Network Manager IP Edition
Version 3.9

Guide d'installation et de configuration

R2E2

Network Manager IP Edition
Version 3.9

Guide d'installation et de configuration

R2E2

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 395.

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.

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

Cette édition s'applique à la version 3.9 d'IBM Tivoli Network Manager IP Edition (numéro de produit 5724-S45) et à toutes les éditions et modifications ultérieures, sauf mentions contraires dans les nouvelles éditions.

Table des matières

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

IBM Tivoli Network Manager IP Edition possède des fonctions de reconnaissance du réseau détaillée, de surveillance des périphériques, de visualisation de la topologie et d'analyse des causes (RCA). Network Manager peut être entièrement personnalisé et configuré pour gérer différents réseaux. Network Manager fournit également des fonctions de génération de rapports étendues ainsi qu'une intégration aux autres produits IBM, tels que IBM Tivoli Application Dependency Discovery Manager, IBM Tivoli Business Service Manager et IBM Systems Director.

Le manuel *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration* décrit comment installer Network Manager IP Edition. Le guide décrit également les tâches de configuration post-installation. Elle est destinée aux administrateurs qui doivent installer et paramétrer Network Manager IP Edition.

Personnes concernées

Cette publication est destinée aux administrateurs qui doivent installer Network Manager et effectuer la configuration post-installation.

Les lecteurs doivent être familiers avec :

- la gestion de réseau
- la configuration des systèmes d'exploitation

IBM Tivoli Network Manager IP Edition fonctionne avec IBM Tivoli Netcool/OMNIbus ; pour comprendre cette publication, vous devez comprendre comment fonctionne IBM Tivoli Netcool/OMNIbus. Pour plus d'informations sur IBM Tivoli Netcool/OMNIbus, voir les publications décrites dans «Publications», à la page x.

Contenu de cette publication

Cette publication contient les sections suivantes :

- Chapitre 1, «Planification de l'installation», à la page 1

  Fournit des informations sur ce qu'il faut considérer avant d'installer Network Manager, tel que les configurations de déploiement avec reprise en ligne et domaines réseau, ainsi que les spécifications quant au matériel, au système d'exploitation, aux logiciels et aux communications.
- Chapitre 2, «Installation», à la page 57

  Décrit comment installer Network Manager.
- Chapitre 3, «Mise à niveau et migration», à la page 143

  Décrit comment effectuer une mise à niveau vers la dernière version de Network Manager, y compris la migration des données existantes provenant de votre environnement de production précédent.
- Chapitre 4, «Configuration de Network Manager», à la page 175

  Décrit les tâches à effectuer après l'installation de Network Manager ainsi que les paramètres que vous pouvez modifier ultérieurement lors de l'utilisation du produit.

Publications

Cette section contient la liste des publications de la bibliothèque Network Manager ainsi que les documents associés. Elle indique également comment accéder aux publications Tivoli en ligne et comment commander des publications Tivoli.

Votre bibliothèque Network Manager

Les documents suivants sont disponibles dans la bibliothèque Network Manager :

- *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*, GI11-7410-00

  Fournit d'importantes informations récentes sur IBM Tivoli Network Manager IP Edition. Cette publication s'adresse aux chargés du déploiement et aux administrateurs et doit être lue en premier lieu.
- *IBM Tivoli Network Manager - Guide d'initiation*, GI11-7409-00

  Décrit comment configurer IBM Tivoli Network Manager IP Edition après avoir installé le produit. Ce guide indique comment démarrer le produit, vérifier qu'il s'exécute correctement et reconnaître le réseau. Pour une utilisation correcte de Network Manager IP Edition, il est indispensable d'effectuer une reconnaissance appropriée du réseau. Ce guide indique comment configurer et surveiller une première reconnaissance, vérifier les résultats de cette dernière, configurer une reconnaissance de production et conserver la topologie réseau à jour. Une fois la topologie de réseau mise à jour, ce guide indique comment mettre celle-ci à la disposition des opérateurs réseau et comment surveiller le réseau. Les tâches essentielles sont abordées dans cet aide-mémoire, en liaison avec les tâches et éléments de référence plus détaillés, facultatifs ou avancés dans le reste de la documentation.
- *IBM Tivoli Network Manager IP Edition - Présentation du produit*, GC11-6907-00

  Cette publication présente IBM Tivoli Network Manager IP Edition. Elle décrit l'architecture, les composants et les fonctionnalités du produit. Elle est destinée à tous ceux intéressés par IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*, SC11-6908-00

  Cette publication décrit comment installer IBM Tivoli Network Manager IP Edition. Elle décrit également les tâches de configuration post-installation facultatives et obligatoires. Elle est destinée aux administrateurs qui doivent installer et paramétrer IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition - Guide d'administration*, SC11-6909-00

  Cette publication décrit les tâches d'administration pour IBM Tivoli Network Manager IP Edition, telles que l'administration de processus, l'interrogation de bases de données et le démarrage et l'arrêt du produit. Elle est destinée aux administrateurs chargés de la maintenance et de la disponibilité d'IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition - Guide de reconnaissance* , SC11-6910-00

  Cette publication décrit comment utiliser IBM Tivoli Network Manager IP Edition pour reconnaître votre réseau. Elle est destinée aux administrateurs chargés de la configuration et de l'exécution de la reconnaissance de réseaux.
- *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*, SC11-6911-00

  Décrit comment utiliser IBM Tivoli Network Manager IP Edition pour interroger les périphériques réseau, configurer l'enrichissement des événements à partir des périphérique réseau et pour gérer les plug-in vers la passerelle d'événements Tivoli Netcool/OMNIbus, y compris la configuration du plug-in RCA à des fins

d'analyse de la cause première. Cette publication est destinée aux administrateurs chargés de la configuration et de l'exécution de l'interrogation de réseaux, de l'enrichissement d'événement, de l'analyse de la cause première et des plug-in de passerelle d'événements.

- *IBM Tivoli Network Manager IP Edition - Guide de traitement des incidents liés au réseau*, GC11-6914-00

  Cette publication décrit comment utiliser IBM Tivoli Network Manager IP Edition pour résoudre les incidents de réseau identifiés par le produit. Elle est destinée aux opérateurs de réseau qui sont chargé d'identifier ou de résoudre les incidents réseau.

- *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*, SC11-6912-00

  Décrit comment configurer les outils de visualisation du réseau IBM Tivoli Network Manager IP Edition afin de fournir à vos opérateurs de réseau un environnement de travail personnalisé. Cette publication s'adresse aux administrateurs de produit ou aux chefs d'équipe qui sont chargés de faciliter le travail des opérateurs de réseau.

- *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données de gestion*, SC27-2767-00

  Cette publication décrit les schémas des bases de données de composants dans IBM Tivoli Network Manager IP Edition. Elle est destinée aux utilisateurs avancés qui doivent interroger les bases de données de composants directement.

- *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données topologiques*, SC11-6913-00

  Cette publication décrit les schémas de la base de données utilisés pour stocker des données topologiques dans IBM Tivoli Network Manager IP Edition. Elle est destinée aux utilisateurs avancés qui doivent interroger la base de données topologique directement.

- *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*, SC11-6916-00

  Cette publication décrit les langages système utilisés par IBM Tivoli Network Manager IP Edition, tels que les langages Stitcher et Object Query Language. Elle est destinée aux utilisateurs avancés qui doivent personnaliser le fonctionnement d'IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition - Guide de l'interface de programme d'application Perl*, SC11-6917-00

  Décrit les modules Perl qui permettent aux développeurs d'écrire des applications personnalisées qui interagissent avec IBM Tivoli Network Manager IP Edition. Les exemples d'applications personnalisées pouvant être écrites par les développeurs incluent les agents d'interrogation et de reconnaissance. Cette publication s'adresse aux développeurs Perl avancés qui doivent écrire des applications personnalisés de ce type.

- *IBM Tivoli Monitoring for Tivoli Network Manager IP - Guide d'utilisation*, SC11-6918-00

  Fournit des informations sur l'installation et l'utilisation de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. Cette publication est destinée aux administrateurs systèmes chargés de l'installation et de l'exécution de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition pour surveiller et gérer les ressources IBM Tivoli Network Manager IP Edition.

Publications prérequises

Pour utiliser correctement les informations de la présente publication, vous devez posséder certaines connaissances prérequises, que vous pouvez obtenir dans les publications suivantes :

- *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*, SC23-9680

  Inclut les procédures d'installation et de mise à niveau de Tivoli Netcool/OMNIbus et décrit comment configurer la sécurité et les communications des composants. Cette publication comprend également des exemples d'architectures Tivoli Netcool/OMNIbus et décrit leur implémentation.
- *IBM Tivoli Netcool/OMNIbus User's Guide*, SC23-9683

  Fournit un résumé des outils du bureau et décrit les tâches de l'opérateur liées à la gestion des événements, effectuées à l'aide des outils de bureau.
- *IBM Tivoli Netcool/OMNIbus Administration Guide*, SC23-9681

  Décrit comment effectuer des tâches d'administration à l'aide de l'interface graphique d'administration, des outils de ligne de commande et de la commande de processus Tivoli Netcool/OMNIbus. Cette publication contient également des descriptions et des exemples de la syntaxe SQL ObjectServer et des automatisations.
- *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*, SC23-9684

  Contient des informations de présentation et de référence sur l'analyse et les passerelles, notamment la syntaxe du fichier de règles d'analyse et les commandes de passerelles.
- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* SC23-9682

  Décrit comment exécuter des tâches d'administration et de visualisation d'événement à l'aide de interface graphique Web Tivoli Netcool/OMNIbus.

Accès en ligne à la terminologie

Le site Web de terminologie IBM regroupe la terminologie des bibliothèques de produits IBM dans un emplacement unique et pratique. Vous pouvez y accéder à l'adresse suivante :

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

Accès en ligne aux publications

IBM sort des publications pour ce produit et pour tous les autres produits Tivoli (au moment de leur mise à disposition et à chaque mise à jour) sur le site Web IBM Knowledge Center à l'adresse :

http://www-01.ibm.com/support/knowledgecenter/

La documentation Network Manager se trouve sous **Cloud & Smarter Infrastructure** sur ce site Web.

Remarque : Si vous imprimez des documents PDF sur du papier autre qu'au format lettre, définissez l'option qui permet à votre application de lecture de PDF d'imprimer des pages au format lettre sur votre papier local dans la fenêtre **Fichier** > **Imprimer**.

Commande de publications

Vous pouvez commander de nombreuses publications Tivoli en ligne sur le site Web suivant :

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss

Vous pouvez également passer votre commande par téléphone en composant l'un des numéros suivants :

- Aux Etats-Unis : 800-879-2755
- Au Canada : 800-426-4968

Pour les autres pays, contactez votre représentant logiciel local pour commander des publications Tivoli. Pour connaître le numéro de téléphone de votre représentant local, procédez comme suit :

1. Accédez au site Web suivant :

   http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss
2. Sélectionnez votre pays dans la liste et cliquez sur **Go**. La page de bienvenue d'IBM Publications Center est affichée pour votre pays.
3. Dans la partie gauche de la page, cliquez sur **A propos de ce site** pour afficher la page d'informations qui comporte le numéro de téléphone de votre représentant local.

Accessibilité

Les fonctions d'accessibilité aident les utilisateurs ayant un handicap physique, comme les personnes à mobilité réduite ou avec une vision limitée, à utiliser les produits logiciels.

Fonctions d'accessibilité

La liste suivante répertorie les principales fonctions d'accessibilité dans Network Manager :

- Le programme d'installation basé sur une console prend en charge les opérations clavier.
- Le programme d'installation basé sur une console prend en charge l'utilisation du lecteur d'écran.
- Network Manager inclut les fonctions suivantes pour les utilisateurs malvoyants :
  - Tout le contenu autre que textuel de l'interface graphique comporte un texte descriptif associé.
  - Les utilisateurs malvoyants peuvent régler les paramètres d'affichage du système, notamment le mode de contraste élevé, et peuvent contrôler les tailles de police dans les paramètres de navigateur.
  - La couleur n'est pas le seul moyen visuel de véhiculer les informations qui indiquent une action, demandent une réponse ou différencient un élément visuel.
- Network Manager inclut les fonctions suivantes pour les utilisateurs atteints d'épilepsie photosensible :
  - Les pages Web ne contiennent pas d'animation qui clignote à une fréquence supérieure à deux fois par seconde.

Les fonctions d'accessibilité du Knowledge Center Network Manager sont décrites dans le Knowledge Center lui-même.

Etapes supplémentaires permettant de configurer les fonctions d'accessibilité d'Internet Explorer

Si vous utilisez Internet Explorer comme navigateur Web, il se peut que vous deviez effectuer des étapes de configuration supplémentaires pour activer les fonctions d'accessibilité.

Pour activer le contraste élevé, procédez comme suit :

1. Cliquez sur **Outils** > **Options Internet** > **Accessibilité**.
2. Cochez toutes les case de la section Mise en forme.

Si vous ne parvenez pas à accroître la taille de la police lorsque vous cliquez sur **Affichage** > **Taille du texte** > **La plus grande**, cliquez sur **Ctrl +** et **Ctrl -**.

IBM® et l'accessibilité

Consultez le centre IBM Human Ability and Accessibility Center pour obtenir plus d'informations sur l'engagement d'IBM envers l'accessibilité.

Formation technique à Tivoli

Pour des informations sur la formation technique à Tivoli, consultez le site Web de formation IBM Tivoli suivant :

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

Informations de support technique

Si vous avez un problème avec votre logiciel IBM, vous voulez le résoudre rapidement. IBM vous offre les moyens suivants pour obtenir le support nécessaire :

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

IBM Support Assistant
IBM Support Assistant (ISA) est un plan de travail de maintenabilité logicielle local gratuit, qui vous aide à résoudre des questions et des problèmes avec des logiciels IBM. ISA offre un accès rapide à des informations de support technique et à des outils de maintenabilité pour la détermination des problèmes. Pour installer le logiciel ISA, accédez à http://www.ibm.com/software/support/isa

Conventions utilisées dans cette publication

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

Conventions typographiques

Cette publication utilise les conventions typographiques suivantes :

Gras

- Commandes en minuscules et commandes à casse mixte difficiles à distinguer du texte environnant
- Contrôles de l'interface (cases à cocher, boutons, boutons d'option, sélecteurs rotatifs, zones, dossiers, icônes, zones de liste, éléments dans les zones de liste, listes multicolonnes, conteneurs, choix de menu, noms de menu, onglets, feuilles de propriétés), intitulés (tels que **Astuce :** et **Considérations sur le 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 non commutée appelée une ligne *point à point*)
- Mise en évidence de mots et de lettres (mots comme exemples de mots : "Utilisez le mot *that* pour introduire une clause restrictive."; lettres comme exemple de lettres : "L'adresse LUN doit commencer par la lettre *L*.")
- Nouveaux termes dans le texte (excepté dans une liste de définitions) : une *vue* est un cadre dans un espace de travail qui contient des données
- Variables et valeurs que vous devez fournir : ... où *mon_nom* représente....

`Espacement fixe`

- Exemples et exemples de code
- Noms de fichier, mots clés de programmation et autres éléments difficiles à distinguer du texte environnant
- Texte de message et invites destinés à l'utilisateur
- Texte que l'utilisateur doit saisir
- Valeurs d'argument ou options de commande

Variables et chemins d'accès dépendant du système d'exploitation

Cette publication utilise des variables d'environnement sans les préfixes et suffixes spécifiques aux plateformes, sauf si la commande s'applique à des plateformes spécifiques. Par exemple, le répertoire où les composants centraux de Network Manager sont installés est représenté par NCHOME.

Lors de l'utilisation de la ligne de commande Windows, préfixez et suffixez les variables d'environnement par le signe de pourcentage **%**, et remplacez chaque barre oblique (*/*) par une barre oblique inversée (\) dans les chemins d'accès des répertoires. Par exemple, sur les systèmes Windows, NCHOME est %NCHOME%.

Sur les systèmes UNIX, préfixez les variables d'environnement par le signe dollar **$**. Par exemple, sur les systèmes UNIX, NCHOME est $NCHOME.

Les noms des variables d'environnement ne sont pas toujours les mêmes dans les environnements Windows et UNIX. Par exemple, %TEMP% dans les environnements Windows est équivalent à $TMPDIR dans les environnements UNIX. Si vous utilisez l'interpréteur de commandes bash sur un système Windows, vous pouvez utiliser les conventions UNIX.

Chapitre 1. Planification de l'installation

Consultez les remarques sur le déploiement et les exigences système relatives à Network Manager.

Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Déploiement de Network Manager

Ces informations sont utiles pour la configuration du déploiement physique de votre installation Network Manager.

Scénarios de déploiement

Le mode de déploiement de Network Manager dépend de votre environnement, et notamment de facteurs tels que la taille et la complexité de votre réseau et le nombre d'opérations nécessitant un accès système.

Vous trouverez ci-dessous des scénarios de déploiement de Network Manager standard :

- Déploiement de système éducatif ou de démonstration de petite taille
- Réseau client de petite taille
- Réseau client de taille moyenne
- Réseau de fournisseur de services ou d'entreprise de télécommunications
- Réseau client de grande taille
- Réseau client de très grande taille

Remarque : La reprise en ligne peut ensuite être appliquée à chacun de ces déploiements Network Manager.

Cette section vous aide lors de la prise de décision en matière de mode de déploiement de Network Manager. Pour obtenir des informations plus détaillées, voir les documents *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration* et *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*.

Comparaisons de réseau et de déploiement

Ces informations permettent de comparer les réseaux client exemple et de comparer les déploiements Network Manager pour chaque réseau client exemple.

Comparaison des réseaux client :

Utilisez ces informations pour comparer les exemples de réseaux client et identifier celui qui correspond le mieux à votre réseau.

Le tableau suivant répertorie les fonctions standard pour chacun des exemples de réseaux client. Ces valeurs sont fournies à titre d'exemple uniquement. Elles peuvent être différentes de celles de votre réseau. Vous devez en particulier noter les éléments suivants :

- En ce qui concerne les valeurs indiquées pour *Nombre moyen d'interfaces par périphérique* dans ce tableau, le nombre réel d'interfaces peut varier considérablement par rapport au nombre moyen spécifié. C'est le cas par

exemple des réseaux MPLS dans lesquels le nombre d'interfaces par périphérique est très élevé dans le réseau central et peut être très bas (2 ou 3) pour les périphériques situés à la périphérie.

- En ce qui concerne le nombre de périphériques dans une entreprise de télécommunications, la valeur spécifiée (15 000) est une valeur moyenne. Une entreprise de télécommunications au niveau national comporte un nombre de périphériques bien plus élevé et une petite entreprise locale en aura beaucoup moins.

Tableau 1. Exemples de comparaison de réseaux client

Fonction	**Démonstration**	**Entreprise**				**Telco**
		Petite	**Moyenne**	**Grande**	**Très grande**	
Nombre de périphériques	25	150 à 300	De 250 à 5 000	De 5 000 à 15 000	De 15 000 à 30 000	15 000
Nombre moyen d'interfaces par périphérique	Entre 1 et 2	Entre 3 et 5	20-30	30 ou plus	30 ou plus	1 200
Emplacements réseau	Emplacement unique	Emplacement unique	Répartis	Réseau global	Réseau global, gestion répartie	Un ou plusieurs emplacements
Architecture de réseau	Non hiérarchique	Non hiérarchique	Non hiérarchique	Complexe	Complexe	Complexe
Nombre de clients d'interface graphique actifs	1 à 3	3	5 à 20	5 à 20	5 à 20	5 à 20
Exemples d'interrogation ping de boîtier	Valeurs définies à des fins de démonstration	Intervalles de 2 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes	Entre 2 et 5 minutes
Exemples d'interrogation SNMP	Valeurs définies à des fins de démonstration	3 à 6 valeurs à des intervalles de 30 minutes	Intervalles de 5 à 15 minutes	Intervalles de 10 à 15 minute.	Intervalles de 15 minutes ou plus	5 valeurs à des intervalles de 5 minutes
	Interrogation SNMP v1, 2c ou 3 dans n'importe lequel des environnements répertoriés Interrogations de périphérique et d'interface dans l'un des environnements répertoriés.					
Intégrations de produits Tivoli	Aucune	Aucune	ITM avec TDW	ITM avec TDW TBSM TADDM	ITM avec TDW TBSM TADDM	ITM avec TDW TBSM TADDM
Période de collecte des données de performance	1 à 5 jours	31 jours	31 jours	31 jours	31 jours	7 jours

Comparaison des événements Network Manager :

Utilisez ces informations pour comparer les déploiements Network Manager pour chacun des réseaux client exemples.

Le tableau suivant répertorie les paramètres requis pour les déploiements Network Manager pour chacun des réseaux client exemple. Ces valeurs sont fournies à titre d'exemple uniquement. Elles peuvent être différentes de celles adaptées à votre déploiement spécifique.

Remarque : Les valeurs indiquées pour *Déploiement* dans cette table ne prennent pas en compte les serveurs de reprise en ligne.

Tableau 2. Comparaison d'exemples de déploiement Network Manager

Paramètres	**Démonstration**	**Entreprise**				**Telco**
		Petite	**Moyenne**	**Grande**	**Très grande**	
Plateforme	Windows ou Linux x86	N'importe quelle plateforme prise en charge	N'importe quelle plateforme prise en charge	Linux et UNIX	Linux et UNIX	N'importe quelle plateforme prise en charge
Déploiement	Serveur unique	Serveur unique	1 à 2 serveurs	3 à 4 serveurs	4 serveurs ou plus	3 serveurs
Système client	Processeur unique 2 Go de mémoire DRAM minimum ou 4 Go de mémoire DRAM pour les réseaux étendus Environnement JRE et navigateur Internet pris en charge					
Base de données topologiques	Base de données par défaut	Base de données par défaut	N'importe quel système de gestion de base de données relationnelle	N'importe quel système de gestion de base de données relationnelle	N'importe quel système de gestion de base de données relationnelle	N'importe quel système de gestion de base de données relationnelle
Nombre de domaines réseau	1	1	1 - 2	2 ou plus	2 ou plus	1 - 2
Nombre de moteurs d'interrogation dépendant de la taille du réseau	1	1	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs	Envisagez l'utilisation de plusieurs interrogateurs

Raisons pour lesquelles il existe plusieurs domaines :

Il existe plusieurs raisons pour lesquelles il peut être nécessaire de partitionner votre réseau en plusieurs domaines.

Il peut être nécessaire de partitionner votre réseau en plusieurs domaines pour une des raisons suivantes :

- Votre réseau dépasse une certaine taille définie. Voir la section *Guidelines for number of network domains* afin de déterminer si votre réseau requiert plusieurs domaines.
- La reconnaissance est un processus très long. Vous pouvez réduire cette durée en partitionnant votre réseau en plusieurs domaines.

- Les limites de fonctionnement imposent le besoin de plusieurs domaines. Les limites géographiques et de sécurité sont des limites de fonctionnement.
- Votre réseau contient des adresses IP se chevauchant.

Instructions relatives au nombre de domaines réseau :

Si votre réseau dépasse une certaine taille, il peut être nécessaire de fractionner le réseau en plusieurs domaines. Les instructions fournies permettent de définir le nombre de domaines réseau requis pour votre déploiement. Le nombre de domaines est influencé par le nombre d'entités reconnues, qui dépend des caractéristiques techniques du réseau et des besoins métier qui contrôlent votre environnement.

Selon le système d'exploitation, un seul domaine Network Manager peut prendre en charge environ 250 000 ou 400 000 entités réseau créées pendant une reconnaissance. Les entités réseau comprennent les ports, les interfaces (y compris les éléments d'interface logique), les cartes, les emplacements et les boîtiers. Le tableau suivant identifie pour chaque système d'exploitation compatible, la mémoire maximale prise en charge pour une reconnaissance et le nombre d'entités réseau prises en charge pour chaque domaine Network Manager :

Système d'exploitation	Mémoire maximale pour un processus de reconnaissance	Nombre d'entités de réseau prises en charge pour chaque domaine
Solaris	4 Go	400 000
Linux	4 Go	400 000
zLinux	2 Go	250 000
AIX	3,25 Go (le système d'exploitation se réserve une partie de la plage mémoire du pointeur)	400 000
Windows 2008	2 Go	250 000

Le nombre d'entités de réseau qu'une reconnaissance crée dépend du nombre de facteurs qui peuvent vous obliger à créer et configurer des domaines réseau supplémentaires. Ces facteurs sont les suivants :

- Types de périphériques : par exemple, un routeur Cisco NEXUS ou Juniper avec des instances de routeur virtuel peut fournir des centaines, voire des milliers d'entités de réseau (ports, interfaces, cartes, emplacements, etc.) par châssis.
- Type de réseau : par exemple, une reconnaissance exécutée sur un réseau local fournit plus d'entités de réseau qu'un réseau étendu de taille comparable.
- Types d'agents de reconnaissance activés : par exemple, les agents de reconnaissance Entity et JuniperBoxAnatomy sont des agents de reconnaissance basés sur l'inventaire qui créent généralement des entités de réseau supplémentaires que les autres agents ne créent pas.
- Réseau routé ou commuté : par exemple, les réseaux commutés ont tendance à générer plus d'entités de réseau que les réseaux routés, car ils contiennent des VLAN qui contiennent plusieurs entrées.

La taille d'un domaine Network Manager peut dépendre des besoins de l'entreprise. Par exemple, un client peut nécessiter qu'une reconnaissance de réseau soit exécutée pendant des périodes de maintenance quotidienne spécifiques. Dans ce cas, bien qu'un seul domaine Network Manager exécutant Solaris, Linux ou AIX

puisse prendre en charge environ 400 000 entités réseau, la durée d'une reconnaissance de cette taille peut ne pas être acceptable pour la période de maintenance quotidienne. Par conséquent, deux domaines sectorisés, prenant chacun en charge environ 200 000 entités de réseau, sont nécessaires pour répondre aux besoins de l'entreprise.

La procédure suivante permet de déterminer le nombre de domaines requis. Pour obtenir des informations sur le mode de création et de configuration de domaines réseau supplémentaires, voir le document *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Remarque : Les calculs présentés ici incluent uniquement des chiffres approximatifs. Le nombre de domaines varie en fonction de divers facteurs, y compris les facteurs décrits précédemment.

1. Rassemblez les données suivantes :
   - Nombre de périphériques dans le réseau
   - Nombre moyen d'interfaces par périphérique

     Remarque : Le nombre réel d'interface sur un périphérique donné peut être très éloigné du nombre moyen d'interfaces. Un exemple est disponible dans les réseaux MPLS, où le nombre d'interfaces par périphérique est très élevé dans le réseau principal, mais peut ne pas être supérieur à deux ou trois interfaces par périphérique dans les périphériques extérieurs.
2. Appliquez l'équation suivante pour déterminer un nombre approximatif d'entités réseau :

   Nombre d'entités réseau = Nombre de périphériques * nombre d'interfaces moyen * *multiplicateur*

   Où :
   - *multiplicateur* = 2 pour un réseau acheminé
   - *multiplicateur* = 3,5 pour un réseau commuté

   Remarque : Les réseaux commutés ont tendance à générer plus d'entités réseau car ils contiennent des réseaux virtuels locaux qui contiennent plusieurs entités.
3. Appliquez l'une des équations suivantes pour déterminer le nombre de domaines réseau suggéré :

   Nombre de domaines requis= (nombre d'entités réseau) / 250 000

   où 250 000 est le nombre maximal suggéré d'entités réseau d'un domaine pour les systèmes d'exploitation qui prennent en charge ce nombre d'entités réseau.

   Nombre de domaines requis = (Nombre d'entités réseau) / 400 000

   où 400 000 est le nombre maximal suggéré d'entités réseau d'un domaine pour les systèmes d'exploitation qui prennent en charge ce nombre d'entités réseau.

   Remarque : Le nombre maximal d'unités réseau indiqué ne constitue qu'une estimation approximative de la taille des domaines. Le nombre réel d'entités réseau par domaine varie en fonction de différents facteurs, y compris les facteurs décrits précédemment.

Client de type routeur

Les données de ce client sont les suivantes :

- Nombre de périphériques du réseau : 15 000
- Nombre moyen d'interfaces par périphérique : 20

Ce client est en cours d'exécution sous Linux (qui prend en charge les 400 000 entités réseau).

Ce réseau client génère approximativement 600 000 entités réseau :
Nombre d'entités réseau = 15 000 * 20 * 2 = 600 000

Selon le calcul suivant, le réseau nécessite *deux* domaines de réseau :
Nombre de domaines requis = 600 000 / 400 000 = 1,5

Client de type commutateur

Les données de ce client sont les suivantes :

- Nombre de périphériques du réseau : 1 000
- Nombre moyen d'interfaces par périphérique : 24

Ce client est en cours d'exécution sous Solaris (qui prend en charge les 400 000 entités réseau).

Ce réseau client génère approximativement 84 000 entités réseau :
Nombre d'entités réseau = 1 000 * 24 * 3,5 = 84 000

Selon le calcul suivant, ce réseau requiert *un* domaine réseau :
Nombre de domaines requis = 84 000 / 400 000 < 1

Etape suivante

- Créez et configurez les domaines réseau supplémentaires. Pour plus d'informations sur la création et la configuration de domaines réseau supplémentaires, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.
- Fix Pack 4 Pour lier les domaines reconnus dans une même topologie de réseau, configurez la fonction de reconnaissance interdomaine.

Déploiement de système éducatif ou de démonstration

Il s'agit d'une petite installation à utiliser en tant que système de démonstration ou à des fins éducatives ou de formation.

Les sections suivantes décrivent ce réseau de manière détaillée et incluent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Cet environnement se compose d'environ 25 périphériques réseau et de serveurs de clés. Tous les périphériques se trouvent à un emplacement, sur le même sous-réseau que les périphériques à gérer. Il existe une session client d'interface graphique locale prise en charge par la machine qui héberge les composants du produit Network Manager. Il peut exister une ou deux sessions client d'interface graphique sur d'autres machines. Les périphériques réseau proviennent de plusieurs fournisseurs. L'architecture réseau n'est pas hiérarchique. Tous les périphériques sont connectés à un réseau local et ont des connexions Fast Ethernet. A des fins de démonstration uniquement, plusieurs périphériques réseau disposent de SNMPv3 et plusieurs postes de travail d'IPv6.

Dans l'environnement, les conditions suivantes s'appliquent :

- 1 à 3 clients d'interface graphique actifs.

- L'interrogation ping de boîtier et des activités d'interrogation SNMP sont requises.
- Aucun produit Tivoli principal n'est intégré au système, autre que le produit Tivoli Netcool/OMNIbus requis.
- Des rapports de performances sont requis pour de courtes périodes de collecte de données (généralement, 1 à 5 jours) en fonction de la durée de la formation.

Déploiement de Network Manager

Un déploiement de serveur unique est suffisant pour ce type d'environnement. En plus de la description du déploiement à serveur unique disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Plateforme Windows ou Linux.
- Le système est une machine de classe de poste de travail d'entrée, avec 4 à 6 Go de mémoire, de préférence un processeur double coeur mais un processeur comportant un seul coeur est admis, une vitesse de processeur en cours raisonnable et une fonction Fast Ethernet.
- Base de données par défaut utilisée pour la base de données NCIM.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de petite taille

Ce client est une entreprise avec un réseau se composant d'environ 150-300 périphériques réseau et de serveurs principaux. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et offrent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

Les principaux utilisateurs du produit sont les membres de l'équipe de gestion du réseau. Tous les périphériques se trouvent à un seul emplacement et sont gérés par une équipe comportant peu de membres. Les périphériques réseau proviennent de plusieurs fournisseurs. Un mélange de périphériques réseau de couche 2 et 3 sont présents. 20 à 30 réseaux VLAN sont définis. L'architecture réseau est relativement simple. Tous les périphériques à gérer se trouvent dans le même réseau que le système Network Manager et ont des connexions Fast Ethernet. Les connexions Internet transitent via un pare-feu et l'accès aux systèmes dans le réseau protégé est disponible via un réseau VPN d'entreprise. L'équipe de gestion du réseau assure la connexion des clients via un des moyens suivants : réseau local, connexions WiFi ou via un réseau VPN établi par un fournisseur de services de télécommunication. Les modifications réseau ont lieu une fois par mois et une nouvelle reconnaissance est alors anticipée.

Dans cet environnement, les conditions suivantes s'appliquent :

- 3 clients d'interface graphique actifs.
- Interrogation ping de boîtier à des intervalles de deux minutes. Interrogation SNMP à des intervalles de 30 minutes. Généralement, l'interrogation est requise pour trois à six valeurs MIB SNMP.

- Aucun produit Tivoli principal n'est intégré au système, autre que le produit Tivoli Netcool/OMNIbus requis.
- Des rapports de performances sont requis pour des périodes de collecte de données sur une base de 31 jours.

Déploiement de Network Manager

Un déploiement de serveur unique est suffisant pour ce type d'environnement. En plus de la description du déploiement à serveur unique disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Un domaine réseau unique est suffisant pour un réseau de cette taille.
- Le système peut être une des plateformes prises en charge. Le système requiert de 6 à 8 Go de mémoire, un processeur double coeur et plusieurs disques physiques dans une configuration RAID 5.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Base de données par défaut utilisée pour la base de données NCIM.
- Un moteur d'interrogation ncp_poller unique est suffisant pour cet environnement.
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de taille moyenne

Ce client est une entreprise avec un centre de données central principal et des connexions à différents sites distants. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et offrent des suggestions pour un déploiement de Network Manager afin de répondre aux besoins de ce réseau.

Description

Ce réseau contient entre 250 et 5 000 périphériques réseau et serveurs principaux importants. Les postes de travail ne sont pas gérés lorsque leur nombre est supérieur à 1 000. Les périphériques réseau proviennent de plusieurs fournisseurs. Tous les périphériques de l'emplacement central ont des connexions Fast Ethernet ou Gigabit Ethernet. Les sites distants sont connectés via des liaisons WAN. Les périphériques et les serveurs à gérer sont répartis entre le site central et les sites distants.

Dans l'environnement, les conditions suivantes s'appliquent :

- Il existe 5 à 20 clients d'interface graphique actifs.
- Interrogation ping de boîtier à des intervalles de deux à cinq minutes. Interrogation SNMP à des intervalles de 5 à 15 minutes.
- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis : IBM Tivoli Monitoring avec Tivoli Data Warehouse exécutant DB2 pour la prise en charge de génération de rapports de performances.
- Des rapports de performances sont requis pour des périodes de collecte de données sur une base de 31 jours.

Network Manager déploiement

Chaque environnement client avec ce type de réseau est différent. La clé du succès est une mémoire appropriée et une connaissance approfondie des cibles d'interrogation, des taux d'interrogation combinés et des taux d'événement. Les paramètres de déploiement suivants sont appropriés pour ce type d'environnement.

- Un ou deux domaines réseau sont requis, en fonction de la taille du réseau.
- Déploiement sur un serveur unique

  Au minimum quatre processeurs, jusqu'à huit processeurs pour deux domaines ou de 10 à 20 utilisateurs simultanés Tivoli Integrated Portal

  Au minimum de 12 Go, jusqu'à 32 Go de mémoire pour un grand réseau dans le réseau client moyen ou 10 à 20 utilisateurs Tivoli Integrated Portal

  Plusieurs disques physiques dans une configuration RAID 5
- Le système peut être une des plateformes prises en charge.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Tout système SGBDR utilisé pour la base de données NCIM.
- Nombre de moteurs d'interrogation :

  Déploiement à un seul serveur : 1

  Déploiement à deux serveurs : Un interrogateur pour les opérations ping de boîtier, au moins deux interrogateurs pour les interrogations SNMP
- Nombre de moteurs d'interrogation : un au minimum, avec au moins deux nécessaires en fonction des besoins d'interrogation.

Réseau client de grande taille

Ce client est une entreprise de grande taille avec un réseau globalement déployé. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs et de prendre en charge les périphériques et l'architecture réseau les plus récents.

Les sections suivantes décrivent ce réseau de manière détaillée et offrent des suggestions pour un déploiement de Network Manager afin de répondre aux besoins de ce réseau.

Description

L'architecture du réseau est complexe et contient la technologie la plus récente. Par exemple, le réseau contient des réseaux centraux MPLS. Le nombre de périphériques réseau est compris entre 5 000 et 15 000. La présence d'au moins 30 ports par périphérique indique qu'il s'agit d'un réseau complexe. Les opérations réseau sont effectuées à partir d'un emplacement central avec une équipe surveillant en permanence le réseau central. Les périphériques réseau proviennent de plusieurs fournisseurs.

Dans l'environnement, les conditions suivantes s'appliquent :

- Il existe généralement 5 à 20 clients d'interface graphique actifs simultanément.
- Interrogation :

  Interrogation ping de boîtier à des intervalles de deux à cinq minutes.

  Interrogation SNMP à des intervalles de 10-15 minutes.

  Interrogation SNMPv3 des périphériques réseau principaux

Interrogation SNMPv1 pour le traçage de graphique en temps réel ainsi que pour le stockage des rapports de performances.

- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis :

  IBM Tivoli Monitoring (ITM) avec Tivoli Data Warehouse (TDW) exécutant DB2 pour la prise en charge de génération de rapports de performances.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Des rapports de performances sont requis pour des périodes de collecte de données sur une base de 31 jours.

Déploiement de Network Manager

Les choix de déploiement varient en fonction de la taille du réseau. Pour le réseau à 1 000 périphériques de cette plage de clients, le déploiement peut comporter un seul serveur ou deux serveurs. Les facteurs clé pour la réussite incluent le temps de réponse réseau pour les cibles (à condition qu'il s'agisse d'une distribution pays ou globale des périphériques cible), la disponibilité de la mémoire sur les serveurs de prise en charge, l'interrogation sélectionnée et la fréquence d'interrogation.

Pour la partie supérieure du réseau (15 000 périphériques environ), un déploiement distribué comportant plusieurs domaines est requis. En plus de la description du déploiement à plusieurs serveurs disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Déployez au minimum deux domaines avec un serveur pour chaque groupe de deux domaines.
- Le déploiement d'un serveur de base de données dédié est recommandé.
- Le déploiement d'un serveur dédié pour héberger Tivoli Integrated Portal et Tivoli Netcool/OMNIbus est recommandé.
- Chaque serveur requiert les éléments suivants :

  Quatre processeurs.

  32 Go de mémoire.

  3 disques, grappe de disques multiple RAID 5
- Pour les systèmes utilisés pour chaque domaine, effectuez le déploiement de la manière suivante :

  Serveur 1 : Network Manager

  Serveur 2 : Tivoli Netcool/OMNIbus et Tivoli Integrated Portal

  Système 3 (facultatif) : SGBDR sélectionné par le client prenant en charge les deux domaines
- Systèmes à déployer sur la plateforme Linux ou UNIX.
- Tout système SGBDR utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation minimum sont recommandés :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.

  Créez un élément ncp_poller séparé pour les interrogations SNMP.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau client de très grande taille

Ce client est une entreprise globale de très grande taille avec une architecture réseau simple mais un grand nombre de périphériques. L'objectif de cette installation est de gérer ce réseau client en signalant à l'équipe de production les principales erreurs et de prendre en charge la planification de capacité à court terme.

Les sections suivantes décrivent ce réseau de manière détaillée et offrent des suggestions pour un déploiement Network Manager afin de répondre aux besoins de ce réseau.

Description

La gestion réseau est effectuée à partir d'un emplacement central et à partir d'emplacements régionaux. Le réseau est très grand et contient plus de 15 000 périphériques réseau et serveurs importants Les périphériques réseau proviennent de plusieurs fournisseurs. Les périphériques sont rassemblés en deux catégories :

- Infrastructure de périphériques réseau avec un nombre d'interfaces supérieur ou égal à 30 par périphérique.
- Périphériques gérés avec 1 à 2 interfaces par périphérique.

La plupart des périphériques se trouvent dans la deuxième catégorie (périphériques gérés). Pour gérer un réseau de cette taille, le réseau est partitionné pour la gestion sur une base géographique.

Dans l'environnement, les conditions suivantes s'appliquent :

- Il existe 5 à 20 clients d'interface graphique actifs.
- Interrogation:

  Interrogation ping de boîtier à des intervalles de deux à cinq minutes.

  Interrogation SNMP à des intervalles égaux ou supérieurs à 15 minutes.

  Collecte de données SNMPv1
- Différents principaux produits Tivoli intégrés au système, autres que le produits Tivoli Netcool/OMNIbus requis :

  IBM Tivoli Monitoring (ITM) avec Tivoli Data Warehouse (TDW) exécutant DB2 pour la prise en charge de génération de rapports de performances.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Des rapports de performances sont requis pour des périodes de collecte de données sur une base de 31 jours.

Déploiement de Network Manager

Une assistance d'un groupe de services IBM expérimentés ou d'un partenaire métier IBM qualifié est hautement recommandée pour que le déploiement puisse aboutir. Plusieurs domaines sont requis, pris en charge par une collecte de serveurs individuels ou s'exécutant sur un système de très grande taille. Après avoir effectué une enquête sur le réseau à gérer, fractionnez le réseau en sections incluant environ 300 000 à 400 000 entités de réseau, puis définissez chacune de ces sections comme domaine. En plus de la description du déploiement à plusieurs serveurs disponible ici, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Plusieurs domaines réseau.

- Sélections de plateforme : Linux et UNIX.
- Les systèmes de grande taille (grand nombre de processeurs et quantité de mémoire importante) peuvent héberger plusieurs domaines tant que les allocations de mémoire et le nombre de processeurs sont acceptables.

  Mémoire : 16-32 Go par domaine

  Processeurs : 4-8 par domaine en fonction des charges de travail
- Tout système SGBDR utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation au minimum par domaine :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.

  Créez un élément ncp_poller séparé pour les interrogations SNMP.
- Les limitations de mémoire de processus individuel constituent un facteur dans cet environnement. En cas d'utilisation d'AIX, activez l'accès à la mémoire de grande taille.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Réseau d'entreprise de télécommunications

Ce client est une société de télécommunications et un fournisseur de services Internet. L'objectif de cette installation est de gérer ce réseau client en signalant 24 heures sur 24 et 7 jours sur 7 à l'équipe de production les principales erreurs.

Les sections suivantes décrivent ce réseau de manière détaillée et offrent des suggestions pour un déploiement Network Manager afin de répondre aux besoins du réseau.

Description

Le réseau à gérer contient environ 300 périphériques réseau avec un nombre moyen d'interfaces par périphérique égal à 500. Il s'agit d'un réseau MPLS. Par conséquent, le nombre d'interfaces des périphériques réseau est élevé et les périphériques réseau sont complexes. Les périphériques réseau proviennent de plusieurs fournisseurs. Tous les périphériques se trouvent à un seul emplacement ou à plusieurs emplacements et sont gérées par une équipe comportant peu de membres. Tous les périphériques à gérer sont connectés via Fast Ethernet ou Gigabit Ethernet.

Dans l'environnement, les conditions suivantes s'appliquent :

- Nombre de clients simultanément actifs : 5-20.
- Exigences d'interrogation : interrogation ping de boîtier à des intervalles de 2 à 5 minutes ; interrogation SNMP de cinq valeurs à des intervalles de 5 minutes.
- Certaines interrogations SNMPv3 sont en place.
- Autres principaux produits Tivoli intégrés au système, autres que le produit Tivoli Netcool/OMNIbus requis :

  IBM Tivoli Monitoring (ITM) avec Tivoli Data Warehouse (TDW) exécutant DB2 pour la prise en charge de génération de rapports de performances.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Rapports de performances effectués une fois par jour pour les principaux périphériques, utilisés pour la création des rapports de capacité hebdomadaires.

Déploiement de Network Manager

Un déploiement à trois serveurs est requis pour ce type d'environnement. En plus de la description du déploiement à plusieurs serveurs disponible à un autre emplacement, les paramètres de déploiement suivants sont adaptés à ce type d'environnement.

- Un ou deux domaines.
- Un déploiement à trois serveurs est recommandé.
- Spécifications du système

  Système 1 : deux à quatre processeurs, 6 à 8 Go de mémoire, deux disques ou plus

  Système 1 : pour héberger les composants Network Manager : quatre processeurs, de 16 à 32 Go de mémoire, au moins deux disques. Notez qu'au delà de quatre processeurs ou coeurs de processeur, la vitesse d'horloge des coeurs et la mémoire cache intégrée peuvent s'avérer plus importantes que des coeurs supplémentaires. La règle générale est la suivante : sélectionnez les 4 coeurs les plus rapides avant les autres coeurs.

  Système 2 : pour héberger la base de données NCIM : de deux à quatre processeurs, de 16 à 32 Go de mémoire, au moins deux disques dans une configuration RAID adaptée pour fournir la tolérance aux pannes et les performances nécessaires.

  Système 3 : pour héberger Tivoli Integrated Portal et Tivoli Netcool/OMNIbus : quatre processeurs, 16 Go de mémoire.
- Tout système SGBDR utilisé pour la base de données NCIM.
- Deux moteurs d'interrogation au minimum :

  Utilisez le processus ncp_poller par défaut pour l'interrogation ping de boîtier.

  Créez un élément ncp_poller distinct pour les interrogations SNMP.
- Système client : processeur unique, 3 Go de mémoire, navigateur Internet et JRE pris en charge
- Le support à double pile IPv6 est requis lorsque des postes de travail ou des périphériques réseau incluent IPv6.

Remarques relatives au déploiement

Vous pouvez déployer l'ensemble de l'installation Network Manager sur un serveur unique ou dans une installation répartie.

Au cours d'une installation de Network Manager, vous installez les quatre composants Network Manager ci-dessous.

Composant central Network Manager
: Ce composant est constitué des processus Network Manager centraux suivants : reconnaissance de réseau, interrogation, analyse de la cause première et enrichissement des événements.

base de données NCIM
: Cette base de données stocke les données de topologie. Vous pouvez choisir d'installer la base de données Informix par défaut ou utiliser une base de données MySQL, DB2, Informix ou Oracle existante.

Tivoli Netcool/OMNIbus
: Ce composant est constitué du logiciel de gestion des événements Tivoli Netcool/OMNIbus. Un grand nombre de clients optent pour un système de génération de ticket d'incident intégré à Tivoli Netcool/OMNIbus.

Tivoli Integrated Portal
Ce composant est constitué de la structure d'interface utilisateur Tivoli Integrated Portal, associée aux applications web.

L'installation a pour objet de placer ces composants sur un ou plusieurs serveurs.

Les configurations de déploiement standard de Network Manager sont les suivantes :

- Déploiement sur un serveur unique
- Déploiement réparti : deux serveurs ou plus

Les facteurs qui exigent un nombre croissant de serveurs dans un déploiement réparti incluent les suivants :

- Débits d'événements actifs
- Quantité et débit des données d'interrogation stockées
- Début d'interrogation du statut d'unité et nombre de cibles d'interrogation
- Temps de réponse du réseau pour les cibles interrogées
- Fréquence de reconnaissance et
- Taille du réseau à reconnaître (pour chaque domaine comportant plusieurs domaines)

Remarque : Ces configurations de déploiement ne prennent pas en compte les exigences d'intégrations d'autres produits.

De plus, vous devez prendre en compte le déploiement des systèmes appropriés pour prendre en charge les sessions client d'interface graphique.

En outre, le support à double pile IPv6 est requis lorsque les postes de travail ou les périphériques réseau utilisent IPv6.

Déploiement sur un serveur unique

Les déploiements sur un serveur unique sont adaptés aux systèmes de démonstration ou de formation de petite taille et pour les systèmes devant prendre en charge des réseaux client de petite ou de moyenne taille.

