont définis dans l'éditeur de serveur, mais ils peuvent être configurés et sont rarement utilisés avec les valeurs par défaut. Le cas échéant, modifiez les numéros de port, puis sauvegardez vos modifications. Sur les systèmes UNIX ne disposant pas d'interface graphique, vous pouvez modifier les numéros de port en éditant le fichier `$NCHOME/etc/omni.dat`. Pour plus d'informations relatives à la modification des numéros de port, voir «Configuration des détails de communication du serveur dans l'éditeur de serveur», à la page 207.
IDUC : valeur de variable	Le système d'exploitation fournit le numéro de port. Pour le modifier, procédez de l'une des façons suivantes : • Editez la propriété **`Iduc.ListeningPort`** du fichier `$NCHOME/omnibus/etc/`*`nom_serveur`*`.props`, où *nom_serveur* est le nom du serveur ObjectServer. • Utilisez l'option de ligne de commande `-listeningport` lors de l'exécution de la commande **`nco_objserv`**. • Indiquez le port dans le fichier `/etc/services` du poste de travail hôte. Pour plus d'informations sur l'utilisation de cette propriété ou option de ligne de commande, voir *Guide d'administration d'IBM Tivoli Netcool/OMNIbus*.
IBM Eclipse Help System (IEHS)	Le numéro de port par défaut utilisé pour accéder au serveur IEHS est 8888. En général, il est possible d'accéder au serveur en spécifiant l'adresse suivante : `http://`*`adresse_IP`*`:`*`port`* où *adresse_IP* est l'adresse IP de l'ordinateur hôte, et *port* est 8888.

Tableau 103. Ports par défaut (suite)

Composant et port par défaut	**Configuration du port**
Sondes : voir les publications correspondantes	Les numéros de port des sondes individuelles varient. Ils sont présentés dans la publication de chaque sonde spécifique. Dans le centre de documentation (http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp), vous pouvez accéder à ces publications en développant le nœud *IBM Tivoli Netcool/OMNIbus* dans le panneau de navigation de gauche, puis en accédant au nœud *Tivoli Netcool/OMNIbus probes and TSMs*.

Annexe C. Propriétés server.init

Les propriétés des sessions de serveur et d'environnement du serveur de l'Interface graphique Web sont stockées dans le fichier d'initialisation *REP_INSTALL_WEBGUI*/etc/server.init. Il s'agit d'un fichier d'initialisation ASCII qui peut être édité directement et lu au démarrage du serveur.

Après avoir édité le fichier server.init, redémarrez le serveur Concentrateur des services d'application du tableau de bord.

Les propriétés contenues dans le fichier server.init sont répertoriées par ordre alphabétique.

A

admin.stylesheets
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est %%/etc/system/stylesheets/.

ael.top-n.mode
Indique le mode top-n. Les valeurs possibles sont les suivantes :

- 1 : StateChange sera ajouté aux demandes de mise à jour d'événement SQL d'AEL.
- 0 : StateChange ne sera pas ajouté aux demandes d'AEL.

La valeur par défaut est 0.

ael.top-n.refresh
Indique le type d'actualisation. Les valeurs possibles sont les suivantes :

- 1 : L'AEL est actualisée uniquement avec les lignes nouvelles et mises à jour du serveur ObjectServer. StateChange doit avoir une valeur supérieure à 0. L'exécution des outils SQL et les recherches de différences entre AEL et serveur ObjectServer ne repassent pas la valeur de StateChange à 0.
- 0 : Si le nombre de lignes dans l'AEL et le nombre de lignes dans le serveur ObjectServer ne correspondent pas, l'AEL est actualisée avec les données du serveur ObjectServer jusqu'au nombre de lignes spécifié dans la propriété **ael.top-n.value** et la valeur de StateChange est repassée à 0. L'exécution des outils SQL repasse la valeur de StateChange à 0.

La valeur par défaut est 0.

ael.top-n.value
L'Interface graphique Web prend en charge le mot clé TOP dans la syntaxe SQL ObjectServer. La propriété **ael.top-n.value** autorise les administrateurs de l'Interface graphique Web à imposer une limite concernant le nombre d'alertes renvoyées à l'AEL. Si cette propriété est définie sur une valeur supérieure à 0, les requêtes d'AEL sont modifiées afin d'inclure une condition TOP. Par exemple, si un filtre AEL correspond à 8000 lignes du serveur ObjectServer et si la valeur **ael.top-n.value** est paramétrée sur 4000, seules les 4000 premières alertes s'affichent. L'affichage de plus de 20 000 événements dans une même AEL peut affecter les performances. La barre d'état de la liste d'événements actifs affiche le nombre total d'alertes pour chaque niveau de gravité et le nombre total d'alertes affichées. En outre, un message Début défini sur s'affiche au-dessus de la barre d'état de distribution dans l'AEL, indiquant

qu'une condition TOP est appliquée. La propriété **ael.top-n.value** peut être prise en considération pour les systèmes :

- Qui contiennent régulièrement un volume élevé d'événements
- Dans lesquels les filtres AEL correspondent à plus de 20 000 alertes
- Dans lesquels le nombre d'utilisateurs AEL simultanés affecte de manière négative les performances du système

Si la valeur de **ael.top-n.value** est définie sur 0 (zéro), elle est ignorée ; l'AEL n'affichera pas zéro ligne.

La valeur par défaut est `0`.

aelview.queries.enabled
Lorsque cette propriété est définie sur `true`, l'utilisateur peut exécuter des demandes avancées sur le servlet `AELView` en ajoutant des critères de configuration à l'adresse URL contenant l'adresse de l'AEL.

La valeur par défaut est `true`.

alerts.status.sort.displayvalue
Spécifie les zones de la table alert.status d'ObjectServer qui requièrent un tri par valeur d'affichage plutôt que par valeur réelle lorsqu'elles sont extraites par le biais du service REST de données d'événement.

La valeur de la propriété est une liste séparée par des virgules de noms de zone (de type entier) dans la table alerts.status. La valeur par défaut est : `Acknowledged,Class,ExpireTime,Flash,NmosCauseType,NmosManagedStatus, OwnerGID,OwnerUID,SupressEscl,TaskList,Type,X733EventType, X733ProbableCause`

B

browser.prp
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est `%%/etc/browsers.prp`.

C

cluster.hostname
Identité de l'hôte sur lequel s'exécute le serveur Interface graphique Web. La valeur est le nom d'hôte ou son adresse TCP/IP. Définissez cette propriété uniquement lorsque **cluster.mode** est paramétré sur `on`.

cluster.mode
Indique si le serveur Interface graphique Web s'exécute dans un cluster d'équilibrage de charge. Les valeurs possibles sont les suivantes :

- `on` : le serveur fait partie d'un cluster.
- `off` : le serveur est un système autonome.

Lorsque cette propriété a pour valeur `on`, indiquez des valeurs pour **cluster.hostname** et **cluster.port** également.

La valeur par défaut est `off`.

cluster.port
Port SSL utilisé par le serveur Interface graphique Web. La valeur est une valeur de port numérique. Définissez cette propriété uniquement lorsque **cluster.mode** est paramétré sur `on`.

cluster.waapi.notification.delay
Définit un temps d'attente (en millisecondes) avant de notifier à d'autres nœuds dans le cluster que des changements de configuration ont été effectués à l'aide des fichiers de commande WAAPI. La valeur par défaut est 2 000.

columngrouping.allowedcolumns
Liste de colonnes ObjectServer pouvant être utilisées pour grouper des événements dans l'Afficheur d'événements (Afficheur d'événements). Lorsque les utilisateurs créent un regroupement d'événements, seules les colonnes indiquées dans cette propriété peuvent être sélectionnées. Cette restriction garantit que les utilisateurs ne spécifient pas de colonnes qui ne sont pas appropriées pour être utilisées dans un groupement. La valeur est une liste séparée par des virgules de noms de colonne.

La valeur par défaut est :

```
Acknowledged,AlertGroup,Class,Customer,Location,Node,NodeAlias,
NmosCauseType,NmosManagedStatus,Severity,Service
```

columngrouping.maximum.columns
Définit le nombre maximum de niveaux qui peuvent être définis pour le groupement de colonnes dans le Générateur de vues. La valeur par défaut est 3.

D

datasource.failback.delay
Spécifie la durée d'attente après une reprise par restauration avant que l'Interface graphique Web ne revienne au serveur ObjectServer principal. Au cours de cette période, le serveur ObjectServer de secours est utilisé. Vous pouvez régler cette valeur en fonction du temps d'attente d'une architecture ObjectServer tierce

La valeur par défaut est de 120.

datasource.response.timeout
Seuil de délai d'attente, en millisecondes, de la vérification du temps de réponse d'une source de données associée à une mappe.

La valeur par défaut est `3000`.

E

ee.entitydir
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est `%%/etc/entities/`.

eventprovider.eventdataservice.threadpool.size
Spécifie la taille du pool d'unité d'exécution par défaut pour le service de données d'événement. Si vous augmentez la valeur de cette propriété au-dessus de la valeur par défaut, les performances peuvent en être affectées.

La valeur par défaut est `20`.

eventprovider.eventsummarydataservice.threadpool.size
Spécifie la taille du pool d'unité d'exécution par défaut pour le service de données récapitulatives d'événement. Si vous augmentez la valeur de cette propriété au-dessus de la valeur par défaut, les performances peuvent en être affectées.

La valeur par défaut est `20`.

eventviewer.pagesize.max:<*nombre*>
Indique le nombre maximum d'événements de ligne qui sont chargés dans un Afficheur d'événements. Si le nombre de lignes excède cette valeur, seul le nombre de lignes spécifié par cette propriété est affiché dans l'Afficheur d'événements. La valeur `-1` supprime cette limite et l'Afficheur d'événements affiche tous les événements.

Remarque : Si vous indiquez une valeur trop élevée, une saturation de la mémoire du serveur peut avoir lieu. La valeur possible pour cette propriété est fonction de la taille maximale du segment de mémoire définie pour l'hôte.

La valeur par défaut est `20000`.

eventviewer.tools.command
Ce paramètre est utilisé pour activer ou désactiver les outils de commande dans l'Afficheur d'événements. Les outils de commande permettent d'exécuter des commandes sur le système d'exploitation de l'utilisateur client, ce qui nécessite l'utilisation d'un plug-in de navigateur Web. Les options valides sont :

true : Les outils de commande seront activés dans l'Afficheur d'événements. Les outils de commande inclus dans la définition de menu seront visibles et, s'ils sont choisis, ils seront exécutés à l'aide d'un plug-in de navigateur.

false : Les outils de commande seront désactivés dans l'Afficheur d'événements. Les outils de commande inclus dans la définition de menu ne seront pas visibles et aucun plug-in de navigateur ne sera chargé ou utilisé par l'Afficheur d'événements.

La valeur par défaut est `false`.

F

fips.security.key
Nom du fichier de clés de sécurité de l'Interface graphique Web. La valeur par défaut pointe vers la clé de sécurité par défaut de Concentrateur des services d'application du tableau de bord.

La valeur par défaut est `%%/etc/encrypt/vault.key`.

G

groups.reload.mode
Paramètre de l'algorithme utilisé pour demander une liste de groupes Interface graphique Web à partir du système d'authentification. Les valeurs possibles sont les suivantes :

- `0` : tous les groupes sont demandés.
- `1` : seuls les groupes dont les noms de rôle commencent par `ncw_` sont demandés.

La valeur par défaut est `1`.

I

illegalchar.file
Ce fichier définit les caractères interdits dans les noms de filtres, de vues et d'outils ainsi que les caractères qui ne peuvent pas être utilisés en première position des noms de filtres, de vues et d'outils.

La valeur par défaut est `%%/etc/illegalChar.prop`.

internationalisation.cache.enabled
Indique si le serveur de l'Interface graphique Web met en cache des ressources de langue dans la mémoire. Lorsque cette propriété est définie sur `false`, la mise en cache des données de localisation n'est pas activée et le serveur ne peut dont pas relire régulièrement les fichiers de configuration de l'environnement local sélectionné.

La valeur par défaut est `true`.

L

lel.pagesize.default
Indique le nombre de lignes renvoyées par page dans la LEL.

La valeur par défaut est `500`.

log.count
Nombre maximum de fichiers journaux à stocker.

La valeur par défaut est `5`.

log.directory
Répertoire dans *REP_INSTALL_JazzSM* qui contient les fichiers journaux et de trace. Ne modifiez pas cette propriété.

La valeur par défaut est `/logs/ncw`.

log.filename
Nom du fichier journal. Ne pas modifier.

La valeur par défaut est `ncw.%g.log`.

log.level
Gravité minimale des événements à enregistrer dans le fichier journal. Les valeurs possibles sont les suivantes :

- `NONE`
- `FINEST`
- `FINER`
- `FINE`
- `CONFIG`
- `INFO`
- `AUDIT`
- `WARNING`
- `SEVERE`
- `ALL`

La valeur par défaut est `INFO`.

log.maxsize
Taille maximale du fichier journal en mégaoctets.

La valeur par défaut est `10`.

logfile
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est `%%/log/webtop.log`.

M

maplet.noeventcolor
Spécifie la couleur des éléments actifs qui ne sont pas associés à des événements. Indiquez une valeur de couleur hexadécimale pour ce paramètre, par exemple 0xDDDDDD pour le gris ou 0xFFFFFF pour le blanc. Si aucune valeur n'est spécifiée, la couleur associée au niveau de gravité 0 est utilisée.

La valeur par défaut est `Aucun`.

maplet.plugin.classic
Spécifie le marquage HTML pour l'intégration des objets de mappe :

- Si cette propriété est définie sur `true`, la carte est imbriquée dans l'élément &ltAPPLET> et la machine virtuelle Java Netscape ou Internet Explorer par défaut est utilisée.
- Si elle est définie sur `false`, la carte est imbriquée dans les éléments &ltOBJECT>&ltEMBED>.

La valeur par défaut est `false`.

maplet.refresh
Indique l'intervalle de temps, en secondes, entre les actualisations des objets de carte. Ne définissez pas la valeur de cette propriété par une valeur inférieure à 10. En outre, si votre site utilise des cartes complexes, utilisez une valeur supérieure pour cette propriété.

La valeur par défaut est `10`.

maps.directory
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est `%%/etc/maps/`.

maxtablesize
Nombre maximum de lignes autorisées dans une table.

La valeur par défaut est `200`.

metricdataservice.threadpool.size
Spécifie la taille du pool d'unités d'exécution par défaut pour le service de données métriques. Si vous augmentez la valeur de cette propriété au-dessus de la valeur par défaut, les performances peuvent en être affectées.

La valeur par défaut est `20`.

P

passwd.file
Emplacement de fichier système - ne pas modifier.

La valeur par défaut est `%%/etc/users/passwds`.

plugin.classid
Spécifie la version du plug-in Java utilisée par les applets via l'attribut `classid` de la balise <OBJECT>, et vous permet d'imposer le plug-in à utiliser. Si la propriété **maplet.plugin.classic** est définie sur `false` et si l'utilisateur dispose d'une version plus ancienne du plug-in que celle spécifiée dans l'attribut classid de l'élément <OBJECT>, cet utilisateur est invité à télécharger la nouvelle version. Si l'utilisateur dispose d'une version identique ou d'une version plus récente, celle-ci est utilisée.

Default `clsid:8AD9C840-044E-11D1-B3E9-00805F499D93`

plugin.iedownload
Indique l'adresse URL complète d'un fichier .cab à partir duquel vous pouvez installer le plug-in Java. Avec cette propriété, le client est assuré de disposer de la version adéquate du plug-in. Si la version du plug-in n'est pas correcte, l'utilisateur est automatiquement redirigé vers le dernier fichier .cab afin d'obtenir la version la plus récente de la gamme. Cette propriété est utilisée dans l'élément <OBJECT> pour Windows Internet Explorer.

Default `http://java.sun.com/update/1.5.0/jinstall-1_5_0_11-windows-i586.cab`

plugin.page
Indique l'adresse URL complète depuis laquelle le plug-in Java peut être téléchargé si la version appropriée n'est pas encore installée. Cette propriété est utilisée dans l'élément <EMBED> pour les navigateurs Mozilla.

Default `https://java.sun.com/products/plugin/index.jsp`

plugin.type
Spécifie la version du plug-in Java via l'attribut type de l'élément <EMBED>, et vous permet d'imposer le plug-in à utiliser. Si la propriété **maplet.plugin.classic** prend la valeur `false` et si l'utilisateur dispose d'une version antérieure à celle indiquée dans cette propriété, cet utilisateur est invité à télécharger la nouvelle version. Si l'utilisateur dispose d'une version identique ou d'une version plus récente, celle-ci est utilisée.

Default `application/x-java-applet;version=1.5`

profile.count
Nombre maximal de fichiers journaux de profil à conserver.

Default `5`

profile.filename
Nom de fichier journal de profil. Ne modifiez pas cette propriété.

Default `ncw.%g.profile`

profile.maxsize
Taille maximale du fichier journal du profil en mégaoctets.

Default `10`

profilereport.runperiod
Définit la fréquence (en secondes) de génération du rapport de profil.

Default `60`

profilereport.startdelay
Définit la durée (en secondes) avant génération du premier rapport de profil.

R

resources.directory
Emplacement de fichier système. Ne pas modifier.

La valeur par défaut est `%%/etc/resources/`.