Un déploiement sur un serveur unique doit être conforme à la spécification minimale suivante :

- Minimum deux processeurs de vitesse en cours, quatre processeurs recommandés. Les exemples de vitesse en cours incluent 3 GHz ou plus pour les processeurs de la ligne de produit Intel et 1,6 GHz ou plus pour les processeurs de la ligne de produit Sun.
- 6 Go de mémoire minimum, 8 Go recommandés.

Déploiement réparti : deux serveurs ou plus

Dans les déploiements répartis, les composants Network Manager sont répartis sur plusieurs serveurs, c'est-à-dire sur deux serveurs ou plus. Voici quelques instructions concernant les déploiements répartis :

- Les déploiements sur deux serveurs concernent la gamme supérieure de la famille de réseaux client de taille moyenne.
- Les déploiements peuvent exiger trois serveurs ou plus dans les situations où il existe plusieurs domaines réseau.

- Les déploiements sur trois serveurs peuvent également être appliqués dans le cas où un serveur séparé est requis pour prendre en charge un produit de base de données relationnelle qui fournit un stockage des données de topologie. De plus, un serveur de base de données séparé autorise la base de données relationnelle à prendre en charge plusieurs applications, en plus de Network Manager.

Déploiement sur deux serveurs

Un exemple de déploiement sur deux serveurs est constitué de l'allocation suivante de postes de travail hôte :

- *Serveur 1* : Les composants Network Manager centraux et la base de données NCIM. Les composants centraux sont les composants de reconnaissance de réseau, d'interrogation, d'analyse de la cause première et d'enrichissement des événements.
- *Serveur 2* : Tivoli Integrated Portal avec applications Web Network Manager associées.

Dans ce déploiement sur deux serveurs, chaque serveur doit être conforme aux spécifications minimales suivantes :

- Minimum deux processeurs de vitesse en cours, quatre processeurs recommandés.
- 8 Go de mémoire minimum nécessaires.
- Pour améliorer le temps de réponse des rapports de performance, système d'E-S sur disque amélioré, constitué de 3 à 6 disques physiques de type RAID prenant en charge un volume logique.

Déploiement sur trois serveurs

Un exemple de déploiement sur trois serveurs est constitué de l'allocation suivante de postes de travail hôte :

- *Serveur 1* : Composants centraux Network Manager.
- *Serveur 2* : Tivoli Netcool/OMNIbus
- *Serveur 3* : Tivoli Integrated Portal avec les applications web Network Manager associées, ainsi que la base de données NCIM.

Systèmes client

Vous devez prendre en compte le déploiement de systèmes appropriés pour prendre en charge les sessions client d'interface graphique.

La spécification système suivante permet de prendre en charge une gamme plus large d'activités d'utilisateur final dans les sessions client d'interface graphique :

Remarque : Les clients d'application web, et notamment la liste d'événements actifs de l'interface graphique Web Tivoli Netcool/OMNIbus et les vues de réseau Network Manager, Tronçon et Navigateur de structure, sont fondées sur Java et dépendent des performances du système client. Il convient donc que la mémoire et les performances d'UC du système client soient les plus élevées possible.

- Windows 2008 ou Windows 7
- Ecran plus large permettant un affichage plus confortable avec une résolution plus élevée (par exemple, 1280x1024)
- Processeur à un ou deux coeurs à la vitesse actuelle

- 3 Go de mémoire
- Environnement JRE et navigateur Internet pris en charge
- Fast Ethernet.
- Spécification du processeur :

  Pour les affichages de topologie normaux ou les affichages d'événements
  Processeur unique offrant les vitesses suivantes : 1 GHz ou supérieur, comme sur de nombreux ordinateurs portables, 2,4 GHz comme sur de nombreux postes de travail

  Durée supérieure pour l'affichage de mappes de topologie plus complexes et de plus grande taille et l'affichage avancé de graphiques MIB
  Processeur de dernière génération (3,0 GHz ou supérieur) généralement disponible sur les systèmes de classe de poste de travail les plus récents.

Exemples de déploiements

Utilisez ces exemples de Network Manager pour planifier votre architecture de déploiement.

Contraintes d'installation et de démarrage des composants

Certains composants doivent être installés et démarrés avant d'autres. Utilisez ces informations et les exemples d'installations pour comprendre l'ordre dans lequel vous devez installer et démarrer les composants.

Contraintes de la base de données topologiques

Vous devez installer une base de données topologiques avant d'installer les composants principaux de Network Manager ou lors du même processus d'installation.

Vous devez installer une base de données topologiques avant d'installer les applications Web de Network Manager (y compris Tivoli Integrated Portal) ou au cours du même processus d'installation.

Vous devez créer des tables de base de données uniquement lors de la première installation des composants principaux de Network Manager ou des applications Web de Network Manager (y compris Tivoli Integrated Portal), et non lors d'une installation ultérieure.

Contraintes de Tivoli Netcool/OMNIbus

Vous devez installer Tivoli Netcool/OMNIbus avant d'installer les applications Web de Network Manager (y compris Tivoli Integrated Portal) ou au cours du même processus d'installation.

Contraintes d'une application Web

Vous devez installer les composants principaux de Network Manager avant d'installer les applications Web de Network Manager ou lors du même processus d'installation.

Si vous utilisez l'authentification ObjectServer pour les applications Web de Network Manager, Tivoli Netcool/OMNIbus doit être en cours d'exécution lors de l'installation des applications Web de Network Manager.

Démarrage des composants dans le bon ordre

Ne démarrez pas les composants principaux de Network Manager avant que l'installation des applications Web de Network Manager ne soit terminée.

Vérifiez que Tivoli Netcool/OMNIbus et la base de données topologiques sont en cours d'exécution avant de démarrer les composants principaux de Network Manager.

Assurez-vous que Tivoli Netcool/OMNIbus, la base de données topologiques et les composants centraux Network Manager sont en cours d'exécution avant d'utiliser les applications Web Network Manager.

Référence associée:

«Allocation de serveur pour la reprise en ligne», à la page 319
Tout système principal doit être installé sur un hôte distinct d'un système de sauvegarde, de sorte que s'il tombe en panne, l'hôte de sauvegarde ne soit pas touché.

Exemple d'architecture de déploiement simple

Cet exemple vous permet de vous familiariser avec l'architecture d'un déploiement simple de Network Manager.

Composants

Cet exemple de déploiement simple comporte les composants suivants :

- Une paire virtuelle ObjectServer.
- Un serveur Tivoli Integrated Portal.
- Une installation Network Manager exécutant un domaine avec reprise en ligne.
- Une instance de la base de données topologiques NCIM.

La figure suivante présente l'architecture pour ce déploiement.

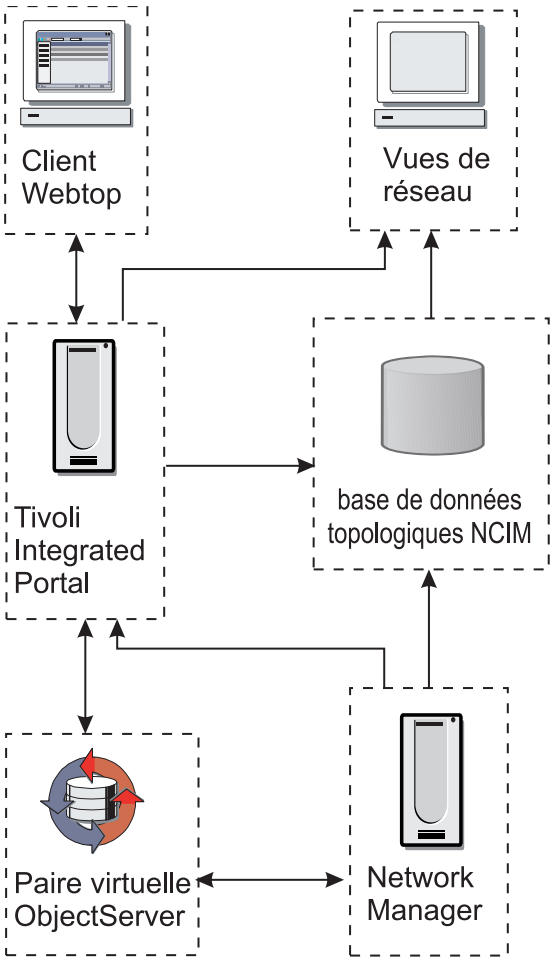

Figure 1. Architecture de déploiement simple

Allocation des postes de travail hôte

La figure suivante illustre l'allocation des postes de travail hôtes pour ce déploiement.

Remarque : Si votre topologie est très importante, vous pouvez installer la base de données topologiques sur un serveur distinct. Ce choix dépend des spécifications de vos machines et de la répartition de la charge souhaitée.

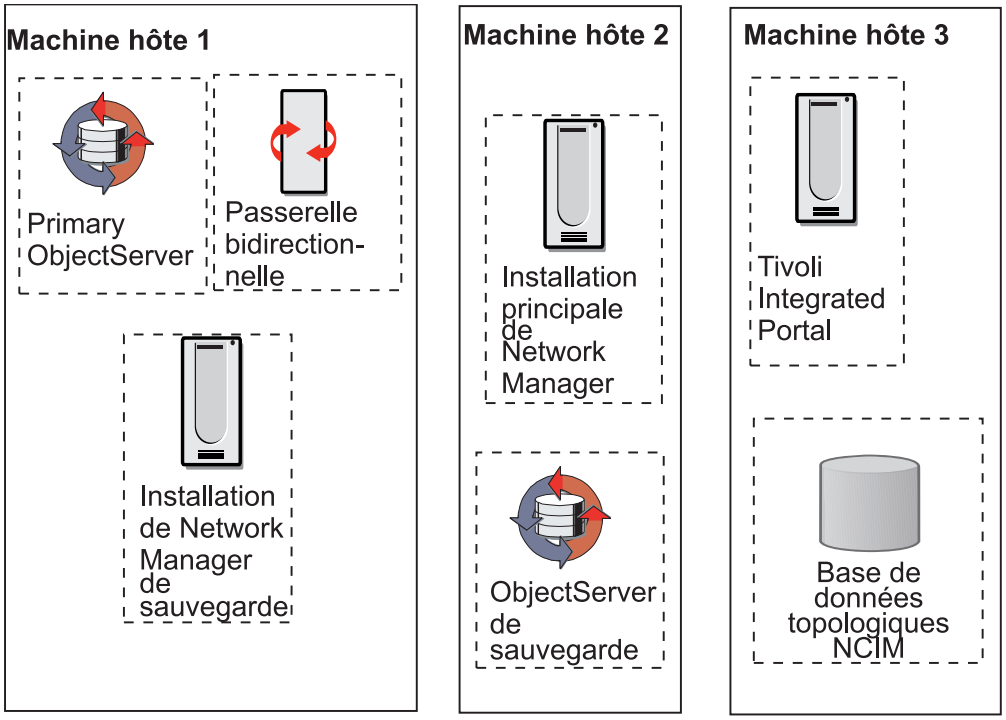

Figure 2. Allocation des machines hôtes pour un déploiement simple

Etapes d'installation d'un déploiement simple

Les étapes ci-après présentent les tâches requises pour ce déploiement et permettent de planifier un déploiement similaire. .

Pour installer le déploiement décrit ci-dessus, procédez comme suit :

1. Installez la base de données topologiques sur la machine hôte 3, créez les tables nécessaires et lancez la base de données.

   Remarque : La base de données topologiques doit être installée et démarrée avant le démarrage des composants centraux de Network Manager afin de pouvoir sauvegarder les données de reconnaissance.
2. Installez les composants ObjectServer et les composants liés suivants :
   a. Installez le serveur ObjectServer principal et la passerelle bidirectionnelle sur la machine hôte 1.
   b. Installez l'ObjectServer de sauvegarde sur la machine hôte 2.
3. Configurez et exécutez les serveurs ObjectServer.

   Remarque : Ces derniers doivent être en cours d'exécution avant le démarrage des composants centraux de Network Manager.
4. Installez les composants centraux du Network Manager principal sur la machine hôte 2.
5. Installez les composants centraux du Network Manager de sauvegarde sur la machine hôte 1.
6. Installez les applications Web Network Manager sur la machine hôte 3 (catégorie des **composants d'interface graphique** dans l'assistant d'installation).

   Le serveur Tivoli Integrated Portal est installé automatiquement lors de l'installation des applications Web Network Manager.

Conseil : Les performances de la machine sont meilleures si vous installez Tivoli Integrated Portal sur une machine où aucun autre produit n'est installé.

Lorsque vous installez les applications Web Network Manager, l'interface graphique Web Tivoli Netcool/OMNIbus est installée et configurée automatiquement sur la machine hôte 3, si elle n'est pas déjà installée. L'interface graphique Web Tivoli Netcool/OMNIbus était appeléeNetcool/Webtop dans les versions 2.2 et antérieures.

Remarque : Les composants centraux de Network Manager doivent être installés avant les applications Web.

7. Configurez le Network Manager principal pour la reprise en ligne et démarrez-le.
8. Configurez le Network Manager de sauvegarde pour la reprise en ligne et démarrez-le.

Exemple d'architecture de déploiement de grande taille

Utilisez cet exemple pour vous familiariser avec l'architecture d'un déploiement Network Manager de grande taille.

Composants

Ce déploiement exemple comprend :

- Un serveur d'objets et une installation Network Manager à Londres. Le domaine de Londres envoie des événements et la topologie à San Francisco.
- Un serveur d'objets et une installation Network Manager à New York. Le domaine de New York envoie également des événements et une topologie à San Francisco.
- Un serveur d'objets et une installation Tivoli Integrated Portal à San Francisco. Le serveur d'objets de San Francisco consolide les événements issus de Londres et New York. Le serveur Tivoli Integrated Portal de San Francisco peut accéder à la topologie depuis Londres et New York, mais ne consolide pas les topologies. Les clients répartis dans le monde entier peuvent se connecter au serveur Tivoli Integrated Portal et afficher la topologie depuis Londres et New York.

La figure suivante présente l'architecture de ce déploiement.

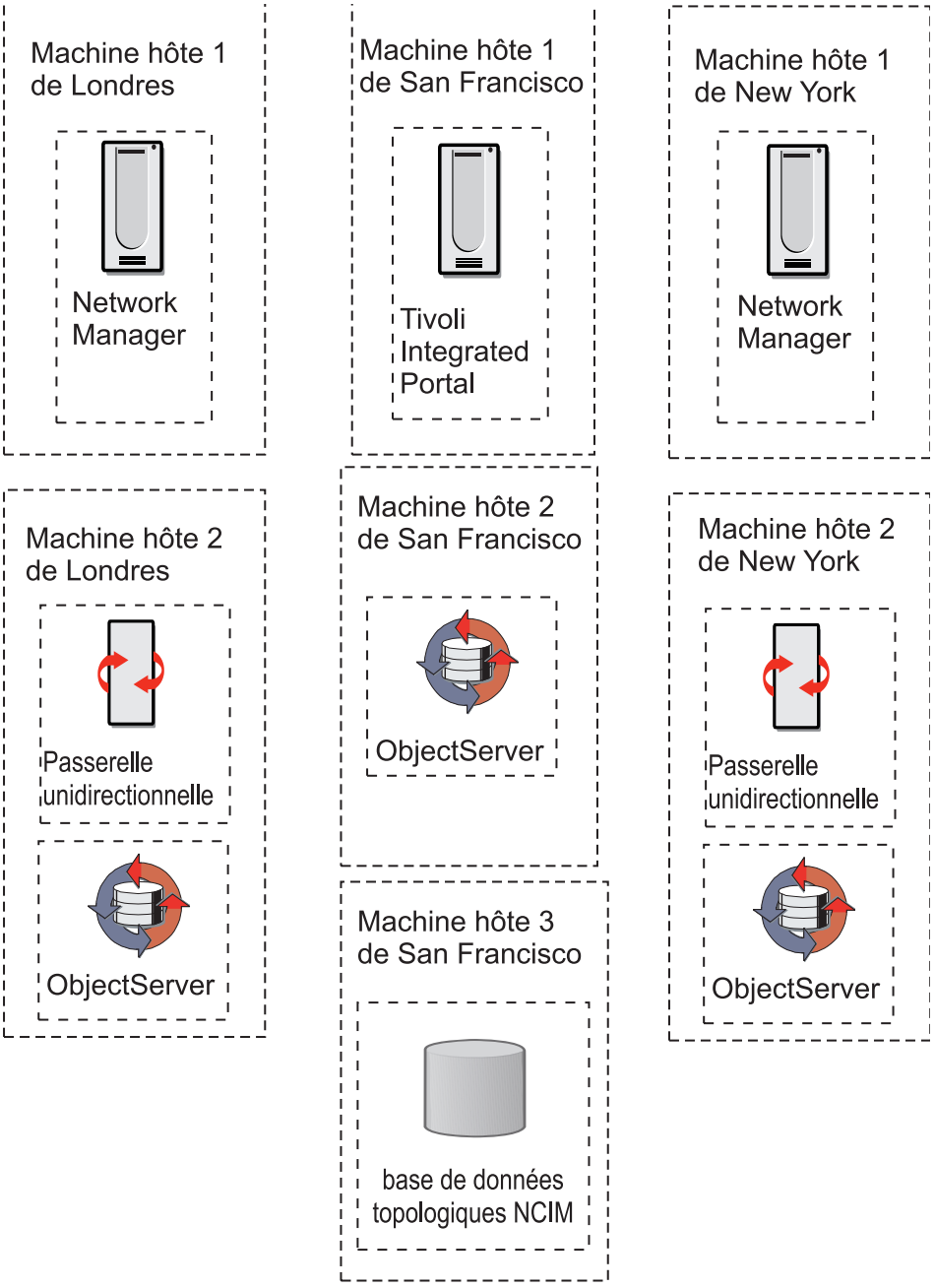

Figure 3. Architecture de déploiement large

Allocation des postes de travail hôte

La figure suivante présente un exemple d'allocation de serveurs pour ce déploiement.

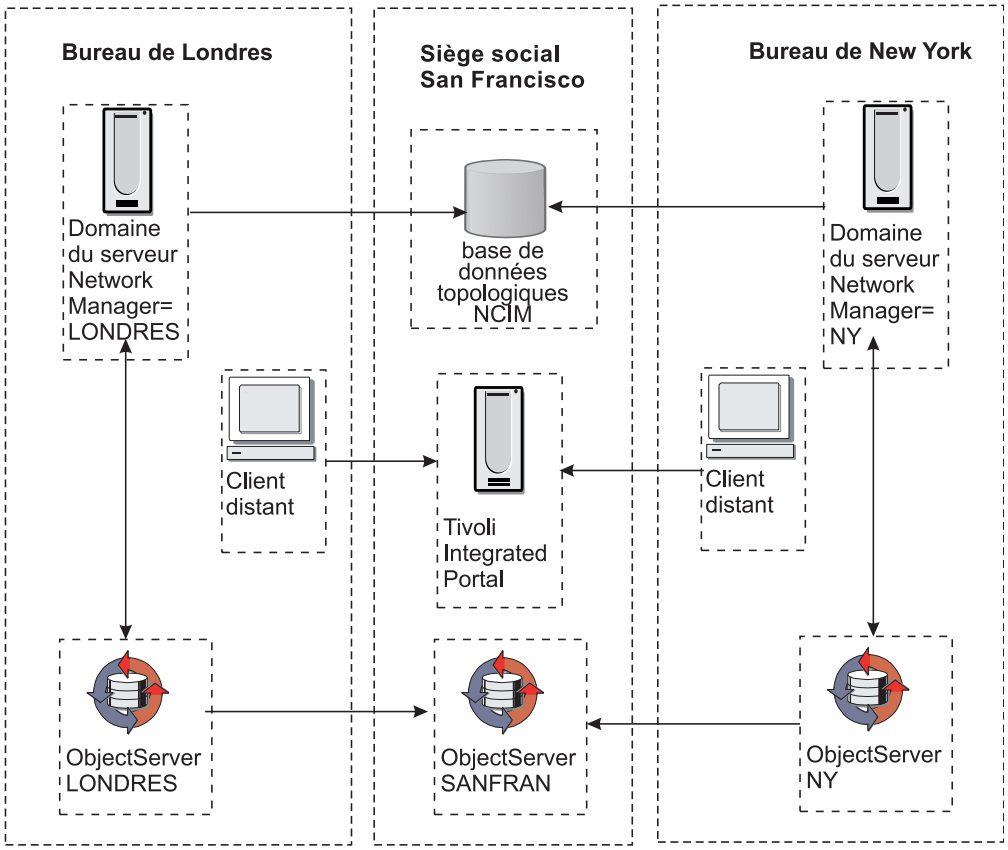

Figure 4. Allocation de machine hôte de déploiement large

Etapes d'installation d'un déploiement de grande taille

Les étapes ci-après présentent les tâches requises pour ce déploiement et permettent de planifier un déploiement similaire. .

Pour installer ce déploiement, accomplissez les étapes suivantes :

1. Installez la base de données topologiques sur la machine hôte 3 de San Francisco et créez les tables de base de données nécessaires.

   Remarque : La base de données topologiques doit être installée et démarrée avant le démarrage des composants centraux de Network Manager afin de pouvoir sauvegarder les données de reconnaissance.
2. Installez les composants ObjectServer et les composants liés suivants :
   - Installez ObjectServer sur la machine hôte 2 de San Francisco.
   - Installez le serveur ObjectServer et la passerelle unidirectionnelle sur la machine hôte 2 de Londres.
   - Installez le serveur ObjectServer et la passerelle unidirectionnelle sur la machine hôte 2 de New York.
3. Configurez et exécutez les serveurs d'objets.

   Remarque : Ces derniers doivent être en cours d'exécution avant le démarrage des composants centraux de Network Manager.
4. Installez les composants principaux de Network Manager sur la machine hôte 1 de Londres.

Remarque : Les composants centraux de Network Manager doivent être installés avant les applications Web.

5. Installez les composants principaux de Network Manager sur la machine hôte 1 de New York.
6. Si une version de l'Netcool/Webtop antérieure à la version 2.1 est déjà présente sur la machine hôte 3, mettez cette version à niveau vers interface graphique Web Tivoli Netcool/OMNIbus version 7.3.1. Network Manager n'est pas compatible avec les versions de l'interface graphique Web Tivoli Netcool/OMNIbus antérieures à la version 2.2.
7. Installez les applications Web Network Manager sur la machine hôte 3 (catégorie des **composants d'interface graphique** dans l'assistant d'installation).

   Le serveur Tivoli Integrated Portal est automatiquement installé lors de l'installation des applications Web Network Manager.

   Conseil : Les performances de la machine sont meilleures si vous installez Tivoli Integrated Portal sur une machine où aucun autre produit n'est installé.

   Lors de l'installation des applications Web Network Manager, l'interface graphique Web Tivoli Netcool/OMNIbus version 7.3.1 est installé et automatiquement configuré sur la machine hôte 3 s'il n'y est pas déjà installé.

Domaines réseau

Avant l'installation, vous devez déterminer si vous souhaitez partitionner votre réseau en domaines ou si vous souhaitez conserver un domaine unique pour l'ensemble de votre réseau. Un domaine réseau est une collection d'entités réseau définie pour être reconnue et gérée.

Restriction : Utilisez uniquement des caractères alphanumériques et des traits de soulignement (_) dans les noms de domaine. Tous les autres caractères, par exemple le tiret (-), sont interdits.

Raisons pour lesquelles partitionner un réseau en plusieurs domaines

Le partitionnement de votre réseau en plusieurs domaines vous permet de reconnaître votre réseau par section. Les raisons pour lesquelles partitionner votre réseau comprennent :

- Evolutivité : il se peut que votre réseau soit trop grand pour être reconnu en une fois.
- Géographie : il se peut que vous souhaitiez diviser votre réseau en régions dont chacune correspond à un domaine.
- Limites du réseau logique : il se peut que vous souhaitiez reconnaître et gérer le réseau en fonction de limites réseau particulières.

Les domaines reconnus peuvent être contrôlés indépendamment.

Vous pouvez exécuter plusieurs domaines afin d'effectuer plusieurs reconnaissances de réseau. De plus, plusieurs processus Network Manager peuvent fonctionner indépendamment sur le même serveur s'ils appartiennent à différentes domaines.

Identification du domaine d'un événement

L'identification du domaine des événements permet aux vues réseau et de tronçon de générer la mappe topologique correcte pour cet événement.

Le domaine dans lequel un événement se produit peut être identifié des manières suivantes :

- En utilisant un domaine par ObjectServer et le nom du serveur ObjectServer pour identifier le domaine dans lequel l'événement s'est produit.
- Lors de l'utilisation de plusieurs domaines par ObjectServer cette fonctionnalité nécessite la configuration de sondes dans chaque domaine pour permettre à l'événement lui même de recueillir des informations identifiant le domaine. Cette approche permet à plusieurs domaines Network Manager d'être connectés à un seul ObjectServer.

Collecte des événements à l'aide d'un seul domaine par ObjectServer

Vous pouvez configurer des domaines Network Manager indépendants à l'aide d'un *ObjectServer de collecte* et d'un *ObjectServer d'agrégation*.

Restriction : L'architecture décrite dans cette rubrique s'applique uniquement aux versions 7.2.1, ou antérieures, de Tivoli Netcool/OMNIbus et se base sur l'architecture ESF (Event Services Framework) standard (ESF) déjà publiée par IBM Tivoli Netcool Advanced Architecture Group.

L'ObjectServer de collecte recueille les événements via les sondes connectées à chaque domaine alors que l'ObjectServer d'agrégation regroupe les événements depuis chaque ObjectServer de collecte.

Par conséquent les domaines Network Manager sont indépendants. Un domaine peut être actif alors qu'un autre peut être inactif pour la maintenance. De plus, les portées de reconnaissance peuvent se chevaucher.

Cette structure est flexible étant donné qu'il est possible d'ajouter d'autres ObjectServer lorsque de nouveaux domaines sont requis. Cela permet de bénéficier d'une évolutivité lors de l'utilisation de réseaux importants. Toutefois, cette approche nécessite plusieurs ObjectServer et est donc plus avantageuse pour les clients disposant de réseaux importants.

La figure suivante illustre un exemple d'architecture utilisant un domaine par ObjectServer.

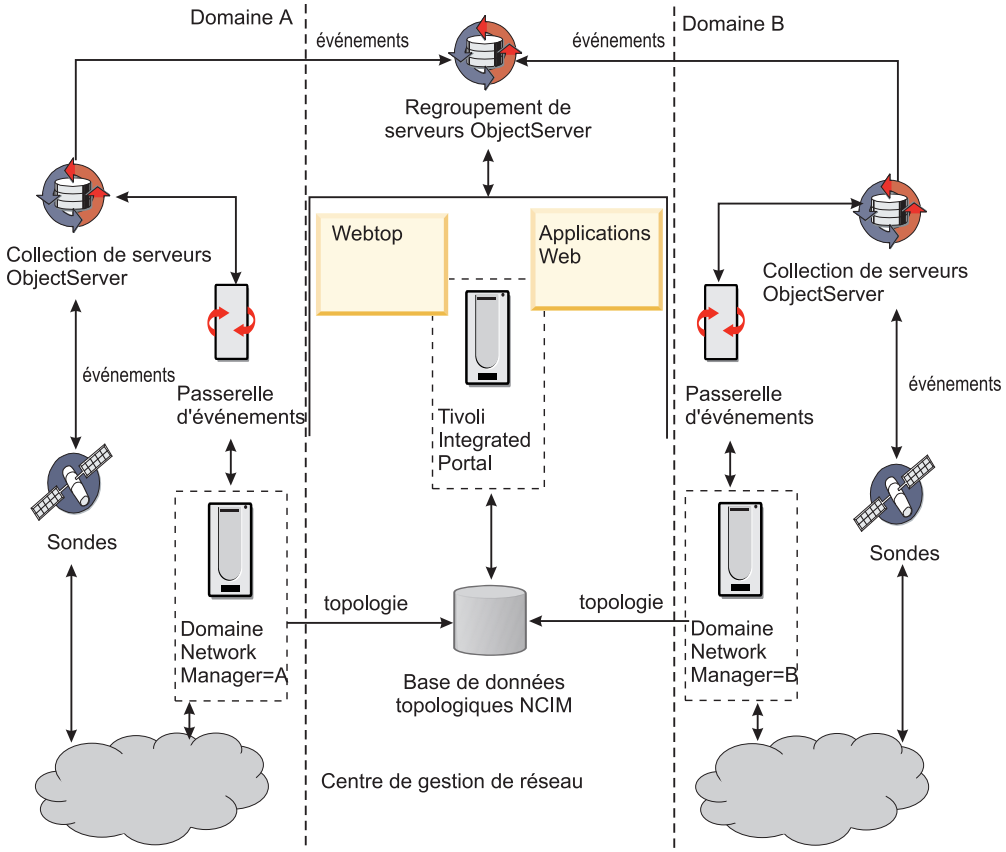

Figure 5. Gestion de la propriété des événements : architecture pour ObjectServer à un seul domaine

Collecte des événements à l'aide de plusieurs domaines par ObjectServer

Vous pouvez connecter plusieurs domaines Network Manager à un même serveur ObjectServer.

Dans cette configuration, les sondes Tivoli Netcool/OMNIbus collectent les informations relatives au nom du domaine lorsqu'un événement est généré et renseignent la zone NmosDomainName afin de conserver ce nom de domaine.

Pour implémenter cette configuration, vous devez d'abord modifier tous les fichiers de règles d'analyse de Tivoli Netcool/OMNIbus pour garantir que chaque événement contienne une zone `NmosDomainName`. Cette zone est utilisée pour stocker le nom de domaine associé à l'événement. Ceci garantit aussi que l'événement est traité par la passerelle d'événements.

Remarque : Par défaut, le filtre d'événement entrant dans la passerelle d'événements gère aussi bien les systèmes à domaine unique que ceux à domaines multiples. Pour plus d'informations, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Remarque : Cette approche est plus économique car elle ne nécessite qu'un seul ObjectServer. L'évolutivité peut être un problème car chaque nouveau domaine nécessite la configuration d'une sonde supplémentaire.

La figure suivante illustre un exemple d'architecture utilisant plusieurs domaines par ObjectServer.

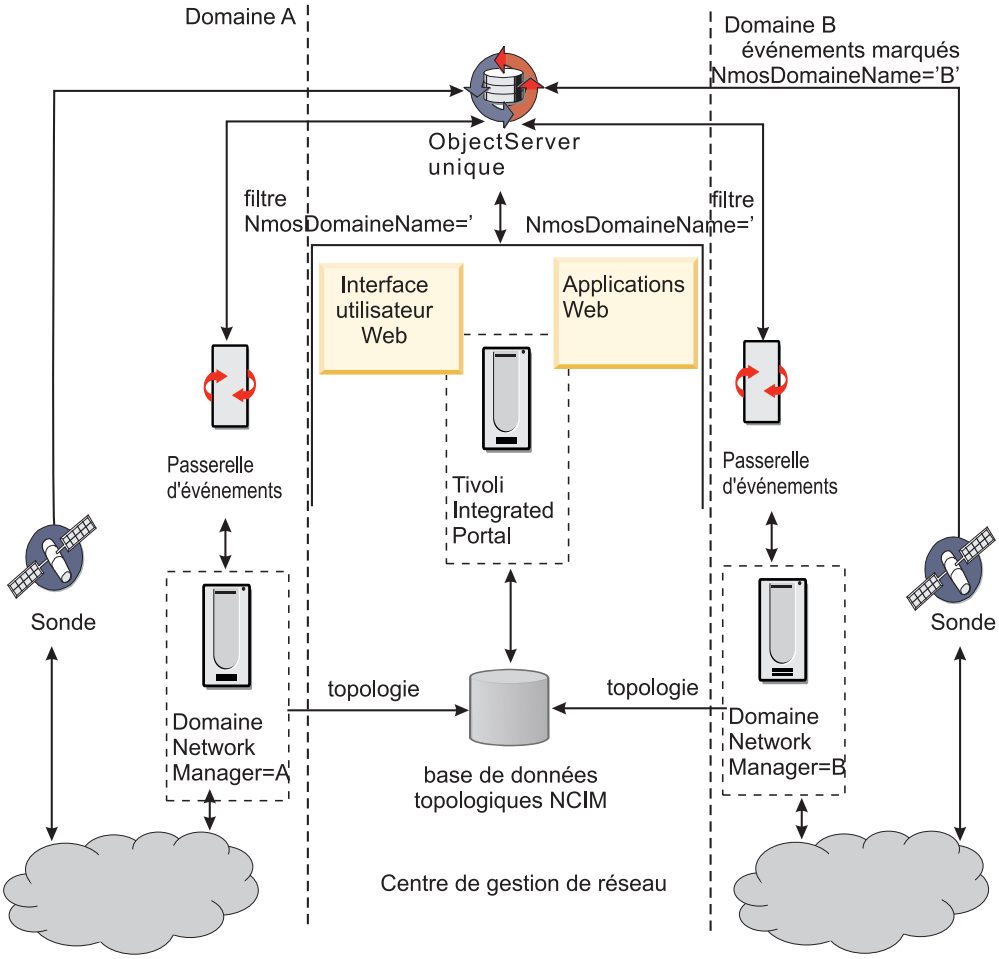

Figure 6. Gestion de la propriété des événements : architecture pour ObjectServer à plusieurs domaines.

Exemple d'affichage d'une topologie depuis plusieurs domaines

Les clients Web utilisant un Tivoli Integrated Portal unique peuvent afficher la topologie depuis plusieurs domaines Network Manager.

Pour plus d'informations sur la visualisation de la topologie, voir *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*.

Pour activer l'affichage de la topologie depuis plusieurs domaines, chaque domaine Network Manager transmet les informations relatives à la topologie à la base de données NCIM (Network Connectivity and Inventory). Lorsque vous disposez de plusieurs domaines, la topologie de chaque domaine est stockée dans la base de données NCIM.

Fix Pack 4

Lien des domaines reconnus

Vous pouvez trouver des liens entre les périphériques dans différents domaines, en configurant et exécutant une reconnaissance interdomaine. La figure suivante montre un exemple de trois domaines de reconnaissance fournissant des données à une seule base de données topologiques NCIM. Dans Tivoli Integrated Portal, vous pouvez afficher les mappes de topologie dans n'importe lequel des domaines en choisissant un seul domaine dans le menu de domaine.

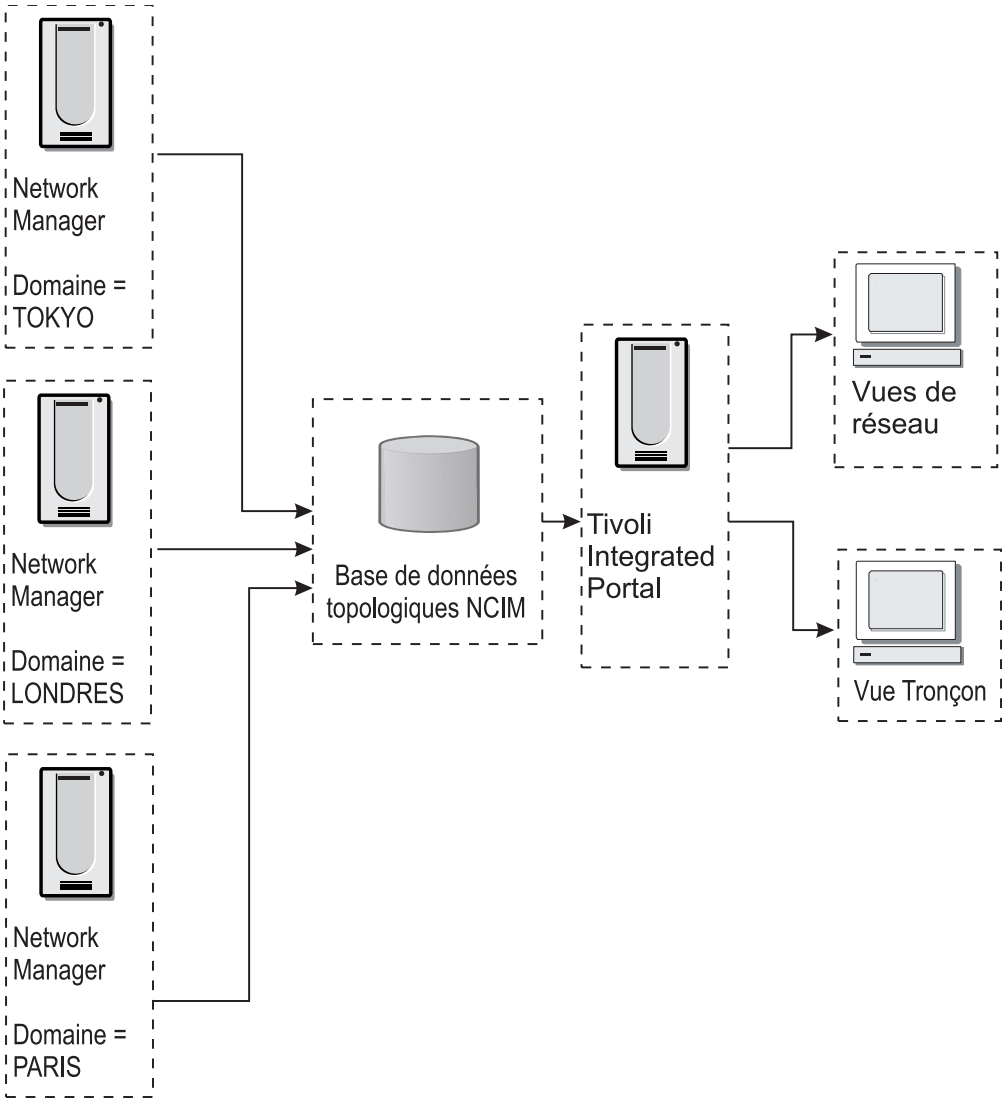

Figure 7. Affichage de la topologie depuis plusieurs domaines

Lorsque des reconnaissances interdomaines sont exécutées, un domaine agrégé est créé dans la base de données topologiques. Le domaine agrégé contient les collectes de périphériques de tous les domaines reconnus. Dans Tivoli Integrated Portal, vous pouvez afficher les mappes de topologie dans tous les domaines en choisissant le domaine **AGGREGATION** dans le menu de domaine.

Configuration matérielle requise

La configuration matérielle requise varie suivant la taille et la composition de votre réseau ainsi que les fonctions de Network Manager que vous souhaitez utiliser.

Vérifiez que vos serveurs disposent de la configuration matérielle requise avant d'installer Network Manager.

Important : N'exécutez aucune autre application nécessitant beaucoup de ressources pendant l'installation de Network Manager.

Directives pour le choix des processeurs

Lisez les directives pour le choix des processeurs avant de sélectionner le serveur approprié pour y installer Network Manager.

Les directives présentées ici concernent les serveurs destinés seulement à prendre en charge des composants Network Manager. Les directives supposent le déploiement des autres produits Tivoli, tels que IBM Tivoli Monitoring, Tivoli Data Warehouse, et IBM Tivoli Business Service Manager, sur d'autres serveurs. Pour combiner le déploiement de plusieurs produits majeurs sur un même serveur, additionnez les spécifications minimales pour chaque produit (consultez la documentation de chacun des produits pour plus d'informations).

Pour les petits réseaux et les déploiements de démonstration ou de formation, utilisez deux processeurs au moins sur toutes les plateformes. Les déploiements de réseaux de taille moyenne ou grande requièrent quatre processeurs.

Remarque : Pour les processeurs multicoeurs, la vitesse individuelle des coeurs peut être plus importante que le nombre de coeurs. Si des processeurs de n'importe quelle vitesse peuvent être utilisés, le choix de la vitesse de coeur la plus rapide et de la mémoire cache intégrée la plus grande apporte une différence significative quant à la taille du réseau à reconnaître et à interroger.

Pour les paramètres virtualisés (pris en charge par AIX LPARS, VMWare ESX, etc.), utilisez des ressources processeur et mémoire fixes pour un système virtuel prenant en charge Network Manager.

Pour les paramètres zLinux, utilisez l'allocation de processeur équivalente à celle de deux processeurs modernes, depuis n'importe quelle plateforme UNIX ou Windows native prise en charge par Network Manager.

Pour plus d'informations sur le choix des processeurs et sur les autres considérations en matière de déploiement, voir «Déploiement de Network Manager», à la page 1.

Configuration requise pour l'exécution du programme d'installation

Pour installer tout composant de Network Manager, votre serveur doit respecter la configuration matérielle suivante.

Espace disque requis pour le programme d'installation

Certains répertoires doivent disposer d'un certain espace libre afin d'exécuter le programme d'installation, quels que soient les composants installés.

Sur les systèmes d'exploitation UNIX, vous devez disposer d'au moins 170 Mo d'espace libre dans le répertoire `/tmp`, d'au moins 350 Mo d'espace libre dans le répertoire `/usr` et de 500 Ko dans le répertoire `/var`. Si vous installez Network Manager à un emplacement autre que `/opt`, vous devez disposer d'au moins 50 Mo d'espace dans le répertoire `/opt`.

Espace requis pour l'installation en tant qu'utilisateur non-root

Sur les systèmes d'exploitation UNIX, l'installation en tant que non-root requiert au moins 350 Mo d'espace libre dans le répertoire de base pour stocker les fichiers relatifs à l'installation.

Exigences relatives aux composants centraux

Pour installer les composants centraux de Network Manager vos serveurs doivent disposer de la configuration matérielle minimale.

Exigences relatives à la mémoire

Vérifiez que les serveurs sur lesquels vous souhaitez exécuter Network Manager répondent aux exigences suivantes concernant la mémoire.

- Pour un déploiement sur un seul serveur, sur lequel les composants centraux, les applications Web, la base de données topologique Network Manager et Tivoli Netcool/OMNIbus se trouvent sur le même serveur, vous avez besoin d'un minimum de 6 Go de mémoire DRAM, de préférence 8 Go dans un environnement de production, et de 0 à 12 Go pour les grands réseaux.

  Remarque : Le programme d'installation vérifie qu'un minimum de 4 Go de mémoire DRAM est disponible pour les déploiements de système de démonstration et de formation. Un minimum de 6 Go de mémoire DRAM est cependant requis dans les environnements de production.
- Pour un déploiement distribué où seuls les composants centraux de Network Manager sont installés sur le serveur, vous avez besoin d'un minimum de 4 Go de mémoire DRAM.

  Remarque : Le programme d'installation vérifie qu'un minimum de 3 Go de mémoire DRAM est disponible pour les déploiements de système de démonstration et de formation. Un minimum de 4 Go de mémoire DRAM est cependant requis dans les environnements de production.

La quantité de mémoire requise dépend de la façon dont vous déployez Network Manager. Pour des informations plus détaillées sur les spécifications en matière de mémoire, voir «Déploiement de Network Manager», à la page 1.

Espace disque requis

Vérifiez que le serveur sur lequel vous souhaitez exécuterNetwork Manager répond aux exigences suivantes en matière d'espace disque.

- 2 Go d'espace disque pour stocker le logiciel
- 2 Go d'espace disque pour stocker le cache
- Comme estimation de référence pour les fichiers journaux, si l'on considère que chaque fichier journal a une taille d'1 Go et que le niveau de débogage complet est défini pour six processus, 24 Go d'espace disque sont nécessaires. (6 processus x 4 fichiers journaux ou de trace chacun = 24 fichiers journaux ou de trace X 1 Go = 24 Go).

Exigences relatives à la bande passante

Le serveur Network Manager nécessite une connexion Fast Ethernet bidirectionnelle de 100 Mbps (ou équivalent) avec le serveur DNS.

Il est nécessaire que les systèmes prenant en charge des composants Network Manager soient placés dans le centre de données avec des connexions de réseau local Fast Ethernet 100 Mbps ou Gigabit Ethernet au système DNS et au périphérique du réseau central à reconnaître et à gérer. Des vitesses de connexion moins rapides peuvent être utilisées, mais elles peuvent avoir un impact sur les temps de réponse des sessions clientes et doivent être adaptées aux charges de travail principales telles que l'interrogation (y compris les temps de réponse, le nombre de tentatives et le trafic réseau total induit).

Remarque : Lors de la reconnaissance d'un périphérique réseau, de nombreuses requêtes SNMP sont effectuées pour ce périphérique. Après la reconnaissance, l'interrogation de routine (ICMP et SNMP) peut induire un trafic significatif sur le réseau. Avec un réseau bénéficiant des vitesses des réseaux locaux modernes, ces charges de travail peuvent être prises en charge.

Pour plus d'informations sur les spécifications de bande passante pour la reconnaissance, voir «Exigences en bande passante de la reconnaissance», à la page 32.

Autres exigences

Une unité de DVD-ROM est également nécessaire, si vous n'installez pas le logiciel depuis un téléchargement.

Configuration requise pour les composants de l'interface graphique

Le serveur où vous installez les composants d'interface graphique de Network Manager (également appelés "applications Web", qui comprennent Tivoli Integrated Portal, Tivoli Common Reporting, et l'interface graphique Web Tivoli Netcool/OMNIbus) doit répondre à la configuration matérielle requise suivante.

- 5,5 Go d'espace disque libre.
- Un minimum de 4 Go de mémoire DRAM.

  Remarque : Le programme d'installation vérifie qu'un minimum de 3 Go de mémoire DRAM est disponible pour les déploiements de système de démonstration et de formation. Un minimum de 4 Go de mémoire DRAM est cependant requis dans les environnements de production.
- 500 Mo dans le répertoire `/tmp`.
- Unité de DVD-ROM si l'installation n'est pas effectuée à partir d'un téléchargement.

Configuration matérielle requise pour Tivoli Common Reporting

Examinez la configuration matérielle requise pour Tivoli Common Reporting pour vous assurer de répondre à vos exigences en matière de performance.

Pour des informations détaillées sur la configuration matérielle requise pour Tivoli Common Reporting, voir le centre de documentation de Tivoli Common Reporting

à l'adresse URL : http://www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html

Exigences relatives au répertoire d'installation

Lors d'une installation sur le même ordinateur, les composants d'interface graphique des produits Tivoli utilisant Tivoli Integrated Portal 1.1.x ne peuvent pas être installés dans le même répertoire que les composants d'interface graphique des produits utilisant Tivoli Integrated Portal 2.1.

Par exemple, les composants d'interface graphique de Network Manager 3.9 doivent être installés dans un répertoire différent de celui des composants d'interface graphique de IBM Tivoli Business Service Manager 4.2.1 (le premier utilise Tivoli Integrated Portal 2.1, alors que le second utilise la version 1.1.x). Lors de l'installation de Network Manager, il est possible que le processus d'installation reconnaisse des répertoires Tivoli Integrated Portal existants. Assurez-vous d'utiliser un répertoire différent si vous avez des produits exécutant une version antérieure de Tivoli Integrated Portal.

Configuration requise pour le serveur de base de données topologiques

Lisez les informations sur les spécifications de la base de données topologiques de Network Manager.

Exigences relatives à la mémoire

Si vous installez localement la base de données par défaut Informix avec le programme d'installation de Network Manager, assurez-vous que le serveur où vous voulez exécuter Informix a un minimum de 4 Go de mémoire DRAM disponible (davantage de mémoire peut être nécessaire pour les grands réseaux). Pour des informations sur les spécifications quant à la mémoire pour d'autres bases de données, voir la documentation de la base de données concernée.

Pour plus d'informations sur la configuration d'une base de données Informix distante ou d'autres bases de données distantes, voir les tâches décrites dans «Configuration d'une base de données topologiques», à la page 62.