S

Web GUI Fix Pack 1 **scala.app.keyword**
Spécifie les noms des applications personnalisées IBM SmartCloud Analytics -

Log Analysis, ce qui dépend de la version de l'Insight Pack Tivoli Netcool/OMNIbus utilisé par le produit IBM SmartCloud Analytics - Log Analysis dans votre environnement. Les valeurs possibles sont les suivantes :

- Default `OMNIbus_SetSearchFilter` : Utilisez cette valeur pour la version V1.1.0.1 de l'Insight Pack.
- `OMNIbus_KeywordSearch` : Utilisez cette valeur pour la version V1.1.0.2 de l'Insight Pack.

Les noms des applications personnalisées diffèrent selon la version de l'Insight Pack. Pour déterminer la version de l'Insight Pack qui est installée, exécutez la commande `pkg_mgmt.sh -list` à partir de `$SCALA_HOME/utilities`. Pour plus de détails concernant les applications personnalisées et l'intégration entre produits Tivoli Netcool/OMNIbus etIBM SmartCloud Analytics - Log Analysis, reportez-vous à la documentation Netcool Operations Insight à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSTPTP_1.2.0/com.ibm.netcool_ops.doc_1.2.0/soc/event_search/concept/soc_es_overview.html.

Web GUI Fix Pack 1 **scala.app.static.dashboard**

Spécifie le nom de l'application personnalisée de tableau de bord IBM SmartCloud Analytics - Log Analysis, ce qui dépend de la version de l'Insight Pack Tivoli Netcool/OMNIbus utilisé par le produit IBM SmartCloud Analytics - Log Analysis dans votre environnement. Les valeurs possibles sont les suivantes :

- Default `OMNIbus_Event_Distribution` : Utilisez cette valeur pour la version V1.1.0.1 de l'Insight Pack.
- `OMNIbus_Static_Dashboard` : Utilisez cette valeur pour la version V1.1.0.2 de l'Insight Pack.

Le nom de l'application de tableau de bord diffère selon la version de l'Insight Pack. Pour déterminer la version de l'Insight Pack qui est installée, exécutez la commande `pkg_mgmt.sh -list` à partir de `$SCALA_HOME/utilities`. . Pour plus de détails concernant les tableaux de bord et l'intégration entre produits Tivoli Netcool/OMNIbus etIBM SmartCloud Analytics - Log Analysis, reportez-vous à la documentation Netcool Operations Insight à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSTPTP_1.2.0/com.ibm.netcool_ops.doc_1.2.0/soc/event_search/concept/soc_es_overview.html.

scala.datasource

Spécifie le nom de la source de données pour IBM SmartCloud Analytics - Log Analysis. Dans le produit IBM SmartCloud Analytics - Log Analysis, une source de données est une source de données brutes - des fichiers journaux, en règle générale. Dans le cas d'intégrations au produit Tivoli Netcool/OMNIbus, la source de données est constituée des événements en provenance de Tivoli Netcool/OMNIbus. La définition d'une source de données diffère pour l'Interface graphique Web.

Default `omnibus`

scala.url

Spécifie l'adresse URL pour le produit IBM SmartCloud Analytics - Log Analysis. Vous indiquerez cette adresse selon le modèle suivant :

protocole`://`*hôte*`:`*port*

Default `https://localhost:9987/Unity`

Web GUI Fix Pack 1 **scala.version**

Spécifie la version de IBM SmartCloud Analytics - Log Analysis de telle sorte que la syntaxe de recherche appropriée soit utilisée pour les requêtes. Les options possibles sont les suivantes :

- Default `1.2.0.2`
- `1.2.0.3`

server.mode

Définit s'il convient de rendre certaines fonctions Interface graphique Web indisponibles. Les fonctions sont définies dans le fichier *REP_INSTALL_WEBGUI/*`etc/restricted_urls.lst`. Les valeurs possibles sont les suivantes :

- Default `0` : Le serveur s'exécute en mode normal. Toutes les fonctions Interface graphique Web sont disponibles.
- `1` : Le serveur s'exécute en mode restreint. Les adresses URL correspondant à des modèles dans le fichier `restricted_urls.lst` ne sont pas disponibles pour les utilisateurs.

T

tableview.escapehtml

Empêche le rendu du script HTML dans les zones de la vue Table. Si cette propriété est définie sur `true`, le texte du script HTML est traité comme du texte simple dans les zones de la vue Table. Si elle est définie sur `false`, le texte du script HTML est rendu dans les zones de la vue Table.

La valeur par défaut est `false`.

tableview.pixelmultiply

Paramètre facultatif transmis aux vues Table et servant au rendu des tables.

La valeur par défaut est `10`.

tableviewparams

Paramètres facultatifs transmis aux Vues Table et qui gouvernent le rendu de table.

La valeur par défaut est `border="0" cellpadding="1" cellspacing="1" width="100%"`.

timedtasks.default.runperiod

Période d'exécution (en secondes) des tâches du minuteur de mise à jour du magasin de configuration.

La valeur par défaut est `120`.

timedtasks.default.startdelay

Délai de démarrage (en secondes) des tâches du minuteur de mise à jour du magasin de configuration.

La valeur par défaut est `120`.

timedtasks.enabled

Indique si les tâches minutées sont activées ou désactivées. Cette propriété peut être définie sur `true` ou `false`.

La valeur par défaut est `false`.

trace.count

Nombre maximal de fichiers de trace à conserver.

La valeur par défaut est `5`

trace.filename
Nom du fichier de trace. Ne modifiez pas cette propriété.

La valeur par défaut est `ncw.%g.trace`.

trace.level
Gravité minimale des événements à enregistrer dans le fichier de trace. Les valeurs possibles sont les suivantes :

- `NONE`
- `FINEST`
- `FINER`
- `FINE`
- `PROFILE`
- `CONFIG`
- `INFO`
- AUDIT
- `WARNING`
- `SEVERE`
- `ALL`

La valeur par défaut est `FINE`.

trace.maxsize
Taille maximale du fichier journal en octets. Utilisez les suffixes M ou K pour désigner des mégaoctets ou des kilooctets, respectivement.

La valeur par défaut est `100M`.

U

uploadfile.maxsize
Taille maximale d'un fichier que le gestionnaire de pages peut charger, en mégaoctets.

La valeur par défaut est `5`.

users.credentials.sync
Spécifie si la synchronisation automatique des données d'identification de l'utilisateur entre VMM et le serveur ObjectServer est activée. Si cette propriété est définie sur `true`, la synchronisation est activée.

La valeur par défaut est `false`.

users.credentials.sync.groupname
Spécifie le nom du groupe d'utilisateurs utilisé dans le serveur ObjectServer si la synchronisation automatique des données d'identification de l'utilisateur entre VMM et le serveur ObjectServer est activée. Tous les utilisateurs synchronisés sont membres de ce groupe.

La valeur par défaut est `vmmusers`.

users.global.filter.mode
Paramètre permettant la modification des filtres globaux via les droits d'utilisateur non administrateur. Les valeurs possibles sont les suivantes :

- `0` : les utilisateurs non administrateur ne peuvent pas ajouter, modifier ou supprimer les filtres globaux.
- `1` : les utilisateurs non administrateurs peuvent ajouter et modifier des filtres globaux mais pas les supprimer.

La valeur par défaut est 1.

users.global.view.mode
Paramètre permettant la modification des vues globales via les droits d'utilisateur non administrateur. Les valeurs possibles sont les suivantes :

- 0 : les utilisateurs non administrateur ne peuvent pas ajouter, modifier ou supprimer les vues globales.
- 1 : les utilisateurs non administrateurs peuvent ajouter et modifier des vues globales mais pas les supprimer.

La valeur par défaut est 1.

users.group.filter.mode
Détermine si des utilisateurs sans privilège d'administration peuvent éditer et supprimer des filtres de groupe. Les valeurs possibles sont les suivantes :

- 0 : les utilisateurs ne peuvent pas éditer ni supprimer des filtres de groupe.
- 1: les utilisateurs peuvent éditer et supprimer des filtres de groupe.

users.reload.mode
Paramètre de l'algorithme utilisé pour demander une liste d'utilisateurs de l'Interface graphique Web à partir du système d'authentification d'utilisateur. Les valeurs possibles sont les suivantes :

- 0 : tous les utilisateurs sont demandés. Cette option permet une récupération plus rapide des données.
- 1 : seuls les utilisateurs dont les noms de rôle commencent par ncw_ sont demandés. Cette option peut s'avérer longue s'il existe un grand nombre d'utilisateurs système.

La valeur par défaut est 1.

utility.debug
Définit le niveau de débogage en augmentant le niveau de détail de 0 (messages critiques uniquement) à 9 (tous les messages).

La valeur par défaut est 0.

utility.debug.destination
Définit la destination des messages de débogage. Les options disponibles sont les suivantes :

- stdout : sortie standard
- stderr : sortie d'erreur standard
- log : fichier journal spécifié par l'option log.filename dans server.init

La valeur par défaut est log.

utility.monitor
Définit le niveau de surveillance des utilisateurs en augmentant le niveau de détail de 0 (messages critiques uniquement) à 9 (tous les messages).

La valeur par défaut est 0.

utility.monitor.destination
Définit la destination des messages de surveillance. Les options disponibles sont les suivantes :

- stdout : sortie standard
- stderr : sortie d'erreur standard
- log : fichier journal spécifié par l'option log.filename dans server.init

La valeur par défaut est log.

V

views.directory
Emplacement de fichier système. Ne pas modifier.

La valeur par défaut est %%/etc/views/.

W

webtop.fips
Active le chiffrement FIPS 140–2 et peut être paramétrée sur on ou off.

A faire : Si vous paramétrez cette propriété sur on, activez également le chiffrement FIPS 140–2 dans le Concentrateur des services d'application du tableau de bord.

Default off

webtop.keepalive.interval
Le serveur Interface graphique Web envoie régulièrement une commande PING au serveur Concentrateur des services d'application du tableau de bord pour éviter une expiration de délai de ce serveur lorsqu'une page AEL ou Maplet est active. Cette propriété spécifie la durée (en minutes) entre chaque opération PING.

Default 3

webtop.password.encryption
Définit les mots de passe conservés dans server.init qui doivent être chiffrés. Les valeurs possibles sont les suivantes :

- none : les mots de passe dans server.init ne sont pas chiffrés.
- aes : les mots de passe dans server.init peuvent être chiffrés par l'outil **ncw_aes_crypt**.
- fips : les mots de passe dans server.init peuvent être chiffrés par l'outil **ncw_fips_crypt**.

Remarque : FIPS 140-2 Les seules options admises sont none ou fips.

Default aucun

webtop.ssl.trustManagerType
Type de gestionnaire d'accréditation utilisé. Paramétrez cette propriété sur IbmX509 si vous utilisez l'environnement d'exécution Java groupé avec l'Interface graphique Web ou un environnement d'exécution Java AIX. Paramétrez cette propriété sur SunX509 si vous n'utilisez pas l'environnement d'exécution Java groupé ou un environnement d'exécution Java AIX.

La valeur par défaut est IbmX509.

webtop.ssl.trustStore
Définit l'emplacement du fichier de clés certifiées SSL utilisé par l'Interface graphique Web. Si aucune valeur n'est indiquée, le fichiers de clés certifiées Concentrateur des services d'application du tableau de bord par défaut est utilisé, ce qui permet d'accéder à l'interface graphique du fichier de clés certifiées de Concentrateur des services d'application du tableau de bord pour la configuration de ce fichier de clés.

webtop.ssl.trustStorePassword
Définit le mot de passe utilisé pour accéder au fichier de clés certifiées. Si cet attribut n'a pas de valeur, aucun mot de passe n'est requis pour accéder au

fichier de clés certifiées. Pour les types de fichiers PKCS12 (définis dans `webtop.ssl.trustStoreType`), un mot de passe doit être fourni. Pour les types de fichiers JKS (définis dans `webtop.ssl.trustStoreType`), le mot de passe est facultatif.

`webtop.ssl.trustStoreType`
Type de fichier de clés certifiées utilisé.

La valeur par défaut est `PKCS12`.

Annexe D. Rapports Tivoli Common Reporting pour Tivoli Netcool/OMNIbus

Utilisez ces informations pour vous familiariser avec les rapports Tivoli Netcool/OMNIbus fournis pour Tivoli Common Reporting (TCR).

Notez que l'accès en modification aux rapports peut être désactivé par l'administrateur.

Tâches associées:

«Importation des rapports récapitulatifs des événements dans Tivoli Common Reporting», à la page 484
Pour exécuter les rapports récapitulatifs des événements, connectez Tivoli Common Reporting à une base de données relationnelle via une passerelle. Puis, importez le module de rapports qui est fourni avec Tivoli Netcool/OMNIbus dans Tivoli Common Reporting.

Distribution d'événement

Utilisez ce rapport pour afficher les entités, les sondes, les emplacements, etc., qui ont généré la plupart des événements au cours d'une période de temps définie, pour identifier les parties de votre système qui requièrent une attention ou une action corrective.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 104. Caractéristiques du rapport Event_Distribution

Fonction	Description
Nom	Distribution d'événement

Tableau 104. Caractéristiques du rapport Event_Distribution (suite)

Fonction	Description
Paramètres	**Plage de dates** Sélectionnez une plage de dates prédéfinie. Vous avez également la possibilité de sélectionner une **Plage de dates (ci-dessous)** et d'utiliser les zones de **Date de début** et de **Date de fin** pour définir votre propre plage de dates. **Critères de regroupement** Sélectionnez un critère selon lequel le rapport regroupe les événements, puis sélectionnez le nombre d'événements à afficher dans le rapport, comme suit : **Regrouper par** Les éléments affichés dans cette liste représentent les colonnes de la table de liste d'événements. Sélectionnez une seule colonne qui est utilisée pour propager l'axe des X du diagramme à barres Comptage total dans la sortie du rapport. Par exemple, si vous sélectionnez **Noeuds**, la distribution d'événements est regroupée par nœud. Vous indiquez le nombre de nœuds inclus dans le rapport dans la zone **Nombre de groupes à inclure**. **Nombre de groupes à inclure** Entrez le nombre de groupes que vous voulez inclure dans la sortie du rapport. Une fois générée, la sortie du rapport contient les groupes dont le nombre d'événements est le plus élevé.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS

Tableau 104. Caractéristiques du rapport Event_Distribution (suite)

Fonction	Description
Sortie	Le rapport renvoie la sortie suivante : **Comptage total** Graphique à colonnes empilées indiquant le nombre total d'instances de chaque événement (c'est-à-dire, le nombre d'événements avant dédoublonnage), classés par gravité, pour le nombre spécifié de groupes. L'axe des X montre les groupes, par exemple, les nœuds. L'axe des Y mesure le nombre d'événements sur une échelle logarithmique. Les mêmes informations sont affichées sous forme tabulaire, sous le diagramme à barres. **Nombre d'événements uniques** Diagramme à barres présentant le nombre d'événements uniques (c'est-à-dire le nombre d'événements après le dédoublonnage), classés par gravité, pour le nombre spécifié de groupes. L'axe des X montre les groupes, par exemple, les nœuds. L'axe des Y mesure le nombre d'événements sur une échelle logarithmique. Les mêmes informations sont affichées sous forme tabulaire, sous le diagramme à barres.
Exploration	Event_Selection
Problèmes connus	Si vous spécifiez votre propre plage de dates, lorsque vous tentez d'explorer le rapport Event_Selection, vous êtes dirigé vers la fenêtre Sélection des paramètres du rapport, où vous devez saisir la plage de dates.

Event_Selection

Utilisez ce rapport pour afficher le nombre d'événements, classés par gravité et par jour, sur une plage de dates donnée, pour des critères particuliers.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 105. Caractéristiques du rapport Event_Selection

Fonction	Description
Nom	Event_Selection

Tableau 105. Caractéristiques du rapport Event_Selection (suite)

Fonction	Description
Paramètres	**Plage de dates** Sélectionnez une plage de dates prédéfinie. Vous avez également la possibilité de sélectionner une **Plage de dates (ci-dessous)** et d'utiliser les zones de **Date de début** et de **Date de fin** pour définir votre propre plage de dates. **Sélectionner par** Les éléments affichés dans cette liste représentent les colonnes de la liste d'événements, par exemple, Noeud, Emplacements, etc. Sélectionnez une colonne. **Valeur** Entrez une valeur. Notez que cette zone est sensible à la casse. La valeur doit correspondre à l'élément que vous avez sélectionné dans la zone **Sélectionner par**. Par exemple, si vous avez sélectionné **Noeud**, vous devez indiquer le nom d'une entrée valide provenant de la colonne Noeud. Si une valeur non valide est entrée, par exemple un nœud qui n'existe pas, la sortie du rapport est vide.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS

Tableau 105. Caractéristiques du rapport Event_Selection (suite)

Fonction	Description
Sortie	Le rapport renvoie la sortie suivante : **Nombre d'événements par gravité et jour** Le graphique à courbes indiquant le nombre d'événements uniques (c'est-à-dire, le nombre d'événements après dédoublonnage), classés par gravité, pour chaque jour de la plage de dates spécifiée pendant lequel un ou plusieurs événements se sont produits. L'axe des X représente les dates auxquelles les événements se sont produits. Si la plage de dates s'étend sur un jour ou moins, les unités sur l'axe des X sont des heures. L'axe des Y indique le nombre d'événements. **Répartition des gravités** Diagramme à secteurs présentant le nombre d'événements uniques (c'est-à-dire le nombre d'événements après dédoublonnage), classés par gravité. **Evénements sélectionnés :** *groupe*: *valeur* Table contenant des informations de la base de données relationnelle, basées sur les paramètres du rapport spécifiés.
Exploration	Event_Details