Espace disque requis

Pour stocker des données Network Manager, assurez-vous de disposer au moins de l'espace disque minimal suivant disponible pour votre base de données topologiques :

- 5 Go pour Informix et, sous Linux for Z Series, vous avez besoin d'au moins 500 Mo d'espace libre dans le répertoire `/tmp` et d'au moins 500 Mo dans le répertoire `/`.
- 3 à 5 Go pour DB2, MySQL et Oracle.

Remarque : Ces chiffres correspondent à des valeurs minimales. L'espace disque réel requis dépend de la taille de votre réseau et de la quantité de données stockées. Le stockage de données de performance peut nécessiter une grande quantité d'espace disque. Si vous prévoyez de stocker de grandes quantités de données, prévoyez 50 Go pour l'espace disque relatif à Network Manager.

Vérifiez que les disques du serveur où vous voulez exécuter la base de données topologiques répondent aux spécifications suivantes :

- Trois disques en configuration RAID 1 (davantage de disques pour RAID 5)
- Disques SATA ou SCSI grande vitesse

Espace disque pour les événements et les interfaces

Vous devez calculer et prévoir de l'espace disque supplémentaire pour les événements et les interfaces de votre installation.

Configuration matérielle supplémentaire pour Network Manager :

- 4 Ko d'espace disque pour chaque événement attendu, par jour de stockage requis
- 4 Ko d'espace disque pour chaque interface ou port d'une unité gérée

Par exemple, si vous disposez de 5 000 ports sur les unités de votre réseau, que vous attendez 3 000 événements par jour et que ces derniers doivent être stockés pendant 30 jours, vous avez besoin de :

```
3 000 * 30 * 4 Ko = 360 Mo
```

L'espace disque total requis est donc de :

```
512 Mo + 512 Mo de mémoire cache + 360 Mo + (4 Ko * 5 000) = 1.4 Go
```

Spécifications d'espace de permutation (UNIX)

Sur les plateformes UNIX, vous devez vous assurer de disposer de l'espace disque libre approprié qui est configuré pour être utilisé comme espace de permutation.

La quantité exacte d'espace de permutation nécessaire dépend de la taille et de la composition de votre réseau et du type de reconnaissance. Pour les quantités inférieures de mémoire RAM, vous avez besoin de quantités proportionnellement supérieures d'espace de permutation. Les chiffres suivants montrent la quantité approximative d'espace de permutation selon la quantité de mémoire RAM physique.

4 Go de mémoire RAM
Configurez 10 Go d'espace de permutation.

8 Go de mémoire RAM
Configurez 16 Go d'espace de permutation.

12 Go de mémoire RAM
Configurez 18 Go d'espace de permutation.

Pour les quantités de mémoire RAM supérieures à 12 Go, configurez la même quantité d'espace de permutation. Par exemple, pour 24 Go de mémoire RAM, configurez 24 Go d'espace de permutation.

Exigences en bande passante de la reconnaissance

Les opérations de reconnaissance du réseau nécessitent au minimum une connexion à large bande.

Ne tentez pas de lancer des reconnaissances avec une connexion modem. Si la vitesse de connexion n'est pas suffisante, il est possible que des paquets soient perdus en raison de la quantité de trafic SNMP généré par les opérations de reconnaissance et de surveillance par défaut. Même avec une connexion à large bande, le nombre d'unités d'exécution des auxiliaires SNMP doit rester faible. La reconnaissance peut donc prendre beaucoup de temps.

Les reconnaissances doivent être exécutées lorsque vous disposez d'une connexion Ethernet (ou similaire). La vitesse requise de votre connexion Ethernet dépend de la taille de votre réseau :

- Une connexion 10 Mbits/s en duplex intégral est nécessaire pour prendre en charge jusqu'à 100 unités d'exécution d'auxiliaires SNMP et un nombre relativement faible d'unités. Si vous utilisez Telnet avec SSH pour accéder à de nombreuses unités de la reconnaissance, le nombre d'unités d'exécution de l'auxiliaire SNMP doit être réduit pour prendre en compte la bande passante utilisée par l'auxiliaire Telnet.
- Une connexion Fast Ethernet 100 Mbits/s en duplex intégral (ou équivalente) est nécessaire pour reconnaître un réseau de grande taille. La bande passante ne devrait pas poser de problème avec une connexion 100 Mbits/s, et ce quel que soit le nombre d'unités d'exécution de l'auxiliaire SNMP utilisées, sauf si des applications exigeant une bande passante importante partagent la liaison.

Les chiffres ci-dessus partent du principe qu'un aller-retour moyen pour un paquet SNMP est de 10 millisecondes et qu'un paquet a une taille de 125 octets en moyenne. Cela signifie que chaque unité d'exécution de l'auxiliaire SNMP peut transmettre et récupérer 12 500 octets par seconde, ce qui équivaut à 100 000 bits par seconde. Dans le cas de 20 unités d'exécution, 20 multiplié par 100 000 équivaut à 2 000 000 bits par seconde, soit 2 Mbits/s. Pour 100 unités d'exécution, cela nous donne 10 Mbits/s. Par défaut, l'auxiliaire SNMP exécute 120 unités d'exécution.

Ces estimations partent du principe que chaque unité d'exécution de l'auxiliaire SNMP est en activité en même temps, ce qui n'est généralement pas le cas. Cependant, si la bande passante est insuffisante, les paquets UDP utilisés pour transporter SNMP pourraient être perdus ou se retrouver en file d'attente et arriver à destination en retard.

Pour plus d'informations sur la configuration de l'auxiliaire SNMP, voir *IBM Tivoli Network Manager IP Edition - Guide de reconnaissance* .

Exigences en mémoire de la reconnaissance

Lors de la reconnaissance de réseaux de très grandes tailles, le processus de reconnaissance (ncp_disco) et le processus de modèle de topologie (ncp_model) utilisent la plupart de la mémoire. Si votre réseau est de taille très importante, pensez à le diviser en plusieurs domaines.

Configuration logicielle

La configuration logicielle requise dépend du système d'exploitation,des produits et des fonctions de Network Manager que vous souhaitez utiliser.

Configuration requise pour les autres produits

Vérifiez que la configuration requise des produits intégrés à Network Manager est respectée.

Exigences supplémentaires relatives aux produits

Important : Ces exigences s'ajoutent notamment aux autres exigences relatives au matériel, aux logiciels, au répertoire d'installation et à l'utilisateur. Ces exigences sont présentées dans la documentation du produit. Avant d'installer un produit, assurez-vous d'en comprendre tous ses pré-requis et exigences.

Tivoli Netcool/OMNIbus

Vérifiez que Tivoli Netcool/OMNIbus version 7.2.1, version 7.3, version 7.3.1, version 7.4, Fix Pack 5 ou version 8.1 est installé sur un serveur auquel Network Manager peut se connecter. Installez Tivoli Netcool/OMNIbus, si vous n'en disposez pas déjà. Vous devez télécharger Tivoli Netcool/OMNIbus séparément.

Le programme d'installation de Network Manager recherche uniquementTivoli Netcool/OMNIbus version 7.3.1. S'il ne trouve pas l'image Tivoli Netcool/OMNIbus (en fonction du nom de l'image ou du numéro de référence), il demande l'emplacement du fichier. Si vous souhaitez que le programme d'installation installe une version de Tivoli Netcool/OMNIbus prise en charge, autre que 7.3.1, créez un sous-répertoire nommé `OMNIbus` dans le module d'installation Network Manager extrait et extrayez le package Tivoli Netcool/OMNIbus téléchargé dans ce répertoire.

Restriction : Du fait d'un problème connu, le programme d'installation de Network Manager 3.9 ne peut pas installer ou configurer Tivoli Netcool/OMNIbus 7.4 sur les systèmes Linux et Solaris. Par conséquent, le script **`ConfigOMNI`** fourni avec Network Manager 3.9 ne peut pas configurer Tivoli Netcool/OMNIbus 7.4 sur les systèmes Linux et Solaris. Pour plus d'informations sur ce problème et sa solution, voir la note technique de traitement de l'incident http://www-01.ibm.com/support/docview.wss?uid=swg21615671.

Si vous installez Tivoli Netcool/OMNIbus sans le programme d'installation Network Manager, vous devez l'installer à partir d'une autre fenêtre que celle utilisée pour l'installation de Network Manager, en vérifiant que les variables d'environnement sont correctement définies d'après la documentation Tivoli Netcool/OMNIbus.

Restriction : Vous devez installer Network Manager 3.9 dans un autre **répertoire** pour une installation existante de Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure. Sous Windows, vous devez installer Network Manager 3.9 sur un autre **serveur** pour une installation existante de Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure.

Restriction : Fix Pack 5 Les restrictions suivantes s'appliquent à Tivoli Netcool/OMNIbus version 8.1 :

- Vous ne pouvez pas installer Tivoli Netcool/OMNIbus version 8.1 sur le même serveur que Network Manager.

- Vous ne pouvez pas installer Tivoli Netcool/OMNIbus version 8.1 avec le programme d'installation de Network Manager. Si vous voulez utiliser Tivoli Netcool/OMNIbus version 8.1, vous devez l'installer sur un hôte distant et vous y connecter.

interface graphique Web Tivoli Netcool/OMNIbus
L'interface graphique Web Tivoli Netcool/OMNIbus était appelée Netcool/Webtop dans les versions 2.2 et antérieures. Si vous installez l'interface graphique Web sans avoir recours au programme d'installation de Network Manager, vous devez l'installer à partir d'une autre fenêtre que celle utilisée pour l'installation de Network Manager, en vérifiant que les variables d'environnement sont correctement définies d'après la documentation Tivoli Netcool/OMNIbus.

Tivoli Common Reporting
Network Manager installe le package de rapports requis pour les rapports de gestion du réseau sur le serveur sur lequel les composants de l'interface graphique de Network Manager sont installés. Si l'emplacement d'installation choisi pour Network Manager comporte déjà des instances de Tivoli Integrated Portal et Tivoli Common Reporting, Network Manager configure automatiquement les rapports à utiliser avec cette instance de Tivoli Common Reporting.

Si Tivoli Common Reporting n'est pas installé lorsque vous installez Network Manager, vous pouvez l'installer ultérieurement et configurer ensuite les rapports, comme décrit dans «Configuration de rapports pour des installations existantes», à la page 277.

IBM Tivoli Business Service Manager
Vous devez installer IBM Tivoli Business Service Manager à partir d'une autre fenêtre que celle utilisée pour l'installation de Network Manager, en vérifiant que les variables d'environnement sont correctement définies d'après la documentation de IBM Tivoli Business Service Manager.

Versions précédentes
Installez Network Manager 3.9 dans un répertoire différent pour Network Manager V3.8 ou antérieur, et Netcool/Webtop V2.1 ou antérieur.

Tâches associées:

«Configuration des intégrations à d'autres produits», à la page 175
Vous pouvez configurer Network Manager pour l'utiliser avec plusieurs produits Tivoli. Consultez les informations relatives aux tâches de configuration requises pour configurer les intégrations disponibles.

Compatibilité avec d'autres produits Tivoli

Network Manager est compatible avec d'autres produits Tivoli, ce qui permet l'intégration avec d'autres produits pour créer une solution répondant à vos spécifications.

Le tableau suivant décrit la compatibilité de Network Manager version 3.9 avec d'autres produits Tivoli.

Tableau 3. Compatibilité de Network Manager version 3.9 avec d'autres produits

Produit	Versions compatibles
IBM Tivoli Netcool/OMNIbus	7.2.1 7.3 7.3.1 7.4 **Remarque :** Fix Pack 5 Si vous souhaitez utiliser Oracle 11 et Oracle 12 comme base de données topologiques et qu'IBM Tivoli Netcool/OMNIbus est installé sur le même serveur Solaris qu'Network Manager groupe de correctifs, vous devez installer ou effectuer une mise à niveau vers IBM Tivoli Netcool/OMNIbus 7.4 avant d'installer le groupe de correctifs 5. Fix Pack 5 8.1 (IBM Tivoli Netcool/OMNIbus à distance uniquement)
interface graphique Web Tivoli Netcool/OMNIbus	7.3.1 7.4
IBM Tivoli Netcool Configuration Manager	6.3 6.4
Tivoli Integrated Portal	2.1 2.2 **Remarque :** Fix Pack 5 Si vous accordez de l'importance à la conformité avec la norme FIPS 140-2, n'utilisez pas les versions antérieures à la version 2.2.0.17. La version 2.2.0.17 de Tivoli Integrated Portal a introduit la conformité avec l'algorithme de hachage sécurisé SHA-2.

Tableau 3. Compatibilité de Network Manager version 3.9 avec d'autres produits (suite)

Produit	Versions compatibles
Tivoli Common Reporting	2.1 2.1.1 Fix Pack 5 3.1 **Restriction :** Tivoli Common Reporting 3.1 est disponible uniquement pour les utilisateurs de Netcool Operations Insight. **Restriction :** Si vous souhaitez utiliser la fonction de génération de rapports et que vous installez Network Manager sur Red Hat Enterprise Linux 6.0, vous devez installer Tivoli Common Reporting version 2.1 ou 2.1.1 sur un hôte distinct, car ces versions de Tivoli Common Reporting ne sont pas prises en charge sous Red Hat Enterprise Linux 6.0. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports lors du lancement de la procédure d'installation de Network Manager en utilisant l'option `-DinstallReports=0`, comme indiqué dans les tâches d'installation dans «Installation de Network Manager», à la page 81. **Restriction :** Tivoli Common Reporting version 2.x n'est pas compatible avec Internet Explorer 10 et Firefox 24 Extended Support Release (ESR). Cela implique que vous ne pouvez pas utiliser la fonction de génération de rapport si vous utilisez ces versions de navigateur pour l'interface graphique Network Manager. **Restriction :** Fix Pack 5 Tivoli Common Reporting version 3.1 ne prend pas en charge MySQL.
Tivoli Data Warehouse	2.1
IBM Tivoli Change and Configuration Management Database	7.1.1
IBM Tivoli Application Dependency Discovery Manager	7.2 7.2.1
IBM Systems Director	6.2.1
IBM Tivoli Business Service Manager	4.2.1 6.1 **Remarque :** La compatibilité entre Network Manager 3.9 et IBM Tivoli Business Service Manager 4.2.1 est limitée aux capacités de lancement en contexte et d'exportation DLA. Pour plus d'informations, voir «Exportation de données de reconnaissance vers CCMDB, TADDM, et TBSM», à la page 203, ainsi que le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.

Tableau 3. Compatibilité de Network Manager version 3.9 avec d'autres produits (suite)

Produit	Versions compatibles
IBM Tivoli Monitoring	Fix Pack 5 6.2.2 ou version ultérieure.

Bases de données topologiques prises en charge

Par défaut, une base de données IBM Informix est incluse dans le produit pour stocker les données de topologie. D'autres types de bases de données sont compatibles. Si vous n'utilisez pas la base de données par défaut, utilisez uniquement une base de données compatible.

Important : Appliquez tous les correctifs recommandés à la base de données.

Si vous utilisez des bases de données distinctes pour les données MIB et les données de topologie, toutes les bases de données doivent être de même type. Par exemple, vous ne pouvez pas utiliser une base de données DB2 pour les données topologiques et une base de données Informix pour les données MIB.

Le tableau suivant répertorie les types, les versions et les éditions de bases de données compatibles.

Tableau 4. Types, versions et éditions de bases de données compatibles

Type de base de données	Version et édition	Remarques
IBM DB2	• DB2 V9.1 • DB2 V9.5 • DB2 V9.7 • Fix Pack 4 DB2 V10.1 • Fix Pack 5 DB2 V10.5	En cas de reprise en ligne de la configuration, vous pouvez configurer Network Manager pour qu'il fonctionne dans l'environnement HADR (High Availability Disaster Recovery) DB2. **Restriction :** La base de données DB2 livrée avec Network Manager est une version dont la licence est limitée. En fonction de votre environnement, de la taille de votre réseau et de la quantité de données que vous prévoyez de stocker, vous pourrez avoir besoin de mettre à niveau votre licence de DB2. Pour plus d'informations, prenez contact avec votre interlocuteur IBM habituel.

Tableau 4. Types, versions et éditions de bases de données compatibles (suite)

Type de base de données	Version et édition	Remarques
MySQL	• 5.1 • Fix Pack 4 5.5 • Fix Pack 4 5.6	Si vous utilisez MySQL pour la base de données topologiques, vous ne pouvez pas employer Tivoli Common Reporting version 3.1. Vous devez utiliser Tivoli Common Reporting version 2.1. Pour les mises à niveau vers MySQL 5.5 ou MySQL 5.6, appliquez le groupe de correctifs avant de mettre à niveau la base de données. Si vous omettez de le faire, des erreurs peuvent se produire dans l'interface graphique des Vues de réseau. (La bibliothèque JDBC MYSQL utilisée dans les versions antérieures au groupe de correctifs 4 n'est pas compatible avec MySQL 5.5 ou MySQL 5.6.) Pour plus d'informations, voir le fichier `INSTALL` inclus dans le groupe de correctifs.
Oracle	• V11*g* Standard Edition • V11*g* Enterprise Edition • Fix Pack 5 V12c	Si vous utilisez Oracle V12c, vous ne pouvez pas employer Tivoli Common Reporting version 2.1.1. Vous devez utiliser Tivoli Common Reporting version 3.1. Fix Pack 5 En cas de reprise en ligne de la configuration, vous pouvez configurer Network Manager pour qu'il fonctionne dans l'environnement RAC (Real Application Clusters) d'Oracle. **Restriction :** Fix Pack 5 L'utilisation d'Oracle 11 comme base de données topologiques n'est pas prise en charge si Network Manager est exécuté sur Linux for zSeries and System z.

Tableau 4. Types, versions et éditions de bases de données compatibles (suite)

Type de base de données	Version et édition	Remarques
IBM Informix	• V11.5 Ultimate Edition • V11.5 Ultimate Edition • V11.7 Enterprise Edition • V11.5 Workgroup Edition	La version d'Informix incluse dans le produit est différente selon l'image du produit que vous avez téléchargée. L'image du produit GA de base contient Informix Workgroup Edition version 11.5 (11.50.xC6). L'image du produit publiée le 14 septembre 2012 (niveau de génération 3.9.0.71) contient Informix Growth Edition 11.7 (11.70.xC5). Si vous exécutez l'image du produit GA de base, vous pouvez effectuer une mise à niveau Informix Workgroup Edition version 11.5 vers Informix Growth Edition 11.7. La mise à niveau est un processus manuel et varie en fonction du système d'exploitation utilisé. Pour plus d'informations, recherchez *Upgrading Informix from V11.5 to V11.7* dans le document *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*. Pour plus d'informations sur l'installation d'Informix en tant qu'utilisateur non-root, voir «Installation d'Informix comme utilisateur non-root». Linux Informix V11.7 n'est pas compatible avec SUSE Linux Enterprise Server (SLES) 10. Utilisez Informix V11.5 ou une autre base de données compatible. Pour plus d'informations, recherchez *Installing Informix 11.5 on SuSE Enterprise Linux 10* dans *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*. AIX Informix V11.5 n'est pas compatible avec AIX V7.1.

Installation d'Informix comme utilisateur non-root

Pour installer Informix dans le cadre d' une installation non root, définissez les droits d'accès à tous les répertoires dans le chemin Informix sur 775. Par exemple, sur un hôte linux dans lequel la variable d'environnement $NCHOME est définie

sur /home/IBM/tivoli/, le chemin Informix est /home/IBM/tivoli/platform/linux2x86/users/informix/. Dans cet exemple, définissez les droits des répertoires suivants sur 775 :

- /home/
- /home/IBM/
- /home/IBM/tivoli/
- /home/IBM/tivoli/platform/
- /home/IBM/tivoli/platform/linux2x86/
- /home/IBM/tivoli/platform/linux2x86/users/
- /home/IBM/tivoli/platform/linux2x86/users/informix/

Tâches associées:

«Installation de groupes de correctifs», à la page 141
Pour obtenir les derniers correctifs, appliquez les groupes de correctifs. Des groupes de correctifs sont disponibles pour le produit Network Manager, ainsi que pour d'autres produits et composants tels que Tivoli Integrated Portal et l'interface graphique Web Tivoli Netcool/OMNIbus. Vous pouvez télécharger les groupes de correctifs depuis IBM Fix Central. Assurez-vous que le niveau du groupe de correctifs reste à jour.

«Configuration d'une base de données topologiques», à la page 62
A part la base de données Informix par défaut, vous pouvez utiliser une base de données DB2, MySQL ou Oracle pour stocker votre topologie. A moins que vous n'installiez la base de données Informix par défaut livrée avec Network Manager, vous devez configurer une base de données existante ou en installer et configurer une nouvelle avant d'installer Network Manager.

«Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC», à la page 351
Vous pouvez configurer les processus principaux de Network Manager en vue de l'utilisation du catalogue DB2 et de l'interface graphique Network Manager pour qu'ils fonctionnent dans l'environnement de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Fix Pack 5 De la même manière, vous pouvez également configurer les processus principaux de Network Manager et l'interface graphique de Network Manager pour qu'ils fonctionnent dans l'environnement RAC (Real Application Clusters) d'Oracle.

Systèmes d'exploitation pris en charge

Network Manager est pris en charge sous différentes versions de UNIX, Linux et Windows.

Network Manager V3.9 est pris en charge sur les systèmes d'exploitation suivants au moment de l'édition.

Pour obtenir les toutes dernières informations sur les systèmes d'exploitation pris en charge, voir les rapports de compatibilité des produits logiciels sur :

http://www.ibm.com/software/reports/compatibility/clarity/index.html

Important : Vérifiez que tous les modules de correction recommandés sont installés sur le système d'exploitation, y compris les niveaux de correctif les plus récents.

Sur les processeurs Sun Microsystems, les versions suivantes sont prises en charge :

- Solaris 10 SPARC
- Zones SPARC

Sur les systèmes IBM PowerPC, les versions suivantes sont prises en charge :

- AIX 6.1 iSeries et pSeries
- AIX 7.1 iSeries et pSeries

Sur les processeurs Intel et Advanced Micro Devices (AMD) x86, les versions suivantes sont prises en charge :

- Red Hat Enterprise Linux 5.0 (x86-32, x86-64)
- Red Hat Enterprise Linux 6.0 (x86-32, x86-64)

  Restriction : Si vous souhaitez utiliser la fonction de génération de rapports et que vous installez Network Manager sur Red Hat Enterprise Linux 6.0, vous devez installer Tivoli Common Reporting version 2.1 ou 2.1.1 sur un hôte distinct, car ces versions de Tivoli Common Reporting ne sont pas prises en charge sous Red Hat Enterprise Linux 6.0. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports lors du lancement de la procédure d'installation de Network Manager en utilisant l'option `-DinstallReports=0`, comme indiqué dans les tâches d'installation dans «Installation de Network Manager», à la page 81.
  Avertissement : Veillez à désactiver Security-Enhanced Linux (SELinux) ou définissez l'option comme "permissive" dans le fichier de configuration `selinux` avant d'installer ou d'utiliser Network Manager. Les systèmes Linux exécutant SELinux (Security-Enhanced Linux) ne sont pas pris en charge.
- SuSE Linux Enterprise Server (SLES) 10.0 (x86-32, x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-32, x86-64)

  Remarque : Network Manager ne prend pas en charge SuSE Linux Enterprise Server (SLES) 11.0 SP2 (pour plus d'informations, voir http://www-01.ibm.com/support/docview.wss?uid=swg21619336).

  Remarque : Fix Pack 4 Network Manager prend en charge SuSE Linux Enterprise (SLES) 11.0 SP2 et SP3.
- SuSE Linux Enterprise Desktop (SLED) 11 (x86-64)
- Windows Server 2008 (R1) Standard Edition (x86-32, x86-64)
- Windows Server 2008 (R2) Standard Edition (x86-64)
- Windows Server 2008 (R1) Enterprise Edition (x86-32, x86-64)
- Windows Server 2008 (R1) Enterprise Edition (x86-64)
- Windows Server 2008 (R2) Enterprise Edition (x86-64)
- Windows Server 2008 (R2) Datacenter Edition (x86-64)

Sur les mainframes IBM System z, les versions suivantes sont compatibles :

- Red Hat Enterprise Linux 5.0 (zSeries et System z)
- Red Hat Enterprise Linux 6.0 (zSeries et System z)

  Restriction : Si vous souhaitez utiliser la fonction de génération de rapports et que vous installez Network Manager sur Red Hat Enterprise Linux 6.0, vous devez installer Tivoli Common Reporting version 2.1 ou 2.1.1 sur un hôte distinct, car ces versions de Tivoli Common Reporting ne sont pas prises en charge sous Red Hat Enterprise Linux 6.0. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports lors du lancement de la procédure

d'installation de Network Manager en utilisant l'option `-DinstallReports=0`, comme indiqué dans les tâches d'installation dans «Installation de Network Manager», à la page 81.
Avertissement : Veillez à désactiver Security-Enhanced Linux (SELinux) ou définissez l'option comme "permissive" dans le fichier de configuration `selinux` avant d'installer ou d'utiliser Network Manager. Les systèmes Linux exécutant SELinux (Security-Enhanced Linux) ne sont pas pris en charge.

- SuSE Linux Enterprise Server (SLES) 10.0 (zSeries et System z)
- SuSE Linux Enterprise Server (SLES) 11.0 (zSeries et System z)

Les combinaisons suivantes de programme Hypervisor et de système d'exploitation sont prises en charge :

- Fix Pack 5 La fonction Kernel-Based Virtualization est prise en charge sur toutes les versions prises en charge de SUSE Linux
- IBM PowerVM Hypervisor (LPAR, DPAR, Micro-Partition) - toutes les versions prises en charge : sous AIX
- IBM PR/SM toutes les versions : environnements SLES et RHEL
- IBM z/VM 6.1 : environnements SLES et RHEL
- VMware ESX 3.5 : SLES, RHEL et Windows 2008 Enterprise Edition et Standard Edition
- VMware ESX et ESXi 3.5, 4.0, 4.1 et 5.0 : SLES, RHEL et Windows 2008 Enterprise Edition et Standard Edition
- Domaines logiques (LDOM) Sun et Oracle - toute version : Solaris SPARC

Restriction :

- Les systèmes Linux exécutant AppArmor ne sont pas pris en charge. Désactivez AppArmor pour que l'installation puisse continuer.
- Les systèmes Linux exécutant SELinux (Security-Enhanced Linux) ne sont pas pris en charge. Désactivez SELinux lors de l'installation et de l'utilisation de Network Manager.

Exigences supplémentaires pour les systèmes d'exploitation UNIX

Si vous effectuez l'installation sur une configuration UNIX vous permettant d'installer l'interpréteur de commandes Korn (ksh), par exemple, SUSE Enterprise Linux, vous devez vous assurer que l'interpréteur de commandes Korn est installé avant l'exécution du programme d'installation Network Manager.

Désinstallez les montages de système NFS (Network File System) qui ne sont pas accessibles avant d'exécuter le programme d'installation. Pour rechercher les montages NFS inaccessibles, exécutez la commande suivante :

```
df -kP
```

Si cette commande s'exécute correctement, il n'existe plus de montage NFS inaccessible.

Exigences supplémentaires pour AIX

Si vous installez Network Manager sur des systèmes d'exploitation AIX, assurez-vous que vous disposez des ensembles de fichiers X11, y compris `X11.apps.xterm` et qu'ils ont été installés avant le lancement de l'installation de Network Manager.

Exigences supplémentaires pour Red Hat Enterprise Linux 6.0 sous zSeries et System z

Si vous installez RHEL 6.0 sur des systèmes zSeries et System z, vérifiez que les exigences suivantes sont satisfaites :

- Vérifiez que le shell Korn (ksh) est installé avant d'exécuter le programme d'installation de Network Manager. Le fichier exécutable ksh est requis dans le répertoire `/bin` pour les scripts Network Manager, et que dans le répertoire `/usr/bin` pour la base de données Informix.
- Vérifiez que la bibliothèque 32 bits libstdc++.so.6.0.8 se trouve dans le répertoire `/usr/lib`.
- Si vous utilisez Tivoli Netcool/OMNIbus, vérifiez que vous disposez des RPM 32 bits requis. Voir la section *Prerequisites for operating systems* dans *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* .

Exigences supplémentaires pour Solaris

Si vous installez Network Manager sur les systèmes d'exploitation Solaris, installez d'abord le package SUNWsprot.

Exigences supplémentaires pour Tivoli Common Reporting sous Linux et Linux on System z

Si vous installez Network Manager sur des systèmes d'exploitation Linux ou zLinux associés à une base de données Informix sous zLinux, ou avec une base de données Informix ou MySQL sous Linux, assurez-vous qu'un RPM unixODBC 32 bits est disponible sur le système où vous installez des composants d'interface graphique avant l'installation.

- Sur toutes les versions de Linux, vérifiez que vous disposez du fichier `libXm.so.3` ou version ultérieure (disponible sur openmotif RPM 22 ou version ultérieure) sur votre système avant l'installation. Pour les versions de `libXm.so.x` postérieures à `libXm.so.3`, créez un lien symbolique à partir de la version ultérieure de `libXm.so.3`, à l'aide d'une commande similaire à l'exemple suivant : **`ln -s /usr/lib/libXm.so.4 libXm.so.3`**.
- Sur des systèmes Red Hat Enterprise Linux, vérifiez que le RPM `unixODBC-2.2.x.x` ou ultérieur est disponible sur le système avant l'installation.
- Sur des systèmes SuSE Linux Enterprise Server (SLES), assurez-vous que le RPM `unixODBC-2.2.X.X` ou ultérieur est disponible sur le système avant l'installation.

Important :

Certaines versions d'unixODBC définissent la bibliothèque principale dans le répertoire `/usr/lib/` comme étant `libodbcinst.so.1`. La bibliothèque principale doit être définie comme étant `/usr/lib/libodbcinst.so`. Si nécessaire, créez un lien symbolique.

```
ln -s /usr/lib/libodbcinst.so.x /usr/lib/libodbcinst.so
```

Restriction : Vous ne pouvez pas utiliser Tivoli Common Reporting avec MySQL sous zLinux.

Pour des informations détaillées sur la configuration logicielle requise pour Tivoli Common Reporting, voir le centre de documentation de Tivoli Common Reporting à l'adresse URL : http://www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html

Restriction : Si vous souhaitez utiliser la fonction de génération de rapports et que vous installez Network Manager sur Red Hat Enterprise Linux 6.0, vous devez installer Tivoli Common Reporting version 2.1 ou 2.1.1 sur un hôte distinct, car ces versions de Tivoli Common Reporting ne sont pas prises en charge sous Red Hat Enterprise Linux 6.0. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports lors du lancement de la procédure d'installation de Network Manager en utilisant l'option `-DinstallReports=0`, comme indiqué dans les tâches d'installation dans «Installation de Network Manager», à la page 81.

Exigences supplémentaires pour Red Hat Enterprise Linux AS, ES et WS 5

Si vous installez Network Manager sous Red Hat Enterprise Linux AS, ES ou WS 5, vérifiez que les gestionnaires RPM suivants sont disponibles sur votre système avant l'installation :

- `compat-libstdc++-33-3.2.3-61`
- `libXp-1.0.0-8`
- `openmotif22-2.2.3-18`
- `libXmu-1.0.2-5`
- `libXpm-3.5.5-3`
- `compat-libstdc++-296-2.96-138`

Ces fichiers doivent figurer sur les CD ROM d'installation du système d'exploitation.

Pour plus d'informations sur l'obtention des packages, accédez au centre de documentation d'IBM WebSphere Application Server à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/as_ditamaps/welcome_nd.html, et recherchez le nom du package.

Exigences supplémentaires pour Linux on System z

Si vous utilisez Oracle 12c sur zLinux, assurez-vous que la bibliothèque suivante est installée : `libaio.so.1`.

Exigences supplémentaires pour SuSE Linux Enterprise Server (SLES)

Si vous installez Network Manager sous SLES, vous devez vous assurer que les fichiers RPM suivants sont disponibles sur votre système avant l'installation :

- `libstdc++33.rpm (anciennement appelé compat-libstdc++-5.0.7-22.2)`
- `openmotif-libs-2.2.4-21.17`
- `openmotif-devel-32bit-2.2.4-21.17`
- `openmotif-2.2.4-21.17`
- `openmotif-libs-32bit-2.2.4-21.17`
- `openmotif21-libs-32bit-2.1.30MLI4-143.9`
- `openmotif-devel-2.2.4-21.17`

Pour plus d'informations sur l'obtention des packages, accédez au centre de documentation d'IBM WebSphere Application Server à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/as_ditamaps/welcome_nd.html, et recherchez le nom du package.

Remarque : SLES 10 n'est pas compatible avec Informix 11.7. Consultez les Notes sur l'édition pour votre version de Network Manager pour plus de détails sur la base de données topologiques à installer et pour savoir comment l'obtenir et l'installer.

Configuration supplémentaire requise pour les systèmes Linux

Sur les installations Intel, Linux et IBM System z, assurez-vous que vous disposez à la fois des versions 32 bits et 64 bits des modules pam-1.1.1-10.el6.*système*. Par exemple, pour les installations System z, vérifiez que vous disposez des deux modules suivants :

- `pam-1.1.1-10.el6.s390`
- `pam-1.1.1-10.el6.s390x`

Navigateurs compatibles

Veillez à ce que les clients utilisent l'un des navigateurs Web compatibles. Si le navigateur que vous utilisez n'est pas compatible, une application Web peut se bloquer.

Le tableau suivant répertorie les navigateurs compatibles et les versions JRE (Java Runtime Environment) de chaque système d'exploitation client. Certains navigateurs fonctionnent avec des niveaux spécifiques de Tivoli Integrated Portal V2.2. Pour plus d'informations, recherchez *Tivoli Integrated Portal compatibility* dans le document *IBM Tivoli Network Manager IP Edition - Notes sur l'édition*.

Tableau 5. Navigateurs compatibles avec les systèmes d'exploitation client

Navigateur	Système d'exploitation client	Version JRE
Internet Explorer 7.0 Internet Explorer 8.0 Internet Explorer 9.0. Pris en charge dans le groupe de correctifs 2 et les versions suivantes, y compris l'actualisation de l'image du produit complet (niveau de génération 3.9.0.71). Nécessite Tivoli Integrated Portal V2.2.0.5 ou une version ultérieure. Fix Pack 4 Internet Explorer 10. Nécessite Tivoli Integrated Portal V2.2.0.13 ou version ultérieure et l'interface graphique Web Tivoli Netcool/OMNIbus V7.4.0.2 ou version ultérieure. **Restriction :** Tivoli Common Reporting version 2.x n'est pas compatible avec Internet Explorer 10. Par conséquent, vous ne pouvez pas utiliser la fonction de génération de rapport si vous utilisez Internet Explorer 10 pour l'interface graphique Network Manager.	Windows XP Service Pack 3 Windows 7 Enterprise Windows Vista Enterprise Windows Server 2008 (R1) Standard Edition Windows Server 2008 (R1) Enterprise Edition Windows Server 2008 (R2) Datacenter Edition Windows Server 2008 (R2) Enterprise Edition Windows Server 2008 (R2) Standard Edition	Oracle JRE 1.6 Fix Pack 4 Oracle JRE 1.7 Fix Pack 5 Oracle JRE 1.8 Fix Pack 4 Vérifiez que la version JRE est compatible avec Oracle JRE Security Baseline. Pour plus d'informations, voir *Deploying Java Applets With Family JRE Versions in Java Plug-in for Internet Explorer* sur le site http://www.oracle.com/technetwork/java/javase/family-clsid-140615.html.

Tableau 5. Navigateurs compatibles avec les systèmes d'exploitation client (suite)

Navigateur	Système d'exploitation client	Version JRE
Mozilla Firefox 3.6.x Firefox 10 Extended Support Release (ESR). Pris en charge dans le groupe de correctifs 2 et les versions ultérieures, y compris l'actualisation de l'image du produit complet (niveau de génération 3.9.0.71). Nécessite Tivoli Integrated Portal V2.2.0.7 ou une version ultérieure. Fix Pack 3 Firefox 17 ESR. Nécessite Tivoli Integrated Portal V2.2.0.11 ou une version ultérieure. Fix Pack 4 Firefox 24 ESR nécessite Tivoli Integrated Portal V2.2.0.13 ou une version ultérieure et l'interface graphique Web Tivoli Netcool/OMNIbus V7.4.0.2 ou une version ultérieure. **Restriction :** Tivoli Common Reporting version 2.x n'est pas compatible avec Firefox 24 ESR. Par conséquent, vous ne pouvez pas utiliser la fonction de génération de rapport si vous utilisez Firefox 24 ESR pour l'interface graphique Network Manager. Fix Pack 5 Internet Explorer 11	Red Hat Enterprise Linux Desktop 5.0 Red Hat Enterprise Linux (RHEL) 5.0 SuSE Linux Enterprise Desktop (SLED) 10 et 11 SuSE Linux Enterprise Server (SLES) 10 et 11 Solaris 9, 10 et Zones SPARC Windows XP Service Pack 3 Windows 7 Enterprise Windows Vista Enterprise Windows Server 2008 (R1) Standard Edition Windows Server 2008 (R1) Enterprise Edition Windows Server 2008 (R2) Datacenter Edition Windows Server 2008 (R2) Enterprise Edition Windows Server 2008 (R2) Standard Edition VMWare ESX Server 3.5	Oracle JRE 1.6 Fix Pack 4 Oracle JRE 1.7 Fix Pack 5 Oracle JRE 1.8 Vérifiez que la version JRE est compatible avec Oracle JRE Security Baseline. **Conseil :** UNIX Linux Vérifiez que le plug-in Java™ est correctement installé et que tous les liens symboliques nécessaires existent. Pour plus d'informations, voir la documentation de Firefox.

Navigateurs pris en charge pour le tableau de bord du programme d'installation

Pour exécuter le tableau de bord du programme d'installation, assurez-vous qu'un navigateur pris en charge est installé. Les navigateurs pris en charge ne sont pas nécessairement les mêmes que pour les applications Web.

Le tableau suivant présente les navigateurs pris en charge pour le tableau de bord du programme d'installation.

Restriction : Linux Sous Red Hat Enterprise Linux et SUSE Enterprise Linux (S/390 et S/390x uniquement), seul Firefox 2.x est pris en charge.

Tableau 6. Navigateurs pris en charge pour le tableau de bord du programme d'installation

Navigateur	Version
Firefox	2.0 et suivantes
Mozilla	1.7 et suivantes
Internet Explorer	6.0
SeaMonkey	1.1.4 et suivantes

Outils de système d'exploitation

La stabilité du processus d'installation dépendant de celle des outils du système d'exploitation, vérifiez que les versions de système d'exploitation des outils standard apparaissent avant les autres versions (utilitaires GNU, par exemple) des mêmes outils dans votre chemin.

Exigences du service de noms de domaine (DNS)

Vérifiez que le DNS des serveurs est configuré correctement avant d'installer Network Manager.

Noms de domaine

Vérifiez que tous les serveurs sur lesquels vous voulez installer des composants de Network Manager ont un nom d'hôte défini comme nom de domaine complet. Une configuration DNS incomplète ou incorrecte peut occasionner des problèmes lors de l'installation ou de l'utilisation de Network Manager.

UNIX Sur les plateformes UNIX, le nom d'hôte est défini dans le fichier `/etc/hosts`.

Windows Sous Windows, le nom d'hôte est défini dans le fichier `%WinDir%\system32\drivers\etc\hosts`.

Sur la machine sur laquelle vous installez les composants Network Manager, veillez à inclure l'adresse IP, le nom de domaine complet et le nom abrégé dans le fichier `/etc/hosts` dans le fichier avant d'installer Network Manager,, et vérifiez que le nom de domaine complet et le nom abrégé sont résolus uniquement dans la même adresse IP, et résolus en inverse en nom de domaine complet ou nom abrégé.

Le format est *`adresse IP Nom de domaine complet nom abrégé`*. Par exemple, ajoutez une ligne similaire à la ligne suivante à `/etc/hosts`:
`9.10.11.12 yourserver.domainname.com yourserver`

Ainsi, le nom de domaine complet est défini comme entrée de nom d'hôte lorsque Network Manager est installé.

Restriction : N'utilisez pas de trait de soulignement lors de la spécification des noms d'hôte. Sinon, l'installation de Tivoli Integrated Portal échouerait.

Restrictions utilisateur UNIX

Sous les systèmes d'exploitation UNIX, si vous avez installé d'autres produits Tivoli Network Management sur un serveur spécifique, vous devez installer Network Manager dans le même répertoire et sous le même nom d'utilisateur.

Si vous installez les applications Web Network Manager en tant que superutilisateur, Network Manager ne s'intègre pas avec IBM Tivoli Business Service Manager. Si vous souhaitez utiliser Network Manager avec TBSM, vous devez créer un autre utilisateur afin d'installer et de gérer tous les produits Tivoli sur ce serveur.

Si vous installez Network Manager en tant que non superutilisateur, vous devez effectuer une procédure de configuration supplémentaire après l'installation afin d'exécuter les composants centraux en tant que superutilisateur.

Si vous installez Network Manager en tant que non superutilisateur, vous devrez installer tous les produits Tivoli ultérieurs sous le même nom d'utilisateur.

Si vous installez et exécutez Network Manager en tant que non superutilisateur, vous ne pouvez pas installer deux versions différentes de Network Manager sur le même serveur.

Tâches associées:

«Configuration des autorisations d'utilisateur root/non root», à la page 248
Sous UNIX, si vous avez installé Network Manager en tant qu'utilisateur non root, vous devez effectuer une configuration supplémentaire.

Restrictions utilisateur Windows

Sous les systèmes d'exploitation Windows, tous les produits de gestion de réseau Tivoli doivent être installés dans le même répertoire, par le même utilisateur.

Vous pouvez installer Network Manager en tant qu'utilisateur administrateur.

Restriction : Vous devez être l'utilisateur administrateur pour effectuer l'installation sur des systèmes Windows Server 2008.

Vous devez également disposer du droit d'accès en écriture au répertoire d'installation ainsi que des privilèges d'administration sur le poste de travail.

Configuration requise pour les zones Solaris

Si vous installez Network Manager sur des serveurs exécutant des zones Solaris 10, certaines tâches de configuration supplémentaires peuvent être nécessaires.

Installation sur des zones globales

Il n'existe pas d'exigence spécifique pour l'installation de Network Manager dans des zones Solaris globales.

Installation dans des zones locales

Si vous prévoyez d'effectuer l'installation dans une zone locale, configurez d'abord cette dernière pour autoriser Network Manager à générer ses propres paquets bruts. Une zone locale par défaut n'autorise pas les applications à l'exécuter pour générer ses propres paquets bruts.

Pour configurer Network Manager de sorte qu'il génère ses propres paquets, configurez la zone afin qu'elle inclue le privilège net-rawaccess, comme indiqué dans les étapes suivantes.

1. Dans la zone locale, entrez les commandes suivantes :

   ```
   zonecfg -z nom_zone
   zonecfg:nom_zone> set limitpriv=default,net_rawaccess
   zonecfg:nom_zone> verify
   zonecfg:nom_zone> commit
   zonecfg:nom_zone> exit
   ```

   Où *nom_zone* correspond au nom de la zone locale.

2. Arrêtez et réamorcez la zone afin de sélectionner les nouveaux paramètres.

   ```
   zlogin nom_zone shutdown
   zoneadm -z nom_zone boot
   ```

3. Vérifiez que le privilège a été ajouté avec succès par le biais de la commande `ppriv`. L'exemple suivant présente un exemple de sortie de cette commande à laquelle le privilège net-rawaccess a été ajouté.

   ```
   # ppriv $$
   4547:   -sh
   flags =

   E: basic,contract_event,contract_observer,file_chown,
   file_chown_self,file_dac_execute,file_dac_read,
   file_dac_search,file_dac_write,file_owner,file_setid,
   ipc_dac_read,ipc_dac_write,ipc_owner,
   net_bindmlp,net_icmpaccess,net_mac_aware,net_privaddr,
   net_rawaccess,proc_audit,proc_chroot,proc_owner,
   proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
   sys_mount,sys_nfs,sys_resource

   I: basic
   P: basic,contract_event,contract_observer,file_chown,
   file_chown_self,file_dac_execute,file_dac_read,
   file_dac_search,file_dac_write,file_owner,file_setid,
   ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,
   net_icmpaccess,net_mac_aware,net_privaddr,
   net_rawaccess,proc_audit,proc_chroot,proc_owner,
   proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
   sys_mount,sys_nfs,sys_resource

   L: basic,contract_event,contract_observer,file_chown,
   file_chown_self,file_dac_execute,file_dac_read,
   file_dac_search,file_dac_write,file_owner,file_setid,
   ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,
   net_icmpaccess,net_mac_aware,net_privaddr,
   net_rawaccess,proc_audit,proc_chroot,proc_owner,
   proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
   sys_mount,sys_nfs,sys_resource
   ```

Les zones racine complète et les zones éparses sont des variantes de la zone locale. La section suivante présente en détail les exigences requises pour ces types de zone.

Installation dans des zones racine complète

Il n'existe pas d'exigence spécifique pour l'installation de Network Manager dans des zones racine complète.

Installation dans des zones éparses

Dans une installation par défaut, le Tivoli Integrated Portal est installé automatiquement. Dans une installation personnalisée, vous pouvez choisir d'installer ou non le Tivoli Integrated Portal. Lorsque le Tivoli Integrated Portal est installé, certains fichiers utilisés par un composant appelé moteur

de déploiement sont placés dans le répertoire /usr/ibm/common/acsi. Dans des zones éparses, l'utilisateur root ne dispose pas des droits d'accès en écriture au répertoire /usr, ce qui cause l'échec de l'installation de Tivoli Integrated Portal.

Si vous souhaitez installer le Tivoli Integrated Portal en tant qu'utilisateur root dans une zone éparse, vous ne pouvez pas utiliser le tableau de bord du programme d'installation. Vous devez lancer l'installation à partir de la ligne de commande et remplacer l'emplacement par défaut du moteur de déploiement à l'aide du paramètre suivant :

```
-DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi
```

Où /opt/ibm/common/acsi est un répertoire quelconque pour lequel l'utilisateur root dispose des droits d'accès en écriture.

Exemples de commandes pour l'installation en tant qu'utilisateur root dans une zone éparse

Utilisez des commandes similaires à celles-ci pour effectuer l'installation en tant qu'utilisateur root dans une zone éparse.

Mode interface graphique

```
./install.sh -DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi –i gui
```

Mode console

```
./install.sh -DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi –i console
```

Mode silencieux

Modifiez le fichier de réponses exemple, en ajoutant la ligne IAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi après la ligne : IAGLOBAL_INSTALL_LOCATION_SELECTION=create.

IBM Tivoli License Compliance Manager

Network Manager est compatible avec IBM Tivoli License Compliance Manager. IBM Tivoli License Compliance Manager vous permet de surveiller et de gérer votre utilisation des logiciels IBM et des accords de licence.

Network Manager ne nécessite pas de clé de licence pour s'exécuter. IBM Tivoli License Compliance Manager est disponible séparément de Network Manager.

Configuration requise pour Windows Installer

Vous devez disposer de la version de Windows Installer appropriée pour votre version de Windows.

Pour Windows 64 bits

Avant d'effectuer l'installation sur Windows 2008 Server 64 bits, vous devez installer Windows Installer version 4.5.

Par défaut, Windows Installer version 4.0 est fourni avec Windows 2008 Server. Network Manager ne s'installe pas correctement avec Windows Installer version 4.0 sous les systèmes 64 bits.