Event_Severity

Ce rapport permet de visualiser les événements ayant une gravité supérieure ou égale à une gravité particulière, et une première occurrence par jour, au cours d'une période de temps définie.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 106. Caractéristiques du rapport Event_Severity

Fonction	Description
Nom	Event_Severity

Tableau 106. Caractéristiques du rapport Event_Severity (suite)

Fonction	Description
Paramètres	**Plage de dates** Sélectionnez une plage de dates prédéfinie. Vous avez également la possibilité de sélectionner une **Plage de dates (ci-dessous)** et d'utiliser les zones de **Date de début** et de **Date de fin** pour définir votre propre plage de dates. **Gravité minimale** Sélectionnez une gravité d'événement. Tous les événements dont le niveau de gravité supérieur ou égal à la gravité sélectionnée sont affichés.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS
Sortie	Le rapport renvoie la sortie suivante : **Total des événements par gravité et heure** Diagramme à courbes présentant le nombre total d'instances d'événements (c'est-à-dire le nombre d'événements après dédoublonnage), classées par gravité. L'axe des X représente les dates auxquelles un ou plusieurs événements se sont produits dans la plage de dates spécifiée. Si vous sélectionnez une date unique, les unités deviennent des heures. L'axe des Y affiche la somme des événements, les unités sont sur une échelle logarithmique. **Total des événements par gravité** Diagramme à secteurs présentant le nombre total d'instances d'événements (c'est-à-dire le nombre d'événements après dédoublonnage), classées par gravité. **Evénements regroupés par date et gravité** Table affichant les événements, classés par gravité aux dates auxquelles ils se sont produits. La table est classée par ordre chronologique, par ordre croissant.
Exploration	Event_Details

Event_Details

Utilisez ce rapport pour afficher les détails complets d'un événement unique afin de déterminer la source des problèmes dans votre système.

En règle générale, vous générez ce rapport en utilisant la fonctionnalité d'exploration des rapports Event_Selection ou Event_Severity.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 107. Caractéristiques du rapport Event_Details

Fonction	Description
Name	Event_Details
Paramètres	**Nom de serveur** Entrez le nom du serveur ObjectServer. **Série de serveur** Entrez le numéro de série de Tivoli Netcool/OMNIbus pour la ligne de la table d'alertes.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS, REPORTER_DETAILS, REPORTER_JOURNAL, REP_AUDIT_SEVERITY
Sortie	Le rapport affiche quatre tables qui affichent des informations sur l'événement. Le tableau **Entrées de journal** affiche les entrées de journal classées par date dans l'ordre inverse. La table **Historique des événements** affiche les modifications apportées à l'accusé de réception, à la gravité, au propriétaire ou au groupe de l'événement, avec une modification pour chaque ligne de la table.
Exploration	Aucun
Problèmes connus	En fonction de la base de données relationnelle utilisée, dans la table **Entrées de journal**, les entrées de journal longues sont tronquées.

Acknowledgement_Summary

Utilisez ce rapport pour afficher la durée moyenne nécessaire aux opérateurs pour accuser réception d'un nouvel événement.

La durée moyenne d'accusé de réception pour un événement est calculée à partir de la durée de la période ou des périodes au cours desquelles l'événement est à l'état de non réception, la *durée de non réception*. Les durées de non réception se trouvent dans la table REP_AUDIT_ACK.

Le calcul est effectué comme suit :

période_non_réception_totale / nombre_périodes_non_réception

Où *période_non_réception_totale* est la durée totale où l'événement a été à l'état de non réception et *nombre_périodes_non_réception* est le nombre de fois où l'événement a été à l'état de non réception.

La durée entre l'occurrence initiale d'un événement et le temps de l'accusé de réception est enregistrée sous la forme d'une durée de non réception dans une ligne de la table REP_AUDIT_ACK. Si l'accusé de réception de l'événement est annulé par la suite, l'événement repasse à l'état de non réception. La durée entre l'annulation d'accusé de réception et le nouvel accusé de réception est une durée de non réception supplémentaire qui est enregistrée en tant que ligne séparée dans la table REP_AUDIT_ACK, etc.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 108. Caractéristiques du rapport Acknowledgement_Summary

Fonction	Description
Nom	Acknowledgement_Summary
Paramètres	**Plage de dates** Sélectionnez une plage de dates prédéfinie. Vous avez également la possibilité de sélectionner une **Plage de dates (ci-dessous)** et d'utiliser les zones de **Date de début** et de **Date de fin** pour définir votre propre plage de dates. **Regrouper par** Les valeurs de cette liste correspondent aux colonnes de la liste d'événements. Sélectionnez la colonne qui contient la valeur que vous souhaitez entrer dans la zone **Valeur de sélection**. Par exemple, si vous sélectionnez **Noeuds**, la distribution d'événements est regroupée par nœud. Vous indiquez le nombre de nœuds inclus dans le rapport dans la zone **Nombre de groupes à inclure**. **Remarque :** L'utilisateur propriétaire est le dernier utilisateur à posséder un événement et le groupe propriétaire est le dernier groupe à posséder un événement. Cet utilisateur ou ce groupe peut être différent de l'utilisateur ou du groupe auquel l'événement a été initialement affecté. **Nombre de groupes à inclure** Entrez le nombre de groupes que vous voulez inclure dans la sortie du rapport. Une fois générée, la sortie du rapport contient les groupes dont le nombre d'événements est le plus élevé. **Afficher** Indiquez si la valeur du **Nombre de groupes à inclure** capture les durées moyennes les plus rapides ou les plus lentes d'accusé de réception.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS, REP_AUDIT_ACK, REP_AUDIT_OWNERGID REP_AUDIT_OWNERUID, REP_AUDIT_SEVERITY

Tableau 108. Caractéristiques du rapport Acknowledgement_Summary (suite)

Fonction	Description
Sortie	Le rapport renvoie la sortie suivante. Dans toutes les sorties, le temps est exprimé sous la forme HH:MM:SS. **Délai d'accusé de réception moyen par date** Le graphique à courbes indique le délai moyen d'accusé de réception pour les événements au sein de la plage de dates donnée, par groupe, par exemple Noeud. L'axe des X représente les plages de dates spécifiées où les unités sont les dates de la première occurrence des événements. Si la plage de dates représente une journée, les unités sont des heures. L'axe des Y indique le délai dans lequel les unités sont des moyennes calculées à partir de la somme des durées moyennes d'accusé de réception. **Délai d'accusé de réception moyen par groupe** Diagramme à barres présentant le délai moyen des accusés de réception pour le nombre spécifié de groupes. L'axe des X indique le nombre de groupes indiqué par les paramètres de recherche. L'axe des Y indique le délai dans lequel les unités sont des moyennes calculées à partir de la somme des durées moyennes d'accusé de réception. **Délai d'accusé de réception moyen** Tableau présentant les informations dans le diagramme à barres Délai d'accusé de réception moyen par groupe, avec les groupes classés dans l'ordre décroissant.
Exploration	Acknowledgement_Details
Problèmes connus	Si le rapport est utilisé avec un regroupement Par sélection qui produit un grand nombre de valeurs différentes, la clé graphique risque de ne pas afficher toutes les valeurs. Si ce cas est fréquent, le graphique peut être agrandi à l'aide de Report Studio. Si un rapport

Acknowledgement_Details

Utilisez ce rapport pour afficher la somme des délais d'accusé de réception pour les événements dans le temps, sélectionnés selon différents critères.

La durée moyenne d'accusé de réception pour un événement est calculée à partir de la durée de la période ou des périodes au cours desquelles l'événement est à l'état de non réception, la *durée de non réception*. Les durées de non réception se trouvent dans la table REP_AUDIT_ACK.

Le calcul est effectué comme suit :

```
période_non_réception_totale / nombre_périodes_non_réception
```

Où *période_non_réception_totale* est la durée totale où l'événement a été à l'état de non réception et *nombre_périodes_non_réception* est le nombre de fois où l'événement a été à l'état de non réception.

La durée entre l'occurrence initiale d'un événement et le temps de l'accusé de réception est enregistrée sous la forme d'une durée de non réception dans une ligne de la table REP_AUDIT_ACK. Si l'accusé de réception de l'événement est annulé par la suite, l'événement repasse à l'état de non réception. La durée entre l'annulation d'accusé de réception et le nouvel accusé de réception est une durée de non réception supplémentaire qui est enregistrée en tant que ligne séparée dans la table REP_AUDIT_ACK, etc.

Le tableau ci-dessous décrit les caractéristiques de ce report :

Tableau 109. Caractéristiques du rapport Acknowledgement_Details

Fonction	Description
Nom	Acknowledgement_Details

Tableau 109. Caractéristiques du rapport Acknowledgement_Details (suite)

Fonction	Description
Paramètres	**Plage de dates** Sélectionnez une plage de dates prédéfinie. Vous avez également la possibilité de sélectionner une **Plage de dates (ci-dessous)** et d'utiliser les zones de **Date de début** et de **Date de fin** pour définir votre propre plage de dates. **Sélectionner par** Les valeurs de cette liste correspondent aux colonnes de la liste d'événements. Sélectionnez la colonne qui contient la valeur que vous souhaitez entrer dans la zone **Valeur de sélection**. **Remarque :** L'utilisateur propriétaire est le dernier utilisateur à posséder un événement et le groupe propriétaire est le dernier groupe à posséder un événement. Cet utilisateur ou ce groupe peut être différent de l'utilisateur ou du groupe auquel l'événement a été initialement affecté. **Valeur** Entrez une valeur valide pour la colonne que vous avez sélectionnée dans la zone **Valeur de sélection**.
Tables ou vues utilisées pour générer le rapport	REPORTER_STATUS, REP_AUDIT_ACK
Sortie	Le rapport renvoie la sortie suivante : **Délai d'accusé de réception moyen par gravité** Diagramme à barres présentant la somme des délais d'accusé de réception pour le groupe donné, regroupés par gravité d'origine et par moyenne. L'axe des X montre les groupes, par exemple, les nœuds. L'axe des Y indique le délai dans lequel les unités sont des moyennes calculées à partir de la somme des durées moyennes d'accusé de réception. **Délai d'accusé de réception moyen pour chaque événement** Tableau présentant le délai moyen des accusés de réception à partir de tous les accusés de réception d'événements, par groupe.
Exploration	Event_Details

Remarques

Ces informations ont été développées pour les produits et les services proposés aux Etats-Unis.

IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, programme ou service IBM n'implique pas que seul ce produit, programme ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous octroie aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Pour obtenir des informations sur les licences concernant les produits utilisant un jeu de caractères codé sur deux octets, contactez le service de propriété intellectuelle d'IBM de votre pays ou envoyez vos demandes par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT

D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069
Australia

IBM Corporation
896471/H128B
76 Upper Ground
London SE1 9PZ
United Kingdom

IBM Corporation
JBF1/SOM1
294 Route 100
Somers, NY, 10589-0100
United States of America

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les

résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Des parties de ce produit contiennent du logiciel développé par Daniel Veillard.

- `libxml2-2.7.8`

Le logiciel `libxml2-2.7.8` est distribué conformément au contrat de licence suivant :
© Copyright 1998-2003 Daniel Veillard.
All Rights Reserved. Toute personne possédant une copie de ce Logiciel et des fichiers de documentation associés (le «Logiciel») est autorisée gratuitement à exploiter le Logiciel sans restriction, y compris et sans limitation à utiliser, copier, modifier, fusionner, publier, distribuer, octroyer une sous-licence, et/ou vendre des copies du logiciel et à autoriser les personnes auxquelles le Logiciel est fourni à en faire de même, sous réserve des conditions suivantes :
Les déclarations relatives au copyright ci-dessus et cette déclaration de permission, doivent être incluses dans toutes les copies ou toute partie substantielle du Logiciel.
LE LOGICIEL EST FOURNI «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. DANIEL VEILLARD NE POURRA EN AUCUN CAS ÊTRE TENU RESPONSABLE POUR TOUT DOMMAGE, QUELLES QU'EN SOIT

LA CAUSE ET LES RESPONSABILITES, CONTRACTUELLES OU NON, OU PAR FAUTE LIEE A L'UTILISATION DE CE LOGICIEL.
Sauf indication contraire dans cette notice, le nom de Daniel Veillard ne doit pas être utilisé à des fins de publicité ou de promotion de ce Logiciel sans autorisation écrite préalable de Daniel Veillard.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Marques

AIX, DB2, IBM, le logo IBM, ibm.com, iSeries, Netcool, Passport Advantage, pSeries, Service Request Manager, System p, System z, Tivoli, Tivoli Enterprise Console, TotalStorage, WebSphere et zSeries sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays.

Adobe, Acrobat, Portable Document Format (PDF), PostScript ainsi que toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Index

A

accessibilité xiii
affichage
  détails des certificats 403
agents de processus
  configuration des serveurs 209
  configuration FIPS 140-2 284
aide en ligne
  configuration requise 51
  navigateurs Web 51
AIX
  variable d'environnement
    DISPLAY 573
ajout
  certificats 399
  de valeurs chiffrées aux fichiers de
    propriétés 369
  serveurs ObjectServer de secours 213
arch
  répertoire du système
    d'exploitation xiv
architecture à plusieurs niveaux 223
  alerts.login_failures 263
  configuration standard 223
  conventions de dénomination 226
  création de déclencheurs
    personnalisés 257
  déclencheurs de performances 258
  déclencheurs utilisateur 263
  disable_inactive_users 263
  emplacements des fichiers 232
  équilibrage de charge 255
  étapes finales 261
  événements Resynchronisation
    terminée 260
  gestion de la gravité 229
  nombre de serveurs ObjectServer 228
  ObjectServer d'affichage 241, 243
  passerelle d'affichage
    unidirectionnelle 243, 245
  passerelle d'agrégation
    bidirectionnelle 237
  passerelle de collecte de secours
    unidirectionnelle 240
  passerelle de collecte de secours
    unidirectionnelle
    supplémentaire 250
  passerelle de collecte principale
    unidirectionnelle 239
  passerelle de collecte principale
    unidirectionnelle
    supplémentaire 248
  plus de passerelles d'affichage
    unidirectionnelles 254
  plus de serveurs d'affichage
    ObjectServer 253
  plus de serveurs ObjectServer
    d'affichage 251
  plus de serveurs ObjectServer de
    collecte 246
  security_watch 263
architecture à plusieurs niveaux *(suite)*
  serveur d'agrégation ObjectServer de
    secours 236
  serveur d'agrégation ObjectServer
    principal 235
  serveur de collecte ObjectServer de
    secours 239
  serveur de collecte ObjectServer de
    secours supplémentaire 249
  serveur de collecte ObjectServer
    principal 238
  serveur de collecte ObjectServer
    principal supplémentaire 247
arrêt
  ObjectServer 205, 206
attributs
  fichiers de configuration 569
authentification
  PAM 354
authentification externe 354
automatisation
  description 2
autorisation 359
autorité de certification 371

B

bases de données de clés
  création 381

C

CA (autorité de certification) 371
centre de documentation de Tivoli xi
certificat 183
certificat autosigné
  création 385
certificat par défaut
  spécification 402
certificats
  activation 530
  affectation 532
  ajout 399, 527, 530
  ajout au fichier 529
  demande 388, 527
  extraction 397
  génération 531
  obtention 529
  réception 395, 529
  remplacement 527
  suppression 404
certificats d'autorité de certification
  activation 530
  ajout 399, 527
  ajout au fichier 529
  demande 527
  obtention 529
  réception 529
certificats numériques
  activation 530
certificats numériques *(suite)*
  affectation 532
  affichage des détails 403
  ajout 399, 527, 530
  ajout au fichier 529
  demande 388, 527
  extraction 397
  génération 531
  obtention 529
  réception 395, 529
  remplacement 527
  suppression 404
certificats serveur
  activation 530
  affectation 532
  affichage des détails 403
  ajout 527, 530
  ajout au fichier 529
  demande 388, 527
  génération 531
  obtention 529
  réception 395, 529
  remplacement 527
  spécification de valeur par
    défaut 402
  suppression 404
chaînes
  chiffrement 368
chiffrement
  chaînes 368
  Interface graphique Web 520
  mots de passe du contrôle de
    processus 340
  mots de passe pour les scripts
    SQL 341
  valeurs dans les fichiers de
    propriétés 366
chiffrement de mots de passe 340, 341
  serveur d'Interface graphique Web,
    AES 532
  serveur d'Interface graphique Web,
    mode FIPS 140–2 537
chiffrement de valeur de propriété 367,
  368, 369
chiffrement des valeurs de propriété 366
clés
  génération 367
codage Windows UTF-8 418
commande d'arrêt (ObjectServer) 206
commande de publications xi
communications
  distribution du fichier d'interfaces sur
    plusieurs plateformes 219
compatibilité
  octroi de licence 54
  passerelles 54
  versions précédentes 54
configuration
  communications à l'aide du protocole
    SSL 371
  événements TADDM 459

configuration *(suite)*
gestion des événements prévisibles 448
informations de communication du serveur 209
Interface graphique Web 501
IPv6 413
mode équilibrage de charges 333
mode FIPS 140-2 283, 288
mode FIPS 140-2 pour les serveurs 284
ObjectServer de bureau 327, 328
tri localisé 423
virtualisation 469
Configuration
aide en ligne
IEHS 95
mode autonome 95
mode centre d'informations 95
configuration Interface graphique Web (mode silencieux) 180
environnement d'exécution Java
FIPS 140-2 97
passerelles 93
sondes 93
configuration de reprise en ligne 267
configuration de VMM 512
configuration requise
aide en ligne 51
environnement d'exécution Java 49
espace disque 29
interface utilisateur 51
mode FIPS 140-2 288
connexion 182, 649
configuration pour HTTP et HTTPS 520
connexions multiples à un utilisateur 610
connexion unique 573
configuration 574, 576
gestion des clés LTPA 575
importation des clés LTPA 577
procédures 576
connexion uniqueexportation des clés LTPA 577
connexions multiples à un compte utilisateur 610
connexions sécurisées
avec FIPS 140-2 538
en mode non-FIPS 525
contrôle de processus
arrêt d'un serveur ObjectServer 205
configuration FIPS 140-2 284
démarrage d'un serveur ObjectServer 203
présentation 5
sécurité 340
services Windows 203
conventions, typographiques xiv
conventions de dénomination
ObjectServer 195
conventions typographiques xiv
conversion
UTF-8 131
conversion UTF-8 131
création
base de données de clés 381
création *(suite)*
certificat autosigné 385
fichier stash 381
fichiers de liste de configuration 303
ObjectServer 197
ObjectServer de bureau 328