Pour savoir quelle version de Windows Installer est installée, exécutez la commande **msiexec -help** dans l'invite de commande. Vous pouvez télécharger Windows Installer version 4.5 en recherchant "Windows Installer 4.5" à l'adresse suivante :

http://www.microsoft.com/downloads

Pour les autres versions de Windows

Pour toutes les versions de Windows à l'exception de Windows 64 bits 2008 Server, vérifiez que vous disposez de Windows Installer version 3.1 ou ultérieure avant d'installer Network Manager.

Exigences relatives au répertoire d'installation

Le répertoire dans lequel vous installez Network Manager doit répondre à certaines exigences.

Exigences communes à tous les systèmes d'exploitation

Par défaut, le programme d'installation place les produits Tivoli Network Management dans le même répertoire.

Le chemin complet d'accès au répertoire d'installation ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9), des tirets, des traits de soulignements, des points, deux points, des barres obliques ou des espaces.

Exigences des systèmes d'exploitation UNIX

L'utilisateur installant Network Manager doit avoir le droit d'accès en écriture sur le répertoire d'installation et, s'il est différent, sur le répertoire `/opt`.

Exigences de Windows

Sous Windows, vous ne pouvez pas procéder à l'installation sur une unité réseau mappée. L'installation ne peut avoir lieu que sur un disque physique ou une partition de bas niveau d'un disque physique visible par tous les utilisateurs Windows.

Si vous souhaitez utiliser une base de données Oracle pour les données topologiques, vous devez installer Network Manager dans un emplacement ne contenant aucune occurrence du caractère "(". Si vous installez Network Manager dans un emplacement contenant le caractère "(", vous devez télécharger un correctif d'Oracle comme décrit dans l'incident Oracle #3807408, puis configurer et renseigner la base de données topologiques NCIM manuellement après l'installation du correctif Oracle.

Exigences du programme d'installation

Le programme d'installation installe des fichiers dans le répertoire d'installation principal que vous choisissez au cours du processus d'installation. Il installe également des fichiers dans d'autres répertoires, en fonction du système d'exploitation en cours d'installation et de l'utilisateur procédant à ladite installation. Passez en revue la structure de répertoire par défaut et vérifiez que l'utilisateur dispose d'un accès en écriture sur les répertoires appropriés.

Référence associée:

«Structure de répertoire par défaut», à la page 374
Utilisez ces informations pour comprendre la structure de répertoire de Network Manager.

Exigences relatives au descripteur de fichier

Sur les systèmes d'exploitation UNIX et Linux, vérifiez qu'un nombre suffisant de descripteurs de fichier est autorisé.

Si vous installez Network Manager sur un système d'exploitation UNIX ou Linux, vérifiez que le nombre de fichiers ouverts pour les processus est défini avec une valeur appropriée dans tous les environnements pour l'utilisateur qui exécute Network Manager. Définissez une valeur minimale de 512 pour le nombre de fichiers ouverts sur le serveur sur lequel les composants de base sont installés, et de 8192 pour le serveur d'interface graphique. Vous pouvez vérifier cette valeur à l'aide de la commande suivante en tant qu'utilisateur exécutant Network Manager : `ulimit -n`

Si cette valeur est trop faible, prenez contact avec votre administrateur système afin de l'augmenter pour votre utilisateur.

Exemples d'utilisation de la commande pour l'augmentation de la valeur :

AIX `chuser nofiles=8192 ID_utilisateur`

Solaris, Linux et Linux on System z

```
ulimit -n 8192
```

Définissez le nombre de processus par utilisateur défini avec un minimum de 1024. Vous pouvez vérifier cette valeur à l'aide de la commande suivante : `ulimit -u`

Remarque : La valeur 1024 est un minimum et cette valeur peut devoir être adaptée pour votre environnement en fonction de vos besoins.

Configuration requise pour Représentations graphiques

Représentations graphiques est un composant en option qui vous permet d'afficher des graphiques à partir des produits Tivoli pris en charge, ainsi que les graphiques créés avec le concepteur Outils Business Intelligence and Reporting.

L'option Représentations graphiques installe également service Web ITM avec Tivoli Integrated Portal Server. Lorsque Tivoli Management Services fait partie de votre infrastructure réseau service Web ITM est utilisé pour obtenir les valeurs d'attribut collectées par vos produits IBM Tivoli Monitoring or OMEGAMON XE et les placer dans des portlets de graphique sur la console.

Important : Si votre doit utiliser service Web ITM, lisez la rubrique «Configuration d'une connexion unique entre le module Représentations Graphiques et Tivoli Monitoring», à la page 385 avant l'installation de Tivoli Integrated Portal.

Votre produit peut avoir été mis à disposition avec des graphiques prédéfinis, ou bien le format des graphiques peut être inapproprié pour votre produit. Dans les deux cas, si l'option Représentations graphiques n'a pas été jointe à votre produit, vous ne verrez pas apparaître cette option lors d'une installation avancée.

Connexion à un service Web sécurisé

Représentations graphiques prend en charge le protocole HTTPS pour la confidentialité. Lors d'une demande de données depuis la portail vers le serveur d'applications IBM Tivoli Monitoring (serveur Tivoli Enterprise Portal), les données d'identification de l'utilisateur connecté sont dirigés sur le service Web pour authentification et autorisation. En cas de demande d'extraction de données Tivoli Monitoring dans un portlet de graphique, le nom d'utilisateur et le mot de passe fournis lors de l'installation sont transmis au serveur Tivoli Enterprise Portal et un jeton LTPA est transmis au service Web d'arrière plan.

Pour bénéficier de cette connexion sécurisée, le service Web ITM doit être installé et s'exécuter sur la même instance de Tivoli Integrated Portal Server.

Chapitre 2. Installation

Utilisez ces informations pour planifier et réaliser une installation de Network Manager.

Une fois l'installation terminée, il peut être nécessaire d'effectuer les tâches de configuration.

Préparation à l'installation

Avant de démarrer l'installation de Network Manager, vous devez récupérer puis extraire le module d'installation, puis réaliser des tâches supplémentaires (selon votre installation).

Si vous souhaitez intégrer Network Manager à une installation existante de Tivoli Netcool/OMNIbus sur un autre serveur, vous devez configurer l'installation Tivoli Netcool/OMNIbus avant d'installer Network Manager.

Il vous faut réaliser des tâches supplémentaires avant de procéder à l'installation de Network Manager sur un système d'exploitation AIX.

Informix est la base de données topologiques par défaut fournie avec Network Manager ; vous pouvez aussi utiliser une base de données Informix existante. Si vous voulez utiliser une base de données DB2, MySQL, Oracle ou une une base de données Informix distante pour les données topologiques, vous devez effectuer des tâches supplémentaires après avoir extrait le package d'installation et avant d'installer Network Manager.

Cliquez sur le lien suivant pour extraire des remarques techniques sur les problèmes d'installation connus dans la version 3.9 de Network Manager : http://www-01.ibm.com/support/search.wss?word=ow&wfield=install+installation+installing&rs=3118&tc=SSSHRK&atrn=SWVersion&atrv=3.9&ibm-go.x=18&ibm-go.y=12

Restriction : Tous les mots de passe que vous choisissez pour Network Manager doivent être conformes aux règles de mot de passe de l'environnement serveur ou système.

Configuration d'une installation Tivoli Netcool/OMNIbus existante

Si vous souhaitez intégrer Network Manager à une installation existante de Tivoli Netcool/OMNIbus sur un autre serveur ou à une installation existante de Tivoli Netcool/OMNIbus antérieure à la version 7.3.1 sur le même serveur, vous devez configurer l'installation de Tivoli Netcool/OMNIbus avant d'installer Network Manager.

Si vous installez Tivoli Netcool/OMNIbus 7.3.1 lors de l'installation de Network Manager, il n'est pas nécessaire d'effectuer cette tâche.

Si vous souhaitez intégrer Network Manager à une installation existante de Tivoli Netcool/OMNIbus 7.3.1 sur le même serveur, il n'est pas nécessaire d'effectuer cette tâche.

Avertissement : L'utilisation du programme d'installation de Network Manager pour configurer une instance existante de Tivoli Netcool/OMNIbus installe également la sonde SNMP et Netcool/OMNIbus Knowledge Library. Si vous ne voulez pas remplacer votre sonde SNMP existante et vos personnalisations Netcool/OMNIbus Knowledge Library existantes, vous devez sélectionner **Ne pas installer ou configurer Tivoli Netcool/OMNIbus à ce stade** lorsque la question vous est posée dans le panneau **Sélection des composants à installer** sous **Tivoli Netcool/OMNIbus**. Après l'installation, copiez le package d'installation vers le serveur où se trouve votre installation existante de Tivoli Netcool/OMNIbus et exécutez le script **ConfigOMNI** pour configurer Tivoli Netcool/OMNIbus, mais assurez-vous de ne pas sélectionner d'options pour configurer la sonde SNMP ou Netcool/OMNIbus Knowledge Library.

Restriction : Vous devez installer Network Manager 3.9 dans un autre **répertoire** pour une installation existante de Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure. Sous Windows, vous devez installer Network Manager 3.9 sur un autre **serveur** pour une installation existante de Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure.

Restriction : Du fait d'un problème connu, le programme d'installation de Network Manager 3.9 ne peut pas installer ou configurer Tivoli Netcool/OMNIbus 7.4 sur les systèmes Linux et Solaris. Par conséquent, le script **ConfigOMNI** fourni avec Network Manager 3.9 ne peut pas configurer Tivoli Netcool/OMNIbus 7.4 sur les systèmes Linux et Solaris. Pour plus d'informations sur ce problème et sa solution, voir la note technique de traitement de l'incident http://www-01.ibm.com/support/docview.wss?uid=swg21615671.

Pour configurer un composant Tivoli Netcool/OMNIbus existant pour une utilisation avec Network Manager, procédez comme suit.

1. Assurez-vous que vous disposez d'une installation ObjectServer Tivoli Netcool/OMNIbus à configurer.
2. Si votre installation Tivoli Netcool/OMNIbus est une version 7.2.1, assurez-vous d'avoir installé le correctif libncrypt de Tivoli Netcool/OMNIbus 7.2.1 (disponible sur le support d'installation de Network Manager 3.9).
3. Téléchargez et décompressez le package d'installation de Network Manager sur le serveur qui contient l'installation de Tivoli Netcool/OMNIbus.
4. Si vous configurez Tivoli Netcool/OMNIbus version 7.2.1, 7.3 ou 7.3.1, téléchargez le package d'installation pour la version appropriée de la sonde SNMP (également appelée sonde MTTRAPD).
5. Démarrez le script de configuration à partir du tableau de bord du programme d'installation ou de la ligne de commande.

Option	Description
Exécutez le script à partir du tableau de bord.	1. Selon votre système d'exploitation, démarrez le tableau de bord en exécutant le script **launchpad.sh** sous UNIX ou le fichier exécutable **launchpad.exe** sous Windows. 2. Accédez à **Préinstallation et migration** et développez la section **Configuration d'une installation existante de Netcool/OMNIbus**. 3. Cliquez sur **Configurer une installation existante de Netcool/OMNIbus**. 4. Entrez les données d'identification d'accès pour l'élément ObjectServer à configurer.
Exécutez le script à partir du répertoire scripts du package d'installation.	• Selon votre système d'exploitation, exécutez le script ConfigOMNI.sh sous UNIX ou le script ConfigOMNI.bat sous Windows. • Entrez les données d'identification d'accès pour l'élément ObjectServer à configurer.

Si vous installez Tivoli Netcool/OMNIbus dans le cadre de l'installation de Network Manager, le programme d'installation ajoute les utilisateurs itnmadmin et itnmuser au serveur ObjectServer, active le chiffrement AES, active le contrôle de processus pour le serveur Objectserver, et installe la sonde SNMP, ainsi que Netcool/OMNIbus Knowledge Library.

Si vous utilisez l'utilitaire **ConfigOMNI** (depuis le tableau de bord ou la ligne de commande), vous pouvez choisir quelles options sont configurées à l'aide des arguments de ligne de commande appropriés. Si vous configurez Tivoli Netcool/OMNIbus version 7.2.1, 7.3 ou 7.3.1, spécifiez le package d'installation pour la version appropriée de la sonde SNMP à l'aide de l'argument de ligne de commande -m.

6. Obligatoire : Après avoir configuré Tivoli Netcool/OMNIbus, installez Network Manager.
   a. Lors de l'installation, sélectionnez l'option permettant d'utiliser une installation existante de Tivoli Netcool/OMNIbus.
   b. Indiquez les détails de l'élément ObjectServer configuré à l'aide du script.
7. Facultatif : Si vous avez Tivoli Netcool/OMNIbus version 7.2.1 ou 7.3, le processus nco_p_ncpmonitor peut échouer en raison de l'absence des zones NmosEventMap et BSM_Identity dans le serveur ObjectServer. Assurez-vous que votre serveur ObjectServer est en cours d'exécution et exécutez le script **ncp_configure_omnibus.sql** comme décrit dans «Ajout de zones d'événement», à la page 180.

Options de ligne de commande ConfigOMNI

Utilisez le script **ConfigOMNI** avec des arguments avancés facultatifs pour configurer Tivoli Netcool/OMNIbus pour qu'il puisse être utilisé avec Network Manager avant d'installer Network Manager.

Le script **ConfigOMNI** est démarré par le biais de la ligne de commande suivante. Les arguments facultatifs sont présentés entre crochets.

```
ConfigOMNI -o nom -p mot de passe [ -a ] [ -c ] [ -e ] [ -h répertoire ] [ -k package ]
 [ -m package ] [ -n numéroport ] [ -u mot de passe ]
```

L'exemple suivant exécute le script dans ObjectServer DIAMOND avec le mot de passe d'administration p3w0d. Si ObjectServer DIAMOND n'existe pas, il est créé. A l'aide des options appropriées, vous pouvez configurer le script pour ajouter les utilisateurs itnmadmin et itnmuser à ObjectServer, activer le chiffrement AES et le contrôle de processus pour Objectserver, et installer la sonde SNMP, ainsi que Netcool/OMNIbus Knowledge Library.

Remarque : Le script **ConfigOMNI** n'effectue aucune configuration sauf si les options appropriées de la ligne de commande sont fournies ou si vous répondez aux questions appropriées.

```
ConfigOMNI -o DIAMOND -p p3w0d
```

Remarque : Le script **ConfigOMNI** est utilisé lors de la première configuration d'un serveur ObjectServer. Si ce script est exécuté plusieurs fois sur le même hôte, il peut s'avérer nécessaire d'éditer les fichiers suivants :

1. Fichier `nco_p_mttrapd.props` pour supprimer les propriétés en double `Server`, `ServerBackup`, `RulesFile`, `MIBFile` et `QuietOutput` à la fin du fichier.
2. Fichier `nco_pa.conf` pour modifier les noms en double `nco_process` car le script fournit toujours des entrées ayant pour nom `MasterObjectServer` et `Mttrapd`. Pour plus d'informations sur l'édition de ce fichier, voir la documentation Tivoli Netcool/OMNIbus à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html et recherchez la rubrique "Defining processes in the process agent configuration file".

Le tableau suivant décrit les options de ligne de commande pour le script **ConfigOMNI**.

Tableau 7. Options de ligne de commande ConfigOMNI

Options de ligne de commande	Description
`-o` *nom*	Nom du serveur ObjectServer que vous voulez créer ou configurer.
`-p` *mot de passe*	Mot de passe d'administration du serveur ObjectServer que vous voulez créer ou configurer.
`-a`	Facultatif. Exécute le script en mode interactif, ce qui fait que des invites sont émises pour toutes les informations.
`-c`	Facultatif. Configure ObjectServer pour qu'il s'exécute sous le contrôle du processus Tivoli Netcool/OMNIbus. Cela est nécessaire pour que les scripts **itnm_start**, **itnm_stop** et **itnm_status** fonctionnent correctement avec ObjectServer.

Tableau 7. Options de ligne de commande ConfigOMNI (suite)

Options de ligne de commande	Description
`-e`	Facultatif. Définit le chiffrement AES pour le mot de passe ObjectServer.
`-h` *répertoire*	Facultatif. Répertoire contenant l'installation Tivoli Netcool/OMNIbus (OMNIHOME).
`-k` *package*	Facultatif. Installe Netcool/OMNIbus Knowledge Library à partir de ce package. Vous devez spécifier le chemin d'accès au package s'il n'est pas dans le répertoire en cours.
`-m` *package*	Facultatif. Installe SNMP Probe à partir de ce package. Vous devez spécifier le chemin d'accès au package s'il n'est pas dans le répertoire en cours.
`-n` *numéroport*	Facultatif. Numéro de port du serveur ObjectServer que vous voulez créer ou configurer.
`-u` *mot de passe*	Facultatif. Créez les utilisateurs itnmadmin et itnmuser dans l'ObjectServer.

Décompression du fichier d'installation

Si vous avez téléchargé le fichier d'installation, vous devez décompresser le module d'installation avant d'installer le produit.

Pour décompresser le fichier d'installation, procédez comme suit :

Décompressez le fichier.

- UNIX Entrez la commande suivante : `gunzip -d < fichier_installation.tar.gz | tar xvf -`
- Windows Cliquez avec le bouton droit de la souris sur le fichier d'archivage et décompressez-le à l'aide d'une fonctionnalité de décompression quelconque installée.

Vérification des prérequis du système

Le tableau de bord du produit inclut un programme de vérification des prérequis qui vous permet de vérifier qu'un ordinateur est adapté pour l'installation du produit Network Manager ou de composants individuels du produit. Vous pouvez également télécharger et utiliser le scanner de prérequis IBM Prerequisite Scanner, un utilitaire distinct conçu pour la vérification de systèmes.

IBM Prerequisite Scanner V1.2.0.10 prend en charge Network Manager V3.9. IBM Prerequisite Scanner est un outil autonome de vérification des prérequis qui analyse les environnements système avant l'installation ou la mise à niveau d'un produit Tivoli ou d'une solution IBM solution. IBM Prerequisite Scanner n'est pas inclus dans le produit Network Manager. Il peut être téléchargé depuis IBM Fix Central. Vous pouvez utiliser IBM Prerequisite Scanner à la place de la fonction de vérification des éléments prérequis du programme d'installation et tableau de bord Network Manager. Cet outil s'avère utile sur les ordinateurs hôte comportant plusieurs produits ou solutions car il peut évaluer l'adéquation de l'ordinateur pour plusieurs produits. Pour plus d'informations sur comment télécharger et

exécuter l'outil, ainsi que sur les produits pris en charge, voir http://www-01.ibm.com/support/docview.wss?uid=swg24031503.

Pour utiliser le tableau de bord, installez un navigateur prenant en charge le tableau de bord. En outre, téléchargez et décompressez le module d'installation.

Pour exécuter le tableau de bord et vérifier qu'un ordinateur est adapté pour l'installation de Network Manager :

1. Démarrez le tableau de bord en exécutant l'utilitaire **launchpad**.
2. Cliquez sur **Informations prérequises** et entrez le chemin d'installation dans la zone **Emplacement d'installation**.
3. Sélectionnez les composants à vérifier et cliquez sur **Vérifier les prérequis du système**.

Les résultats de la vérification s'affichent, indiquant si l'ordinateur est adapté à l'installation des composants de votre choix.

Référence associée:

«Navigateurs pris en charge pour le tableau de bord du programme d'installation», à la page 48
Pour exécuter le tableau de bord du programme d'installation, assurez-vous qu'un navigateur pris en charge est installé. Les navigateurs pris en charge ne sont pas nécessairement les mêmes que pour les applications Web.

Configuration d'une base de données topologiques

A part la base de données Informix par défaut, vous pouvez utiliser une base de données DB2, MySQL ou Oracle pour stocker votre topologie. A moins que vous n'installiez la base de données Informix par défaut livrée avec Network Manager, vous devez configurer une base de données existante ou en installer et configurer une nouvelle avant d'installer Network Manager.

Vous disposez des options suivantes pour configurer une base de données pour votre topologie:

- Vous pouvez installer et configurer la base de données Informix par défaut livrée avec Network Manager et l'implanter à l'aide du programme d'installation de Network Manager. Dans ce cas, vous n'avez pas besoin de suivre l'une des tâches de configuration de base de données avant d'installer Network Manager. Vous pouvez lancer le programme d'installation et sélectionnner les options pour la configuration d'une nouvelle base de données Informix.
- Si vous désirez utiliser une base de données Informix existante sur un hôte local ou distant, vous devez la configurer avant d'installer Network Manager comme décrit dans les tâches suivantes qui expliquent comment configurer des bases de données Informix existantes sur votre plateforme.
- Si vous désirez utiliser une base de données DB2, MySQL ou Oracle, vous devez effectuer les tâches de configuration de la base de données concernée sur votre plateforme. Le processus d'installation et de configuration est différent en fonction du type de base de données et du système d'exploitation.

Remarque : UNIX Linux Pour installer Informix dans le cadre d' une installation non root, définissez les droits d'accès à tous les répertoires dans le chemin Informix sur 775. Par exemple, sur un hôte linux dans lequel la variable d'environnement $NCHOME est définie sur `/home/IBM/tivoli/`, le chemin Informix est `/home/IBM/tivoli/platform/linux2x86/users/informix/`. Dans cet exemple, définissez les droits des répertoires suivants sur 775 :

- /home/
- /home/IBM/
- /home/IBM/tivoli/
- /home/IBM/tivoli/platform/
- /home/IBM/tivoli/platform/linux2x86/
- /home/IBM/tivoli/platform/linux2x86/users/
- /home/IBM/tivoli/platform/linux2x86/users/informix/

Vous devez configurer les bases de données pour Network Manager après avoir décompressé le package d'installation de Network Manager et avant de lancer l'installation du produit. Pour plus d'informations sur la configuration de votre base de données pour une installation existante de Network Manager, reportez-vous à la rubrique Reportez-vous aux tâches concernant la création de schémas de base de données topologiques dans le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Important : Appliquez tous les correctifs recommandés à la base de données.

Tâches associées:

«Configuration de NCIM pour Tivoli Common Reporting», à la page 287
Si vous souhaitez utiliser Informix, MySQL ou Oracle en tant que base de données NCIM, vous devez configurer les bases de données pour pouvoir utiliser des rapports Tivoli Common Reporting.

Référence associée:

«Bases de données topologiques prises en charge», à la page 38
Par défaut, une base de données IBM Informix est incluse dans le produit pour stocker les données de topologie. D'autres types de bases de données sont compatibles. Si vous n'utilisez pas la base de données par défaut, utilisez uniquement une base de données compatible.

Configuration d'une base de données Informix existante sous UNIX

Pour utiliser une base de données Informix existante en tant que base de données topologiques sous UNIX, vous devez configurer une instance, préparer un espace dbspace et créer une base de données avant d'installer Network Manager.

Remarque : Vous ne devez suivre cette procédure que si vous désirez utiliser une base de données Informix locale ou distante existante pour votre installation Network Manager. Si vous désirez installer et configurer une nouvelle base de données Informix sur un hôte local ou distant pour Network Manager, vous pouvez utiliser la base de données Informix livrée avec Network Manager et la mettre en place à l'aide du programme d'installation de Network Manager.

La base de données est créée par des scripts situés dans le répertoire `/PrecisionIP/scripts` de l'image d'installation extraite. Vous devez avoir décompressé le module d'installation avant de configurer votre base de données Informix existante.

Vous devez configurer l'environnement Informix en tant qu'administrateur Informix sur le serveur d'hébergement Informix. Si l'hôte réside sur un serveur distant, copiez les scripts de création de base de données sur le serveur distant.

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée sur la base de données Informix créée.

1. Accédez à l'hôte sur lequel votre Informix existant est installé.
2. Employez l'utilitaire de ligne de commande `onspaces` Informix pour créer un espace de base de données pour allouer l'espace disque nécessaire pour les tables de base de données NCIM. Vous pouvez créer l'espace de base de données à tout emplacement sur votre système de fichiers, à condition que l'espace disque soit suffisant à cet emplacement pour l'espace de base de données puisse s'accroître en même temps que la base de données.
   a. Créez deux fichiers vides et nommez ces derniers de la manière suivante : *ncimdbspace* pour stocker les tables de base de données normales et *ncimsbspace* pour stocker les tables de base de données contenant des objets BLOB. Vérifiez que ce fichier est accessible en lecture et en écriture par l'utilisateur informix et le groupe informix. Pour effectuer cette action sous UNIX, définissez un masque de fichier de 660.
   b. Créez l'espace de base de données à l'aide de l'utilitaire de ligne de commande `onspaces` Informix, comme cela est présenté dans l'exemple suivant.

      ```
      onspaces -c -d ncimdbspace -p nomchemin/ncimdbspace -o 0 -s
      1000000
      onspaces -c -S ncimsbspace -p nomchemin/ncimsbspace -o 0 -s 100000
      ```

      où :

      nomchemin
      correspond au chemin du répertoire contenant l'espace de base de données.

      Cette commande crée un espace de base de données nommé *ncimdbspace* d'environ 1 Go dans un fichier portant le même nom et un deuxième espace de base de données plus petit pour les objets BLOB nommé *ncimsbspace*. Pour plus d'informations sur la ligne de commande `onspaces`, voir la documentation Informix.
3. Basculez sur le répertoire `/PrecisionIP/scripts` de l'image d'installation extraite.
4. Facultatif : Si vous configurez Informix sur un serveur autre que Network Manager, copiez le script `create_informix_database.sh` sur l'hôte distant sur lequel vous avez installé Informix.
5. Pour créer la base de données, entrez la commande suivante : `./create_informix_database.sh` *`nom_base_de_données nom_utilisateur`*, où :

   nom_base_de_données
   Nom, requis, de la base de données à créer, également utilisé comme préfixe pour le nom de la base de données de données d'interrogation

   nom_utilisateur
   Utilisateur Network Manager Informix à utiliser pour se connecter à la base de données.

   Important : Cet utilisateur ne doit pas être l'administrateur. Il doit s'agir d'un utilisateur existant du système d'exploitation.

   Par exemple, pour créer une base de données Informix appelée «NCIM» destinée à l'utilisateur Informix «ncim», entrez `create_informix_database.sh NCIM ncim`. Une fois la commande exécutée, la base de données Informix est créée. Pour plus d'informations sur le mode d'installation et de configuration d'Informix, voir la documentation Informix.

6. Lors de l'exécution du programme d'installation de Network Manager par la suite, veillez à sélectionner l'option **Démarrer l'installation personnalisée**. Ensuite, dans le panneau Sélection des options d'installation, vous devez sélectionner **Nombre de serveurs** > **Installation multiserveur** (même si vous installez Network Manager sur le même serveur qu'Informix), et sélectionner également **Valeurs par défaut** > **Personnaliser les paramètres**. Vous avez ensuite la possibilité de vous connecter à une base de données Informix existante. Cette opération est nécessaire pour s'assurer que le programme d'installation définisse correctement les variables d'environnement Informix de Network Manager et le fichier de configuration `DbLogins` (par exemple, les valeurs `INFORMIXDIR` et `m_DbServer` sont définies comme requises). Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

Après avoir créé la base de données, vous devez effectuer la procédure suivante sur le serveur qui héberge la base de données Informix pour permettre aux processus Java de trouver cette base de données :

1. Editez le fichier sur lequel pointe la variable d'environnement `INFORMIXSQLHOSTS`.
2. Modifiez la zone Nom d'hôte en lui ajoutant en préfixe un astérisque (par exemple, remplacez *`nom_d'hôte`* par *`*nom_d'hôte`*. La zone Nom d'hôte est généralement la troisième zone sur la dernière ligne du fichier.
3. Arrêtez et redémarrez Informix à l'aide des commandes `onmode -ky` et `oninit`.

Configuration d'une base de données Informix existante sous Windows

Pour utiliser une base de données Informix existante en tant que base de données topologiques sous Windows, vous devez configurer une instance et créer une base de données avant d'installer Network Manager.

Remarque : Vous ne devez suivre cette procédure que si vous désirez utiliser une base de données Informix locale ou distante existante pour votre installation Network Manager. Si vous désirez installer et configurer une nouvelle base de données Informix sur un hôte local ou distant pour Network Manager, vous pouvez utiliser la base de données Informix livrée avec Network Manager et la mettre en place à l'aide du programme d'installation de Network Manager.

La base de données est créée par des scripts situés dans le répertoire `\PrecisionIP\scripts` de l'image d'installation extraite. Vous devez avoir décompressé le module d'installation avant de configurer votre base de données Informix existante.

Vous devez configurer l'environnement Informix en tant qu'administrateur Informix sur le serveur d'hébergement Informix. Si l'hôte réside sur un serveur distant, copiez les scripts de création de base de données sur le serveur distant.

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée sur la base de données Informix créée.

1. Accédez à l'hôte sur lequel votre Informix existant est installé.
2. Employez l'utilitaire de ligne de commande `onspaces` Informix pour créer un espace de base de données pour allouer l'espace disque nécessaire pour les tables de base de données NCIM. Vous pouvez créer l'espace de base de données à tout emplacement sur votre système de fichiers, à condition que

l'espace disque soit suffisant à cet emplacement pour l'espace de base de données puisse s'accroître en même temps que la base de données.

a. Créez deux fichiers vides et nommez ces derniers de la manière suivante : *ncimdbspace* pour stocker les tables de base de données normales et *ncimsbspace* pour stocker les tables de base de données contenant des objets BLOB.

b. Créez l'espace de base de données à l'aide de l'utilitaire de ligne de commande `onspaces` Informix, comme cela est présenté dans l'exemple suivant.

```
onspaces -c -d ncimdbspace -p nom_chemin_accès\ncimdbspace -o 0 -s
1000000
onspaces -c -S ncimsbspace -p nom_chemin_accès\ncimsbspace -o 0 -s
100000
```

où :

nomchemin
correspond au chemin du répertoire contenant l'espace de base de données.

Cette commande crée un espace de base de données nommé *ncimdbspace* d'environ 1 Go dans un fichier portant le même nom et un deuxième espace de base de données plus petit pour les objets BLOB nommé *ncimsbspace*. Pour plus d'informations sur la ligne de commande `onspaces`, voir la documentation Informix.

3. Ouvrez une fenêtre de commande et accédez au répertoire `\PrecisionIP\scripts` de l'image d'installation extraite.
4. Facultatif : Si vous configurez Informix sur un serveur autre que Network Manager, copiez le script `create_informix_database.bat` sur l'hôte distant sur lequel vous avez installé Informix.
5. Pour créer la base de données, entrez la commande suivante : `create_informix_database.bat` *nom_base_de_données nom_utilisateur*, où :

nom_base_de_données
est le nom requis de la base de données à créer et est également utilisé comme préfixe pour le nom de la base de données de données d'interrogation

nom_utilisateur
Utilisateur Network Manager Informix à utiliser pour se connecter à la base de données.

Important : Cet utilisateur ne doit pas être l'administrateur. Il doit s'agir d'un utilisateur existant du système d'exploitation.

Par exemple, pour créer une base de données Informix appelée «NCIM», destinée à l'utilisateur Informix «ncim», entrez `create_informix_database.bat NCIM ncim`. Une fois la commande exécutée, la base de données Informix est créée. Pour plus d'informations sur le mode d'installation et de configuration d'Informix, voir la documentation Informix.

6. Lors de l'exécution du programme d'installation de Network Manager par la suite, veillez à sélectionner l'option **Démarrer l'installation personnalisée**. Ensuite, dans le panneau Sélection des options d'installation, vous devez sélectionner **Nombre de serveurs** > **Installation multiserveur** (même si vous installez Network Manager sur le même serveur qu'Informix), et sélectionner également **Valeurs par défaut** > **Personnaliser les paramètres**. Vous avez ensuite la possibilité de vous connecter à une base de données Informix

existante. Cette opération est nécessaire pour s'assurer que le programme d'installation définisse correctement les variables d'environnement Informix de Network Manager et le fichier de configuration `DbLogins` (par exemple, les valeurs `INFORMIXDIR` et `m_DbServer` sont définies comme requises). Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

Après avoir créé la base de données, vous devez effectuer la procédure suivante sur le serveur qui héberge la base de données Informix pour permettre aux processus Java de trouver cette base de données :

1. Dans le menu **Démarrer** de Windows, cliquez sur **Démarrer** > **Programmes** > **IBM Informix Client-SDK**.
2. Dans la fenêtre IBM Informix Setnet32, ajoutez en préfixe un astérisque à la zone Nom d'hôte (par exemple, remplacez *`nom_d'hôte`* par *`*nom_d'hôte`*.
3. Arrêtez et redémarrez Informix.
   a. Accédez à la fenêtre Services Windows.
   b. Sélectionnez le service IBM Informix Dynamic Server.
   c. Cliquez sur **Redémarrer le service**.

Installation et configuration de bases de données DB2 sous UNIX

Pour utiliser une base de données DB2 en tant que base de données topologique sous UNIX, vous devez installer DB2, configurer une instance et créer une base de données avant d'installer Network Manager.

La base de données est créée par des scripts situés dans le répertoire `/PrecisionIP/scripts` de l'image d'installation extraite. Décompressez le module d'installation avant d'installer DB2 et de créer une base de données.

L'environnement DB2 doit être configuré en tant qu'administrateur DB2 sur le serveur d'hébergement DB2. Si l'hôte réside sur un serveur distant, copiez les scripts de création de base de données sur le serveur distant.

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée dans la base de données DB2 créée.

Restriction : AIX Si vous installez les composants de base de Network Manager en tant qu'utilisateur non superutilisateur sur AIX, et que vous employez DB2 comme base de données topologiques NCIM, vous devez vous assurer que seule la bibliothèque client DB2 est active sur le serveur DB2. La présence de plusieurs clients DB2 actifs sur le serveur peut entraîner des problèmes et n'est pas prise en charge.

Pour plus d'informations sur l'installation et la configuration de DB2, voir le centre de documentation de votre version de DB2.

Fix Pack 4 Si vous envisagez d'utiliser la fonction HADR (High Availability Disaster Recovery) DB2 dans le groupe de correctifs 4 de Network Manager 3.9, vous devez installer DB2 9.7 ou DB2 10.1. La fonction HADR DB2 dans le groupe de correctifs 4 de Network Manager 3.9 est disponible uniquement avec DB2 9.7 et DB2 10.1.

1. Installez DB2 et configurez une instance dans laquelle le processus d'installation peut créer la base de données NCIM.

2. Si vous installez DB2 sur un autre serveur, Network Manager IP Edition, installez les bibliothèques DB2 Runtime Client sur le serveur Network Manager IP Edition.

   Les bibliothèques DB2 Runtime Client doivent être installées sur le serveur de composants centraux Network Manager et le serveur sur lequel Tivoli Integrated Portal et l'interface graphique Web sont installés. Cela signifie que les bibliothèques client peuvent devoir être installées sur deux machines distinctes.
3. Accédez au répertoire dans lequel l'instance est installée, puis accédez au sous-répertoire `sqllib`.
4. Pour configurer l'environnement, entrez la commande suivante :

Interpréteur de commandes	Commande
Bourne	`. db2profile`
C	`source db2cshrc`

   Les scripts encapsuleurs de l'application Network Manager configurent automatiquement l'environnement DB2. Pour plus d'informations sur la configuration de l'environnement via les scripts encapsuleurs, voir «Recherche d'un fichier via les scripts encapsuleurs», à la page 69.
5. Basculez sur le répertoire `/PrecisionIP/scripts` de l'image d'installation Network Manager extraite.
6. Facultatif : Si vous installez DB2 sur un autre serveur que Network Manager, copiez le script `create_db2_database.sh` sur l'hôte distant sur lequel vous avez installé DB2.
7. Exécutez le script en tant qu'administrateur DB2 en entrant la commande suivante : `./create_db2_database.sh` *`nom_base_de_données nom_utilisateur`* `-force`

   où :

   nom_base_de_données
   Correspond au nom de la base de données

   nom_utilisateur

   Correspond à l'utilisateur DB2 qui sera utilisé pour la connexion à la base de données

   Important : Cet utilisateur ne doit pas être l'administrateur. Il doit s'agir d'un utilisateur DB2 d'un système d'exploitation existant.

   -force Correspond à un argument facultatif empêchant tout utilisateur DB2 de quitter l'instance avant que ne soit créée la base de données.

   Par exemple, pour créer une base de données DB2 nommée «NCIM» pour l'utilisateur DB2 «ncim», entrez :

   ```
   ./create_db2_database.sh NCIM ncim
   ```
8. Lors de l'exécution du programme d'installation de Network Manager par la suite, prenez soin de sélectionner l'option de configuration de la base de données DB2 existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.
9. Connectez-vous en tant qu'administrateur DB2 sur le client DB2 en cours d'exécution sur le serveur Tivoli Integrated Portal.
10. Exécutez le script suivant pour cataloguer la base de données :

a. Basculez sur le répertoire /PrecisionIP/scripts de l'image d'installation Network Manager extraite.
b. Facultatif : Si vous installez DB2 sur un autre serveur que Network Manager, copiez le script catalog_db2_database.sh sur l'hôte distant sur lequel vous avez installé DB2.
c. Exécutez la commande ./catalog_db2_database.sh *nom_base_de_données hôte port*

   où *nom_base_de_données* correspond au nom de la base de données NCIM, *hôte* au nom d'hôte du serveur où NCIM est installé et *port* au port sur lequel la base de données NCIM est en cours d'exécution.

   La commande suivante affiche un exemple de syntaxe du script :

   ```
   ./catalog_db2_database.sh ITNM db2server.ibm.com 50000
   ```

11. Facultatif : Si vous avez installé les composants de base de Network Manager en tant qu'utilisateur non superutilisateur sur AIX, vous devez créer manuellement des liens symboliques dans /usr/lib vers les bibliothèques partagées, comme dans l'exemple suivant :

    ```
    ln -s ${NCHOME}/precision/platform/aix5/lib/libNcpDbDb2.so /usr/lib/
    libNcpDbDb2.so
    ln -s ${NCHOME}/precision/platform/aix5/lib/libNcpDb.so /usr/lib/libNcpDb.so
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2.a /usr/lib/libdb2.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2osse.a /usr/lib/libdb2osse.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2locale.a /usr/lib/libdb2locale.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2g11n.a /usr/lib/libdb2g11n.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2genreg.a /usr/lib/libdb2genreg.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2osse_db2.a /usr/lib/
    libdb2osse_db2.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2install.a /usr/lib/libdb2install.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2trcapi.a /usr/lib/libdb2trcapi.a
    ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2dascmn.a /usr/lib/libdb2dascmn.a
    ```

12. Facultatif : Après avoir installé Network Manager, exécutez le script NCHOME/precision/scripts/sql/db2/restrict_db2_privileges.sh en tant qu'utilisateur doté des privilèges système. Utilisez le script ci-après pour placer des restrictions sur les privilèges de l'utilisateur de base de données.

Recherche d'un fichier via les scripts encapsuleurs

Sous le shell Bourne, lors de la configuration des variables d'environnement pour DB2 via les scripts encapsuleurs, les scripts recherchent la ligne suivante et l'exécutent : $ITNMHOME/.db2sqllib.

Ce fichier est créé automatiquement lors de l'installation. Les scripts vérifient la présence d'un fichier nommé db2profile avec lequel l'environnement DB2 peut être configuré. S'il existe, le fichier est exécuté de la manière suivante :

```
if [ -f /home/db2inst/sqllib/db2profile ] ; then
 . /home/db2inst/sqllib/db2profile
fi
```

Le fichier $ITNMHOME/.db2sqllib est analysé par le script **setup_run_as_setuid_root.sh** afin de déterminer l'emplacement des bibliothèques client DB2 (voir «Configuration des composants centraux pour une exécution en tant que non superutilisateur», à la page 249).

Concepts associés:

Fix Pack 4 «A propos de la haute disponibilité de la base de données topologiques NCIM», à la page 309
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Installation et configuration de bases de données DB2 sous Windows

Pour utiliser une base de données DB2 en tant que base de données topologiques sous Windows, vous devez installer DB2, configurer une instance et créer une base de données avant d'installer Network Manager.

La base de données est créée par des scripts situés dans le répertoire `\PrecisionIP\scripts` de l'image d'installation extraite. Décompressez le module d'installation avant d'installer DB2 et de créer une base de données.

L'environnement DB2 doit être configuré en tant qu'administrateur DB2 sur le serveur d'hébergement DB2. Si l'hôte réside sur un serveur distant, copiez les scripts de création de base de données sur le serveur distant.

Lors de l'installation de Network Manager, la base de données topologique NCIM est installée dans la base de données DB2 créée.

Pour plus d'informations sur l'installation et la configuration de DB2, voir le centre de documentation de votre version de DB2 sur le site http://www-01.ibm.com/support/docview.wss?uid=swg27009474.

1. Installez DB2 et configurez une instance dans laquelle le processus d'installation peut créer la base de données NCIM.
2. Si vous installez DB2 sur un autre serveur, Network Manager IP Edition, installez les bibliothèques DB2 Runtime Client sur le serveur Network Manager IP Edition.

   Les bibliothèques DB2 Runtime Client doivent être installées sur le serveur de composants centraux Network Manager et le serveur sur lequel Tivoli

Integrated Portal et l'interface graphique Web sont installés. Cela signifie que les bibliothèques client peuvent devoir être installées sur deux machines distinctes.

3. Ouvrez une fenêtre de commande et accédez au répertoire `\PrecisionIP\scripts` de l'image d'installation extraite.
4. Facultatif : Si vous installez DB2 sur un autre serveur que Network Manager, copiez le script `create_db2_database.bat` sur l'hôte distant sur lequel vous avez installé DB2.
5. Pour créer la base de données, entrez la commande suivante : `create_db2_database.bat` *`nom_base_de_données nom_utilisateur`* `-force`, où :

   nom_base_de_données
   Correspond au nom de la base de données

   nom_utilisateur

   Correspond à l'utilisateur DB2 qui sera utilisé pour la connexion à la base de données

   Important : Cet utilisateur ne doit pas être l'administrateur. Il doit s'agir d'un utilisateur DB2 d'un système d'exploitation existant.

   -force Correspond à un argument facultatif empêchant tout utilisateur DB2 de quitter l'instance avant que ne soit créée la base de données.

   Par exemple, pour créer une base de données DB2 nommée «NCIM» destinée à l'utilisateur DB2 «ncim», entrez `create_db2_database.bat NCIM ncim`.
6. Lors de l'exécution du programme d'installation de Network Manager par la suite, prenez soin de sélectionner l'option de configuration de la base de données DB2 existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.
7. Connectez-vous en tant qu'administrateur DB2 sur le client DB2 en cours d'exécution sur le serveur Tivoli Integrated Portal.
8. Exécutez le script suivant pour cataloguer la base de données :
   a. Basculez sur le répertoire `\PrecisionIP\scripts` de l'image d'installation Network Manager extraite.
   b. Facultatif : Si vous installez DB2 sur un autre serveur que Network Manager, copiez le script `catalog_db2_database.bat` sur l'hôte distant sur lequel vous avez installé DB2.
   c. Exécutez la commande `catalog_db2_database.bat` *`nom_base_de_données hôte port`*

      où *nom_base_de_données* correspond au nom de la base de données NCIM, *hôte* au nom d'hôte du serveur où NCIM est installé et *port* au port sur lequel la base de données NCIM est en cours d'exécution.

      La commande suivante affiche un exemple de syntaxe du script :`catalog_db2_database.bat ITNM db2server.ibm.com 50000`

Une fois la commande exécutée, la base de données DB2 est créée et cataloguée.

Installation et configuration de bases de données MySQL sous UNIX

Pour utiliser une base de données MySQL en tant que base de données topologiques sous UNIX, vous devez installer MySQL et créer l'utilisateur et le schéma nécessaire avant l'installation de Network Manager.

Le schéma de base de données et l'utilisateur sont créés par des scripts résidant dans le répertoire `/PrecisionIP/scripts` de l'image d'installation décompressée. Vous devez avoir décompressé le package d'installation avant de tenter de créer la base de données.

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée sur la base de données MySQL créée.

Pour plus d'informations sur le mode d'installation et de configuration de MySQL, voir la documentation MySQL.

1. Installez une version prise en charge de MySQL.
2. Basculez sur le répertoire `/PrecisionIP/scripts` de l'image d'installation Network Manager extraite.
3. Facultatif : Si vous configurez MySQL sur un serveur autre que Network Manager, copiez le script `create_mysql_database.sh` sur l'hôte distant sur lequel vous avez installé MySQL.
4. Créez les tables nécessaires en exécutant le script **`create_mysql_database.sh`** à l'aide de la commande suivante :

   `create_mysql_database.sh` *`nomutilisateur motdepasse`*

   où *nomutilisateur* est `mysql` ou `root` et *motdepasse* est le mot de passe de cet utilisateur. Le schéma et l'utilisateur utilisés par Network Manager sont créés dans la base de données.
5. Lors de l'exécution ultérieure du programme d'installation de Network Manager, assurez-vous de sélectionner l'option de configuration d'une base de données MySQL existante. Vous pouvez exécuter le programme d'installation sur le serveur où les composants Network Manager doivent être installés ou sur le serveur où la base de données MySQL est installée. Network Manager crée les tables dans la base de données.

Installation et configuration de bases de données MySQL sous Windows

Pour utiliser une base de données MySQL en tant que base de données topologiques sous Windows, vous devez installer MySQL et créer l'utilisateur et le schéma nécessaire avant l'installation de Network Manager.

Le schéma de base de données et l'utilisateur sont créés par des scripts résidant dans le répertoire `\PrecisionIP\scripts` de l'image d'installation décompressée. Vous devez avoir décompressé le package d'installation avant de tenter de créer la base de données.

Lors de l'installation de Network Manager, la base de données topologiques NCIM est installée sur la base de données MySQL créée.

Pour plus d'informations sur le mode d'installation et de configuration de MySQL, voir la documentation MySQL.

1. Installez une version prise en charge de MySQL.
2. Basculez sur le répertoire `\PrecisionIP\scripts` de l'image d'installation Network Manager extraite.

3. Facultatif : Si vous configurez MySQL sur un serveur autre que Network Manager, copiez le script `create_mysql_database.bat` sur l'hôte distant sur lequel vous avez installé MySQL.
4. Exécutez le script **`create_mysql_database.bat`** en utilisant la commande suivante :

   `create_mysql_database.bat` *`nom_utilisateur mot_de_passe`*

   où *nom_utilisateur* est `mysql` ou l'utilisateur Windows d'administration, et *mot_de_passe* est le mot de passe de cet utilisateur. Le schéma et l'utilisateur utilisés par Network Manager sont créés dans la base de données.
5. Lors de l'exécution ultérieure du programme d'installation de Network Manager, assurez-vous de sélectionner l'option de configuration d'une base de données MySQL existante. Vous pouvez exécuter le programme d'installation sur le serveur où les composants Network Manager doivent être installés ou sur le serveur où la base de données MySQL est installée. Network Manager crée les tables dans la base de données.

Installation et configuration de bases de données Oracle sous UNIX

Pour utiliser une base de données topologiques Oracle sous UNIX, vous devez installer Oracle, configurer un schéma, puis créer une base de données avant d'installer Network Manager. Lors de l'installation, la base de données topologiques NCIM est installée dans la base de données Oracle créée.

La base de données est créée par des scripts situés dans le répertoire `/PrecisionIP/scripts` de l'image d'installation extraite. Vous devez avoir décompressé le package d'installation avant de tenter de créer la base de données.

Pour vous connecter à la base de données, il vous faut un accès à une invite de commande qui utilise le client Oracle SQL*Plus.

Pour des informations sur l'installation et la configuration d'Oracle, voir la documentation d'Oracle à l'adresse http://docs.oracle.com/cd/E11882_01/index.htm.