D

dédoublonnage
description 2
demande
certificats 388
demandes de certificats 375, 376
démarrage
ObjectServer 203, 204
détails des certificats
affichage 403
documentation en ligne xi
données BAROC 136
migration 139
droits
objet 360
système 360
droits objet 360
droits système 360

E

éditeur de serveur 207
configuration de SSL sous UNIX 375
configuration de SSL sous Windows 376
configuration des agents de processus 209
configuration des serveurs de passerelle 209
informations de communication du serveur 207
éditeur de serveurs
ajout de serveurs ObjectServer de secours 213
création d'entrées de définition de serveur 214
distribution du fichier d'interfaces 215
fichier de données de connexions 217
informations de communication du serveur 209
masquage de serveurs ObjectServer de secours 216
modification de la priorité des serveurs ObjectServer de secours 216
test de disponibilité du serveur 217
éléments
fichiers de configuration 566
entrées de journal
ObjectServer de bureau 332
entrées de journal manuelles
ObjectServer de bureau 332
environnements locaux
configuration 418
équilibrage de charge 255
configuration 603
espace disque requis 29
événements prévisibles 587
ressources 444
événements TADDM 456, 459
configuration 590
installation et configuration 457
ressources 458
exigences de l'environnement d'exécution Java (JRE) 49
exportation
configurations du serveur ObjectServer 293
extraction
certificats 397

F

fichier application.sql 194
fichier automation.sql 194
fichier d'exclusions
exemple 314
présentation 313
fichier d'initialisation
propriétés 687
fichier d'interfaces
ajout d'un serveur ObjectServer de secours 213
configuration des agents de processus 209
configuration des serveurs de passerelle 209
connexions SSL 375
distributions sur plusieurs plateformes 219
masquage de serveurs ObjectServer de secours 216
test de la disponibilité d'un serveur 217
fichier de clés du coffre 183
fichier de demande de certificat
signature 393
fichier de données de connexions 217
fichier desktop.sql 194
fichier omni.dat
modification 217
fichier security.sql 194
fichier system.sql 194
fichiers CRL
omni.crl 379
fichiers d'interfaces
modification de la priorité des serveurs de secours 216
fichiers DAT
omni.dat 217
fichiers de clés 368, 410
fichiers de clés de certificat
configuration de SSL sous Windows 410
fichiers de configuration
attributs 569
éléments 566
structure 565
fichiers de dissimulation 379
fichiers de la base de données de clés 379
fichiers de liste de configuration
création 303

fichiers de liste de configuration *(suite)*
exemple 309
modification 308
utilisation 299, 303
fichiers KDB
omni.kdb 379
fichiers RDB
omni.rdb 379
fichiers SQL 194
fichiers stash
création 381
fichiers STH
omni.sth 379
FIPS 140-2
liste de contrôle de configuration 653
formation
voir formation technique Tivoli xiii
formation, technique Tivoli xiii
formation technique Tivoli xiii

G

génération
clés 367
gestion des événements prévisibles 448
groupes
fourni 181
par défaut 364
sécurité de niveau ligne 364
groupes par défaut 364

H

haute disponibilité 267
arrêt contrôlé 275
configuration de reprise en ligne 267
réduction de la perte d'événements 274
réduction du temps de resynchronisation 275
reprise en ligne de serveur proxy 279
reprise par restauration contrôlée 269
HP-UX
variable d'environnement
DISPLAY 573
HTTP et HTTPS 520

I

IBM Installation Manager 32
Installation (interface graphique ou console) 36
Installation (mode silencieux) 39
Obtention 35
présentation
modes utilisateur 32
répertoires d'installation par défaut 32
Téléchargement d' 35
IBM Key Management (iKeyman)
présentation 401
identification et résolution des problèmes 657
accès root 657
Interface graphique Web
migration 189
identification et résolution des problèmes *(suite)*
Interface graphique Web *(suite)*
registres d'utilisateurs 516
module PAM 658
nco_pad 657
support multiculturel 666
Identification et résolution des problèmes
Analyseur de traces et de journaux ISA 678
Collecteur de données d'IBM Support Assistant 676
LDAP
Calcul des temps de recherche LDAP 665
Erreurs LDAP communes 660
ldapsearch 659
Test de la configuration LDAP 659
Plan de travail IBM Support Assistant 673
iKeyman
démarrage 401
présentation 401
importation
configurations du serveur ObjectServer 293, 317
informations de communication du serveur 207, 209
informations de support xiii
informations sur l'installation 147
initialisation de la base de données
fichiers 194
nco_dbinit 194
installation 72
configuration d'un environnement de test 643
identification et résolution des problèmes
Interface graphique Web 189
installation de Interface graphique Web (interface graphique) 151
installation Interface graphique Web (console) 154
installation Interface graphique Web (mode silencieux) 156
navigateurs Web pris en charge 50
passerelles 135
pour l'authentification unique 573
protection du fichier de clés du coffre 183
services Windows 100
sondes 135
Tivoli Netcool/OMNIbus 85, 116, 669
Installation
nco_icw 193
assistant de configuration initiale 193
chemins d'accès à la bibliothèque partagée 87
configuration initiale 193
fichier de réponses Installation Manager 35
fonctions installables 65
installation de Tivoli Netcool/OMNIbus (interface graphique) 73
Installation *(suite)*
installation Tivoli Netcool/OMNIbus (console) 78
installation Tivoli Netcool/OMNIbus (mode silencieux) 82
passerelles 93
Préparation à l'installation 65
sondes 93
structure de répertoire 67
tâches de post-installation 86
variables d'environnement
%NCHOME% 67
$NCHOME 67
chemins d'accès de bibliothèque partagée 92
LD_LIBRARY_PATH 87, 92
LIBPATH 87, 92
NCHOME 67, 87
OMNIHOME 67, 87
PATH 87
SHLIB_PATH 87, 92
installation UNIX
répartie 218
installation Windows
répartie 218
installations réparties
introduction 218
instructions
conversion en UTF-8 131
interface de programmation d'application d'administration Webtop (WAAPI)
configuration initiale 186
interface graphique Web
mots de passe des utilisateurs fournis 185
Interface graphique Web 147
configuration 501
présentation 7
référentiels d'utilisateurs
ajout 504
authentification LDAP 514
changement 518
suppression 517
synchronisation 510
interface interactive SQL
présentation 5
sécurité 341
interface SQL interactive 206
IPv4
support 52
IPv6
configuration 413
configuration du fichier de règles de la sonde 413
configuration UNIX 413
configuration Windows 413
exigences de configuration
HP-UX 52, 413
restrictions 52
support 52

J

JRE 50

L

lancement en contexte 592
LC_NUMERIC environment
  variable 418
LDAP 522
  ajout d'un OpenLDAP 506
  configuration pour l'authentification
    externe 343
  exemples LDAP 352
  prérequis 343
  propriétés 348
liste d'événements
  erreur de socket 667
  erreur IDUC 667
liste de contrôle
  configuration du mode FIPS
    140-2 653