Le script de création de la base de données crée des utilisateurs pour plusieurs utilisateurs Oracle. Seul l'utilisateur `ncim` a le droit de se connecter à la base de données. Il possède également un droit d'accès aux schémas des autres utilisateurs. Le mot de passe par défaut créé par le script est identique au nom de l'utilisateur, soit : `ncim`.

1. Installez Oracle et configurez un schéma dans lequel le processus d'installation peut créer la base de données NCIM.
2. Vérifiez l'absence de conflit de port avec le service HTTP de la base de données XML Oracle. Le service HTTP de la base de données XML Oracle est configuré pour utiliser le port par défaut 8888.
3. Vérifiez que le programme d'écoute TNS Oracle s'exécute sur le serveur Oracle en entrant la commande suivante : `$ORACLE_HOME/bin/lsnrctl status`.
4. Si le programme d'écoute TNS Oracle ne s'exécute pas, démarrez-le à l'aide de la commande suivante : `$ORACLE_HOME/bin/lsnrctl start`.
5. En tant qu'utilisateur `système` d'Oracle, accédez au répertoire `/PrecisionIP/scripts` de l'image d'installation Network Manager décompressée.
6. Facultatif : Si vous implantez Oracle sur un serveur autre que Network Manager, copiez le fichier `create_oracle_database.sql` sur l'hôte distant sur lequel vous avez installé Oracle. Ce script est nécessaire afin de préparer

l'environnement pour la base de données topologiques NCIM et doit être exécuté sur le système hôte sur lequel la base de données est installée, comme décrit à l'étape suivante.

7. Pour créer le schéma, exécutez le script suivant : `sqlplus system/password < create_oracle_database.sql`. Pour modifier le mot de passe de l'utilisateur `ncim`, éditez le script et modifiez la deuxième occurrence de `ncim` sur la ligne suivante : `CREATE USER ncim IDENTIFIED BY ncim`.
8. Lors de l'exécution du programme d'installation de Network Manager par la suite, prenez soin de sélectionner l'option de connexion à une base de données Oracle existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

   Remarque : Fix Pack 5 Si vous installez Network Manager dans un environnement à haute disponibilité Oracle à l'aide de RAC (Real Application Clusters), installez Network Manager au préalable avec une connexion directe à un noeud unique dans le cluster Oracle. Une fois que vous avez installé Network Manager, vous pouvez configurer la haute disponibilité pour Network Manager à l'aide d'une adresse SCAN (Single Client Access Name) Oracle, comme décrit dans «Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC», à la page 351.
9. Facultatif : Après avoir installé Network Manager, exécutez le script `NCHOME/precision/scripts/sql/oracle/restrict_oracle_privileges.sh` *`nom_utilisateur mot_de_passe`* en tant qu'utilisateur disposant de privilèges système. Il permet de révoquer les privilèges attribués à l'utilisateur de la base de données NCIM lorsque le schéma de base de données NCIM est créé et d'attribuer des privilèges plus précis.

Installation et configuration de bases de données Oracle sous Windows

Pour héberger NCIM dans une base de données Oracle sous Windows, vous devez installer Oracle, configurer un schéma et créer une base de données avant d'installer Network Manager. Lors de l'installation, NCIM est installé dans la base de données Oracle créée.

La base de données est créée par des scripts situés dans le répertoire `\PrecisionIP\scripts` de l'image d'installation extraite. Vous devez avoir décompressé le package d'installation avant de tenter de créer la base de données.

Pour vous connecter à la base de données, il vous faut un accès à une invite de commande qui utilise le client Oracle SQL*Plus.

Pour des informations sur l'installation et la configuration d'Oracle, voir la documentation Oracle.

Sous Windows, le programme d'écoute TNS Oracle est un service Windows qui peut être démarré et arrêté depuis le Panneau de configuration Windows.

Le script de création de la base de données crée des utilisateurs pour plusieurs utilisateurs Oracle. Seul l'utilisateur `ncim` a le droit de se connecter à la base de données. Il possède également un droit d'accès aux schémas des autres utilisateurs. Le mot de passe par défaut créé par le script est identique au nom de l'utilisateur, soit : `ncim`.

1. Installez Oracle et configurez un schéma dans lequel le processus d'installation peut créer la base de données NCIM.

2. Vérifiez l'absence de conflit de port avec le service HTTP de la base de données XML Oracle. Le service HTTP de la base de données XML Oracle est configuré pour utiliser le port par défaut 8888.
3. Assurez-vous que le programme d'écoute TNS Oracle s'exécute sur le serveur Oracle en vérifiant l'application des services du Panneau de configuration Windows.
4. En tant qu'utilisateur `système` d'Oracle, accédez au répertoire `\PrecisionIP\scripts` de l'image d'installation Network Manager décompressée.
5. Facultatif : Si vous implantez Oracle sur un serveur autre que Network Manager, copiez le fichier `create_oracle_database.sql` sur l'hôte distant sur lequel vous avez installé Oracle.
6. Pour créer le schéma, exécutez le script suivant : `sqlplus system/password < create_oracle_database.sql`. Pour modifier le mot de passe de l'utilisateur `ncim`, éditez le script et modifiez la deuxième occurrence de `ncim` sur la ligne suivante : `CREATE USER ncim IDENTIFIED BY ncim`.
7. Lors de l'exécution du programme d'installation de Network Manager par la suite, prenez soin de sélectionner l'option de configuration d'une base de données Oracle existante. Le programme d'installation de Network Manager peut ensuite créer les tables dans la base de données sur un hôte local ou éloigné, selon l'emplacement d'installation de votre base de données.

Configuration de NCIM pour la gestion des caractères multi-octets

Vous devez configurer la base de données NCIM pour gérer les caractères multi-octets (les caractères chinois simplifiés, par exemple) si vous souhaitez que la base de données NCIM enregistre des données multi-octets. Une telle configuration est utile lorsque, par exemple, vous avez besoin d'entrer des caractères multi-octets dans la zone Description d'une définition d'interrogation.

Si vous exécutez la base de données NCIM sous DB2 ou Informix, vérifiez alors que vous avez les paramètres suivants :

DB2 Si vous exécutez Network Manager dans un environnement local qui prend en charge des caractères multi-octets, aucune modification de configuration n'est requise. Par exemple, les deux environnements locaux suivants prennent en charge les caractères multi-octets lors de l'exécution de NCIM sous DB2 :

- `LANG=zh_CN.gb18030`
  `LC_ALL=zh_CN.gb18030`
- `LANG=en_US.utf8`
  `LC_ALL=en_US.utf8`

Informix

Si vous utilisez Informix, les scripts de création de base de données et le programme d'installation de Network Manager configurent la variable d'environnement DB_LOCALE pour vous.

Si vous installez Informix séparément de Network Manager, vérifiez que la variable d'environnement DB_LOCALE de la base de données NCIM Informix correspond à l'environnement local sur le serveur Network Manager. Etant donné que Network Manager utilise le paramètre DB_LOCALE=en_us.utf8 pour Informix, prenez soin de créer les bases de données Informix en utilisant la valeur de variable d'environnement DB_LOCALE=en_us.utf8. Informix requiert également la prise en charge d'Unicode ; vous devez donc démarrer Informix avec le paramètre de variable d'environnement GL_USEGLU=1. Pour plus d'informations,

reportez-vous au document *Informix GLS User's Guide* à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.70.0/com.ibm.welcome.doc/welcome.htm.

Information associée:

http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.50.0/com.ibm.glsug.doc/ids_gug_068.htm

Configuration de NCIM pour la gestion des caractères multi-octets sur une base de données MySQL :

Ces informations permettent de configurer la base de données NCIM en cours d'exécution sous MySQL pour la gestion des caractères multi-octets.

Par défaut, les clients MySQL se connectent à la base de données NCIM en utilisant l'ensemble de caractères latin1, quel que soit l'ensemble de caractères utilisé par le système d'exploitation. L'ensemble de caractères latin1 ne peut pas afficher correctement les caractères multi-octets.

Pour configurer NCIM en vue de prendre en charge des caractères multi-octets sur une base de données MySQL :

1. Modifiez le fichier de configuration MySQL. Le nom de ce fichier varie en fonction de votre système d'exploitation :
   - UNIX my.cnf
   - Windows my.ini

   L'emplacement de ce fichier est différent selon que vous exécutiez Network Manager dans une installation comportant un seul serveur ou dans une installation incluant plusieurs serveurs.

   Installation de serveur unique
   Le fichier de configuration MySQL se trouve sous `$MYSQL_HOME`.

   Installation de plusieurs serveurs
   Modifiez le fichier de configuration MySQL sur le serveur qui héberge la base de données MySQL NCIM.
2. Mettez à jour la section `[client]` du fichier de configuration MySQL avec la propriété de l'ensemble de caractères par défaut pertinent. Procédez comme suit :
   - S'il n'existe aucune section `[client]` dans le fichier de configuration MySQL, ajoutez ensuite deux lignes similaires aux exemples ci-dessus et appropriés à votre environnement local.
   - S'il existe une section `[client]` dans le fichier de configuration MySQL mais aucune propriété d'ensemble de caractères par défaut, ajoutez à la section `[client]` une propriété d'ensemble de caractères par défaut similaire aux exemples ci-dessous et appropriée à votre environnement local.
   - S'il existe une section `[client]` dans le fichier de configuration MySQL avec une propriété d'ensemble de caractères par défaut qui ne correspond pas à votre environnement local, remplacez la propriété d'ensemble de caractères par défaut par une propriété similaire aux exemples de propriétés ci-dessous et appropriée à votre environnement local.

   Le tableau suivant fournit des exemples d'environnement local et des propriétés d'ensemble de caractères multi-octets par défaut correspondantes.

Tableau 8. Propriétés d'ensemble de caractères par défaut exemple

Environnement local	Propriété d'ensemble de caractères par défaut
en_US.utf8	`[client]` `default-character-set=utf8`
zh_CN.gb2312	`[client]` `default-character-set=gb2312`

Un ensemble complet des ensembles de caractères MySQL est disponible sur le site Web MySQL.

Important : L'ensemble de caractères gb18030 n'est pas pris en charge par MySQL 5.0. Vous ne pourrez pas résoudre ce problème si vous exécutez la base de données NCIM en utilisant MySQL 5.0 avec gb18030 en tant qu'ensemble de caractères.

Information associée:

http://dev.mysql.com/doc/refman/5.0/en/charset-mysql.html

Configuration de NCIM pour la gestion des caractères multi-octets sur une base de données Oracle :

Ces informations permettent de configurer la base de données NCIM en cours d'exécution sous Oracle pour la gestion des caractères multi-octets.

Pour configurer NCIM en vue de prendre en charge les caractères multi-octets sur une base de données ORACLE :

1. Attribuez à la variable d'environnement NLS_LANG Oracle une valeur appropriée. Par exemple, si le système s'exécute sous l'environnement local zh_CN.gb18030, attribuez au paramètre NLS_LANG la valeur suivante : `SIMPLIFIED CHINESE_CHINA.ZHS32GB18030`. Un ensemble complet de valeurs de variable d'environnement NLS_LANG pour différents environnements locaux est disponible sur le site Web Oracle.
2. Configurez l'environnement Network Manager afin de prendre en compte vos modifications après l'installation.
   - UNIX Accédez au répertoire $NCHOME et émettez la commande suivante : `source env.sh`.
   - Windows Accédez au répertoire %NCHOME% et exécutez le script `env.bat`.

Information associée:

http://www.oracle.com/technology/tech/globalization/htdocs/nls_lang%20faq.htm

Installation de Tivoli Common Reporting

Tivoli Common Reporting doit être installé pour que vous puissiez exécuter les rapports de gestion de réseau fournis par Network Manager.

Installation de Tivoli Common Reporting 3.1

Pour exécuter les rapports Tivoli Common Reporting à partir de Network Manager en utilisant Tivoli Common Reporting 3.1, vous devez installer Tivoli Common Reporting 3.1 sur un serveur distinct. Si vous utilisez MySQL pour la base de données topologiques, vous ne pouvez pas employer Tivoli Common Reporting version 3.1. Vous devez utiliser Tivoli Common Reporting version 2.1.1.

architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager :

Ces informations permettent de comprendre comment intégrer Tivoli Common Reporting 3.1 d'un serveur distinct sur le serveur Network Manager.

La figure suivante présente l'architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager.

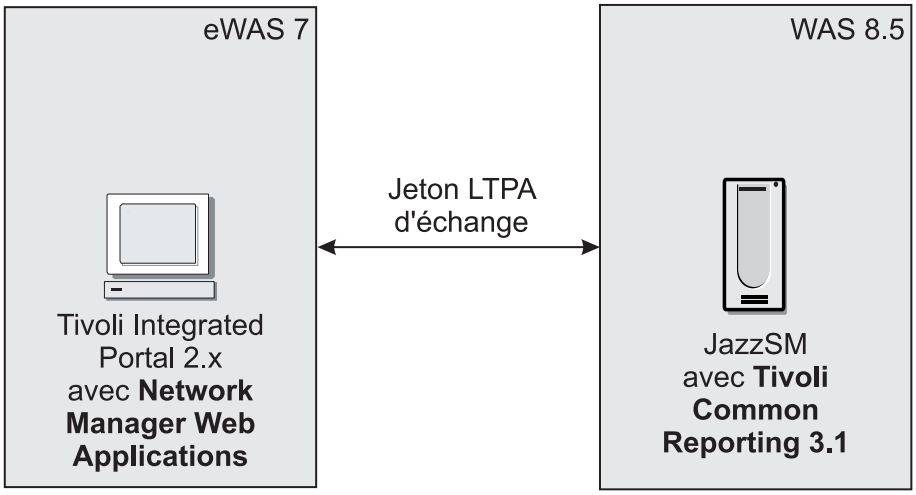

Figure 8. architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager

Configuration requise pour le serveur Tivoli Common Reporting 3.1

Vous devez télécharger et installer le logiciel suivant sur le serveur Tivoli Common Reporting 3.1 :

- JazzSM
- WAS 8.5
- Tivoli Common Reporting 3.1.

Etapes d'installation pour Tivoli Common Reporting 3.1 :

Suivez les instructions suivantes pour télécharger et installer Jazz for Service Management 1.1.0.3 avec Tivoli Common Reporting 3.1.0.1.

Si Tivoli Common Reporting n'est pas installé lorsque vous installez Network Manager, vous pouvez installer Tivoli Common Reporting ultérieurement, puis configurer les rapports.

1. Sur le serveur distant sur lequel vous allez installer Tivoli Common Reporting 3.1, téléchargez Jazz for Service Management version 1.1.0.3, qui inclut Tivoli Common Reporting 3.1.0.3. Tivoli Common Reporting 3.1.0.3 est la version requise pour cette intégration. Vous pouvez télécharger Jazz for Service

Management version 1.1.0.3 à partir de FixPack Central, à l'adresse http://www-933.ibm.com/support/fixcentral/.

2. Accédez à la documentation Tivoli Common Reporting pour obtenir des informations sur l'installation de Tivoli Common Reporting 3.1 ou la mise à niveau vers cette version :

   Installation de Tivoli Common Reporting 3.1
   http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.1.0/com.ibm.psc.doc_1.1.1.0/install/tcr_t_install.html?lang=en

   Mise à niveau vers Tivoli Common Reporting 3.1
   http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.1.0/com.ibm.psc.doc_1.1.1.0/tcr_original/ctcr_upgrade.html?lang=en

3. Installez Tivoli Common Reporting 3.1 sur le serveur distant.
4. Une fois Network Manager installé, vous devez configurer Tivoli Common Reporting 3.1.

Installation de Tivoli Common Reporting 2.1.1

Exécutez ces tâches pour installer Tivoli Common Reporting 2.1.1. Notez que Tivoli Common Reporting 2.1.1 ne prend pas en charge Internet Explorer versions 10 ou 11. Par conséquent, vous ne pouvez pas utiliser la fonction de génération de rapports si vous utilisez Internet Explorer 10 ou 11 pour exécuter l'interface graphique Network Manager.

Network Manager installe le package de rapports requis pour les rapports de gestion du réseau sur le serveur sur lequel les composants de l'interface graphique de Network Manager sont installés. Si l'emplacement d'installation choisi pour Network Manager comporte déjà des instances de Tivoli Integrated Portal et Tivoli Common Reporting, Network Manager configure automatiquement les rapports à utiliser avec cette instance de Tivoli Common Reporting.

Si Tivoli Common Reporting n'est pas installé lorsque vous installez Network Manager, vous pouvez l'installer ultérieurement et configurer ensuite.

Si vous utilisez Oracle V12c, vous ne pouvez pas employer Tivoli Common Reporting version 2.1.1. Vous devez utiliser Tivoli Common Reporting version 3.1.

Avertissement : Si vous avez une installation Tivoli Common Reporting existante, vérifiez que vous disposez du référentiel requis pour la configuration de l'authentification de l'utilisateur avant d'installer les composants de l'interface graphique Network Manager. Vous ne pouvez pas changer la méthode d'authentification d'utilisateur avec le programme d'installation de Network Manager. Par exemple, si vous projetez d'utiliser l'authentification par ObjectServer et qu'elle n'est pas encore configurée sur l'installation Tivoli Integrated Portal utilisée par votre instance de Tivoli Common Reporting, installez le interface graphique Web Tivoli Netcool/OMNIbus (fourni avec le module Network Manager) dans l'installation Tivoli Integrated Portal existante, puis sélectionnez l'option d'activation de l'authentification par ObjectServer. Installez ensuite le composant d'interface graphique Network Manager dans le Tivoli Integrated Portal existant.

Pour installer Tivoli Common Reporting :

1. Téléchargez le package Tivoli Common Reporting. Vous pouvez télécharger Tivoli Common Reporting de façon facultative avec le module Network Manager. Pour plus d'informations, reportez-vous au document de

téléchargement à l'adresse http://www-01.ibm.com/support/docview.wss?rs=3117&uid=swg24035480.

2. Consultez la documentation Tivoli Common Reporting pour des informations sur l'installation de Tivoli Common Reporting : http://www.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html
3. Installez Tivoli Common Reporting sur l'hôte sur lequel les composants de l'interface graphique Network Manager doivent être installés.
4. Installez Network Manager comme décrit dans «Installation de Network Manager», à la page 81. Le processus d'installation de Network Manager installe automatiquement le package des rapports de gestion de réseau et configure les rapports en vue de leur utilisation avec Tivoli Common Reporting.

   Important : Arrêtez Tivoli Common Reporting avant d'installer Network Manager. En tant qu'utilisateur ayant installé Tivoli Common Reporting, exécutez la commande suivante depuis le répertoire `TCR_component_dir/bin`.
   `./stopTCRserver.sh <utilisateur_admin_tip> <mot de passe>`
5. Facultatif : Si vous n'installez pas Tivoli Common Reporting avant d'installer Network Manager, vous pouvez configurer les rapports de gestion de réseau ultérieurement, après l'installation de Network Manager comme décrit dans «Configuration de rapports pour des installations existantes», à la page 277.

Configuration de Red Hat Linux Enterprise Edition

Avant d'installer le produit sous Red Hat Linux Enterprise Edition, vous devez désactiver SELinux.

Lors de l'installation de Red Hat Enterprise Linux, il se peut que SELinux soit activé. Pour désactiver SELinux, modifiez l'option SELinux en procédant comme suit :

1. Ouvrez le fichier suivant :
   `/etc/sysconfig/selinux`
2. Recherchez la ligne suivante :
   `SELINUX=enforcing`
3. Remplacez-la par `SELINUX=disabled`.
4. Redémarrez le serveur.

Vérification des paramètres de port d'achèvement d'E-S (IOCP)

Si vous installez Network Manager sur AIX et que vous envisagez de vous connecter à une base de données Oracle, vous devez vérifier que le paramètre IOCP est correct.

Vous devez effectuer les étapes ci-après en tant qu'utilisateur root.

1. Entrez la commande suivante :
   `/usr/sbin/lsdev -c iocp -F status`

   Procédez comme suit :
   - Si cette commande renvoie le résultat `Disponible`, vous n'avez pas besoin d'effectuer le reste de la procédure.
   - Si la commande renvoie un résultat autre que `Disponible`, par exemple, `Défini`, effectuez les étapes restantes de la procédure.

2. Entrez la commande suivante :
   `smitty iocp2`
3. Sélectionnez `Modification/Affichage des caractéristiques des ports d'achèvement d'E-S`.
4. Modifiez la valeur `Défini` de `Etat configuré lors de la relance du système` en `Disponible`.
5. Réamorcez le serveur AIX.

Installation de Network Manager

Vous pouvez installer Network Manager sous différents modes, selon vos besoins. Utilisez le mode Console pour installer Network Manager si vous ne disposez pas d'un périphérique de pointage, tel qu'une souris.

UNIX Linux Si vous êtes connecté à un ordinateur hôte comme utilisateur root et que vous voulez installer Network Manager comme utilisateur non-root, utilisez la commande **su -** pour changer les utilisateurs. Si vous utilisez la commande **su**, des erreurs peuvent se produire pendant l'installation.

Si vous souhaitez utiliser une installation existante de Tivoli Netcool/OMNIbus, voir «Configuration d'une installation Tivoli Netcool/OMNIbus existante», à la page 57. Le programme d'installation Network Manager ne peut installer que Tivoli Netcool/OMNIbus V7.3.1.

Différences entre l'installation de base et l'installation personnalisée

L'installation personnalisée vous permet de disposer d'un nombre significatif d'options par rapport à l'installation de base.

Installation de base

Choisissez l'installation de base si une des conditions suivantes s'applique.

- Vous installez le produit à des fins de démonstration ou de test.
- Vous installez le produit sur un réseau de petite envergure.
- Vous installez tous les composants sur un même serveur avec les options par défaut.

Remarque : L'installation de base effectue automatiquement une reconnaissance de réseau après l'installation.

Installation personnalisée

Choisissez l'installation personnalisée si une des conditions suivantes s'applique.

- Vous installez le produit sur un réseau de moyenne ou grande envergure.
- Vous avez besoin de distribuer l'installation sur plusieurs serveurs.
- L'installation est destinée à un réseau équipé de technologies avancées, telles que NAT (Network Address Translation) ou MPLS (Multiprotocol Label Path Switching).
- Vous souhaitez utiliser une installation existante de Tivoli Netcool/OMNIbus.
- Vous souhaitez utiliser une installation existante du portail intégré Tivoli.
- Vous avez besoin d'une reprise en ligne.

- Vous souhaitez utiliser une base de données Informix existante pour les données topologiques.
- Vous souhaitez utiliser une base de données DB2, MySQL ou Oracle pour les données de topologie.
- Vous souhaitez disposer de la conformité avec la norme FIPS 140–2.

Remarque : Une installation personnalisée vous permet d'effectuer différents types de reconnaissances de réseau après l'installation.

A propos de l'installation FIPS 140-2

La norme FIPS (Federal Information Processing Standard) 140–2 est une norme cryptographique fédérale des Etats-Unis. Vous pouvez installer Network Manager à l'aide d'un ensemble d'algorithmes de cryptographie restreint.

Important : Network Manager n'est pas reconnu conforme à la norme FIPS 140–2 et aucun élément de ce manuel ou du produit ne doit être considéré comme tel. Toutefois, Network Manager peut être installé dans un mode ayant été conçu pour prendre en compte les spécifications de la norme FIPS 140–2.

Vous pouvez installer Network Manager à l'aide d'un ensemble d'algorithmes de cryptographie restreint en sélectionnant l'option appropriée dans l'Assistant d'installation.

Restriction :

Si vous souhaitez disposer de la conformité avec la norme FIPS 140–2, utilisez uniquement la version 7.3.1 ou ultérieure deIBM Tivoli Netcool/OMNIbus, et installez IBM Tivoli Netcool/OMNIbus en mode FIPS. Vous devez également vérifier que tous les produits s'intégrant à Network Manager, comme IBM Tivoli Netcool/OMNIbus, disposent d'un mode FIPS et configurer les produits si nécessaire. Vous devez également vérifier que votre système d'exploitation utilise uniquement des modules compatibles FIPS 140–2.

Restriction : Si vous choisissez d'installer Network Manager à l'aide d'un ensemble d'algorithmes de cryptographie restreint, les fonctions non compatibles ne sont pas installées. Vous ne pouvez pas passer d'une installation FIPS à une installation non FIPS à moins de désinstaller, puis de de réinstaller le produit. De même, vous ne pouvez pas passer d'une installation non FIPS à une installation FIPS à moins de désinstaller, puis de réinstaller le produit.

Différences dans une installation FIPS 140–2 de Network Manager

Les différences entre une installation FIPS 140–2 et une installation normale sont les suivantes :

- Vous ne pouvez pas installer Informix 11.5, qui était inclus avec Network Manager version 3.9 dans les versions antérieures au groupe de correctifs 1. Les versions de Network Manager après le groupe de correctifs 1 incluent Informix 11.7, qui est compatible à FIPS.
- Vous ne pouvez pas utiliser une base MySQL distante en tant que base de données topologiques.

- Les agents de reconnaissance Telnet n'utilisent pas SSHv1 pour interroger les unités. Cela peut provoquer une erreur de sécurité lors de la connexion à une unité si celui-ci prend uniquement en charge les algorithmes SSHv1 ou les algorithmes SSHv2 non conformes.
- L'aide programmable SNMP et le navigateur MIB ne peuvent pas être configurés pour utiliser le chiffrement MD5 DES.

Installation de Network Manager à l'aide de l'assistant

La manière la plus simple d'installer Network Manager est d'utiliser l'assistant.

Avant de procéder à l'installation, vérifiez que toutes les tâches de préinstallation nécessaires ont été réalisées et que vos serveurs sont adaptés à l'installation de Network Manager.

Restriction : Sous AIX, installez un navigateur Web pris en charge afin d'utiliser le tableau de bord d'installation ou l'assistant.

Conseil : L'assistant d'installation démarre lors de l'affichage des fenêtres. Si vous souhaitez travailler dans une autre fenêtre pendant l'installation du produit, réduisez d'abord la fenêtre d'installation.

Pour démarrer l'assistant d'installation, procédez comme suit :

1. Démarrez l'assistant du programme d'installation à partir du tableau de bord.
   - UNIX Exécutez le script **launchpad.sh**.
   - Windows Lancez l'exécutable **launchpad.exe**.
   a. Sélectionnez l'élément **Installing Network Manager** dans le menu.
   b. Sélectionnez l'installation standard ou personnalisée en cliquant sur le bouton **Démarrer l'installation standard** ou **Démarrer l'installation personnalisée**. L'installation standard installe tous les composants du produit sur un seul serveur à l'aide des valeurs par défaut. Ce type d'installation est plus rapide et plus simple qu'une installation personnalisée et est idéal pour les petits réseaux, les clients de petites entreprises ainsi que les versions de démonstration. Une fois terminée, l'installation standard démarre automatiquement une reconnaissance réseau. Une installation personnalisée est davantage adaptée aux moyens et grands réseaux, à l'intégration avec des produits existants, ou à des installations multiserveurs. Une fois terminée, ce type d'installation vous laisse le choix de démarrer ou non une reconnaissance réseau.
2. Si vous ne pouvez pas démarrer le tableau de bord, démarrez l'assistant d'installation à partir de la ligne de commande.
   - UNIX Exécutez le script **install.sh**.
   - Windows Lancez l'exécutable **install.exe**.

   Lorsque l'assistant d'installation démarre, sélectionnez le type d'installation (standard ou personnalisée) dans le panneau d'assistant Sélectionner le type d'installation (quatrième panneau d'assistant à s'afficher).

   Remarque : Network Manager installe Tivoli Common Reporting par défaut s'il n'est pas présent sur le système. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports et Tivoli Common Reporting à ce stade, en entrant l'option `-DinstallReports=0` sur la ligne de commande. Cette opération peut être nécessaire si vous installez Network Manager sur Red Hat Enterprise

Linux 6.0, car Tivoli Common Reporting ne prend pas en charge RHEL 6.0. Dans ce cas, vous devez installer Tivoli Common Reporting sur un hôte distinct.

Par exemple, pour installer Network Manager sans installer Tivoli Common Reporting, entrez `./install.sh -DinstallReports=0` ou `install.exe -DinstallReports=0` en fonction de votre système d'exploitation.

3. Pour installer le produit, entrez les valeurs appropriées dans les panneaux d'assistant.

Valeurs pour une installation de base

Ces informations vous permettent de comprendre les valeurs à entrer dans les panneaux de l'assistant pour une installation de base.

L'assistant d'installation de base comporte un nombre limité de panneaux permettant d'entrer les informations de configuration.

Le tableau suivant indique les valeurs à entrer dans chaque panneau.

Remarque : L'installation de base installe uniquement la base de données Informix par défaut. Pour utiliser une instance existante d'une base de données Informix ou pour utiliser une base de données autre qu'Informix pour Network Manager, choisissez l'option d'installation personnalisée.

Conseil : Imprimez ce tableau pour vous y référer lors de l'installation du produit. Ce tableau vous permet de vérifier que vous disposez de toutes les informations nécessaires et de mémoriser les valeurs importantes à entrer.

Tableau 9. Panneaux de l'assistant et valeurs

Panneau	Valeur/option	Description
Introduction	Aucune	Après avoir lu le texte d'introduction, cliquez sur **Suivant**.
Validation du système	Aucune	Ce panneau ne s'affiche que si une ou plusieurs vérifications de validation du système échouent. Si des messages d'erreur s'affichent dans ce panneau, vous devez annuler l'installation, résoudre les erreurs et recommencer l'installation. La validation du système détermine si le serveur actuel convient à l'installation du logiciel Network Management. La validation inclut des vérifications de cohérence du DNS et de la mémoire disponible pour le processus d'installation en lui-même.

Tableau 9. Panneaux de l'assistant et valeurs (suite)

Panneau	Valeur/option	Description
Contrat de licence du programme	J'accepte simultanément les dispositions IBM et non IBM	Sélectionnez cette option pour poursuivre l'installation.
	I do not accept the terms in the license agreement (Je n'accepte pas les dispositions du contrat de licence)	Si vous sélectionnez cette option, vous ne pouvez pas poursuivre l'installation.
Select Installation Location (Sélectionner l'emplacement d'installation)	Emplacement d'installation de Tivoli Network Manager	Utilisez l'emplacement par défaut ou entrez l'emplacement où vous souhaitez installer Network Manager. **Restriction :** Si vous effectuez une mise à niveau de Network Manager depuis une version antérieure, vous devez sélectionner un répertoire différent de celui où Network Manager est actuellement installé. Vous ne pouvez pas mettre à niveau Network Manager en écrasant des fichiers. Les caractères autorisés dans le chemin d'installation sont les caractères alphanumériques (A-Z, a-z, 0-9), les tirets, les trait de soulignement, les points, les deux-points, les barres obliques et les espaces.

Tableau 9. Panneaux de l'assistant et valeurs (suite)

Panneau	Valeur/option	Description
Collecte des informations d'installation par défaut	Netcool (Domain NameNom de domaine Netcool)	Entrez le nom de domaine réseau pour Network Manager. Entrez un nom descriptif, par exemple, TESTNETWORK. Le nom de domaine contient au maximum 11 caractères (lettres ou chiffres). Les lettres sont en majuscules et aucun espace ou caractère spécial n'est admis. Notez le nom de domaine car il est utilisé pour le démarrage manuel des composants. Nom de domaine :
	Mot de passe d'administration	Entrez un mot de passe à utiliser comme mot de passe root pour Tivoli Netcool/OMNIbus ObjectServer, le mot de passe de l'administrateur de base de données topologiques et le mot de passe administrateur pour les comptes utilisateur par défaut itnmadmin et itnmuser. Le mot de passe doit comporter de 4 à 8 caractères ASCII et doit respecter les exigences relatives au mot de passe applicables sur la machine où vous effectuez l'installation. Si le compte de base de données Informix existe déjà sur le système d'exploitation, entrez le mot de passe utilisé pour y accéder. **Restriction :** Le mot de passe Informix ne doit pas commencer par un signe dollar ($).
	Confirmation du mot de passe	Entrez à nouveau le mot de passe administrateur.

Tableau 9. Panneaux de l'assistant et valeurs (suite)

Panneau	Valeur/option	Description
Collect Port Connection Information (Collecter les informations de connexion du port)	Netcool/OMNIbus ObjectServer PortPort ObjectServer Netcool/OMNIbus	Entrez le port à utiliser pour le serveur ObjectServer ou acceptez la valeur par défaut. Si vous vous connectez à une paire de serveurs ObjectServer de reprise en ligne, indiquez ici les détails du serveur ObjectServer virtuel.
	Port HTTP Tivoli Integrated Portal	Entrez le port à utiliser pour Tivoli Integrated Portal ou acceptez la valeur par défaut. Notez ce numéro de port, car il vous sera nécessaire pour vous connecter aux applications Web. Port HTTP :
	Port de la base de données Informix	Entrez le port à utiliser pour la base de données Informix ou acceptez la valeur par défaut.
Collect SNMP V1/V2 Community Strings (Collecte des noms de communauté SNMP V1/V2)	Liste des noms de communauté	A la fin de l'installation, une reconnaissance simple du sous-réseau local démarre. Entrez jusqu'à six noms de communauté SNMP (mots de passe). Ces noms de communauté sont utilisés par le processus de reconnaissance afin d'obtenir les informations SNMP des unités du réseau. Pour réduire la durée de la reconnaissance, répertoriez les noms de communauté par ordre décroissant de fréquence d'utilisation. `Public` est installé par défaut.
Récapitulatif avant installation	Aucun(e)	Passez en revue les informations sur les composants sur le point d'être installés. Cliquez sur **Suivant** pour effectuer une dernière vérification des pré-requis avant l'installation.

Tableau 9. Panneaux de l'assistant et valeurs (suite)

Panneau	Valeur/option	Description
Prerequisite Checking Results (Résultats de vérification des pré-requis)	Aucun(e)	Passez en revue les résultats de la vérification des pré-requis. Cette vérification détermine si le serveur actuel convient à l'installation des composants spécifiques choisis. En cas d'erreurs importantes, annulez l'installation, résolvez les erreurs et redémarrez installation. En l'absence d'erreur importante, cliquez sur **Installer** afin d'installer les composants sélectionnés. Lorsque vous y êtes invité, acceptez les contrats de licence pour continuer.

Valeurs pour une installation personnalisée

Ces informations vous permettent de comprendre les valeurs à entrer dans les panneaux de l'assistant pour une installation personnalisée.

Une installation personnalisée utilise différents panneaux afin de collecter les informations de configuration selon les options que vous avez choisies.

Avertissement : L'utilisation du programme d'installation de Network Manager pour configurer une instance existante de Tivoli Netcool/OMNIbus installe également la sonde SNMP et Netcool/OMNIbus Knowledge Library. Si vous ne voulez pas remplacer votre sonde SNMP existante et vos personnalisations Netcool/OMNIbus Knowledge Library existantes, vous devez sélectionner **Ne pas installer ou configurer Tivoli Netcool/OMNIbus à ce stade** lorsque la question vous est posée dans le panneau **Sélection des composants à installer** sous **Tivoli Netcool/OMNIbus**. Après l'installation, copiez le package d'installation vers le serveur où se trouve votre installation existante de Tivoli Netcool/OMNIbus et exécutez le script **`ConfigOMNI`** pour configurer Tivoli Netcool/OMNIbus, mais assurez-vous de ne pas sélectionner d'options pour configurer la sonde SNMP ou Netcool/OMNIbus Knowledge Library.

Le tableau suivant indique les valeurs à entrer dans chaque panneau.

Conseil : Imprimez ce tableau pour vous y référer lors de l'installation du produit. Ce tableau vous permet de vérifier que vous disposez de toutes les informations nécessaires et de mémoriser les valeurs importantes à entrer.

Tableau 10. Panneaux de l'assistant et valeurs

Panneau	Condition d'affichage	Valeur/option	Description
Introduction	Toujours affiché.	Aucun(e)	Après avoir lu le texte d'introduction, cliquez sur **Suivant**.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Validation du système	S'affiche lorsque la validation du système n'aboutit pas.	Aucun(e)	Ce panneau ne s'affiche que si une ou plusieurs vérifications de validation du système échouent. Annulez l'installation, résolvez les erreurs et démarrez à nouveau l'installation. La validation du système détermine si le serveur actuel convient à l'installation du logiciel Network Management. La validation inclut des vérifications de cohérence du DNS et de la mémoire disponible pour le processus d'installation en lui-même.
Contrat de licence du programme	Toujours affiché.	**J'accepte simultanément les dispositions IBM et non IBM**	Sélectionnez cette option pour poursuivre l'installation.
		I do not accept the terms in the license agreement (Je n'accepte pas les dispositions du contrat de licence)	Si vous sélectionnez cette option, vous ne pouvez pas poursuivre l'installation.
Select Installation Location (Sélectionner l'emplacement d'installation)	Toujours affiché.	**Tivoli Network Manager install location (Emplacement d'installation de Tivoli Network Manager)**	Utilisez l'emplacement par défaut ou entrez l'emplacement où vous souhaitez installer Network Manager. **Restriction :** Si vous effectuez une mise à niveau de Network Manager depuis une version antérieure, vous devez sélectionner un répertoire différent de celui où Network Manager est actuellement installé. Vous ne pouvez pas mettre à niveau Network Manager en écrasant des fichiers. Les caractères autorisés dans le chemin d'installation sont les caractères alphanumériques (A-Z, a-z, 0-9), les tirets, les trait de soulignement, les points, les deux-points, les barres obliques et les espaces.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Sélection des options d'installation	Toujours affiché.	**Nombre de serveurs** > **Installation sur serveur unique**	Sélectionnez cette option pour installer Network Manager, la base de données topologiques Informix et les composants d'interface graphique (applications Web Network Manager et Tivoli Integrated Portal) sur le serveur actuel. Si vous disposez de Tivoli Netcool/OMNIbus V7.3.1 et du module d'installation, vous pouvez également installer Tivoli Netcool/OMNIbus V7.3.1 à l'aide de cette option.
		Nombre de serveurs > **Installation multiserveur**	Sélectionnez cette option pour choisir les composants à installer sur le serveur actuel.
		Valeurs par défaut > **Accepter les paramètres par défaut**	Sélectionnez cette option pour réduire le nombre de panneaux d'assistant affichés.
		Valeurs par défaut > **Personnaliser les paramètres**	Sélectionnez cette option afin de personnaliser chaque option d'installation.
		Conformité FIPS > **Utiliser des routines cryptographiques conformes à FIPS 140–2**	Sélectionnez cette option si vous souhaitez effectuer l'installation à l'aide de routines cryptographiques provenant d'un module cryptographique validé. Si vous sélectionnez cette option, vous ne pouvez pas utiliser Informix 11.5 ou MySQL en tant que base de données topologiques. Il existe d'autres restrictions de la fonctionnalité du produit (description dans «A propos de l'installation FIPS 140-2», à la page 82).

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Sélection des composants à installer	S'affiche pour les installations multiserveur.	**Composants principaux**	Sélectionnez si vous souhaitez installer les composants de reconnaissance réseau Network Manager, d'interrogation, d'analyse d'origine du problème et d'enrichissement d'événement sur ce serveur.
		Applications Web	Egalement appelées "composants de l'interface graphique" dans la documentation. Sélectionnez cette option si vous voulez installer les applications Web Network Manager sur ce serveur. Si Tivoli Integrated Portal n'est pas déjà installé, il est installé avec les applications Web. S'il existe déjà une installation de Tivoli Integrated Portal sur ce serveur, vous pouvez choisir de l'utiliser dans un panneau suivant.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Sélection des composants à installer (suite)	S'affiche pour les installations multiserveur.	**Tivoli Netcool/OMNIbus**	Le programme d'installation de Network Manager recherche uniquementTivoli Netcool/OMNIbus version 7.3.1. S'il ne trouve pas l'image Tivoli Netcool/OMNIbus (en fonction du nom de l'image ou du numéro de référence), il demande l'emplacement du fichier. Si vous souhaitez que le programme d'installation installe une version de Tivoli Netcool/OMNIbus prise en charge, autre que 7.3.1, créez un sous-répertoire nommé `OMNIbus` dans le module d'installation Network Manager extrait et extrayez le package Tivoli Netcool/OMNIbus téléchargé dans ce répertoire. Linux Solaris Le programme d'installation Network Manager ne peut pas installer ou configurer Tivoli Netcool/OMNIbus V7.4. Pour plus d'informations, voir https://ibm.biz/BdRGK9.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Sélection des composants à installer (suite)	S'affiche pour les installations multiserveur.	**Tivoli Netcool/OMNIbus (suite)**	Pour configurer une installation de Tivoli Netcool/OMNIbus existante, elle doit déjà se trouver sur ce serveur. **Restriction :** Pour configurer une version Tivoli Netcool/OMNIbus antérieure à la version 7.3.1, exécutez le script **ConfigOMNI** avant d'installer Network Manager, comme décrit dans la rubrique «Configuration d'une installation Tivoli Netcool/OMNIbus existante», à la page 57. Pour vous connecter à une installation Tivoli Netcool/OMNIbus existante sur un autre serveur, ne sélectionnez pas l'option de connexion à une installation existante. Réalisez les tâches supplémentaires décrites dans la rubrique «Configuration de Tivoli Netcool/OMNIbus pour une utilisation avec Network Manager», à la page 175.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Sélection des composants à installer (suite)	S'affiche pour les installations multiserveur.	**Base de données topologiques**	Choisissez d'installer une nouvelle base de données Informix pour les données topologiques ou utilisez une base de données MySQL, DB2, Informix ou Oracle existante. **Remarque :** Informix peut être installé uniquement par l'utilisateur root. Si vous installez Network Manager sans être utilisateur root et que vous souhaitez utiliser Informix, il existe une étape supplémentaire à effectuer après l'installation : Vous devez vous connecter en tant que root après l'installation et installer Informix sur le système en utilisant les valeurs fournies lors de l'installation de Network Manager. Voir «Installation et configuration d'Informix après une installation non root», à la page 251.
Obtenir l'emplacement du package Netcool/OMNIbus 7.3.1	S'affiche si vous avez sélectionné une installation de serveur unique ou si vous avez sélectionné **Installation du logiciel de gestion des événements** dans une installation multiserveur.	**Choose directory containing Netcool/OMNIbus 7.3.1 package (Choisir un répertoire contenant le module Netcool/OMNIbus 7.2.1)**	Entrez l'emplacement du module téléchargé ou du support d'installation. Seule la version 7.3.1 peut être installée à l'aide du programme d'installation de Network Manager.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecte des informations d'installation par défaut	S'affiche si vous avez sélectionné **Accepter les paramètres par défaut**.	**Netcool Domain Name (Nom de domaine Netcool)**	Entrez le nom de domaine réseau pour Network Manager. Entrez un nom descriptif, par exemple, TESTNETWORK. Le nom du domaine doit comporter entre un et 11 caractères (lettres, chiffres ou les deux), les lettres étant en majuscules, sans espace ni caractère spécial. Notez le nom de domaine car il est utilisé pour le démarrage manuel des composants. Nom de domaine :
		Mot de passe d'administration	Entrez un mot de passe à utiliser comme mot de passe root pour Tivoli Netcool/OMNIbus ObjectServer, le mot de passe de l'administrateur de base de données topologiques et le mot de passe administrateur pour les comptes utilisateur par défaut itnmadmin et itnmuser. Le mot de passe doit comporter de 4 à 8 caractères ASCII et doit respecter les exigences relatives au mot de passe applicables sur la machine où vous effectuez l'installation.
		Confirmer le mot de passe	Entrez à nouveau le mot de passe administrateur.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecte des informations de connexion au port	S'affiche si vous avez sélectionné **Accepter les paramètres par défaut**.	**Port ObjectServer de Netcool/OMNIbus**	Entrez le port à utiliser pour le serveur ObjectServer ou acceptez la valeur par défaut.
		Port HTTP Tivoli Integrated Portal	Entrez le port à utiliser pour Tivoli Integrated Portal ou acceptez la valeur par défaut. Notez ce numéro de port, car il vous sera nécessaire pour vous connecter aux applications Web. Port HTTP :
		Port de base de données Informix	Entrez le port à utiliser pour la base de données Informix ou acceptez la valeur par défaut.
Collecte des détails d'installation de Netcool/OMNIbus	S'affiche si vous avez choisi d'installer Tivoli Netcool/OMNIbus et avez sélectionné **Personnaliser les paramètres**.	**Nom Netcool/OMNIbus ObjectServer**	Entrez le nom du serveur ObjectServer en cours d'installation. Le nom ne doit pas contenir d'espace.
		Port ObjectServer de Netcool/OMNIbus	Entrez le port pour l'ObjectServer en cours d'installation. Le port ne doit pas être déjà utilisé.
		Mot de passe du compte administrateur Netcool/OMNIbus	Entrez le mot de passe du compte administrateur.
		Confirmer le mot de passe	Confirmez le mot de passe du compte administrateur.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Configurer un serveur d'objets existant	S'affiche si vous avez choisi de configurer une installation existante de Tivoli Netcool/OMNIbus.	**Emplacement d'installation de Netcool/OMNIbus (OMNIHOME)**	Emplacement de l'installation de Tivoli Netcool/OMNIbus sur ce serveur.
		Nom Netcool/OMNIbus ObjectServer	Entrez le nom du serveur ObjectServer devant être configuré par cette installation. Si vous vous connectez à une paire de serveurs ObjectServer de reprise en ligne, indiquez ici les détails du serveur ObjectServer.
		Port ObjectServer de Netcool/OMNIbus	Entrez le port utilisé par l'ObjectServer. Si vous vous connectez à une paire de serveurs ObjectServer de reprise en ligne, indiquez ici les détails du serveur ObjectServer.
		Nom du compte administrateur Netcool/OMNIbus	Entrez le nom d'utilisateur du compte administrateur.
		Mot de passe du compte administrateur Netcool/OMNIbus	Entrez le mot de passe du compte administrateur.
		Confirmer le mot de passe	Confirmez le mot de passe du compte administrateur.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Connexion à un serveur ObjectServer existant	S'affiche si vous avez choisi d'établir une connexion à une installation existante de Tivoli Netcool/OMNIbus.	**Nom d'hôte du serveur Netcool/OMNIbus**	Entrez le nom du système où se trouve l'installation de Tivoli Netcool/OMNIbus à utiliser.
		Nom Netcool/OMNIbus ObjectServer	Entrez le nom du serveur ObjectServer auquel vous souhaitez que l'installation se connecte. Si vous vous connectez à une paire de serveurs ObjectServer de reprise en ligne, indiquez ici les détails du serveur ObjectServer.
		Netcool/OMNIbus port (Port Netcool/OMNIbus)	Entrez le port utilisé par l'ObjectServer. Si vous vous connectez à une paire de serveurs ObjectServer de reprise en ligne, indiquez ici les détails du serveur ObjectServer.
		Mot de passe du compte administrateur Netcool/OMNIbus	Entrez le mot de passe du compte administrateur.
		Confirmer le mot de passe	Confirmez le mot de passe du compte administrateur.
Sélection du répertoire d'installation TIP	S'affiche si vous avez sélectionné l'option d'installation de la console utilisateur et **Personnaliser les paramètres**.	**Choose an install folder (Choisir un dossier d'installation)**	Choisissez l'emplacement du Tivoli Integrated Portal à installer. Sélectionnez cette option si le Tivoli Integrated Portal n'est pas déjà installé sur ce serveur.
		Reuse an existing install folder (Réutiliser un dossier d'installation existant)	Cliquez sur **Réutiliser** et sélectionnez le chemin de répertoire d'une installation existante de Tivoli Integrated Portal. Si le Tivoli Integrated Portal n'est pas installé sur le serveur, cette option n'est pas disponible. **Restriction :** Vous ne pouvez pas installer l'interface graphique Web Tivoli Netcool/OMNIbus 7.3.1 par dessus la version 7.3.0. Choisissez un dossier d'installation différent.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecter les détails d'installation de Tivoli Integrated Portal	S'affiche si vous avez sélectionné l'option d'installation de la console utilisateur et **Personnaliser les paramètres**.	**Port HTTP de TIP**	Entrez le port à utiliser pour Tivoli Integrated Portal. Notez ce numéro de port, car vous en aurez besoin pour vous connecter aux applications Web. Port HTTP :
		Nom du compte administrateur de TIP	Entrez un nom à utiliser pour le compte administrateur de Tivoli Integrated Portal.
		Mot de passe du compte administrateur de TIP	Entrez le mot de passe du compte administrateur Tivoli Integrated Portal.
		Confirmer le mot de passe	Confirmez le mot de passe du compte administrateur.
		LDAP	Sélectionnez cette option pour utiliser l'authentification LDAP pour les utilisateurs Tivoli Integrated Portal.
		Serveur d'objets	Sélectionnez cette option afin d'utiliser l'ObjectServer pour l'authentification des utilisateurs Tivoli Integrated Portal. **Remarque :** Pour utiliser un référentiel de fichiers pour l'authentification des utilisateurs Tivoli Integrated Portal, vous devez désélectionner les cases à cocher **LDAP** et **ObjectServer**.
Informations LDAP	S'affiche si vous avez sélectionné l'option d'installation de la console utilisateur et **Personnaliser les paramètres** et si vous utilisez une authentification LDAP pour Tivoli Integrated Portal.	**LDAP server host name (Nom d'hôte du serveur LDAP)**	Entrez le nom d'hôte du serveur LDAP.
		Port LDAP	Entrez le port du serveur LDAP.
		Identificateur du référentiel LDAP	Entrez l'identificateur du référentiel du serveur LDAP.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Informations de sécurité LDAP	S'affiche si vous avez sélectionné l'option d'installation de la console utilisateur et **Personnaliser les paramètres** et si vous utilisez une authentification LDAP pour Tivoli Integrated Portal.	**Nom du compte d'administration TIP**	Entrez le nom du compte administrateur Tivoli Integrated Portal. La valeur par défaut est tipadmin.
		Nom distinctif de liaison	Entrez le nom de la liaison. La valeur par défaut est cn=root. **Remarque :** Si le nom de liaison contient un espace, placez l'ensemble du nom entre guillemets, par exemple, `"cn=Directory Manager"`.
		Mot de passe de liaison	Entrez le mot de passe du nom de liaison.
		Confirmer le mot de passe	Confirmez le mot de passe de la liaison.
		Distinguished name of a base entry (Nom distinctif d'une entrée de base)	Entrez le nom distinctif. La valeur par défaut est o=IBM,c=US.
Informations sur l'entité LDAP	S'affiche si vous avez sélectionné l'option d'installation de la console utilisateur et **Personnaliser les paramètres** et si vous utilisez une authentification LDAP pour Tivoli Integrated Portal.	**Type d'entité PersonAccount**	La valeur `PersonAccount` est prédéfinie pour cette zone.
		Entrée de base pour PersonAccount	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.
		Type d'entité Group	La valeur `Group` est prédéfinie pour cette zone.
		Entrée de base pour Group	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.
		Type d'entité OrgContainer	La valeur `OrgContainer` est prédéfinie pour cette zone.
		Entrée de base pour OrgContainer	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecter les détails d'installation de Network Manager	S'affiche si Network Manager est en cours d'installation et si vous avez sélectionné **Personnaliser les paramètres**.	**Nom de domaine Network Manager**	Entrez le nom de domaine réseau pour Network Manager. Entrez un nom descriptif, par exemple, TESTNETWORK. Le nom de domaine contient au maximum 11 caractères (lettres ou chiffres). Les lettres sont en majuscules et aucun espace ou caractère spécial n'est admis. Notez le nom de domaine car il est utilisé pour le démarrage manuel des composants. Notez le nom de domaine car il est utilisé pour démarrer manuellement les composants. Nom de domaine : **Avertissement :** Le nom du domaine est obligatoire. Vous devez indiquer une valeur.
		Reconnaître le sous-réseau	Sélectionnez cette option si vous souhaitez que le processus d'installation démarre une reconnaissance de réseau de votre sous-réseau local.
		Définir l'emplacement de départ de la reconnaissance à partir de l'installation IBM Tivoli NetView	Lance une reconnaissance et utilise les données qui ont été exportées depuis une instance de IBM Tivoli NetView. **Important :** Cette option ne constitue pas la meilleure méthode pour effectuer une transition depuis le produit IBM Tivoli NetView. La méthode la plus efficace consiste à exécuter une nouvelle reconnaissance initiale sans importées les données depuis IBM Tivoli NetView. Des scripts sont fournis pour planifier la transition. Pour plus d'informations, voir «Transition depuis IBM Tivoli NetView», à la page 170.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecter les détails d'installation de Network Manager (suite)	S'affiche si Network Manager est en cours d'installation et si vous avez sélectionné **Personnaliser les paramètres**.	**Définir l'emplacement de départ de la reconnaissance à partir d'une autre application Network Management**	Sélectionnez cette option si vous souhaitez que le processus d'installation démarre une reconnaissance de réseau à l'aide des données d'une autre application Network Management.
		Aucun(e)	Sélectionnez cette option si vous souhaitez terminer l'installation sans effectuer de reconnaissance. Si vous choisissez de ne pas démarrer de reconnaissance maintenant, vous pouvez en démarrer une plus tard en utilisant l'interface graphique État de la reconnaissance. **Remarque :** Le nom du domaine est obligatoire. Vous devez préalablement entrer une valeur sous **Nom de domaine Network Manager** même si vous ne souhaitez pas démarrer une reconnaissance après l'installation.
Collecter les informations de reconnaissance initiales	S'affiche si vous avez choisi d'effectuer une reconnaissance du sous-réseau local.	**Adresse IP du sous-réseau à reconnaître**	Entrez l'adresse IP du sous-réseau à reconnaître. Seules les adresses IPv4 sont admises.
		Masque de réseau	Entrez le masque de réseau du sous-réseau. Pour un sous-réseau de classe C, ce masque est 255.255.255.0.
Collecte des noms de communauté SNMP V1/V2	S'affiche si vous avez choisi d'effectuer une reconnaissance du sous-réseau local.	Liste des noms de communauté	Entrez jusqu'à six noms de communauté SNMP (mots de passe). Ces noms de communauté sont utilisés par le processus de reconnaissance afin d'obtenir les informations SNMP des unités du réseau. Pour réduire la durée de la reconnaissance, répertoriez les noms de communauté par ordre décroissant de fréquence d'utilisation.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Obtenir des données de reconnaissance NetView	S'affiche si vous avez choisi d'utiliser des données NetView afin de définir l'emplacement de départ de la reconnaissance.	**Full name of the NetView migration script output (Nom complet de la sortie de procédure de migration NetView)**	Entrez l'emplacement de la sortie du script de migration de IBM Tivoli NetView que vous avez lancé depuis le tableau de bord comme l'exigeait l'installation.
Obtenir des données de reconnaissance génériques	S'affiche si vous avez choisi d'utiliser les informations d'une autre application Network Management pour définir l'emplacement de départ de la reconnaissance.	**Full name of the file containing the network nodes (Nom complet du fichier contenant les noeuds réseau)**	Entrez le nom du fichier contenant la liste des noeuds de votre réseau. Le format du fichier doit pouvoir être analysé par l'Outil de recherche File, par exemple, un fichier texte contenant une liste d'adresses IP et de noms d'hôtes séparés par des espaces.
		Full name of the file containing the SNMP community strings (Nom complet du fichier contenant les noms de communauté SNMP)	Entrez l'emplacement du fichier contenant la liste des noms de communauté de votre réseau.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Collecte des détails d'installation d'Informix	S'affiche si une base de données Informix est en cours d'installation.	**Port de base de données Informix**	Entrez le port à utiliser pour les connexions à la base de données Informix. Le port ne doit pas être déjà utilisé. La valeur par défaut est 9088.
		Nom du serveur Informix	Entrez un nom à utiliser en tant que nom de serveur Informix. La valeur par défaut est `ITNM`.
		Numéro du serveur Informix	Entrez le numéro des bases de données Informix déjà installées sur ce système. La valeur par défaut est zéro.
		Nom de base de données Informix	Entrez un nom à utiliser en tant que nom de base de données Informix. La valeur par défaut est `itnm`.
		Nom du compte de base de données Informix	Entrez le nom du compte système à utiliser pour accéder à la base de données Informix. Le nom doit contenir des lettres en minuscules et des chiffres. Le compte est créé s'il n'existe pas déjà. La valeur par défaut est `ncim`.
		Mot de passe du compte de base de données Informix	Entrez le mot de passe du compte de base de données Informix. Si le compte de base de données Informix existe déjà sur le système d'exploitation, entrez le mot de passe utilisé pour y accéder. Si le compte est créé lors de l'installation, ce mot de passe est utilisé pour définir le mot de passe du compte. **Restriction :** Le mot de passe Informix ne doit pas commencer par un signe dollar ($).
		Confirmer le mot de passe	Entrez à nouveau le mot de passe de base de données.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Créer des tables de base de données topologiques Network Manager	S'affiche lorsqu'aucune base de données Informix n'est en cours d'installation.	**Créer des tables pour conserver les données topologiques dans la base de données sélectionnée**	Sélectionnez cette option afin de configurer la base de données topologiques sélectionnée. Vous ne devez le faire qu'une fois par base de données topologiques. Si vous avez déjà installé un composant de Network Manager et sélectionné cette option lors d'une installation précédente, ne la sélectionnez pas maintenant. **Remarque :** Si vous devez configurer une base de données après l'installation pour une installation Network Manager existante, par exemple, reportez-vous aux tâches concernant la création de schémas de base de données topologiques dans le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
Connexion à une base de données MySQL existante	S'affiche si une base de données MySQL existante est utilisée pour les données topologiques.	**Nom d'hôte du serveur de base de données MySQL**	Entrez le nom du serveur sur lequel la base de données MySQL est installée.
		Port de base de données MySQL	Entrez le port utilisé pour les connexions à la base de données MySQL.
		Nom du compte administrateur de base de données MySQL	Entrez le nom du compte administrateur MySQL.
		Mot de passe du compte administrateur de base de données MySQL	Entrez le mot de passe du compte administrateur MySQL.
		Confirmer le mot de passe	Entrez à nouveau le mot de passe administrateur.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Connexion à une base de données DB2 existante	S'affiche si une base de données DB2 existante est utilisée pour les données topologiques.	**Nom d'hôte du serveur de base de données DB2**	Entrez le nom du serveur sur lequel la base de données DB2 est installée.
		Port de base de données DB2	Entrez les ports utilisés pour les connexions à la base de données DB2.
		Nom de la base de données DB2	Entrez le nom de la base de données DB2.
		Nom du compte de base de données DB2	Entrez le nom du compte administrateur DB2.
		Mot de passe du compte de base de données DB2	Entrez le mot de passe du compte administrateur DB2.
		Confirmer le mot de passe	Entrez à nouveau le mot de passe administrateur.
		Répertoire de bibliothèque SQL local (panneau séparé)	Entrez le chemin d'accès aux DB2 bibliothèque SQL, par exemple `/export/home/db2inst1/sqllib`.
Connexion à une base de données Oracle existante	S'affiche si une base de données Oracle existante est utilisée pour les données topologiques.	**Nom d'hôte du serveur de base de données Oracle**	Entrez le nom du serveur sur lequel la base de données Oracle est installée.
		Port de base de données Oracle	Entrez le port utilisé pour les connexions à la base de données Oracle.
		SID (identificateur système) de la base de données Oracle	Entrez l'identificateur système de la base de données Oracle.
		Nom du compte administrateur de base de données Oracle	Entrez le nom du compte administrateur Oracle.
		Mot de passe du compte administrateur de base de données Oracle	Entrez le mot de passe du compte administrateur Oracle.
		Confirmer le mot de passe	Entrez à nouveau le mot de passe administrateur.

Tableau 10. Panneaux de l'assistant et valeurs (suite)

Panneau	Condition d'affichage	Valeur/option	Description
Connexion à une base de données Informix existante	S'affiche si une base de données Informix existante est utilisée pour les données topologiques.	**Nom d'hôte du serveur de base de données Informix**	Entrez l'adresse IP ou le nom d'hôte DNS du serveur sur lequel Informix est en cours d'exécution.
		Port de base de données Informix	Entrez le port utilisé pour les connexions à la base de données Informix.
		Nom du serveur Informix	Entrez le nom logique attribué à l'instance de base de données Informix lors de l'installation.
		Nom de base de données Informix	Entrez le nom de la base de données Informix.
		Nom du compte administrateur de base de données Informix	Entrez le nom du compte administrateur Informix.
		Mot de passe du compte administrateur de base de données Informix	Entrez le mot de passe du compte administrateur Informix.
		Confirmer le mot de passe	Entrez à nouveau le mot de passe administrateur.
Récapitulatif avant installation	Toujours affiché.	Aucun(e)	Passez en revue les informations sur les composants sur le point d'être installés. Cliquez sur **Suivant** pour effectuer une dernière vérification des pré-requis avant l'installation.
Résultats de la vérification des prérequis	Toujours affiché.	Aucun(e)	Passez en revue les résultats de la vérification des pré-requis. Cette vérification détermine si le serveur actuel convient à l'installation des composants spécifiques choisis. En cas d'erreurs importantes, annulez l'installation, résolvez les erreurs et redémarrez installation. En l'absence d'erreur importante, cliquez sur **Installer** afin d'installer les composants sélectionnés. Lorsque vous y êtes invité, acceptez les contrats de licence pour continuer.

Installation de Network Manager en mode console

Si vous ne pouvez pas exécuter l'assistant d'installation disponible sous forme d'interface graphique, installez Network Manager en mode console. Vous devez utiliser ce mode pour installer le produit si vous n'avez pas accès à un périphérique de pointage, tel une souris.

Lorsque vous procédez à l'installation en mode console, indiquez les options d'installation en répondant à des menus et des invites dans une interface utilisateur basée sur du texte.

Pour exécuter le programme d'installation en mode console, procédez comme suit :

1. Exécutez le script d'installation à l'aide de l'option **-i console**.
   - UNIX Entrez la commande suivante :
     ```
     install.sh -i console
     ```
   - Windows Entrez la commande suivante :
     ```
     install.exe -i console
     ```

     Remarque : Network Manager installe Tivoli Common Reporting par défaut s'il n'est pas présent sur le système. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports et Tivoli Common Reporting à ce stade, en entrant l'option `-DinstallReports=0` sur la ligne de commande. Cette opération peut être nécessaire si vous installez Network Manager sur Red Hat Enterprise Linux 6.0, car Tivoli Common Reporting ne prend pas en charge RHEL 6.0. Dans ce cas, vous devez installer Tivoli Common Reporting sur un hôte distinct.

     Par exemple, pour installer Network Manager en mode console sans installer Tivoli Common Reporting, entrez `./install.sh -i console -DinstallReports=0` ou `install.exe -i console -DinstallReports=0` en fonction de votre système d'exploitation.
2. Suivez les invites, en utilisant des valeurs identiques à celles d'une installation personnalisée basée sur une interface graphique.
3. A tout moment, entrez `back` pour revenir à l'écran précédent, ou `quit` pour quitter le programme d'installation.

Référence associée:

«Valeurs pour une installation personnalisée», à la page 88
Ces informations vous permettent de comprendre les valeurs à entrer dans les panneaux de l'assistant pour une installation personnalisée.

Installation de Network Manager en mode silencieux

En mode silencieux, le programme d'installation lit les informations de configuration à partir d'un fichier. Il ne requiert aucune information de votre part.

Vous pouvez exécuter le programme d'installation en mode silencieux lorsque vous souhaitez déployer Network Manager avec des options d'installation identiques sur plusieurs ordinateurs ou lorsque vous effectuez l'installation sur un système qui n'a accès à aucune interface graphique. Une fois démarrée, vous ne pouvez interrompre une installation en mode silencieux.

Le mode d'installation silencieux est une opération en deux étapes qui requiert que vous définissiez vos paramètres d'installation dans un fichier de réponses et que vous exécutiez ensuite le programme d'installation avec les paramètres de ce fichier.

Pour procéder à une installation en mode silencieux, procédez comme suit :

1. Créez un fichier de réponses qui définit les fonctions que vous voulez installer. Vous disposez des options suivantes pour créer le fichier de réponses :

Option	Description
Création d'un fichier de réponses à l'aide du tableau de bord	«Création d'un fichier de réponses à l'aide du tableau de bord», à la page 110
Création d'un fichier de réponses en modifiant le fichier exemple fourni	«Création d'un fichier de réponses à l'aide d'un fichier exemple», à la page 110
Création d'un fichier de réponses en exécutant le programme d'installation en mode console	Vous pouvez créer un fichier de réponses en exécutant le programme d'installation en mode console et en répondant `oui` à la question `Générer un fichier de réponses en mode silencieux ?` à l'invite. Vous pouvez ensuite créer un fichier de réponse en mode silencieux de manière interactive en répondant aux questions affichées à l'écran sans utiliser d'interface graphique. Le mode console crée ensuite un fichier nommé `silent-install.txt` dans le répertoire que vous spécifiez en tant que répertoire d'installation. Par défaut, il s'agit du répertoire `/opt/IBM/tivoli/netcool`. Voir «Installation de Network Manager en mode console», à la page 108.

2. Après avoir créé le fichier de réponses, démarrez le script d'installation correspondant à votre système d'exploitation :
   - Windows Exécutez la commande **`install.exe`** à l'aide des options suivantes :

     `install.exe -i silent -f` *`chemin d'accès au fichier de réponses`*

     Si vous ne souhaitez pas que la fenêtre d'installation renvoie immédiatement la commande, créez un fichier de commandes afin d'exécuter la commande **`install.exe`**.
   - UNIX Exécutez le script **`install.sh`** à l'aide de la commande suivante :

     `install.sh -i silent -f` *`chemin d'accès au fichier de réponses`*

   Remarque : Network Manager installe Tivoli Common Reporting par défaut s'il n'est pas présent sur le système. Vous pouvez spécifier de ne pas installer la fonction de génération de rapports et Tivoli Common Reporting à ce stade, en entrant l'option `-DinstallReports=0` sur la ligne de commande. Cette opération peut être nécessaire si vous installez Network Manager sur Red Hat Enterprise Linux 6.0, car Tivoli Common Reporting ne prend pas en charge RHEL 6.0. Dans ce cas, vous devez installer Tivoli Common Reporting sur un hôte distinct.

   Par exemple, pour installer Network Manager en mode silencieux sans installer Tivoli Common Reporting, entrez `./install.sh -i silent -f` *`chemin du fichier de réponses`* `-DinstallReports=0` ou `install.exe -i silent -f` *`chemin du fichier de réponses`* `-DinstallReports=0` en fonction de votre système d'exploitation.

Création d'un fichier de réponses à l'aide du tableau de bord

Vous pouvez créer le fichier de réponses pour l'installation en mode silencieux à l'aide du tableau de bord.

Pour créer le fichier de réponses à l'aide du tableau de bord :

1. Accédez au répertoire où vous avez extrait le module d'installation Network Manager.
2. Démarrez le tableau de bord.
   - UNIX Exécutez le script **launchpad.sh**.
   - Windows Lancez l'exécutable **launchpad.exe**.
3. Cliquez sur **Installation de Network Manager**.
4. Développez **Créer un fichier de réponses pour une installation automatique** et cliquez sur **Générer un fichier de réponses pour une installation standard** ou sur **Générer un fichier de réponses pour une installation personnalisée**, selon que vous voulez effectuer ultérieurement une installation standard ou personnalisée en mode silencieux.
5. Suivez les instructions figurant dans les panneaux afin d'entrer des valeurs pour le fichier de réponses. Les panneaux sont les mêmes que lors de l'installation de Network Manager par le biais de l'assistant.

   Conseil : Vérifiez les valeurs des rubriques d'installation standard et personnalisée afin de savoir quelles valeurs entrer dans les panneaux de l'assistant.
6. Enregistrez le fichier.

Exécutez le script d'installation avec l'option de ligne de commande en mode silencieux et le chemin d'accès complet à ce fichier.

Référence associée:

«Valeurs pour une installation de base», à la page 84
Ces informations vous permettent de comprendre les valeurs à entrer dans les panneaux de l'assistant pour une installation de base.

«Valeurs pour une installation personnalisée», à la page 88
Ces informations vous permettent de comprendre les valeurs à entrer dans les panneaux de l'assistant pour une installation personnalisée.

Création d'un fichier de réponses à l'aide d'un fichier exemple

Vous pouvez créer le fichier de réponses pour votre installation en mode silencieux en modifiant le fichier exemple fourni.

Pour créer le fichier de réponses en modifiant l'exemple, procédez comme suit :

1. Sauvegardez le fichier de réponses exemple. Le fichier de réponses exemple, `ITNM-sample-response.txt`, se trouve dans le répertoire de niveau supérieur, là où le module d'installation a été extrait.
2. Editez le fichier de réponses exemple dans un éditeur de texte.
   a. Supprimez la mise en commentaire des paramètres que vous souhaitez utiliser en supprimant le caractère # en début de ligne.
   b. Vérifiez les valeurs par défaut des paramètres et définissez de nouvelles valeurs si nécessaire.
   c. Remplacez toutes les instances de `--UserInput--` par les valeurs appropriées.

3. Sauvegardez le fichier dans un emplacement approprié (par exemple dans le même répertoire que le script `INSTALL` de Network Manager).

Exécutez le script d'installation avec l'option de ligne de commande en mode silencieux et le chemin complet de ce fichier.

Fichier de réponses exemple pour l'installation en mode silencieux :

Utilisez ces informations pour comprendre comment modifier le fichier de réponses pour une installation en mode silencieux.

Liste des paramètres du fichier de réponses

Le tableau suivant répertorie les paramètres fournis dans le fichier de réponses par défaut pour une installation en mode silencieux, dans l'ordre dans lequel ils apparaissent dans le fichier.

Tableau 11. Paramètres du fichier de réponses

Paramètre	Valeur par défaut	Description
INSTALLER_UI	SILENT	Ne modifiez pas cette valeur et ne supprimez pas cette ligne.
SingleServer	0	Ne modifiez pas cette valeur et ne supprimez pas cette ligne.
DefaultValues	0	Ne modifiez pas cette valeur et ne supprimez pas cette ligne.
$LICENSE_ACCEPTED$	false	Pour accepter l'accord de licence, supprimez la mise en commentaire de la variable et remplacez la valeur par `true`. Si la valeur LICENSE_ACCEPTED est différente de true, l'installation se termine, aucun journal n'est généré et aucune indication de l'échec n'est fournie. En supprimant le signe # avant #LICENSE_ACCEPTED=false et en remplaçant false par true, vous avez accepté l'accord de licence de Network Manager.
USER_INSTALL_DIR	C:\\IBM\\tivoli\\netcool	Si votre installation est sous Windows, fournissez le chemin complet d'accès au répertoire d'installation du produit. **Remarque :** Windows considère la barre oblique inversée \ comme étant un caractère d'échappement, vous devez donc utiliser une barre oblique inversée double \\ lors de la définition d'un chemin sous Windows.
USER_INSTALL_DIR	/opt/IBM/tivoli/netcool	Si votre installation est sous UNIX, fournissez le chemin complet d'accès au répertoire d'installation du produit.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
installOMNI	0	Définissez la valeur comme suit : • Définissez cette valeur sur 1 pour installer et configurer Tivoli Netcool/OMNIbus, les sondes Tivoli Netcool/OMNIbus nécessaires et la IBM Tivoli Netcool/OMNIbus Knowledge Library. • Définissez cette valeur sur 2 pour configurer Tivoli Netcool/OMNIbus qui est déjà installé sur ce système. • Définissez cette valeur sur 3 pour vous connecter à une installation Tivoli Netcool/OMNIbus existante sans la configurer. • Définissez cette valeur sur 0 si vous ne souhaitez pas installer, configurer, ou vous connecter à Tivoli Netcool/OMNIbus à ce stade. **Avertissement :** L'utilisation du programme d'installation de Network Manager pour configurer une instance existante de Tivoli Netcool/OMNIbus installe également la sonde SNMP et Netcool/OMNIbus Knowledge Library. Si vous ne souhaitez pas écraser votre sonde SNMP existante et vos personnalisations Netcool/OMNIbus Knowledge Library, vous devez affecter au paramètre **installOMNI** la valeur 0. Après l'installation de Network Manager, copiez le package d'installation vers le serveur sur lequel réside votre installation Tivoli Netcool/OMNIbus existante et exécutez le script **ConfigOMNI** afin de configurer votre installation Tivoli Netcool/OMNIbus, mais prenez soin de ne pas sélectionner les options de configuration de la sonde SNMP ou de Netcool/OMNIbus Knowledge Library. Pour plus d'informations, voir «Configuration d'une installation Tivoli Netcool/OMNIbus existante», à la page 57.
installTIP	0	Définissez cette valeur sur 1 pour installer et configurer Tivoli Integrated Portal, l'interface graphique Web Tivoli Netcool/OMNIbus et les applications Web Network Manager.
installITNM	0	Définissez cette valeur sur 1 pour installer et configurer les composants principaux de Network Manager (analyse origine du problème, passerelle d'événement, moteurs de reconnaissance et d'interrogation).
installNCIM	0	Définissez cette valeur sur 1 pour installer et configurer Informix pour une utilisation en tant que base de données topologiques.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
complyFIPS	0	Définissez cette valeur sur 1 pour utiliser les routines cryptographiques conçues pour êtres conformes à la norme FIPS 140–2.
IALOCAL_ITNM_ PASSWORD	--UserInput--	Fournissez un mot de passe pour les comptes utilisateur itnmadmin et itnmuser par défaut. Si le compte de base de données Informix existe déjà sur le système d'exploitation, entrez le mot de passe utilisé pour y accéder.
PACKAGE.DIR. NCO	--UserInput--	Si IBM Tivoli Netcool/OMNIbus est installé sur ce système (dans ce cas installOMNI est défini sur 1 ci-dessus) et si le package ne se trouve *pas* au même endroit que le support d'installation, supprimez la mise en commentaire de la variable PACKAGE.DIR.NCO et remplacez "--UserInput--" par le nom de chemin complet du package Tivoli Netcool/OMNIbus sur le système. Supprimez ensuite la mise en commentaire de la variable PACKAGE.NCO et remplacez "--UserInput--" par le nom du répertoire ou du fichier qui contient Tivoli Netcool/OMNIbus. **Remarque :** Le programme d'installation recherche le nom automatiquement associé à un suffixe .tar, .tar.gz, .tar.Z ou .zip. N'ajoutez donc pas de suffixe au nom de fichier.
PACKAGE.NCO	--UserInput--	Voir les instructions relatives au paramètre PACKAGE.DIR.NCO.
OMNIHOME	C:\\IBM\\tivoli\\ netcool\\omnibus	Sous Windows, si IBM Tivoli Netcool/OMNIbus est déjà installé sur ce système et si vous souhaitez le configurer pour une utilisation avec Network Manager (installOMNI est alors défini sur 2 ci-dessus), exécutez les tâches suivantes. 1. Supprimez la mise en commentaire de la variable OMNIHOME pour un répertoire Windows. 2. Indiquez le chemin d'accès complet du répertoire qui contient Tivoli Netcool/OMNIbus.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
OMNIHOME	/opt/IBM/tivoli/netcool/omnibus	Sous UNIX, si IBM Tivoli Netcool/OMNIbus est déjà installé sur ce système et si vous souhaitez le configurer pour une utilisation avec Network Manager (installOMNI est alors défini sur 2 ci-dessus), exécutez les tâches suivantes : 1. Supprimez la mise en commentaire de la variable OMNIHOME pour un répertoire UNIX. 2. Indiquez le chemin d'accès complet du répertoire qui contient Tivoli Netcool/OMNIbus.
IAGLOBAL_OBJECTSERVER_PRIMARY_HOST	--UserInput--	Si cette installation se connectera à IBM Tivoli Netcool/OMNIbus (installOMNI est défini sur 0 ci-dessus), supprimez la mise en commentaire de IAGLOBAL_OBJECTSERVER_PRIMARY_HOST et indiquez le nom abrégé ou l'adresse IP du serveur où IBM Tivoli Netcool/OMNIbus est déjà installé.
IAGLOBAL_OBJECTSERVER_PRIMARY_NAME	--UserInput--	Entrez le nom du serveur d'objets en cours d'installation ou de celui auquel vous souhaitez que cette installation se connecte.
IAGLOBAL_OBJECTSERVER_PRIMARY_PORT	4100	Entrez le port du serveur d'objets en cours d'installation ou de celui auquel vous souhaitez que cette installation se connecte.
IAGLOBAL_OBJECTSERVER_USER	root	Entrez le nom de l'utilisateur administratif du serveur d'objets en cours d'installation ou de celui auquel vous souhaitez que cette installation se connecte.
IALOCAL_OBJECTSERVER_PASSWORD	--UserInput--	Entrez le mot de passe administratif du serveur d'objets en cours d'installation ou de celui auquel vous souhaitez que cette installation se connecte.
IAGLOBAL_WAS_defaulthost	16310	Entrez le port à utiliser pour Tivoli Integrated Portal. Notez ce numéro de port, car vous en aurez besoin pour vous connecter aux applications Web.
IAGLOBAL_WASUserID	tipadmin	Entrez un nom à utiliser pour le compte administrateur de Tivoli Integrated Portal.
IALOCAL_WASPassword	--UserInput--	Entrez un mot de passe à utiliser pour le compte administrateur de Tivoli Integrated Portal.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
TIP_INSTALL_DIR	C:\\IBM\\tivoli\\tip	Si votre installation est sous Windows, fournissez le chemin complet d'accès au répertoire d'installation de Tivoli Integrated Portal. **Remarque :** Windows considère la barre oblique inversée \ comme étant un caractère d'échappement, vous devez donc utiliser une barre oblique inversée double \\ lors de la définition d'un chemin sous Windows.
TIP_INSTALL_DIR	/opt/IBM/tivoli/tip	Si votre installation est sous UNIX, fournissez le chemin complet d'accès au répertoire d'installation de Tivoli Integrated Portal.
IAGLOBAL_INSTALL_LOCATION_SELECTION	create	Définissez cette valeur sur create pour installer Tivoli Integrated Portal. Définissez-la sur reuse pour utiliser une installation existante de Tivoli Integrated Portal.
authLDAP	1	Sélectionnez cette option pour utiliser une authentification LDAP pour les utilisateurs Tivoli Integrated Portal. Si la mise en commentaire d'authLDAP et celle d'authOMNI sont supprimées, LDAP est utilisé par défaut pour les nouveaux utilisateurs. Si ni la mise en commentaire d'authLDAP, ni celle d'authOMNI ne sont supprimées, un référentiel de fichiers interne est utilisé.
authOMNI	1	Sélectionnez cette option afin d'utiliser le serveur d'objets pour l'authentification des utilisateurs Tivoli Integrated Portal. Si la mise en commentaire d'authLDAP et celle d'authOMNI sont supprimées, LDAP est utilisé par défaut pour les nouveaux utilisateurs. Si ni la mise en commentaire d'authLDAP, ni celle d'authOMNI ne sont supprimées, un référentiel de fichiers interne est utilisé.
IAGLOBAL_LDAP_NAME	--UserInput--	Entrez le nom d'hôte du serveur LDAP.
IAGLOBAL_LDAP_PORT	389	Entrez le port du serveur LDAP.
IAGLOBAL_LDAP_REPOSITORY_ID	--UserInput--	Entrez l'identificateur du référentiel du serveur LDAP.
IAGLOBAL_LDAP_PRIMARY_USER	tipadmin	Entrez le nom de l'administrateur Tivoli Integrated Portal.
IAGLOBAL_LDAP_BIND_DN	"cn\=root"	Entrez le nom de liaison.
IALOCAL_LDAP_BIND_PASSWORD	--UserInput--	Entrez le mot de passe correspondant au nom de la liaison.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
IAGLOBAL_LDAP_BASE_ENTRY	"o\=IBM,c\=US"	Entrez le nom distinctif.
IAGLOBAL_LDAP_GROUP_ENTITY	Group	Entrez le type d'entité du groupe.
IAGLOBAL_LDAP_GROUP_SUFFIX	"o\=IBM,c\=US"	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.
IAGLOBAL_LDAP_ORG_ENTITY	OrgContainer	Entrez le type d'entité de l'organisation.
IAGLOBAL_LDAP_ORG_SUFFIX	"o\=IBM,c\=US"	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.
IAGLOBAL_LDAP_USER_ENTITY	PersonAccount	Entrez le type d'entité du compte personnel.
IAGLOBAL_LDAP_USER_SUFFIX	"o\=IBM,c\=US"	Entrez les identificateurs appropriés pour votre **o**rganisation et votre **p**ays.
IAGLOBAL_PRECISION_DOMAIN0	--UserInput--	Entrez le nom de domaine réseau pour Network Manager. Entrez un nom descriptif, par exemple, RESEAUTEST. Le nom du domaine doit comporter entre un et 11 caractères (lettres, chiffres ou les deux), les lettres étant en majuscules, sans espace ni caractère spécial. Notez ce nom de domaine, car il est utilisé pour le démarrage manuel de composants.
UI_Initial_Discovery	0	Définissez cette valeur sur 1 pour que le processus d'installation démarre une reconnaissance réseau de votre sous-réseau local.
UI_Import_Netview	0	Définissez cette valeur sur 1 pour que le processus d'installation démarre une reconnaissance réseau en utilisant les informations déjà exportées depuis une installation IBM Tivoli NetView.
UI_Import_Other	0	Définissez cette valeur sur 1 si vous souhaitez que le processus d'installation démarre une reconnaissance réseau en utilisant les informations issues d'une autre application de gestion du réseau.
UI_No_Discovery	1	Définissez cette valeur sur 1 pour terminer le processus d'installation sans démarrer de reconnaissance. Si vous choisissez de ne pas démarrer de reconnaissance maintenant, vous pouvez en démarrer une plus tard en utilisant l'interface graphique de la configuration du réseau.
UI_Subnet	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, entrez l'adresse IP du sous-réseau à reconnaître. Seules des adresses IPv4 peuvent être entrées pour ce paramètre.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
UI_Netmask	255.255.255.0	Si vous avez choisi de démarrer une reconnaissance, entrez le masque de réseau du sous-réseau à reconnaître. Pour un sous réseau de classe C, il s'agit de 255.255.255.0.
UI_SNMP_1	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_SNMP_2	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_SNMP_3	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_SNMP_4	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_SNMP_5	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_SNMP_6	--UserInput--	Si vous avez choisi de démarrer une reconnaissance, vous pouvez choisir d'entrer jusqu'à six noms de communauté SNMP (mots de passe).
UI_Network_Nodes	--UserInput--	Entrez l'emplacement de la sortie du script de migration de IBM Tivoli NetView que vous avez lancé depuis le tableau de bord comme l'exigeait l'installation.
UI_Network_Nodes	--UserInput--	Si vous définissez l'emplacement de la reconnaissance depuis une autre installation Network Manager, entrez l'emplacement du fichier qui contient une liste des noeuds de votre réseau.
UI_SNMP_Strings	--UserInput--	Si vous définissez l'emplacement de la reconnaissance depuis une autre installation Network Manager, entrez l'emplacement du fichier qui contient une liste des noms de communauté utilisés dans votre réseau.
IAGLOBAL_NCIM_SERVER	informix	Entrez le nom du serveur sur lequel installer la base de données de topologie NCIM.
IAGLOBAL_NCIM_CREATE	yes	Définissez cette valeur sur no pour utiliser une base de données topologiques NCIM existante.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
IAGLOBAL_NCIM_PORT	3306	Si vous utilisez MySQL pour la base de données topologiques, entrez le port de la base de données topologiques NCIM.
IAGLOBAL_NCIM_USERNAME	ncim	Si vous utilisez MySQL pour la base de données topologiques, entrez le nom d'utilisateur du compte administrateur de la base de données topologiques NCIM.
IALOCAL_NCIM_PASSWORD	--UserInput--	Si vous utilisez MySQL pour la base de données topologiques, entrez le mot de passe du compte administrateur de la base de données topologiques NCIM.
connectMySQL	1	Supprimez la mise en commentaire de cette ligne si vous souhaitez utiliser une base de données MySQL existantes pour stocker les données topologiques.
connectDB2	1	Supprimez la mise en commentaire de cette ligne si vous souhaitez utiliser une base de données DB2 existante pour stocker les données topologiques.
connectORACLE	1	Supprimez la mise en commentaire de cette ligne si vous souhaitez utiliser une base de données Oracle pour stocker les données topologiques.
connectIDS	1	Supprimez la mise en commentaire de cette ligne si vous souhaitez utiliser une base de données Informix existante pour stocker les données topologiques.
IAGLOBAL_NCIM_HOST	--UserInput--	Si vous utilisez une base de données existante pour stocker les données topologiques, entrez le nom ou l'adresse IP de l'hôte sur lequel est installée la base de données.
IAGLOBAL_NCIM_CREATE	yes	Si vous utilisez une base de données existante pour stocker les données topologiques, définissez cette valeur sur `yes` pour créer les tables de la base de données NCIM. Définissez cette valeur sur `no` si les tables de la base de données NCIM existent déjà.
IAGLOBAL_NCIM_PORT	3306	Si vous utilisez une base de données MySQL existante pour stocker les données topologiques, entrez le port utilisé par la base de données.
IAGLOBAL_NCIM_USERNAME	ncim	Il s'agit de l'utilisateur que le produit utilise pour se connecter à la base de données. Ne modifiez pas cette valeur.
IALOCAL_NCIM_PASSWORD	--UserInput--	Si vous utilisez une base de données MySQL existante pour stocker les données topologiques, entrez le mot de passe de l'utilisateur ncim.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
IAGLOBAL_NCIM_PORT	50000	Si vous utilisez une base de données DB2 pour stocker les données topologiques, entrez le port utilisé par la base de données.
IAGLOBAL_NCIM_DBNAME	--UserInput--	Si vous utilisez une base de données DB2 existante pour stocker les données topologiques, entrez le nom de l'instance de la base de données DB2 qui stocke ces données.
IAGLOBAL_NCIM_USERNAME	--UserInput--	Si vous utilisez une base de données DB2 existante pour stocker les données topologiques, entrez le nom d'utilisateur administratif utilisé par la base de données.
IALOCAL_NCIM_PASSWORD	--UserInput--	Si vous utilisez une base de données DB2 existante pour stocker les données topologiques, entrez le mot de passe de l'utilisateur administratif.
IAGLOBAL_NCIM_SQLLIB	--UserInput--	Si vous utilisez une base de données DB2 existante pour stocker les données topologiques, entrez le répertoire local de ce serveur où sont stockées les commandes SQL du client DB2. S'il s'agit d'une installation Windows, utilisez des barres obliques inversées double // entre les répertoires.
IAGLOBAL_NCIM_PORT	1521	Si vous utilisez une base de données Oracle existante pour stocker les données topologiques, entrez le port utilisé par la base de données.
IAGLOBAL_NCIM_DBNAME	--UserInput--	Si vous utilisez une base de données Oracle existante pour stocker les données topologiques, entrez l'identificateur système utilisé par la base de données Oracle dans laquelle sont stockées ces données.
IAGLOBAL_NCIM_USERNAME	--UserInput--	Si vous utilisez une base de données Oracle existante pour stocker les données topologiques, entrez le nom d'utilisateur administratif utilisé par la base de données.
IALOCAL_NCIM_PASSWORD	--UserInput--	Si vous utilisez une base de données Oracle existante pour stocker les données topologiques, entrez le mot de passe de l'utilisateur administratif.
IAGLOBAL_NCIM_PORT	9088	Si vous utilisez une base de données Informix existante pour stocker les données topologiques, entrez le port utilisé par la base de données.
IAGLOBAL_IDS_SERVER_NAME	--UserInput--	Si vous utilisez une base de données Informix existante pour stocker les données de topologie, entrez le nom du serveur Informix.
IAGLOBAL_IDS_DB_NAME	--UserInput--	Si vous utilisez une base de données Informix existante pour stocker les données de topologie, entrez le nom de la base de données Informix.

Tableau 11. Paramètres du fichier de réponses (suite)

Paramètre	Valeur par défaut	Description
IAGLOBAL_NCIM_USERNAME	--UserInput--	Si vous utilisez une base de données Informix existante pour stocker les données topologiques, entrez le nom d'utilisateur administratif utilisé par la base de données.
IALOCAL_NCIM_PASSWORD	--UserInput--	Si vous utilisez une base de données Informix existante pour stocker les données topologiques, entrez le mot de passe de l'utilisateur administratif.
StartDaemons	Démarrer IBM Tivoli Network Manager avant de quitter	Supprimez la mise en commentaire de cette ligne si vous souhaitez démarrer Network Manager avant de quitter le programme d'installation.

Tâches de post-installation

Après avoir installé Network Manager, vous pouvez être amené à effectuer des tâches de post-installation.

Vérifiez que vous avez installé avec succès Network Manager.

Pour effectuer les tâches de post-installation :

1. Vérifiez que l'installation de Network Manager est terminée.
2. Facultatif : Si vous utilisez Tivoli Netcool/OMNIbus version 7.3.1 ou une version antérieure avec Network Manager, vous devez exécuter des étapes de post-installation supplémentaires pour configurer l'automatisation des événements SAE (Service-Affected Events), comme indiqué dans «Configuration des automatisations pour les événements affectés par un service», à la page 176.
3. Selon les paramètres supplémentaires requis, exécutez les étapes décrites dans les rubriques suivantes :

Option	Description
Tâches de post-installation non root (UNIX uniquement)	• Informix peut être installé uniquement par l'utilisateur root. Si vous avez installé Network Manager en tant qu'utilisateur non-root et souhaitez utiliser Informix, suivez la procédure décrite dans «Installation et configuration d'Informix après une installation non root», à la page 251 • Si l'installation est effectuée par un utilisateur non-root et que vous installez Informix sur un autre serveur que le serveur sur lequel les composants d'interface graphique sont installés, vous devez installer le logiciel Informix IConnect en tant qu'utilisateur root sur le serveur de composants d'interface graphique pour utiliser des rapports Cognos. Suivez les étapes décrites dans «Configuration d'Informix à distance pour la génération de rapports», à la page 253 • Vous pouvez configurer l'utilisateur qui gère les processus Network Manager, comme indiqué dans «Configuration des autorisations d'utilisateur root/non root», à la page 248
Tâche de post-installation pour Informix sous Windows	Si vous avez installé Network Manager avec une base de données Informix sous Windows, assurez-vous d'effectuer les étapes décrites dans «Configuration de l'espace disque d'Informix sous Windows», à la page 379
Tâches de post-installation pour la configuration de Tivoli Common Reporting	Si vous souhaitez utiliser Informix, MySQL ou Oracle en tant que base de données NCIM, vous devez configurer les bases de données pour pouvoir utiliser des rapports Tivoli Common Reporting, comme décrit dans «Configuration de NCIM pour Tivoli Common Reporting», à la page 287.
Mise à niveau à partir d'une version antérieure de Network Manager	Suivez les étapes décrites dans «Mise à niveau et migration vers la dernière version de Network Manager», à la page 143
Installation de l'agent de surveillance	Si vous voulez utiliser IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, suivez les étapes décrites dans «Intégration à IBM Tivoli Monitoring», à la page 235
Pour toute autre tâche de configuration, consultez les rubriques dans :	Chapitre 4, «Configuration de Network Manager», à la page 175

Option	Description
Si vous devez configurer une base de données topologiques après l'installation pour Network Manager.	Pour plus de détails sur la manière de créer un schéma de base de données manuellement après l'installation, Reportez-vous aux tâches concernant la création de schémas de base de données topologiques dans le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
Fix Pack 4 Mise à niveau des composants pour le dernier support de navigateur	Fix Pack 4 Pour tirer parti du dernier support de navigateur, il peut être nécessaire de mettre à niveau le niveau Tivoli Integrated Portal et d'appliquer le dernier groupe de correctifs de interface graphique Web. Par exemple, le groupe de correctifs 4 de Network Manager 3.9 contient Tivoli Integrated Portal 2.2.0.9 et interface graphique Web 7.4. Cependant, pour pouvoir utiliser Internet Explorer 10 ou Mozilla Firefox 24 ESR, vous devez effectuer une mise à niveau vers Tivoli Integrated Portal 2.2.0.13 et le groupe de correctifs 2 interface graphique Web. Fix Pack 4 Pour effectuer la mise à niveau : 1. Accédez au site du support http://www-933.ibm.com/support/fixcentral/ 2. Recherchez Tivoli Integrated Portal version 2.2.0.13 pour votre plate-forme et téléchargez la version. 3. Recherchez Tivoli Netcool/OMNIbus 7.4, groupe de correctifs 2 (7.4.0.2) pour votre plate-forme, puis le groupe de correctifs 2 interface graphique Web (appelé également OMNIbus_GUI), et effectuez le téléchargement. 4. Suivez les instructions d'installation des groupes de correctifs pour les appliquer.

Tâches associées:

«Affichage des journaux d'installation», à la page 123
L'affichage des journaux d'installation peut être utile à des fins de dépannage.

Référence associée:

«Echec des tâches de postinstallation exécutées à partir du tableau de bord sous AIX 7», à la page 130
En cas d'échec des tâches de post-installation lancées à partir du tableau de bord sous AIX 7, vérifiez que les utilitaires X11 (y-compris xterm) ont été installés et configurés correctement pour le chargement des interfaces graphiques.

Identification des incidents liés à l'installation

Ces informations vous permettent de traiter les erreurs pouvant survenir lors de l'installation de Network Manager.

Les rubriques suivantes décrivent les types de messages d'erreur que vous pouvez rencontrer au cours du processus d'installation, ainsi que les actions que vous pouvez effectuer pour résoudre les erreurs.

Affichage des journaux d'installation

L'affichage des journaux d'installation peut être utile à des fins de dépannage.