M

manuels xi
migration
  fichiers migrés 122
  Interface graphique Web
    de Netcool/Webtop version
      1.3 172, 189
Mise à jour de Tivoli
  Netcool/OMNIbus 111
  application de correctifs
    (console) 114
  application de correctifs (interface
    graphique) 112
  Application de correctifs (mode
    silencieux) 115
  Rétrogradation de mises à jour
    (interface graphique) 118
mise à niveau
  Interface graphique Web
    de l'Interface graphique Web
      version 7.3.0 167
    de l'Interface graphique Web
      version 7.3.1 160
    de Netcool/Webtop version
      1.3 172, 189
    de Netcool/Webtop version
      2.1 167, 189
    de Netcool/Webtop version
      2.2 167
    présentation 158
  mise à niveau d'une architecture à
    plusieurs niveaux 132, 264
  mise à niveau sous UNIX et
    Linux 120
  mise à niveau sous Windows 120
  mises à niveau à partir de Tivoli
    Netcool/OMNIbus V7.4 (et versions
    antérieures) 120
Mise à niveau 142
mode de reprise en ligne d'égal à égal
  sondes 273
mode écriture double
  ObjectServer de bureau 331
mode équilibrage de charges 333
  configuration 333
mode FIPS 140-2
  compatibilité en amont 288
mode FIPS 140-2 *(suite)*
  configuration 283, 284
  création du fichier de
    configuration 283
  Interface graphique Web 534
  SP800-131, chiffrement étendu 286
mode sécurisé
  ObjectServer 340
  serveur proxy 340
modification
  fichiers de liste de configuration 308
  mot de passe de la base de données
    de clés 405
  priorité des serveurs ObjectServer de
    secours 216
module d'installation
  téléchargement 31
module PAM
  configuration du serveur ObjectServer
    comme source
    d'authentification 357
  identification et résolution des
    problèmes 658
mot de passe de la base de données de
  clés
  modification 405
mots de passe
  AES 142
  chiffrement des mots de passe 142
  DES 142
  FIPS 142

N

navigateurs Web 50
nc_gskcmd 406
nco_aes_crypt 368
  options de ligne de commande 370
nco_baroc2sql 137
  options de lignes de commande 139
nco_confpack 293
  affichage du contenu du package de
    configuration 316
  considérations sur l'importation 321
  création de configurations de
    sauvegarde du serveur
    ObjectServer 315
  création de fichiers de liste de
    configuration 303
  édition des fichiers de liste de
    configuration 308
  éléments importables et
    exportables 299
  exportation des configurations du
    serveur ObjectServer 309
  fichier d'exclusions 313
  importation de configurations du
    serveur ObjectServer 317
  options de ligne de commande 301
  présentation des fichiers de liste de
    configuration 299, 303
  présentation du package de
    configuration 299
  propriétés 301
nco_dbinit 194, 197, 328
  options de ligne de commande 198
  propriétés 198
nco_igen 217
nco_keygen 367
nco_objserv 204
nco_pa_crypt 340
nco_sql 206
nco_sql_crypt 341
NCOMS.props 204
numéros de port
  par défaut 685
numéros de port par défaut 685

O

ObjectServer 512
  ajout de serveur de secours 213
  architecture du serveur ObjectServer
    de bureau 325
  arrêt à l'aide de services 206
  arrêt à l'aide du contrôle de
    processus 205
  arrêt manuel 206
  automatisation 2
  configuration FIPS 140-2 284
  connexion SSL 523
  conventions de dénomination 195
  création 197
  création de configurations de
    sauvegarde 315
  dédoublonnage 2
  démarrage à l'aide du contrôle de
    processus 203
  démarrage manuel 204
  exportation des configurations 309
  fichier de propriétés 197
  importation de configurations 317
  initialisation de la base de
    données 194
  isql 206
  masquage de serveurs ObjectServer de
    secours 216
  mode sécurisé 340
  modification de la priorité des
    serveurs de secours 216
  nco_dbinit 197
  nco_objserv 204
  nco_sql 206
  options de configuration 205
  options de ligne de commande 198
  présentation 2, 194
  propriétés 198
  répertoire de bases de données 195
  reprise en ligne automatique 196
  reprise par restauration
    automatique 196
ObjectServer de bureau
  authentification dans 332
  configuration 327, 328
  configuration de passerelle
    unidirectionnelle 329
  configuration du mode équilibrage de
    charge 333
  considérations 327
  création 328
  entrées de journal manuelles 332
  mode écriture double 331
  mode équilibrage de charges 333
  présentation 325

ObjectServer de bureau *(suite)*
présentation de l'architecture 325
omni.crl 379
omni.kdb 379
omni.rdb 379
omni.sth 379
outil de conversion BAROC 137
outils d'administration
présentation 5
outils de bureau
présentation 4

P

packages de configuration 299
PAM 354
activation de l'authentification externe 354
configuration 354
configuration du serveur ObjectServer 356
fichier de configuration 358
fichier de configuration PAM du serveur ObjectServer 359
modification des paramètres du serveur ObjectServer 358, 359
passerelle ObjectServer
description 3
octroi de licence 3
récapitulatif 3
utilise 3
passerelles
configuration des serveurs 209
configuration FIPS 140-2 284
présentation 3
sécurité 340
passerelles unidirectionnelles
utilisation dans l'architecture du serveur ObjectServer de bureau 329
périphériques mobiles 50
plateformes, prises en charge 3
plateformes prises en charge 3
Pluggable Authentication Modules (PAM) 354
Prerequisite Scanner 30
prise en charge de la norme FIPS 534
programmes d'écriture 3
programmes de lecture 3
protocole de communication 53
protocole SSL 371
public xi
publications xi

R

réception
certificats 395
rechargement due fichier de règles 480
référentiels fédérés
VMM pour ObjectServer 512
reloadrules_allprobes 480
répertoire control_shutdown 429
répertoire du système d'exploitation
arch xiv
répertoire eventflood 429
répertoire itmpredictive 429
répertoire itmvirtualization 429
répertoire multitier 429
répertoire roi 429
répertoire taddm 429
reprise en ligne
automatique 196
reprise en ligne de serveur proxy 279
reprise en ligne et reprise par restauration automatique 196
reprise par restauration
automatique 196
reprise par restauration contrôlée 269
Retrait de l'Interface graphique Web 190
Retrait de Tivoli Netcool/OMNIbus 109
rôles
de groupes fournis 181
par défaut 361
rôles par défaut 361

S

sécurité
accès utilisateur 337
authentification 338, 339
autorisation 338
certificat 183
contrôle de processus 340
interface interactive SQL 341
module PAM 354
passerelles 340
serveur proxy 340
sondes 340
traces de contrôle 366
sécurité d'authentification 338
sécurité d'autorisation 338
sécurité des accès utilisateur 337
security 520
server.init
propriétés 687
serveur
chiffrement des mots de passe, AES 532
chiffrement des mots de passe, mode FIPS 140–2 537
serveur d'applications
activation de la norme FIPS 534
serveur ObjectServer
erreur d'échec du programme d'écoute 668
serveurs proxy
configuration FIPS 140-2 284
services Windows 203
signature
fichier de demande de certificat 393
sondes
mode de reprise en ligne d'égal à égal 273
présentation 3
sécurité 340
source de données
fichier de configuration 553
sources de données
exemples 547
multiple 562
spécification
certificat par défaut 402
fichier de clés comme propriété 368
SSL 371, 410
au serveur ObjectServer 523
configuration 522
démarrage d'iKeyman 401
fichiers de la base de données de clés 379
gestion de certificats numériques 401, 527
remplacement d'un certificat client 527
SSL 522
support multiculturel
codage Windows UTF-8 418
configuration de l'environnement local 418
configuration des polices 423
environnements locaux pour le bureau UNIX 423
identification des environnements locaux pris en charge 422
Interface graphique Web 187
tri localisé 423
utilisation du texte d'interface graphique traduit 426
variables d'environnement de localisation 418
suppression
certificats 404
surveillance automatique
état de santé d'ObjectServer, panneau 582
état de santé des clients et des applications 584
tableau de bord Netcool Health 581
systèmes d'exploitation pris en charge 42

T

tester
disponibilité du serveur 217
Tivoli Enterprise Console
migration des données BAROC 136
Tivoli Netcool/OMNIbus
numéros de port par défaut 685
présentation 1
traces de contrôle 366
traitement des problèmes
DISPLAY 669
intégration 671
interface graphique 669
ITM 671
synchronisation des événements 671
X11 669
tri localisé
configuration 423

U

utilisateurs
fourni 181
par défaut 365
utilisateurs par défaut 365
utilisateursconnexions multiples à un compte 610

utilitaire Confpack
  présentation 5
utilitaire d'importation et d'exportation
  présentation 5

V

valeurs chiffrées
  ajout aux fichiers de propriétés 369
variable d'environnement LANG 418
variable d'environnement LC_ALL 418
variable d'environnement
  LC_COLLATE 418
variable d'environnement
  LC_CTYPE 418
variable d'environnement
  LC_MESSAGES 418
variable d'environnement
  LC_MONETARY 418
variable d'environnement LC_TIME 418
variable d'environnement NCO_JRE 49
variables, notation pour xiv
variables d'environnement
  DISPLAY 573
  LANG 418
  LC_ALL 418
  LC_COLLATE 418
  LC_CTYPE 418
  LC_MESSAGES 418
  LC_MONETARY 418
  LC_NUMERIC 418
  LC_TIME 418
  NCO_JRE 49
variables d'environnement, notation xiv
variables d'environnement de
  localisation 418
vérification
  Tivoli Netcool/OMNIbus 85, 116,
    669
virtualisation 469
  ressources 477
VMM
  pour ObjectServer 512

SC43-0822-01