Les informations sur la réussite du processus d'installation sont enregistrées dans différents fichiers journaux. Pour afficher les informations du journal d'installation, procédez comme suit :

Consultez le journal d'installation approprié :

Symptôme	Action
Idée générale de la partie de l'installation ayant échoué.	Consultez le fichier journal InstallAnywhere. 1. Accédez au répertoire racine de l'utilisateur ayant exécuté le programme d'installation. 2. Ouvrez le fichier journal InstallAnywhere. Ce dernier porte un nom du type `IA-ITNM-Install-`*`NN`*`.log`, où *NN* est un nombre. Généralement, le fichier se nomme `IA-ITNM-Install-00.log`

Symptôme	Action
La partie de l'installation qui semble avoir échoué implique les composants principaux Network Manager ou Tivoli Netcool/OMNIbus	Consultez les fichiers journaux suivants : 1. Accédez au répertoire `NCHOME/log/install` 2. Consultez les journaux de ce répertoire : • Le fichier `Configuration.log` affiche les erreurs rencontrées lors des tâches de configuration ultérieures à l'installation • Les fichiers ayant des noms de forme `ncp_create*.log` affichent les erreurs survenues lors de la création de la base de données topologiques NCIM • Windows Le fichier `msi.log` affiche les erreurs rencontrées par le programme d'installation Microsoft. **Remarque :** Si vous installez une nouvelle base de données NCIM sur un serveur distant ou utilisez une instance de base de données existante, le processus d'installation génère un autre ensemble de fichiers journaux que celui généré lors de l'installation d'un seul serveur. Lors d'une installation de base de données distante ou existante, les fichiers de trace et journaux suivants sont générés lors de l'installation d'une nouvelle base de données sur le même serveur que Network Manager: • ncp_create_ncim_core_db.trace • ncp_create_ncim_pip_db.log • ncp_create_ncim_pip_db.trace • ncp_create_ncmib_db.trace • ncp_create_ncmonitor_db.trace • ncp_create_ncpgui_db.trace • ncp_create_ncpolldata_db.trace
Pour plus d'informations sur les processus Tivoli Netcool/OMNIbus et Network Manager qui s'exécutent lors de l'installation	Consultez les fichiers journaux suivants : • Affichez des informations sur les processus Tivoli Netcool/OMNIbus exécutés au cours de l'installation en consultant les journaux de ce répertoire : `NCHOME/omnibus/log`. • Affichez des informations sur les processus Network Manager exécutés au cours de l'installation en consultant les journaux de ce répertoire : `NCHOME/log/precision`.
La partie de l'installation qui semble avoir échoué implique Tivoli Integrated Portal	Consultez les fichiers journaux Composite Offering Installer (COI) : • Les fichiers journaux Composite Offering Installer (COI) sont disponibles dans le répertoire *`RACINETIP`*`/_uninst/ITNM/plan/install/MachinePlan_localhost/*/logs`, où *RACINETIP* correspond au répertoire dans lequel Tivoli Integrated Portal est installé. • Des journaux différents sont générés à chaque étape de l'installation. Vous pouvez identifier l'étape dans laquelle un problème est survenu grâce au fichier journal InstallAnywhere, `~/IA-ITNM-Install-00.log`. • En consultant les fichiers journaux dans Composite Offering Installer (COI), vous pouvez déterminer à quel endroit le problème est survenu dans les étapes de configuration d'IBM Autonomic Deployment Engine (DE) ou Composite Offering Installer.

Symptôme	Action
Le problème sous-jacent de l'installation Tivoli Integrated Portal peut provenir d'IBM Autonomic Deployment Engine	Consultez les fichiers journaux Deployment Engine. Ces fichiers sont disponibles aux emplacements suivants : • Si vous les installez en tant qu'utilisateur root sur UNIX, ils se trouveront dans `/usr/ibm/common/acsi/logs/root`. • Si vous les installez en tant qu'utilisateur non-root sur UNIX, ils se trouveront dans `~/.acsi_$HOSTNAME/logs/$USER`. • Si vous les installez sur Windows, ils se trouveront dans `C:\Program Files (x86)\IBM\Common\acsi\logs\%USERNAME%`. • Sur Windows 32 bits, le répertoire est le suivant `C:\Program Files\IBM\Common\acsi\logs\%USERNAME%`.
Le problème sous-jacent de l'installation Tivoli Integrated Portal peut provenir des étapes de configuration de Composite Offering Installer (COI).	Consultez les fichiers journaux dans *RACINETIP*`/logs`, où *RACINETIP* correspond au répertoire dans lequel Tivoli Integrated Portal est installé.
Il semble que ce soit le démarrage du serveur Tivoli Integrated Portal lui-même qui ait échoué même si aucune erreur n'est répertoriée dans les fichiers journaux présentés ci-dessus.	Examinez les fichiers journaux qui se trouvent dans le répertoire *TIPHOME*`/profiles/TIPProfile/logs/server1`. Ces fichiers contiennent des informations sur le statut du serveur Tivoli Integrated Portal.
La partie de l'installation qui a des problèmes implique Tivoli Common Reporting.	Consultez les fichiers journaux suivants : • *composants_TIP*`/TCRComponent/logs` • *composants_TIP*`/TCRComponent/cognos/logs` **Remarque :** L'emplacement par défaut pour *composants_TIP* est `/opt/IBM/tivoli/tipv2Components`.
La partie de l'installation qui a des problèmes implique BIRTExtension	Examinez les journaux dans *composants_TIP*`/BIRTExtension/logs`. **Remarque :** L'emplacement par défaut pour *composants_TIP* est `/opt/IBM/tivoli/tipv2Components`.
La partie de l'installation qui a des problèmes implique ESSServer	Examinez les journaux dans *composants_TIP*`/ESSServer/logs`. **Remarque :** L'emplacement par défaut pour *composants_TIP* est `/opt/IBM/tivoli/tipv2Components`.
Il semble y avoir des problèmes avec l'installation de la base de données topologiques Informix par défaut.	Affichez des informations sur les processus Informix exécutés au cours de l'installation en consultant les journaux de ce répertoire : NCHOME/platform/*arch*/informix

Journal TIPProfile_create

Parcourez le journal TIPProfile_create lorsque votre installation s'achève par une erreur.

Objectif

Le journal TIPProfile_create enregistre les messages relatifs à la réussite ou à l'échec d'une tâche lors de la création du profil Network Manager au cours de l'installation.

Exemple

Voici un exemple des enregistrements finaux d'un fichier TIPProfile_create.log présentant des erreurs.

```
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1007</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>INFO</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>areCommandLineArgumentsValid</method>
  <thread>10</thread>
  <message>Validation Error for profilePath: The profile path is not valid.
</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1008</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>SEVERE</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Argument Validation Failed.</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1009</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>INFO</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Returning with return code: INSTCONFFAILED</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1010</sequence>
  <logger>com.ibm.wsspi.profile.WSProfileCLI</logger>
  <level>INFO</level>
  <class>com.ibm.wsspi.profile.WSProfileCLI</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Returning with return code: INSTCONFFAILED</message>
</record>
```

Fichiers journaux

Suite à une installation, localisez et consultez les journaux ainsi que les fichiers associés afin de vous assurer que les composants ont été correctement installés.

Voici les journaux créés pendant une installation de Network Manager. Le programme d'installation crée un journal appelé `IA-TIPInstall-xx.log`, qui est situé dans le répertoire de base de l'utilisateur. Ce journal doit être consulté en premier. Il montre la progression de l'installation, en donnant des informations de traçage. Chaque étape exécutée pendant l'installation crée un journal dans le répertoire *rép_base_tip*`/logs`.

Console d'administration

```
createProfile.err
createProfile.out
createTIPService.err
createTIPService.out
deleteProfile.err (uninstall)
deleteProfile.out
enableAppSecurity.err
enableAppSecurity.out
extendJaveMemory.err
extendJaveMemory.out
modifyWASServiceName.err
modifyWASServiceName.out
removeTIPService.err (uninstall)
removeTIPService.out
```

Serveur CGI

```
CGIServer.err
CGIServer.out
configureIAuthzShLib.err
configureIAuthzShLib.out
deployiAuthzEar.err
deployiAuthzEar.out
```

Serveur de stockage Enterprise

```
deployESSApplication.err
deployESSApplication.out
ESSConfiguration.err
ESSConfiguration.out
osgiCfgInit.err
osgiCfgInit.out
```

Service Web IBM Tivoli Monitoring

```
ITMWebServiceEAR.err
ITMWebServiceEAR.out
```

Représentations graphiques

```
assignChartAdminRole.err
assignChartAdminRole.out
TIPChartPortlet.err
TIPChartPortlet.out
```

Reporting Time Scheduling Services

```
TipTssEar.err
TipTssEar.out
TipTssEWASScheduler.err
TipTssEWASScheduler.out
TipTssJDBC.err
TipTssJDBC.out
TipTssSharedLibraries.err
TipTssSharedLibraries.out
```

Tivoli Common Reporting

```
tcr.err
tcr.out
tcrConfigClient.err
tcrConfigClient.out
tcrsPostConfig.err
tcrsPostConfig.out
```

Tivoli Integrated Portal

```
configureTIPTransformationShLib.err
configureTIPTransformationShLib.out
deployTIPChangePassdWar.err
deployTIPChangePassdWar.out
deployTIPRedirectorEar.err
deployTIPRedirectorEar.out
renameIdMgrRealm.err
renameIdMgrRealm.out
```

Virtual Member Manager

```
VMM.err
VMM.out
```

Configuration de LDAP VMM

```
configureVMMLDAP.err
configureVMMLDAP.out
```

Plug-in VMM ObjectServer

```
VMMObjectServerPlugin.err
VMMObjectServerPlugin.out
```

WebSphere

```
checkWAS.err
checkWAS.out
startWAS.err
startWAS.out
```

Affichage des packages installés

Vérifiez que l'installation s'est effectuée correctement en affichant les packages que le programme d'installation a installés. Cette vérification est utile pour résoudre les problèmes d'échec d'installation. En outre, indiquez les packages qui ont été installés et ceux qui ne l'ont pas été dans les informations que vous envoyez à Service de support IBM dans la demande de service.

1. Définissez la variable d'environnement du moteur DE (Deployment Engine) :
   - UNIX Linux Exécutez `/var/ibm/common/acsi/setenv.sh`.
   - Windows Exécutez `C:\Program Files\IBM\Common\acsi\setenv.cmd`.
2. Pour lister les packages installés, exécutez la commande de votre système d'exploitation avec le type d'utilisateur ayant installé le produit :

Système d'exploitation et utilisateur	Location
Utilisation non-root UNIX	`/home/`*`username`*`/.acsi_`*`username`*`/bin/listIU.sh`
Utilisateur root UNIX	`/usr/ibm/common/acsi/bin/listIU.sh`
Administrateur Windows	`C:\Program Files\IBM\Common\acsi\bin\listIU.cmd`

Vérification de l'URL de connexion et des ports par défaut

Si vous ne pouvez pas vous connecter, vérifiez le format de l'URL et les ports que vous utilisez après l'installation.

Format d'URL

Vérifiez que le format de l'URL entrée est le suivant (affiche les ports par défaut) :

- `https://`*`système_hôte_local`*`:16311/ibm/console` (accès sécurisé).
- `http://`*`système_hôte_local`*`:16310/ibm/console` (accès non sécurisé).

Où *système_hôte_local* indique le nom d'hôte ou l'adresse IP du serveur Tivoli Integrated Portal.

Ports par défaut

16310 est le numéro de port non sécurisé par défaut et 16311 est le numéro de port sécurisé par défaut. Si votre environnement a été configuré lors de l'installation avec un numéro de port autre que la valeur par défaut, entrez ce numéro en lieu et place.

Messages d'erreur de dépendance

Les messages d'erreur de dépendance sont générés si le processus d'installation ne trouve pas un module ou un composant de Network Manager requis.

Si un message d'erreur de dépendance s'affiche, suivez les invites et installez les composants requis.

Exécution des procédures d'installation et de maintenance en tant que superutilisateur ou non superutilisateur

L'installation doit être exécutée par le même utilisateur du système d'exploitation à chaque fois. Quel que soit l'utilisateur qui installe le premier produit Tivoli Network Management sur un poste de travail donné, c'est lui qui doit installer, désinstaller et modifier tous les produits Tivoli Network Management suivants de ce poste de travail.

Vous pouvez exécuter l'installation sans être superutilisateur. Toutefois, certaines actions de configuration de Network Manager doivent être exécutées par l'utilisateur `superutilisateur`. A la fin de l'assistant d'installation, un panneau vous rappelle de vous connecter en tant que superutilisateur et d'effectuer ces configurations manuellement.

Concepts associés:

«Installations en tant que superutilisateur et non superutilisateur», à la page 248
Sous UNIX, vous pouvez installer Network Manager en tant que superutilisateur ou en tant que non superutilisateur.

Tâches associées:

«Configuration des composants centraux pour une exécution en tant qu'utilisateur root», à la page 249
Sous UNIX, si vous avez installé Network Manager en tant qu'utilisateur non root, vous devez procéder à une configuration supplémentaire pour exécuter les composants centraux en tant qu'utilisateur root.

Espace disque insuffisant pour terminer l'installation

S'il n'y a pas assez d'espace disque pour terminer l'installation, un message d'erreur s'affiche et l'installation est interrompue.

Le message d'erreur se présente comme suit :

```
Il n'y a pas assez d'espace disque dans REPERTOIRE pour installer le logiciel
Libérez de l'espace et exécutez de nouveau l'installation
```

Dans ce message, *REPERTOIRE* fait référence au répertoire de base d'installation indiqué.

Si vous rencontrez ce message d'erreur, libérez de l'espace disque ou sélectionnez un répertoire de base sur une partition disposant de plus d'espace et exécutez de nouveau le processus d'installation.

Erreur d'installation en mode console

Lors de l'installation de Network Manager en mode console sur des systèmes UNIX, vous pouvez recevoir une erreur liée au fait que la variable d'environnement DISPLAY est définie.

Si vous recevez le message d'erreur suivant lors de l'installation de Network Manager en mode console sur des systèmes UNIX, vous devez supprimer la valeur de la variable d'environnement DISPLAY avant de lancer l'installation en mode console :

```
Installation...

Invocation of this Java Application has caused an InvocationTargetException. This
application will now exit.

Stack Trace:
java.lang.NoClassDefFoundError: sun.awt.X11GraphicsEnvironment (initialization failure)
 at java.lang.J9VMIntervals.initialize(J9VMIntervals.java:140)
 at java.lang.Class.forNameImpl (Native Method)
 at java.lang.Class.forName(Class.java:136)
```

Utilisez la commande suivante : `unset DISPLAY`, puis lancez à nouveau l'installation de la console.

Echec des tâches de postinstallation exécutées à partir du tableau de bord sous AIX 7

En cas d'échec des tâches de post-installation lancées à partir du tableau de bord sous AIX 7, vérifiez que les utilitaires X11 (y-compris xterm) ont été installés et configurés correctement pour le chargement des interfaces graphiques.

Si les erreurs suivantes apparaissent lors du lancement des tâches de postinstallation à partir du tableau de bord :

```
Could not load program /usr/X11R7/bin/xterm:
Dependent module /usr/lib/libXpm.a(shr_64.o) could not be loaded.
Member shr_64.o is not found in archive
```

Pour corriger l'erreur, vérifiez l'emplacement vers lequel pointe la bibliothèque `libXpm.a`, par exemple :

```
ls -ln /usr/lib/libXpm.a
lrwxrwxrwx 1 0 0 26 May 17 10:06 /usr/lib/libXpm.a ->
/opt/freeware/lib/libXpm.a
```

Dans cet exemple, `libXpm.a` ne pointe pas vers l'emplacement correct.

Vérifiez que `/usr/lib/libXpm.a` pointe vers `/usr/lpp/X11/lib/R7/libXpm.a`. Utilisez la commande suivante pour corriger le lien :

```
ln -s -f /usr/lpp/X11/lib/R7/libXpm.a /usr/lib/libXpm.a
```

La base de données topologiques ne s'initialise pas

En cas de problèmes de mémoire et de performances, l'installation de la base de données Informix peut échouer en générant le code d'erreur 8 et le message indiquant que `Informix ne peut pas s'initialiser`. Pour installer la base de données, vous devez augmenter l'espace de pagination et définir 600 secondes comme délai d'attente de l'initialisation.

Pour augmenter l'espace de pagination pour disposer d'une mémoire totale de 8 Go, consultez les instructions relatives à votre système d'exploitation ou contactez l'administrateur.

Pour augmenter le délai d'attente et exécuter de nouveau l'installation d'Informix suite à un échec d'installation :

1. Définissez la variable d'environnement Network Manager en utilisant `NCHOME/env.sh|.bat`, en fonction du système d'exploitation.
2. Connectez-vous comme utilisateur root. Informix peut être installé uniquement par l'utilisateur root.
3. Supprimez l'installation Informix en utilisant le script `NCHOME/bin/CleanSystem -i` (l'option `-i` supprime la base de données topologiques Informix).
4. Faites passer à 600 secondes le délai d'attente dans le script de configuration Informix en modifiant la ligne 55 dans `NCHOME/precision/install/scripts/install_ids_informix.ksh`.
5. Accédez au répertoire `NCHOME/precision/install/scripts`.
6. Exécutez le script d'installation Informix : `./install_ids_root|admin.ksh -f ../data/ids.properties`

Sauvegarde et restauration du moteur de déploiement

Utilisez le script de sauvegarde du moteur de déploiement (DE, Deployment Engine) avant toute installation de composants supplémentaires ou d'autres produits basés sur la plateforme Tivoli Integrated Portal. S'il s'avère nécessaire de récupérer la configuration d'origine suite à défaillance, vous pourrez alors exécuter le script de restauration du moteur de déploiement.

Le moteur de déploiement effectue l'installation des produits nouveaux ou mis à niveau. Ce moteur assure un suivi des composants installés et saute l'installation d'un composant donné si celui-ci est déjà présent sur le système. Pour sauvegarder ou restaurer la base de données du moteur de déploiement, procédez comme suit.

1. A partir de la ligne de commande, accédez au répertoire `acsi` :
   - Windows `cd C:\Program Files\IBM\Common\acsi`
   - Linux UNIX Pour les systèmes Linux et Unix, le chemin d'accès au répertoire `acsi` est différent si vous procédez à l'installation en tant qu'utilisateur root ou utilisateur non-root :
     - Pour l'installation en tant qu'utilisateur non-root, le chemin inclut le répertoire principal de l'utilisateur :
       `< rép_principal_utilisateur_non_root>/.asci_<nom_utilisateur>`

- Pour l'installation en tant qu'utilisateur root, le chemin est le suivant : `/var/ibm/common/asci`

2. Initialisez l'environnement du moteur de déploiement à partir de la ligne de commande :
   - Windows `setenv.bat`
   - Linux UNIX `. setenv.sh`
3. Accédez au répertoire `bin` :
   - Windows Accédez au répertoire enfant `bin`, à savoir : `C:\Program Files\IBM\Common\acsi\bin`
   - Linux UNIX Pour les systèmes Linux et Unix, le chemin d'accès au répertoire `bin` est différent si vous procédez à l'installation en tant qu'utilisateur root ou utilisateur non-root :
     - Pour un utilisateur non-root, accédez au répertoire enfant `bin`, à savoir : *<rép_principal_utilisateur_non_root* `>/.asci_<`*nom_utilisateur*`>/bin`
     - Pour un utilisateur root, le chemin est le suivant : `/usr/ibm/common/asci/bin`
4. Exécutez le script de sauvegarde afin de sauvegarder la base de données du moteur de déploiement, comme suit :
   - Windows `de_backupdb.cmd`
   - Linux UNIX `de_backupdb`
5. Si vous devez restaurer la base de données du moteur de déploiement, exécutez le script de restauration à partir du répertoire `bin` :
   - Windows `de_restoredb.cmd`
   - Linux UNIX `de_restoredb`

Si vous avez sauvegardé la base de données du moteur de déploiement, vous pouvez maintenant exécuter le programme d'installation afin d'ajouter les composants ou produits supplémentaires. Si vous avez restauré la base de données du moteur de déploiement, vous pouvez à nouveau utiliser l'environnement installé d'origine.

Messages d'installation pouvant être ignorés

Un passage en revue de l'historique d'installation peut mettre à jour des messages d'erreur qui peuvent être ignorés.

Une fois Network Manager installé, une erreur de reflet peut se produire lors du passage en revue des historiques d'installation. L'installation a réussi mais le journal indique des variations de l'erreur suivante :

```
+++ Avertissement +++ :   IWAV0003E Impossible de refléter les
méthodes pour com.ibm.sec.iauthz.
InstanceAuthzServiceLocalHome car l'une des méthodes référence un type qui
ne peut être chargé.
Exception : java.lang.NoClassDefFoundError: com.ibm.sec.iauthz.InstanceAuthorization
+++ Avertissement +++ :   IWAV0002E Echec du reflet des valeurs
+++ Avertissement +++:   java.lang.NoClassDefFoundError : com.ibm.sec.
iauthz.InstanceAuthorization
```

Cette erreur peut être ignorée sans danger.

Espace disque insuffisant pour l'installation

Libérez suffisamment d'espace dans le répertoire temporaire pour l'installation sinon celle-ci échouera.

L'installation nécessite au minimum 500 Mo d'espace disque pour les fichiers temporaires utilisés pendant le processus d'installation. Sous Linux et UNIX, allouez suffisamment d'espace dans le répertoire /tmp ou /opt de l'ordinateur.

Scénario d'échec de l'installation

Consultez le fichier `IA-TIPInstall-xx.log` pour rechercher les erreurs qui ont pu se produire lors de l'installation.

IA-TIPInstall-xx.log

Généralement, le processus d'installation s'arrête lorsqu'une erreur survient. Mais il est possible que l'installation semble avoir abouti et qu'un incident survienne ultérieurement, par exemple lors de la tentative de connexion. Consultez le fichier `IA-TIPInstall-xx.log` qui se trouve dans le répertoire principal afin de vérifier que l'installation a réussi. Par exemple, si vous êtes connecté en tant qu'administrateur sur un système Windows, vous devez rechercher dans `C:\Documents and Settings\Administrator`.

Scénario de consultation de journal

Dans cet exemple sous Windows, l'étape `ESSServerConfig.xml` a échoué et `IA-TIPInstall-xx.log` présente un échec de type COI (Composite Offering Installer) à la ligne 134.

```
C:\IBM\tivoli\tip\_uninst\ITNM\plan\install\MachinePlan_localhost\
0011_IAGLOBAL_COI_STEP_ESSServerConfig\IAGLOBAL_COI_STEP_ESSServerConfig.xml:134:
xec returned: 105
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.ProjectHelper.
addLocationToBuildException(ProjectHelper.java:539)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.taskdefs.Ant.
execute(Ant.java:384)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.Task.perform
(Task.java:364)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at com.ibm.ac.coi.impl.utils.
AntHelper.ant(AntHelper.java:88)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :  ... 3 more
```

Le journal indique le chemin complet du fichier ayant entraîné l'incident. Accédez à cet emplacement, ouvrez le fichier indiqué et consultez la ligne qui a échoué. Dans cet exemple, vous accédez à l'emplacement :

```
C:\IBM\tivoli\tip\_uninst\ITNM\plan\install\MachinePlan_localhost\
00011_IAGLOBAL_COI_STEP_ESSServerConfig\IAGLOBAL_COI_STEP_ESSServerConfig.xml
```

et consultez la ligne 134. Dans cette ligne de la cible `configureESS`, la commande suivante a échoué :

```
<
target name="configureESS" depends="setProperties">
        <echo message="Start to configure Authentication Service..."/>
        <iaecho message="$ESSSERVER_CONFIGURING$"/>
                        ......................
line134:  <exec
```

```
dir="${IAGLOBAL_installLocation}/bin"
executable="${IAGLOBAL_installLocation}/bin/wsadmin${platform.script.ext}"
failonerror="true">
          <redirector output="${IAGLOBAL_installLocation}/logs/
ESSConfiguration.out" error="${IAGLOBAL_installLocation}/logs
/ESSConfiguration.err"/>
    ...
```

Comme vous pouvez le voir, l'appel de `wsadmin` depuis Ant envoie `stdout` vers *rép_base_tip*`/logs/ESSConfiguration.out` et `stderr` vers *rép_base_tip*`/logs/ESSConfiguration.err`. Lorsque vous consultez le fichier `ESSConfiguration.out`, vous voyez que le serveur Tivoli Integrated Portal Server (WAS) a peut-être un problème :

```
WASX7209I: Connected to process "server1" on node TIPNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and
are available as arguments that are stored in the argv variable:
"[C:/IBM/tivoli/tip/logs/ltpaOutput.txt, 1ntegrate]"
WASX7017E: Exception received while running file "C:\IBM\tivoli\tip\bin
\configureESS.jacl";
exception information: com.ibm.bsf.BSFException: error while eval'ing
Jacl expression:
no accessible method "isESSConfigured" in class
com.ibm.ws.scripting.adminCommand.AdminTask
    while executing
"$AdminTask isESSConfigured"
    invoked from within
"set essCheck [$AdminTask isESSConfigured]"
```

Consultez le fichier *rép_base_tip*`/profiles/TIPProfile/logs/server1/SystemOut.log` pour rechercher des exceptions relatives au service d'authentification. Si vous ne savez pas comment procéder, contactez votre expert Tivoli Integrated Portal Server ou rassemblez les journaux Network Manager, notamment `SystemOut.log`, et contactez le support IBM.

L'installation échoue après la mise à niveau du moteur de déploiement

L'exécution du programme d'installation sur un ordinateur disposant d'un environnement Tivoli Integrated Portal existant peut échouer si le moteur de déploiement (DE) a été mis à niveau à partir d'une version antérieure.

Si une ancienne version du DE est installée, le programme d'installation de Tivoli Integrated Portal le met à jour et poursuit l'installation. Il peut arriver que la mise à niveau de des versions antérieures du DE échoue. Lorsque cela se produit, l'installation peut échouer. S'il s'avère que votre produit utilise une version très ancienne du DE (telle que la version 1.2), vous pouvez effectuer l'installation sur la même machine, mais devez vous connecter à l'portail avec un autre nom d'utilisateur. Si vous avez installé l'ancienne version du DE en tant qu'utilisateur root sous Linux ou UNIX, procédez à une désinstallation si la nouvelle installation échoue après la mise à niveau du DE.

Désinstallation de Network Manager

Utilisez les scripts fournis pour désinstaller le produit.

Sur Windows, vous devez supprimer tous les services des domaines supplémentaires avant de désinstaller le produit.

Les scripts permettent de désinstaller le produit dans son intégralité ou certains composants.

Important : Vous devez obligatoirement utiliser les scripts pour désinstaller le produit. La désinstallation du produit effectuée grâce à la suppression de fichiers et de répertoires peut occasionner des problèmes lors de la réinstallation de certains composants.

Désinstallation sous UNIX

Sur les systèmes d'exploitation UNIX, utilisez le script de désinstallation pour désinstaller le produit. Vous pouvez désinstaller des composants spécifiques ou tout le produit.

Avertissement : Ne tentez pas de désinstaller un produit en supprimant des fichiers ou des répertoires. Si vous supprimez des fichiers ou des répertoires, des problèmes peuvent apparaître pendant la réinstallation. Utilisez le script de désinstallation fourni avec le produit pour désinstaller Network Manager.

1. Pour supprimer des produits intégrés à Network Manager sur un même serveur, supprimez-les en utilisant leur propre programme de désinstallation avant de supprimer Network Manager. Par exemple, supprimez Tivoli Netcool/OMNIbus en utilisant le programme de désinstallation de Tivoli Netcool/OMNIbus. Pour plus d'informations sur la désinstallation des bases de données autres qu'Informix, voir la documentation des bases de données.

   DB2 Avant de supprimer une base de données DB2, utilisez le script `uncatalog_db2_database` pour décataloguer la base de données. Veillez également à exécuter l'étape 6, à la page 137. Une base de données DB2 peut être utilisée comme base de données topologiques NCIM ou comme Tivoli Data Warehouse. Pour plus d'informations sur l'utilisation de DB2 comme Tivoli Data Warehouse, voir *IBM Tivoli Monitoring for Tivoli Network Manager IP - Guide d'utilisation*.
2. Retrouvez la source de l'environnement en exécutant la commande `$NCHOME/env.sh`.
3. Exécutez le script de désinstallation `$NCHOME/Uninstall_ITNM`. Cette commande démarre le script `$NCHOME/bin/CleanSystem`. Les options de ligne de commande s'affichent dans l'interface. Elles sont décrites dans le tableau ci-dessous.

Tableau 12. Options **`Uninstall_ITNM`**

Option	Description
`-p`	Arrête tous les processus associés à l'installation.
Informix `-i`	Supprime la base de données topologiques locale de l'installation Network Manager. Cette option fonctionne uniquement avec la base de données Informix par défaut fournie avec le produit. Voir l'étape 5, à la page 137 et exécutez cette étape.

Tableau 12. Options **Uninstall_ITNM** *(suite)*

Option	Description
-n	Supprime l'installation Network Manager.
-t	Supprime l'interface graphique de Network Manager et les composants de l'interface graphique Web Tivoli Netcool/OMNIbus du serveur Tivoli Integrated Portal. Utilisez cette option sur le serveur où Tivoli Integrated Portal est installé.
-c	Supprime Tivoli Integrated Portal. Les composants associés Tivoli Common Reporting et l'interface graphique Web Tivoli Netcool/OMNIbus, COI (Composite Offering Installer), ainsi qu'IBM Autonomic Deployment Engine (DE) sont également supprimés. **Remarque :** L'utilisation des options -c et -a pour supprimer Tivoli Integrated Portal, COI et DE affecte négativement les autres produits Tivoli installés sur le système. Vérifiez qu'aucun autre produit Tivoli sur le système nécessite ces composants avant d'utiliser ces options.
-a	Supprime tous les produits et composants ayant des fichiers ou des données stockés dans les emplacements NCHOME et TIPHOME, y compris les composants backend et d'interface graphique, Tivoli Netcool/OMNIbus, et Informix. **ATTENTION :** **Si vous utilisez cette option, les autres produits installés sur le même serveur, tels que Tivoli Netcool/OMNIbus, l'interface graphique Web Tivoli Netcool/OMNIbus et IBM Tivoli Business Service Manager, peuvent ne pas fonctionner. N'utilisez pas cette option si d'autres produits Tivoli sont installés sur le serveur.**
-h	Utilisez cette option pour spécifier le répertoire principal d'installation si vous n'utilisez pas l'élément NCHOME par défaut.

4. Sélectionnez les composants à supprimer en entrant l'option appropriée. Vous pouvez définir plusieurs options.

   Par exemple, pour arrêter tous les processus et supprimer les composants de Network Manager et de l'interface graphique Web Tivoli Netcool/OMNIbus de Tivoli Integrated Portal :

   ```
   ./Uninstall_ITNM -p -t
   ```

   Avertissement : La suppression des composants peut entraîner un dysfonctionnement des produits dépendants. La suppression des composants de base ou de la base de données topologiques génère des erreurs dans les composants Web Network Manager.

5. Informix Pour supprimer une instance de Network Manager installé par un utilisateur non-root et qui utilise une base de données Informix installée sur le même serveur, exécutez deux fois le script **Uninstall_ITNM**, une fois comme utilisateur root et une fois comme utilisateur non-root.
   a. Exécutez `./Uninstall_ITNM -i` comme utilisateur root pour supprimer la base de données Informix.
   b. En tant qu'utilisateur root, vérifiez que le répertoire `$NCHOME/netcool/platform/linux2x86/informix` est supprimé. Si ce n'est pas le cas, supprimez-la manuellement.
   c. Exécutez `./Uninstall_ITNM -a` comme utilisateur non-root ayant installé Network Manager.
6. DB2 Après la désinstallation et la réinstallation d'une base de données DB2, recataloguez la base de données. Utilisez le script `catalog_db2_database`.
7. Pour réinstaller Network Manager après l'avoir supprimé, utilisez un nouvelle fenêtre d'interpréteur de commandes. N'utilisez pas l'interpréteur de commandes utilisé pour désinstaller l'installation précédente Network Manager.

Information associée:

Désinstallation de Tivoli Netcool/OMNIbus V7.3.1 sur UNIX

Centre de documentation IBM DB2

Désinstallation sous Windows

Vous disposez de plusieurs options pour désinstaller Network Manager sur des systèmes d'exploitation Windows.

Désinstallation à l'aide de l'assistant

Pour désinstaller Network Manager à l'aide d'un assistant d'interface graphique sur des systèmes d'exploitation Windows, vous devez exécuter le script de désinstallation avec l'option swing. Vous pouvez désinstaller des composants spécifiques ou le produit dans son intégralité en mode de ligne de commande.

Si vous souhaitez supprimer des produits intégrés à Network Manager sur le même serveur, supprimez-les en utilisant leurs programmes d'installation avant de supprimer Network Manager. Par exemple, si vous utilisez une base de données DB2 pour l'enregistrement de la topologie, vous devez la supprimer à l'aide du programme d'installation DB2.

Avertissement : Ne tentez pas de désinstaller un composant ou un produit en supprimant des fichiers ou des répertoires. Des problèmes peuvent survenir lors de la réinstallation de certains composants. Vous devez utiliser le script de désinstallation fourni avec le produit pour désinstaller Network Manager.

Pour désinstaller Network Manager en partie ou dans son intégralité à l'aide de l'assistant, procédez comme suit :

1. Retrouvez la source de l'environnement en exécutant la commande `%NCHOME%\env.bat`.
2. Exécutez la commande `%NCHOME%\`**`Uninstall_ITNM.exe`** avec l'option `-i swing`. L'assistant d'installation démarre et affiche les composants à désinstaller. Tous les composants qui ont été installés par le programme d'installation Network Manager sont sélectionnés pour être supprimés.
3. Sélectionnez les composants à supprimer.

Avertissement : La suppression de composants peut provoquer l'échec d'autres produits dépendant de ces composants. Par exemple, la suppression de Tivoli Netcool/OMNIbus provoque l'échec d'IBM Tivoli Business Service Manager. La suppression des composants centraux ou de la base de données topologiques provoque des erreurs dans les composants Web de Network Manager.

ATTENTION :
Si vous supprimez les composants Web de Network Manager de Tivoli Integrated Portal, les composants de l'interface graphique Web Tivoli Netcool/OMNIbus sont également supprimés.

ATTENTION :
Si vous sélectionnez l'option permettant de supprimer tous les composants, la structure d'installation et Tivoli Integrated Portal, d'autres produits installés sur le même serveur, tels Tivoli Netcool/OMNIbus, l'interface graphique Web Tivoli Netcool/OMNIbus et IBM Tivoli Business Service Manager peuvent ne pas fonctionner. Ne choisissez pas cette option si d'autres produits Tivoli sont installés sur ce serveur.

4. Cliquez sur **Suivant** pour désinstaller les composants. Si vous êtes invité à redémarrer le serveur, vous devez effectuer cette action avant de réinstaller un composant de Network Manager.
5. DB2 Facultatif : Si vous utilisez une base de données DB2 pour NCIM, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Utilisez la commande suivante :

   Windows

   ```
   %NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat nom_base_de_données
   ```

   où *nom_base_de_données* est le nom de la base de données NCIM.
6. DB2 Facultatif : Si vous utilisez une base de données DB2, telle que la base de données Tivoli Data Warehouse, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Pour des instructions, voir le manuel *IBM Tivoli Monitoring for Tivoli Network Manager IP - Guide d'utilisation*.

Désinstallation en mode console

Pour désinstaller Network Manager en mode console sur des systèmes d'exploitation Windows, vous devez exécuter le script de désinstallation avec l'option de console. Vous pouvez désinstaller des composants spécifiques ou le produit dans son intégralité en mode de ligne de commande.

Si vous souhaitez supprimer des produits intégrés à Network Manager sur le même serveur, supprimez-les en utilisant leurs programmes d'installation avant de supprimer Network Manager. Par exemple, si vous utilisez une base de données DB2 pour l'enregistrement de la topologie, vous devez la supprimer à l'aide du programme d'installation DB2.

Avertissement : Ne tentez pas de désinstaller un produit en supprimant des fichiers ou des répertoires. Des problèmes peuvent survenir lors de la réinstallation de certains composants. Vous devez utiliser le script de désinstallation fourni avec le produit pour désinstaller Network Manager.

Pour désinstaller Network Manager en partie ou dans son intégralité en mode console, procédez comme suit :

1. Retrouvez la source de l'environnement en exécutant la commande `%NCHOME%/env.bat`.

2. Exécutez la commande `%NCHOME%\Uninstall_ITNM.exe` avec l'option `-i console`.
3. Sélectionnez les composants à supprimer et suivez les invites à l'écran.

   Avertissement : La suppression de composants peut provoquer l'échec d'autres produits dépendant de ces composants. Par exemple, la suppression de Tivoli Netcool/OMNIbus provoque l'échec d'IBM Tivoli Business Service Manager. La suppression des composants centraux ou de la base de données topologiques provoque des erreurs dans les composants Web de Network Manager.

   ATTENTION :
   Si vous supprimez les composants Web de Network Manager de Tivoli Integrated Portal, les composants de l'interface graphique Web Tivoli Netcool/OMNIbus sont également supprimés.

   ATTENTION :
   Si vous sélectionnez l'option permettant de supprimer tous les composants, la structure d'installation et Tivoli Integrated Portal, d'autres produits installés sur le même serveur, tels Tivoli Netcool/OMNIbus, l'interface graphique Web Tivoli Netcool/OMNIbus et IBM Tivoli Business Service Manager peuvent ne pas fonctionner. Ne choisissez pas cette option si d'autres produits Tivoli sont installés sur ce serveur.
4. DB2 Facultatif : Si vous utilisez une base de données DB2 pour NCIM, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Utilisez la commande suivante :

   Windows

   `%NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat` *nom_base_de_données*

   où *nom_base_de_données* est le nom de la base de données NCIM.
5. DB2 Facultatif : Si vous utilisez une base de données DB2, telle que la base de données Tivoli Data Warehouse, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Pour des instructions, voir le manuel *IBM Tivoli Monitoring for Tivoli Network Manager IP - Guide d'utilisation*.
6. Si vous êtes invité à redémarrer le serveur, vous devez redémarrer le serveur avant de réinstaller un composant de Network Manager

Désinstallation en mode silencieux

Pour désinstaller Network Manager en mode silencieux sur des systèmes d'exploitation Windows, vous devez configurer le fichier de réponses et exécuter le script de désinstallation avec l'option silent. Vous pouvez désinstaller des composants spécifiques ou le produit dans son intégralité en mode de ligne de commande.

Si vous souhaitez supprimer des produits intégrés à Network Manager sur le même serveur, supprimez-les en utilisant leurs programmes d'installation avant de supprimer Network Manager. Par exemple, si vous utilisez une base de données DB2 pour l'enregistrement de la topologie, vous devez la supprimer à l'aide du programme d'installation DB2.

Avertissement : Ne tentez pas de désinstaller un produit en supprimant des fichiers ou des répertoires. Des problèmes peuvent survenir lors de la réinstallation de certains composants. Vous devez utiliser le script de désinstallation fourni avec le produit pour désinstaller Network Manager.

Pour désinstaller Network Manager en partie ou dans son intégralité, procédez comme suit :

1. Accédez au répertoire d'installation.
2. Sauvegardez et modifiez le fichier `ITNM-uninstall-response.txt`.
3. Pour supprimer Network Manager, annulez la mise en commentaire de la ligne suivante et vérifiez que cette dernière a la valeur 1 :

   ```
   #DEL.NCP.BOOLEAN=1
   ```

   Important : La suppression de Network Manager provoque des erreurs dans les composants Web Network Manager.
4. Pour supprimer les applications Web de Network Manager et les composants Web de l'interface graphique Web Tivoli Netcool/OMNIbus (mais pas Tivoli Integrated Portal), supprimez la mise en commentaire de la ligne suivante et assurez-vous qu'elle a pour valeur 1 :

   ```
   #DEL.TIP.BOOLEAN=1
   ```
5. Pour supprimer Tivoli Netcool/OMNIbus, annulez la mise en commentaire de la ligne suivante et vérifiez que cette dernière a la valeur 1 :

   ```
   #DEL.NCO.BOOLEAN=1
   ```

   Avertissement : La suppression de Tivoli Netcool/OMNIbus provoque l'échec d'autres produits dépendant de Tivoli Netcool/OMNIbus, tels IBM Tivoli Business Service Manager.
6. Pour supprimer tous les composants des répertoires NCHOME et TIPHOME, y compris la structure d'installation, annulez la mise en commentaire de la ligne suivante et vérifiez que cette dernière a la valeur 1 :

   ```
   #DEL.ALL.BOOLEAN=1
   ```

   ATTENTION :
   Si vous sélectionnez l'option permettant de supprimer tous les composants, la structure d'installation et Tivoli Integrated Portal, d'autres produits installés sur le même serveur, tels Tivoli Netcool/OMNIbus, l'interface graphique Web Tivoli Netcool/OMNIbus et IBM Tivoli Business Service Manager peuvent ne pas fonctionner. Ne choisissez pas cette option si d'autres produits Tivoli sont installés sur ce serveur.
7. Sauvegardez le fichier `ITNM-uninstall-response.txt`.
8. Retrouvez la source de l'environnement en exécutant la commande `%NCHOME%\env.bat`.
9. Exécutez la commande `%NCHOME%\`**`Uninstall_ITNM.exe`** avec l'option `-i silent -f` *`chemin_accès_fichier_réponses`*. Par exemple :

   ```
   Uninstall_ITNM.exe -i silent -f C:\temp\ITNM-uninstall-response.txt
   ```

   Important : Si le fichier de réponses n'est pas spécifié ou trouvé, le programme de désinstallation supprime les composants installés lors de la dernière exécution du programme d'installation.
10. Si vous êtes invité à redémarrer le serveur, vous devez effectuer cette action avant de réinstaller un composant de Network Manager.
11. DB2 Facultatif : Si vous utilisez une base de données DB2 pour NCIM, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Utilisez la commande suivante :

    Windows

    ```
    %NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat nom_base_de_données
    ```

    où *nom_base_de_données* est le nom de la base de données NCIM.

12. DB2 Facultatif : Si vous utilisez une base de données DB2, telle que la base de données Tivoli Data Warehouse, vous devez décataloguer la base de données lors de la désinstallation, puis la cataloguer à nouveau si vous réinstallez. Pour des instructions, voir le manuel *IBM Tivoli Monitoring for Tivoli Network Manager IP - Guide d'utilisation*.

Installation de groupes de correctifs

Pour obtenir les derniers correctifs, appliquez les groupes de correctifs. Des groupes de correctifs sont disponibles pour le produit Network Manager, ainsi que pour d'autres produits et composants tels que Tivoli Integrated Portal et l'interface graphique Web Tivoli Netcool/OMNIbus. Vous pouvez télécharger les groupes de correctifs depuis IBM Fix Central. Assurez-vous que le niveau du groupe de correctifs reste à jour.

Un groupe de correctifs est constitué de l'image d'installation, du fichier d'installation et des fichier readme. Le nom des images d'installation fait référence au produit, au système d'exploitation et niveau du groupe de correctifs, par exemple `3.9.0-TIV-ITNMIP-zLinux-FP0003`. Groupes de correctifs cumulatifs. Par exemple, le groupe de correctifs 3 inclut tous les correctifs des groupes de correctifs antérieurs.

Pour plus d'informations sur les versions de Tivoli Integrated Portal compatibles avec Network Manager, voir la matrice de certification Tivoli Integrated Portal sur IBM DeveloperWorks. Par exemple, certaines versions de Tivoli Integrated Portal V2.2.0.x sont compatibles uniquement avec les versions de groupe de correctifs Network Manager.

Important : Le reconditionnement de l'image du produit Network Manager complet (niveau de compilation 3.9.0.71, date d'édition 14 septembre 2012) comprend tous les correctifs du groupe de correctifs 2, ainsi que les modifications apportées à l'image de base. Vous pouvez appliquer les groupes de correctifs publiés après le groupe de correctifs 2 à l'image de la disponibilité générale (GA) de base et au reconditionnement de l'image du produit complet.

Remarque : Fix Pack 5 Si vous installez Network Manager version 3.9 groupe de correctifs 5, et que vous souhaitez utiliser Oracle 12c comme base de données topologiques, vous devez effectuer l'installation dans l'ordre suivant :

1. Installez Network Manager version 3.9 groupe de correctifs 5, comme décrit dans cette rubrique.
2. Créez et remplissez votre base de données Oracle 12.
3. Reconfigurez les composants de base et l'interface graphique de Network Manager afin qu'ils se connectent à la nouvelle base de données Oracle 12c, comme indiqué dans Modification des détails d'accès NCIM.

1. Pour identifier la version en cours des processus Network Manager, exécutez-les avec l'option `-version`.
2. Téléchargez le groupe de correctifs depuis le site Fix Central à l'adresse http://www-933.ibm.com/support/fixcentral/. Puis, décompressez l'image d'installation du groupe de correctifs.
3. Lisez les informations des fichiers associés au groupe de correctifs. Dans un groupe de correctifs Network Manager, les fichiers suivants contiennent des informations. Les fichiers seront différents pour d'autres produits ou d'autres composants.
   - `README.1ST` : fournit l'emplacement des fichiers `INSTALL` et `README`.

- `INSTALL` : Donne des informations importantes sur l'installation du groupe de correctifs, y compris les étapes préinstallation, les étapes d'installation et les étapes postinstallation, ainsi que sur les restrictions et les conditions requises.
- `README` : Décrit les correctifs et les améliorations inclus dans le groupe de correctifs.

4. Arrêtez tous les processus Network Manager en cours d'exécution. Pour plus d'informations sur l'arrêt du produit, voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
5. Installez le groupe de correctifs comme décrit dans le fichier `INSTALL` .
6. Fix Pack 4 Une fois le groupe de correctifs installé, effectuez les tâches suivantes si elles sont applicables pour votre déploiement :
   - Vérifiez le fichier `$NCHOME/log/install/manuallyUpdate.log`, qui liste les fichiers de configuration qui doivent être modifiés manuellement. Lors de l'installation du groupe de correctifs, le programme d'installation recherche dans ces fichiers les éventuelles modifications par rapport aux valeurs par défaut. Si des modifications sont détectées, ces fichiers ne sont pas remplacés. Remplacez-y toutes les occurrences de `list type text` par `list type undef`. Par exemple, l'instruction suivante doit être modifiée :

     ```
     connects&1 = "eval(list type text, '&RelatedTo')",
     ```

     Cet exemple d'instruction doit être remplacé par ce qui suit :

     ```
     connects&1 = "eval(list type undef, '&RelatedTo')",
     ```
   - Copiez le script `CleanSystem` depuis le répertoire `$NCHOME/precision/install/scripts` vers le répertoire `$NCHOME/precision/bin`. Ces scripts sont mis à jour dans ce groupe de correctifs.
   - Pour les environnements distribués 64 bits protégés par SSL : sur l'hôte Network Manager, changez le niveau JRE de l'utilitaire **`nc_common`**. Editez `$NCHOME/bin/nc_common` et remplacez toutes les entrées `NCO_JRE` par `NCO_JRE_64_32`. Cette modification n'est pas obligatoire dans les environnements à un seul serveur.
   - Si votre installation de Tivoli Netcool/OMNIbus correspond à V7.4, groupe de correctifs 2 ou une version ultérieure, supprimez la mise en commentaire de la ligne suivante dans le fichier `$NCHOME/probes/`*`arch`*`/nco_p_ncpmonitor.props` où *arch* représente le système d'exploitation. Ensuite, redémarrez le processus **`nco_p_ncpmonitor`**.
     - UNIX `NHttpd.ConfigFile: "$NCHOME/omnibus/etc/libnhttpd.json"`
     - Windows `NHttpd.ConfigFile: "%NCHOME%\\omnibus\\etc\\libnhttpd.json"`
   - Exécutez la commande **`ncp_mib`** avec l'option `-override`. Cette commande charge les modifications dans les fichiers MIB.
7. Dans le fichier `README`, recherchez les éventuels problèmes connus affectant le groupe de correctifs et apportez les modifications requises par les correctifs APAR.

Information associée:

Matrice de certification Tivoli Integrated Portal sur IBM DevelopWorks

Chapitre 3. Mise à niveau et migration

Prenez connaissance des informations sur la mise à niveau de la version de Network Manager et la migration des installations existantes.

Remarque : Les ports par défaut pour la consignation sur le serveur d'application sont différents d'une version à l'autre. L'accès non sécurisé vous redirige vers le port sécurisé à moins que vous ne l'ayez configuré autrement (voir «Configuration de l'accès HTTP et HTTPS», à la page 230). Les ports par défaut pour Network Manager V3.9 sont les suivants :

- `https://`*`système_hôte_local`*`:16311/ibm/console` (accès sécurisé).
- `http://`*`système_hôte_local`*`:16310/ibm/console` (accès non sécurisé).

Restriction : Seules les configurations suivantes sont prises en charge lors de la migration vers Network Manager version 3.9 à partir de la version 3.7 ou 3.8 ou lors de la copie d'une installation existante de la version 3.9 :

- Vous pouvez migrer d'un système UNIX vers tout autre système UNIX, mais la migration de systèmes UNIX vers des systèmes Windows (ou inversement) n'est pas prise en charge.
- Les machines source et cible doivent utiliser le même type de base de données. Ce n'est pas le cas uniquement si vous effectuez une migration de la source MySQL par défaut précédente vers la base Informix par défaut de la version 3.9 sur le système cible.
- Les systèmes source et cible doivent tous deux correspondre à des installations FIPS ou non FIPS. La migration d'une installation FIPS vers une installation non FIPS ou inversement, n'est pas prise en charge.

Avertissement : Si vous disposez de plusieurs produits Tivoli utilisant l'infrastructure Tivoli Integrated Portal, reportez-vous au document *Cross Product Migration Reference* à l'adresse https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Business%20Service%20Manager1/page/Migration pour consulter les dépendances et les considérations à prendre en compte lors de la mise à niveau et de la migration.

Mise à niveau et migration vers la dernière version de Network Manager

Vous pouvez effectuer une mise à niveau vers Network Manager V3.9 à partir des versions 3.7 ou 3.8.

La mise à niveau vers la dernière version de Network Manager implique la collecte de données à partir de l'installation existante de Network Manager, l'exportation des données, l'installation de la nouvelle version de Network Manager et l'importation des données dans votre nouvelle installation.

Remarque : Vous devez exécuter les scripts d'exportation-importation à l'aide du même utilisateur que celui qui a installé le produit.

Les différentes versions de Network Manager et les composants liés utilisent différentes structures de répertoire et ont des fichiers de configuration à différents emplacements. Cela est principalement dû aux modifications de la structure dans

les différentes versions. Par exemple, Network Manager V3.8 utilise Tivoli Integrated Portal 1.1.x, Network Manager V3.9 utilise Tivoli Integrated Portal V2.1, et Network Manager V3.7 utilise Netcool GUI Foundation. Pour savoir où trouver les fichiers, voir tableau 13.

Le tableau suivant présente de manière générale comment l'emplacement par défaut des fichiers de configuration a changé au fil des versions.

Tableau 13. Emplacements par défaut des fichiers de configuration

Elément	Emplacement dans la version 3.7	Emplacement dans la version 3.8	Emplacement dans la version 3.9
NCHOME	• UNIX `/opt/IBM/tivoli` • Windows `C:\IBM\tivoli`	• UNIX `/opt/IBM/tivoli/netcool` • Windows `C:\IBM\tivoli\netcool`	• UNIX `/opt/IBM/tivoli/netcool` • Windows `C:\IBM\tivoli\netcool`
ITNMHOME	Non applicable	Non applicable	• UNIX `/opt/IBM/tivoli/netcool/precision` • Windows `C:\IBM\tivoli\netcool\precision` **Remarque :** Par défaut, PRECISION_HOME est défini au même emplacement que ITNMHOME, mais il est utilisé par d'autres éléments du produit.
TIPHOME	Non applicable	• UNIX `/opt/IBM/tivoli/tip` • Windows `C:\IBM\tivoli\tip`	• UNIX `/opt/IBM/tivoli/tipv2` • Windows `C:\IBM\tivoli\tipv2`
Fichiers des propriétés d'interface utilisateur	NCHOME/etc/precision	TIPHOME/profiles/TIPProfile/etc/tnm	ITNMHOME/profiles/TIPProfile/etc/tnm
Modèles de vue dynamique	NCHOME/etc/precision/dynamictemplates	TIPHOME/profiles/TIPProfile/etc/tnm/dynamictemplates	ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates
Cliquez à l'aide du bouton droit sur le menu et sur les fichiers de définition d'outil	NCHOME/etc/precision/menus	TIPHOME/profiles/TIPProfile/etc/tnm/menus	ITNMHOME/profiles/TIPProfile/etc/tnm/menus
	NCHOME/etc/precision/tools	TIPHOME/profiles/TIPProfile/etc/tnm/tools	ITNMHOME/profiles/TIPProfile/etc/tnm/tools

Tableau 13. Emplacements par défaut des fichiers de configuration (suite)

Elément	Emplacement dans la version 3.7	Emplacement dans la version 3.8	Emplacement dans la version 3.9
Fichiers d'icône d'interface graphique	NCHOME/etc/precision/resource	TIPHOME/profiles/TIPProfile/etc/tnm/resource	ITNMHOME/profiles/TIPProfile/etc/tnm/resource
Fichiers de configuration WebTools	NCHOME/etc/precision/tools	TIPHOME/profiles/TIPProfile/etc/tnm/tools	ITNMHOME/profiles/TIPProfile/etc/tnm/tools

Présentation de la mise à niveau et de la migration

Utilisez ces informations comme guide étape par étape pour la mise à niveau de Network Manager et la migration des paramètres existants vers la version mise à niveau.

Etapes de mise à niveau et de migration à partir de Network Manager V3.8

Le passage à la dernière version de Network Manager à partir de la version 3.8 se déroule en plusieurs étapes. Le processus utilise des scripts séparés pour transférer les paramètres du composant d'interface graphique et centraux au sein de la nouvelle installation.

Pour effectuer la mise à niveau vers Network Manager V3.9 à partir de la version 3.8 et migrer vos paramètres et personnalisations, suivez les étapes décrites dans le tableau ci-dessous.

Tableau 14. Tâches de mise à niveau et de migration à partir de Network Manager V3.8

Action	Etape
1. Préparez votre système existant.	«Préparation à la mise à niveau», à la page 148
2. Exportez les données de personnalisation centrales.	«Exportation de données de personnalisation», à la page 149
3. Exportez les données de configuration de l'interface graphique.	«Exportation de données d'interface graphique version 3.8», à la page 151

Tableau 14. Tâches de mise à niveau et de migration à partir de Network Manager V3.8 (suite)

Action	Etape
4. Installez Network Manager V3.9.	Chapitre 2, «Installation», à la page 57 **Important :** Si vous installez la version V3.9 sur le même serveur qu'une installation existante de la version V3.8, vous devez effectuer les tâches supplémentaires suivantes : • Utilisez un nouveau répertoire pour installer la version V3.9. • Ne modifiez pas le répertoire existant utilisé par la version V3.8, même si vous envisagez de la supprimer plus tard. • Installez la version V3.9 utilisant le même compte d'utilisateur que celui utilisé pour installer la version V3.8. • Choisissez des ports différents pour la version V3.9 afin d'éviter des conflits. • Sur les plateformes non Windows, utilisez des fenêtres de terminal séparées pour toutes les étapes de migration et d'installation, ainsi que pour toutes les commandes d'exécution du produit. • Vérifiez que vous utilisez les variables d'environnement correctes pour la version concernée. Notez que sous Windows, vous ne pouvez pas exécuter la version V3.8 après l'installation de la version V3.9
5. Installez IBM Tivoli Netcool/OMNIbus	Vous pouvez installer IBM Tivoli Netcool/OMNIbus comme faisant partie de votre installation Network Manager. Pour plus d'informations sur la mise à niveau et la migration d'IBM Tivoli Netcool/OMNIbus, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*. **Remarque :** Si vous avez installé une nouvelle instance de IBM Tivoli Netcool/OMNIbus faisant partie de l'installation de Network Manager, le nom du serveur ObjectServer que vous avez fourni au cours de l'installation est stocké dans le fichier `NCHOME/etc/precision/ConfigItnm.`*`nom_domaine_Network_Manager`*`.cfg`
6. Importez les données de configuration centrales dans la nouvelle installation.	«Importation de données de personnalisation», à la page 152 **Remarque :** Tous les fichiers de configuration exportés à partir de votre installation 3.8 antérieure et importés dans Network Manager V3.9 contenant des mots de passe ou toute autre chaîne chiffrés à l'origine avec des outils de chiffrement de la version 3.8 seront rechiffrés à l'aide d'outils de chiffrement conformes à FIPS 140–2 au cours de cette mise à niveau. Les fichiers de la version 3.9 qui sont remplacés par les fichiers version 3.8 migrés au cours du processus de mise à jour sont sauvegardés sous le nom *`nomfichier`*`_39`, où *nomfichier* correspond au nom du fichier de la version 3.9 originale.
7. En raison des modifications du produit, certains paramètres de configuration centraux doivent être migrés manuellement vers le nouveau système.	«Importation de données de personnalisation - étapes manuelles», à la page 155

Tableau 14. Tâches de mise à niveau et de migration à partir de Network Manager V3.8 (suite)

Action	Etape
8. Importez les données de configuration d'interface graphique précédentes dans la nouvelle installation	«Importation de données d'interface graphique V3.8», à la page 162
9. En raison des modifications du produit, certains paramètres de configuration d'interface graphique doivent être migrés manuellement vers le nouveau système.	«Importation de données d'interface graphique V3.8 - étapes manuelles», à la page 163
10. Identifiez les modifications apportées au schéma de base de données de la topologie NCIM	«Identification des personnalisations de la base de données de topologiques NCIM», à la page 165
11. Arrêtez et démarrez Network Manager, y compris Tivoli Integrated Portal.	Démarrage et arrêt de Network Manager

Etapes de mise à niveau et de migration à partir de Network Manager V3.7

Le passage à la dernière version de Network Manager à partir de la version 3.7 se déroule en plusieurs étapes. Le processus utilise un script d'exportation pour collecter toutes les données et un script d'importation pour ajouter les données collectées à la nouvelle installation. Vous devez exécuter les scripts sur toutes les machines si vous disposez d'un environnement distribué avec des composants Network Manager installés sur plusieurs serveurs.

Pour effectuer la mise à niveau vers Network Manager V3.9 à partir de la version 3.7 et migrer les paramètres et la personnalisation, suivez les étapes décrites dans le tableau ci-dessous.

Tableau 15. Tâches de mise à niveau et de migration à partir de Network Manager V3.7

Action	Etape
1. Préparez votre système existant.	«Préparation à la mise à niveau», à la page 148
2. Exportez les données centrales et de personnalisation de l'interface graphique.	«Exportation de données de personnalisation», à la page 149
3. Installez Network Manager V3.9.	Chapitre 2, «Installation», à la page 57
4. Installez IBM Tivoli Netcool/OMNIbus	Vous pouvez installer IBM Tivoli Netcool/OMNIbus comme faisant partie de votre installation Network Manager. Pour plus d'informations sur la mise à niveau et la migration d'IBM Tivoli Netcool/OMNIbus, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*. **Remarque :** Si vous avez installé une nouvelle instance de IBM Tivoli Netcool/OMNIbus faisant partie de l'installation de Network Manager, le nom du serveur ObjectServer que vous avez fourni au cours de l'installation est stocké dans le fichier `NCHOME/etc/precision/ConfigItnm.`*`nom_domaine_Network_Manager`*`.cfg`

Tableau 15. Tâches de mise à niveau et de migration à partir de Network Manager V3.7 (suite)

Action	Etape
5. Importez les données antérieures de configuration centrales et de l'interface graphique dans la nouvelle installation.	«Importation de données de personnalisation», à la page 152 **Remarque :** Tous fichiers de configuration exportés à partir de votre installation 3.7 antérieure et importés dans Network Manager V3.9 contenant des mots de passe ou toute autre chaîne chiffrés à l'origine avec des outils de chiffrement de la version 3.7 seront rechiffrés à l'aide d'outils de chiffrement conformes à FIPS 140–2 au cours de cette mise à niveau. Les fichiers de la version 3.9 qui sont remplacés par les fichiers version 3.7 migrés au cours du processus de mise à jour sont sauvegardés sous le nom *nomfichier*_39, où *nomfichier* correspond au nom du fichier de la version 3.9 originale.
6. En raison des modifications du produit, certains paramètres de configuration doivent être migrés manuellement vers le nouveau système.	«Importation de données de personnalisation - étapes manuelles», à la page 155
7. Identifiez les modifications apportées au schéma de base de données de la topologie NCIM	«Identification des personnalisations de la base de données de topologiques NCIM», à la page 165
8. Arrêtez et démarrez Network Manager, y compris Tivoli Integrated Portal.	Démarrage et arrêt de Network Manager

Préparation à la mise à niveau

Préparez votre système existant pour la mise à niveau en effectuant la copie sur les fichiers requis pour le processus de mise à niveau et de migration. Le package d'installation de Network Manager contient tous les fichiers requis.

Si vous souhaitez effectuer une mise à niveau vers Network Manager version 3.9 groupe de correctifs 5, vous devez tout d'abord mettre à jour les scripts d'importation et d'exportation suivants : `$NCHOME/precision/install/scripts/nmExport`, `$NCHOME/precision/install/scripts/nmImport` et `$NCHOME/scripts/upgrade/ITNMExportNetworkViews.pl`. Après avoir installé Network Manager groupe de correctifs 5, copiez les scripts `nmExport` et `nmImport` dans le répertoire `scripts` à l'emplacement dans lequel vous avez décompressé le fichier d'installation de la version principale de Network Manager. Sinon, si vous utilisez `ExportPackage.tar`, copiez les scripts dans le répertoire `scripts` de l'emplacement dans lequel vous avez décompressé le fichier `.tar`. Vous ne pouvez pas exécuter ces scripts à partir d'une installation existante ou d'une installation de groupe de correctifs. Copiez également le script `ITNMExportNetworkViews.pl` dans le répertoire `migration/bin/` au même emplacement.

Préparation pour la mise à niveau :

1. Accédez à l'emplacement où vous avez placé votre package d'installation Network Manager V3.9.
2. Recherchez le fichier UNIX `ExportPackage.tar` ou Windows `ExportPackage.zip` en fonction de votre système d'exploitation.
3. Copiez le fichier compressé dans votre installation Network Manager existante. Si les composants centraux et les composants d'interface graphique se trouvent sur plusieurs serveurs, vous devez copier le fichier dans chacun d'entre eux.
4. Extrayez les fichiers à un emplacement temporaire. Les fichiers et les utilitaires requis pour le processus de mise à niveau et de migration sont disponibles

après l'extraction du fichier compressé. Les principaux éléments pour lesquels une attention est requise sont présentés ci-dessous.

- Utilitaire de `tableau de bord` : cet utilitaire permet de démarrer l'interface graphique de tableau de bord à partir de laquelle vous pouvez exécuter une collecte de données sur votre installation précédente. Les données collectées peuvent ensuite être exportées pour l'application aux nouvelles installations. Un utilitaire d'importation est disponible pour être utilisé dans votre nouvelle installation. Vous pouvez utiliser une interface graphique ou une ligne de commande pour démarrer et utiliser cet utilitaire.

  Remarque : Vous pouvez employer l'utilitaire d'exportation pour collecter des données sur Network Manager versions 3.7, 3.8 ou même dans les installations de la version 3.9. Si vous avez une installation Network Manager version 3.7, l'utilitaire exporte également les données Netcool GUI Foundation.
- Fichier `Preupgrade.tar` ou `Preupgrade.zip` : contient des utilitaires pour l'exportation de paramètres d'interface graphique précédents sur Network Manager version 3.8 puis leur importation dans votre nouvelle installation.

  Remarque : Ce fichier est requis uniquement pour l'exportation/importation des données de composant d'interface graphique version 3.8.

5. Les noms de règles d'interrogation et les noms de définitions d'interrogation doivent être uniques. Dans les versions antérieures de Network Manager, une limitation connue permettait la création de noms de règles d'interrogation et de noms de définitions d'interrogation en doublons. Dans Network Manager V3.9, les noms de règles d'interrogation et les noms de définitions d'interrogation en doublons ne sont pas autorisés. Si vous avez créé des règles d'interrogation et des définitions d'interrogation avec le même nom dans votre installation version 3.7 ou 3.8 précédente, vous devez renommer une des règles de la paire en doublon de façon à ce que chaque règle d'interrogation et chaque définition d'interrogation soit unique dans votre système. Vous devez faire cela avant d'effectuer l'exportation de données.

   Remarque : L'interrogateur doit être en cours d'exécution lorsque vous effectuez l'opération de renommage. Ceci est requis pour que les noms soient propagés de façon appropriée vers les zones de la base de données requérant ces informations (par exemple l'historique des données d'interrogation lors de la migration depuis un système version 3.8).

Exportation de données de personnalisation

Vous devez collecter et exporter les données de personnalisation de versions précédentes afin de les rendre disponibles pour importation vers votre installation Network Manager V3.9.

Pour utiliser le tableau de bord, un navigateur pris en charge doit être installé sur le serveur. Assurez-vous d'avoir copié le fichier UNIX `ExportPackage.tar` ou Windows `ExportPackage.zip` à partir du package d'installation Network Manager V3.9 vers chaque serveur sur lequel votre installation Network Manager a des composants.

Pour exporter des données de personnalisation, procédez comme suit :

1. Sur chaque serveur où des composants de votre version précédente sont installés, accédez à l'emplacement où vous avez extrait `ExportPackage` et exécuté le script d'exportation de données :

- Pour exécuter le script à partir du tableau de bord du programme d'installation, lancez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Préinstallation et migration**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Exporter les données Network Manager**.
- Pour exécuter le script à partir de la ligne de commande, exécutez le script UNIX **nmExport** sous UNIX ou le script Windows **nmExport.bat** sous Windows à partir du sous-répertoire `scripts`.

Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

Restriction : Les données de l'historique d'interrogation ne sont pas collectées lors de l'exportation des données à partir de systèmes version 3.7. L'exportation des données de l'historique d'interrogation à partir de systèmes version 3.8 est facultative. L'exportation et l'importation des données de l'historique d'interrogation à partir de systèmes version 3.8 peuvent être longues, selon la quantité de données à migrer.

2. Fournissez des réponses aux invites. Selon la version de votre installation Network Manager précédente, les données suivantes sont extraites et sauvegardées dans un fichier d'exportation à un emplacement de votre choix (`.pkg` sous des systèmes UNIX ou `.zip` sous des systèmes Windows) :
   - Pour la version 3.7 : données de domaine, fichiers de configuration, fichiers de cache, fichiers MIB supplémentaires, configurations spécifiques à l'interface graphique incluant les vues réseau et les pages Netcool GUI Foundation, les règles d'interrogation, les rapports et les mots de passe.
   - Pour la version 3.8 : données de domaine, données de configuration de reconnaissance, vues réseau et règles d'interrogation.

     Remarque : Pour les installations V3.7, toutes les données de composant central et d'interface graphique sont collectées. Pour les installations V3.8, seules les données de composant central sont collectées. Pour collecter les données du composant d'interface graphique 3.8, vous devez exécuter un autre script, comme cela est décrit dans «Exportation de données d'interface graphique version 3.8», à la page 151. Il n'est pas nécessaire d'exécuter ce script pour la version 3.7.

   Remarque : Ce processus d'exportation crée ses propres fichiers journaux. Si cette opération aboutit, tous les fichiers journaux liés sont regroupés dans le fichier `.pkg` ou `.zip` du package d'exportation, les rendant disponibles sur le système mis à jour. Si le processus échoue, le package n'est pas créé et les journaux sont enregistrés dans le répertoire principal de l'utilisateur :
   - UNIX `$HOME/itnmExportLogs`
   - Windows `%UserProfile%\itnmExportLogs`
3. Si vous installez Network Manager V3.9 sur un autre serveur, copiez toutes les données exportées sur ce serveur ou des serveurs, rendant les données disponibles pour l'importation vers de nouveaux systèmes.
4. Si vous exportez également les données de personnalisation Netcool/OMNIbus, copiez toutes les données exportées vers le serveur dans lequel vous souhaitez installer Netcool/OMNIbus.

Après l'exportation de données de personnalisation, vous devez installer Network Manager V3.9 puis importer les données de personnalisation.

Référence associée:

«Navigateurs pris en charge pour le tableau de bord du programme d'installation», à la page 48

Pour exécuter le tableau de bord du programme d'installation, assurez-vous qu'un navigateur pris en charge est installé. Les navigateurs pris en charge ne sont pas nécessairement les mêmes que pour les applications Web.

Exportation de données d'interface graphique version 3.8

Vous devez exporter vos données de personnalisation d'interface graphique version 3.8 précédentes avant d'installer Network Manager V3.9.

Pour utiliser le tableau de bord, un navigateur pris en charge doit être installé sur le serveur. Assurez-vous d'avoir copié le fichier UNIX `ExportPackage.tar` ou Windows `ExportPackage.zip` à partir du package d'installation Network Manager V3.9 vers le serveur sur lequel sont installés vos composants d'interface graphique version 3.8.

Restriction : Le processus de mise à niveau n'exporte pas les données de périphérique entièrement non géré. Une fois la reconnaissance de réseau terminée sur le système cible, vous devez à nouveau définir manuellement les périphériques appropriés sur l'état non géré.

Pour exporter des données de personnalisation d'interface graphique, procédez comme suit :

1. Sur chaque serveur où sont installés les composants d'interface graphique de votre système version 3.8 précédent, accédez à l'emplacement où vous avez extrait `ExportPackage`.
2. Extrayez le fichier UNIX `Preupgrade.tar` ou Windows `Preupgrade.zip` dans `TIPHOME/profiles/TIPProfile`.
3. Exécutez le script d'exportation de données d'interface graphique :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, lancez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Préinstallation et migration**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Exporter des données d'interface graphique Network Manager**.
   - Pour exécuter le script à partir de la ligne de commande, accédez au sous-répertoire `scripts` et, selon votre système d'exploitation, exécutez la commande UNIX **nmGuiExport** ou Windows **nmGuiExport.bat** comme suit :

     ```
     nmGuiExport | bat -u nom utilisateur administrateur TIP -p
     mot de passe pour administrateur
     TIP -d emplacement de l'installation TIP à migrer
     ```

     Remarque : Si les valeurs ne sont pas fournies, vous êtes invité à les entrer. Si l'emplacement de l'installation Tivoli Integrated Portal à migrer n'est pas fourni, la variable d'environnement `TIPHOME` est utilisée. Si `TIPHOME` n'existe pas, vous êtes invité à entrer un emplacement.

Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

Les données suivantes sont extraites et sauvegardées dans le fichier d'exportation `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip` :

- Rôles utilisateur : l'exportation enregistre les rôles qui existaient dans la version 3.8 et applique les rôles au même utilisateur si ce dernier existe dans la version 3.9.

  Remarque : Les utilisateurs actuels définis pour l'environnement version 3.9 doivent être créés séparément dans le référentiel approprié (LDAP ou ObjectServer).
- Pages, vues et rôles Tivoli Integrated Portal personnalisés.
- Rapports.

Le processus d'exportation crée ses propres fichiers journaux dans les répertoire suivants :

- `TIPHOME/profiles/TIPProfile/upgrade/logs`
- `TIPHOME/profiles/TIPProfile/logs`

4. Créez des utilisateurs pour la version 3.9, comme cela est requis dans le référentiel approprié (LDAP ou ObjectServer).
5. Si vous installez des composants d'interface graphique Network Manager V3.9 sur un autre serveur, copiez le fichier d'exportation `upgradeData.zip` sur ce serveur, ce qui rend les données disponibles pour l'importation dans le nouveau système. Si vous effectuez l'installation sur des serveurs séparés, assurez-vous de copier les données appropriées sur le serveur où vous souhaitez installer le composant.

Après l'exportation de données de personnalisation, vous devez installer Network Manager V3.9 puis importer les données de personnalisation.

Importation de données de personnalisation

Après l'installation de Network Manager V3.9, vous pouvez importer vos données de personnalisation provenant d'une version précédente.

Avant de pouvoir importer des données de personnalisation, vous devez exporter les données à partir de votre installation précédente et installer la version 3.9.

Important : Vous devez exécuter ncp_mib si vous avez copié des bases MIB personnalisées dans le cadre de cette migration de données. Si vous l'omettez, des processus (tels que l'auxiliaire SNMP, ncp_dh_snmp) ne seront pas lancés au démarrage de Network Manager.

Pour importer les données de personnalisation, procédez comme suit :

1. Connectez-vous à votre installation précédente. Si vous avez une configuration distribuée, vous devez vous connecter à chaque serveur contenant des composants de votre installation précédente et répéter la procédure suivante pour chaque serveur.
2. Copiez le fichier d'exportation (`.pkg` sur les systèmes UNIX ou `.zip` sur les systèmes Windows) sur le serveur où vous avez installé Network Manager V3.9. Vous pouvez avoir plusieurs fichiers d'exportation si vous aviez un environnement distribué.
3. Sur votre nouvelle installation, assurez-vous que les composants centraux de Network Manager pour chaque domaine sont en cours d'exécution. Pour cela, utilisez l'interface graphique des services Windows sur les systèmes Windows ou bien la commande suivante sur les systèmes UNIX : **itnm_start** `ncp -domain` *DOMAINE*. Par exemple, pour démarrer le domaine `NCOMS`, entrez :

`itnm_start ncp -domain NCOMS` . Ceci garantit que Network Manager est complètement initialisé et que les tables du domaine sont remplies. Vous devez à nouveau arrêter les composants centraux pour effectuer l'importation elle-même, comme décrit à l'étape suivante.

4. Arrêtez les composants centraux de Network Manager pour chaque domaine sur votre nouvelle installation à l'aide de l'interface graphique des services Windows sur les systèmes Windows ou bien à l'aide de la commande suivante sur les systèmes UNIX : **`itnm_stop`** `ncp -domain` *`DOMAINE`*. Par exemple, pour arrêter le domaine `NCOMS`, entrez : `itnm_stop ncp -domain NCOMS`

   Remarque : Si vous ne spécifiez pas un nom de domaine avec **`itnm_stop`**, il arrête le domaine par défaut créé lors de l'installation.

5. Sur votre nouvelle installation, accédez à l'emplacement du package d'installation.

   Remarque : Si vous migrez depuis la version 3.7, le serveur Tivoli Integrated Portal doit être en cours d'exécution pour importer les données des composants de l'interface graphique.

6. Exécutez le script d'importation de données via une des méthodes suivantes :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, démarrez le tableau de bord en exécutant le script UNIX **`launchpad.sh`** sous UNIX ou l'exécutable Windows **`launchpad.exe`** sous Windows, sélectionnez l'option **Postinstallation**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Importer les données Network Manager**.
   - Pour exécuter le script depuis la ligne de commande, lancez le script UNIX **`nmImport`** sous UNIX ou le script Windows **`nmImport.bat`** sous Windows à partir du sous-répertoire `scripts` du support d'installation.

   Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

7. Lorsque vous y êtes invité, indiquez le chemin du fichier `.pkg` ou `.zip` qui contient les données de personnalisation précédemment exportées.
8. Répondez aux différentes questions posées par le processus d'importation.

   Remarque : La question suivante requiert une attention particulière :

   ```
   Allocate new entityIds during import [ N ]
   ```

   Chaque périphérique du système a un élément `entityId`. Le processus d'importation peut conserver les éléments `entityId` ou en allouer de nouveaux. Si vous répondez `no`, chaque périphérique conserve l'élément `entityId` de l'installation précédente. Cela est nécessaire lorsque vous avez des liens vers des systèmes externes qui utilisent les données Network Manager, par exemple, Tivoli Data Warehouse.

   Si vous répondez `yes`, des éléments `entityId` sont alloués à des périphériques.

   Pour conserver les éléments `entityId`, le systèmes cible doit être vide. Si le système cible n'est pas vide (par exemple suite à une reconnaissance ou une importation de données précédente), la conservation des élémentsentityId peut être une opération complexe suite à des conflits potentiels entre les éléments `entityId` existants et ceux importés, et les résultats peuvent être imprévisibles. Par conséquent, la fusion de données de domaine n'est pas prise en charge.

Avertissement : Si un domaine sur le système cible a le même nom que sur votre système précédent, vérifiez le domaine sur le système cible ne contient pas de données. Les noms de domaine ne peuvent pas être modifiés pendant le processus de migration.
Les données exportées sont importées dans la nouvelle installation. Vos mots de passe sont déchiffrés, importés, puis de nouveau chiffrés.

Important : Les données importées dépendent de la version de votre installation Network Manager précédente. Pour les installations V3.7, l'importation de toutes les données précédentes est gérée par ce script. Pour les installations V3.8, les données du composant central sont importées alors que les données du composant d'interface graphique sont importées par le script décrit dans «Importation de données d'interface graphique V3.8», à la page 162.

Le processus d'importation crée ses propres fichiers journaux. Les journaux du processus d'importation sont enregistrés dans `NCHOME/log/precision` :

- `ITNMDataImport.log`
- `ITNMImportHistoricalData.log`
- `get_policies.`*`nom domaine`*`.log`
- `ITNMImportNetworkViews.log`

Le processus d'exportation/importation détecte et recrée automatiquement les domaines à partir d'une installation précédente. Le script d'importation détecte les domaines potentiels à partir du système précédent en fonction des fichiers de données. A l'aide du script **`domain_create.pl`**, le processus crée automatiquement les domaines sur la nouvelle installation en utilisant les noms de domaine du système précédent. Une fois que les domaines ont été créés, la topologie principale et les données de règle sont importées pour chacun d'entre eux.

Le script **`domain_create.pl`** crée les fichiers de configuration de la reconnaissance pour les nouveaux domaines dans `NCHOME/etc/precision` en utilisant les valeurs des fichiers de configuration du domaine par défaut. Le processus d'importation enregistre les fichiers importés dans le répertoire `NCHOME/etc/precision/migration` en tant que fichiers en lecture seule. Vous pouvez utiliser les fichiers importés pour mettre à jour manuellement les fichiers nouvellement créés dans `NCHOME/etc/precision`.

Avertissement : Des messages d'avertissement peuvent être générés référençant les types de données obsolètes. Ces messages d'avertissement indiquant les modifications planifiées dans les types de données entre les versions et peuvent être ignorés. Un exemple est disponible ci-dessus :

```
Level: INFO Message: ncp_config command:- "/opt/IBM/tivoli/netcool/
precision/bin/ncp_config" -domain CC -read_schemas_from
"/opt/IBM/tivoli/netcool/var/precision/export/importPending"
-write_schemas_to "/opt/IBM/tivoli/netcool/etc/precision" -schema
DiscoCollectorFinderSchema.cfg
Sun Oct 3 05:48:30 2010 Warning: A generic non-fatal error has occurred
found in file RivOQL.y at line 2552 - Deprecated type 'long' in OQL
statement will be evaluated as type 'time'
```

Après l'importation de vos données système précédentes, il peut être nécessaire de définir manuellement certains paramètres sur le nouveau système. Le processus d'exportation/importation indique pour quels fichiers une attention particulière est requise ainsi qu'une édition manuelle afin de mener à terme le processus de migration et de mise à niveau.

Tâches associées:

«Chargement des informations MIB mises à jour», à la page 274
Pour garantir que le navigateur de la base d'informations de gestion (MIB) contient les informations MIB les plus récentes, chargez les informations MIB mises à jour en exécutant l'application de ligne de commande **ncp_mib**.

Importation de données de personnalisation - étapes manuelles

En raison des modifications du produit et des personnalisations utilisateur potentielles, vous devez migrer manuellement des paramètres de configuration centraux vers le nouveau système. Consultez les tâches suivantes pour déterminer les ajustements manuels supplémentaires à apporter à votre nouveau système.

Assurez-vous que vous avez effectué une collecte et une exportation de données sur le système précédent et que vous avez importé les données vers la nouvelle installation.

Pour suivre les étapes de migration manuelle :

1. Connectez-vous à la nouvelle installation.
2. Consultez le fichier `NCHOME/log/precision/ITNMCompareSystemsFinal.txt` pour accéder aux informations sur les éventuelles modifications manuelles requises. Ce journal répertorie les changements entre le précédent système et le nouveau, y compris :
   - Les fichiers qui ont changé seulement en raison de modifications apportées au produit d'une version à la suivante. Ces fichiers sont indiqués par les expressions `Different` et `System`. Par exemple, `Different,,System,precision/aoc/CiscoNonRoutingSwitch.aoc`.

     Remarque : Ces fichiers ne nécessitent pas d'actions ; le journal les mentionne uniquement pour information.
   - Les fichiers qui ont changé seulement en raison de personnalisations effectuées par les utilisateurs sur l'installation précédente. Ces fichiers sont indiqués par les expressions `Different` et `User`. Par exemple, `Different,User,,etc/precision/DbLogins.NCOMS.cfg`.

     Remarque : Ces fichiers ne nécessitent pas d'actions ; le journal les mentionne uniquement pour information.
   - Les fichiers qui ont changé à la fois en raison de modifications apportées au produit entre les versions et de personnalisations effectuées par les utilisateurs sur l'installation précédente. Ces fichiers sont indiqués par les expressions `Different` et `User,System`. Par exemple, `Different,User,System,etc/precision/CtrlServices.cfg`. Ces fichiers nécessitent votre attention car les personnalisations des utilisateurs doivent être examinées et réappliquées manuellement.
   - Les fichiers qui n'existaient pas sur le système précédent, mais qui existent sur la nouvelle installation sont indiqués par l'expression `Inserted`. Par exemple, `Inserted ,,,etc/precision/DiscoDNSHelperSchema.NCOMS.cfg`.
   - Les fichiers qui existaient sur l'ancien système, mais qui ne sont plus requis et sont obsolètes sont indiqués par l'expression `Removed`. Par exemple, `Removed ,,,etc/precision/AmosSchema.cfg`
   - Les fichiers qui n'ont pas changé sont indiqués par l'expression `Same`. Par exemple, `Same ,,,etc/precision/ClassSchema.cfg`.

   Remarque : Il existe trois fichiers `CompareSystems` :

- ITNMCompareSystemsTgt.log
- ITNMCompareSystemsFinal.log
- ITNMCompareSystemsFinal.txt

Les deux premiers sont des fichiers de travail et vous pouvez les ignorer. Seul le troisième fichier, ITNMCompareSystemsFinal.txt, requiert votre attention.

Conseil : Pour un rapport détaillé du processus de migration d'exportation-importation, voir NCHOME/log/precision/ITNMDataImport.log. Ce fichier est destiné au débogage et au support.

3. Tous les fichiers provenant de l'installation précédente pouvant nécessiter des ajustements manuels sont archivés dans NCHOME/etc/precision/migration. En vous basant sur les informations du fichier ITNMCompareSystemsFinal.txt, examinez et ajustez si nécessaire les paramètres dans les fichiers archivés suivants :
   - Tout fichier *.aoc de classe d'unité.
   - Tout fichier *.agnt d'agent.
   - Tout fichier *.stch de programme stitcher.
   - Tout fichier *.mib MIB.
   - SnmpStackSecurityInfo.*DOMAINE*.cfg
   - TelnetStackPasswords.*DOMAINE*.cfg
   - ModelNcimDb.*DOMAINE*.cfg
   - CtrlServices.*DOMAINE*.cfg

     Remarque :
     - Si vous avez migré les fichiers CtrlServices.*DOMAINE*.cfg qui étaient utilisés pour configurer la reprise en ligne, un conflit peut survenir entre les options de ligne de commande -primaryDomain, -backupDomain, -virtualDomain, -backup et -server dans le fichier CtrlServices.*DOMAINE*.cfg et les paramètres dans le fichier ConfigItnm.*DOMAINE*.cfg. Les options de ligne de commande dans le fichier CtrlServices.*DOMAINE*.cfg sont prioritaires par défaut et un avertissement est consigné. Vous pouvez désactiver l'utilisation d'un fichier CtrlServices.*DOMAINE*.cfg migré en le renommant (en CtrlServices.OLD.cfg par exemple), ce qui a pour effet que le système utilise par défaut le fichier CtrlServices.cfg.
     - Si le fichier CtrlServices.*DOMAINE*.cfg migré contient d'autres paramètres personnalisés pour les processus définis (par exemple -latency et -debug), vous devez reconfigurer ces paramètres dans le fichier CtrlServices.cfg par défaut.
   - NcoGateInserts.*DOMAINE*.cfg
   - NcoGateSchema.*DOMAINE*.cfg
   - VirtualDomainSchema.*DOMAINE*.cfg
   - DbEntityDetails.cfg

     Remarque : Vous devez également recréer les nouvelles tables NCIM.
   - DiscoCollectorFinderSeeds.*DOMAINE*.cfg
   - DiscoFileFinderParseRules.*DOMAINE*.cfg
   - DiscoPingFinderSeeds.*DOMAINE*.cfg
   - DiscoScope.*DOMAINE*.cfg

Remarque : Le fichier DiscoSchema.*DOMAINE*.cfg a été scindé en deux fichiers dans Network Manager V3.9. Les instructions d'insertion dans ce fichier ont été montées dans le nouveau fichier DiscoConfig*DOMAINE*.cfg. Cela offre la possibilité de séparer les personnalisations utilisateur des définitions de schéma fixes.

Selon la configuration système précédente, vous pouvez être amené à effectuer des tâches manuelles comme l'ajustement de plusieurs paramètres de domaine, la copie des propriétés de l'adaptateur de bibliothèque de reconnaissance (DLA), l'application manuelle de paramètres d'interrogation et de rapport, ou la consultation des paramètres de gestion d'événements et la compréhension des modifications apportées au fonctionnement de l'enrichissement et de la corrélation des événements dans Network Manager V3.9.

Remarque : Après avoir terminé l'importation des données de configuration et la réconciliation des personnalisations manuellement, assurez-vous de démarrer vos domaines avant d'utiliser Network Manager. Le domaine par défaut spécifié à l'installation est démarré lors du démarrage de Network Manager ; cependant, si vous avez plusieurs domaines, démarrez chacun de ceux-ci à l'aide de la commande **itnm_start** ncp -domain *DOMAINE*.

Migration des propriétés de l'adaptateur de bibliothèque de reconnaissance (DLA)

Si vous utilisez l'adaptateur de bibliothèque de reconnaissance (DLA) pour collecter les données sur les ressources réseau et disposez de fichiers de propriétés DLA configurés sur le système précédent, les paramètres doivent être migrés manuellement.

Pour migrer les paramètres DLA :

1. Connectez-vous à la nouvelle installation.
2. Accédez au répertoire NCHOME/var/precision/export et recherchez les fichiers de propriétés DLA archivés par le processus d'exportation-importation sur le système précédent et écrasés à la suite d'une copie. Chaque domaine comporte un fichier ncp_dla.properties.*nom de domaine* archivé par le processus d'exportation-importation.
3. Utilisez les fichiers de propriétés DLA archivés pour chaque domaine afin de recréer les mêmes paramètres LDA sur la nouvelle installation :
   a. Accédez au répertoire NCHOME/precision/adapters/ncp_dla.
   b. A l'aide du fichier ncp_dla.properties préconfiguré, créez un fichier de propriétés DLA équivalent basé sur le fichier DLA de chaque domaine précédent, en nommant les fichiers d'après chaque domaine, ncp_dla.properties.NCOMS, par exemple.
   c. Ouvrez le fichier de propriétés DLA archivé pour chaque domaine et effectuez les mêmes paramétrages dans le nouveau fichier spécifique du domaine que dans le fichier ncp_dla.properties.*nom de domaine* archivé précédent, ce qui recrée le fichier DLA pour chaque domaine respectif sur le nouveau système.

      ATTENTION :
      Ne copiez-collez pas le contenu en l'état du fichier précédent dans le nouveau fichier, mais copiez les paramètres qui ont été modifiés sur le système précédent pour remplacer les précédents. Le nouveau fichier contient les nouveaux paramètres qui n'existaient pas dans les versions précédentes et pourraient ne pas fonctionner correctement si le contenu est écrasé.

4. Sauvegardez et fermez chaque fichier de propriétés DLA.

Tâches associées:

«Configuration de l'adaptateur de bibliothèque de reconnaissance», à la page 204
L'adaptateur de bibliothèque de reconnaissance (DLA) requiert un fichier de propriétés de configuration pour déterminer la source de données à laquelle se connecter, le domaine à analyser, le répertoire cible pour les livres de bibliothèque de reconnaissance et les paramètres de connexion.

Migration des personnalisations de la gestion des événements

L'enrichissement et la corrélation des événements ont beaucoup changé dans Network Manager V3.9. Si vous avez personnalisé la gestion des événements, vous devez connaître les modifications apportées à l'enrichissement et à la corrélation des événements et réimplémenter les personnalisations dans la nouvelle installation.

Pour comprendre les modifications et les réimplémenter :

1. Connectez-vous à la nouvelle installation.
2. Vérifiez les modifications que vous avez apportées aux fichiers `NcoGateSchema.DOMAINE.cfg` et `NcoGateInserts.DOMAINE.cfg` et, le cas échéant, apportez-en d'autres :
   a. Accédez au répertoire `NCHOME/etc/precision/migration`.
   b. Recherchez les fichiers `NcoGateSchema.DOMAINE.cfg` et `NcoGateInserts.DOMAINE.cfg` pour chaque domaine que vous avez personnalisé.
   c. Etudiez les tables d'événements pour déterminer comment réappliquer les personnalisations apportées aux tables config.precedence, config.eventMap, config.ncp2nco et config.nco2ncp. Pour plus d'informations, voir *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données de gestion*

   Remarque : Les règles d'analyse renseignent la zone NmosEventMap de la table alerts.status pour tous les événements Network Manager émis par l'interrogateur. Les entrées de la table config.precedence ne sont pas obligatoires à moins de remplacer la mappe d'événements ou de modifier la valeur de préséance par défaut.
3. Si vous avez personnalisé les tables config.ncp2nco ou config.nco2ncp, lisez les informations sur les programmes stitcher dans le répertoire `NCHOME/precision/eventGateway/stitchers` et étudiez comment ceux-ci fonctionnent dans l'édition en cours afin de réimplémenter les personnalisations d'enrichissement des événements. Pour plus d'informations sur les programmes stitcher, voir *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*

Migration des paramètres d'interrogation

Pour utiliser vos personnalisations d'interrogation précédentes dans la version 3.9, vous devez définir la portée de chaque règle d'interrogation manuellement après avoir terminé l'importation.

Les règles d'interrogation et les définitions d'interrogation personnalisées sont déplacées vers votre nouveau système par le processus d'exportation-importation. La portée est importée dans une vue de réseau qui doit être définie manuellement pour chaque règle. Ceci est dû aux modifications apportées à la façon dont la portée (les entités réseau que la règle doit interroger) est définie :

- Dans la version 3.7, la portée est définie par classe de périphérique et par filtre de périphérique définis dans la règle d'interrogation.

- Dans la version 3.8, la portée est définie par classe de périphérique, par filtre de périphérique et par filtre d'interface définis dans la règle d'interrogation.
- Dans la version 3.9, la portée est définie par la vue de réseau à laquelle elle s'applique et elle peut être affinée en définissant des filtres de classe et d'interface au niveau de la définition d'interrogation. Des filtres de périphérique peuvent aussi être définis pour les règles d'interrogation, mais ils sont limités à la table mainNodeDetails, et sont destinés à fournir un filtrage de périphérique pour la prise en charge du grapheur MIB et des règles d'interrogation créées via des vues de réseau pour des menus contextuels.

Dans la version 3.9, la méthode principale de définition d'une portée consiste à utiliser une vue de réseau. Vous pouvez affecter une ou plusieurs vues de réseau à une règle d'interrogation pour définir la portée en matière de périphériques à interroger. Pour comprendre les règles d'interrogation dans la version 3.9, créez de nouvelles règles et définissez leur portée à l'aide de vues de réseau.

Remarque : Une règle d'interrogation peut être associée à plusieurs définitions d'interrogation dans la version 3.9, alors que dans la version 3.8 vous ne pouvez avoir qu'une seule définition par règle. Ceci peut être pratique, par exemple lorsque vous voulez interroger des informations spécifiques au fournisseur du périphérique. Dans les scénarios de ce type, vous devez configurer une définition d'interrogation pour chaque fournisseur (chaque fournisseur pouvant avoir différentes MIB), mais n'avoir qu'une seule règle avec toutes les définitions d'interrogation ajoutées pour obtenir les données provenant de la totalité de votre réseau.

Le processus d'exportation-importation crée des vues de réseau basées sur les portées de vos règles d'interrogation antérieures et nomme ces vues de réseau d'après la règle d'interrogation. Vous devez éditer chaque règle d'interrogation et sélectionner la vue de réseau appropriée pour chacune après avoir importé les données dans votre nouveau système. Vous pouvez aussi sélectionner un filtre de périphérique dans la règle d'interrogation, ou bien créer une portée encore plus granulaire à l'aide des paramètres de classe de périphérique et de filtre d'interface des définitions d'interrogation.

Pour migrer les paramètres d'interrogation, procédez selon les étapes suivantes.

1. Connectez-vous à votre installation version 3.9.
2. Vérifiez que les vues de réseau existent pour votre système : cliquez sur **Disponibilité** > **Disponibilité du réseau** > **Vues de réseau**.
3. Cliquez sur **Administration** > **Réseau** > **Interrogation du réseau**.
4. Sélectionnez une règle qui était disponible sur votre système précédent en cliquant sur le nom de la règle d'interrogation. L'Editeur de règles d'interrogation est affiché pour la règle que vous avez sélectionnée et ses paramètres sont automatiquement chargés dans les zones.
5. Accédez à l'onglet **Vues de réseau** et sélectionnez la vue de réseau ayant le même nom que la règle. Ceci définit la portée de la règle aux périphériques de la vue de réseau qui est basée sur les paramètres de votre système précédent.

   Remarque : Les règles d'interrogation de votre système précédent qui avaient été configurées pour tous les périphériques n'auront pas de vue de réseau. Dans ce cas, assurez-vous que **Tous les périphériques** est sélectionné dans l'onglet **Vues de réseau**.
6. Facultatif : Vous pouvez affiner davantage la portée de la règle en créant un filtre plus limité dans l'onglet **Filtre de périphériques**. Les définitions

d'interrogation attachées à la règle peuvent aussi contenir un filtrage plus granulaire basé sur la classe de périphérique et sur des filtres d'interfaces.

Conseil : Si un filtre de classe ou d'interface avait été configuré dans votre système précédent pour une règle d'interrogation, dans la version 3.9, ces paramètres sont maintenant définis dans les définitions d'interrogation. Le processus d'exportation-importation prend en charge le déplacement des paramètres de classe de périphérique sur la nouvelle installation en créant le filtre de classe de périphérique de la version 3.8 au niveau de la définition d'interrogation de la version 3.9.

7. Cliquez sur **Sauvegarder**.
8. Répétez les étapes pour chaque règle d'interrogation de votre système précédent.

Migration des rapports version 3.7

Si vous avez modifié ou créé des rapports dans Network Manager 3.7, vous devez les migrer manuellement.

Avant d'effectuer cette tâche, vous devez d'abord importer les données de personnalisation 3.7, qui comprennent les rapports, à l'aide du script **nmExport**. Le script place les rapports dans un fichier compressé de votre choix.

Pour migrer des rapports 3.7 personnalisés, procédez selon les étapes suivantes :

1. Importez les rapports 3.7 dans le concepteur BIRT.
   a. Copiez le fichier compressé contenant les rapports 3.7 (que vous avez créé à l'aide du script **nmExport**) sur le serveur où le concepteur BIRT est installé. Vous pouvez télécharger BIRT Report Designer à l'adresse http://www.ibm.com/developerworks/spaces/tcr.
   b. Démarrez BIRT Report Designer en exécutant **eclipse.exe**. Vous êtes invité à spécifier un dossier d'espace de travail pour stocker vos projets.
   c. Créez un projet en cliquant sur **Fichier** > **Nouveau** > **Projet** > **Business Intelligence and Reporting Tools** > **Projet de rapport**.
   d. Nommez le projet. Par exemple, Rapports ANZ.
   e. Dans la fenêtre du navigateur, cliquez avec le bouton droit sur le projet que vous venez de créer et sélectionnez **Importer** > **Sélectionner le fichier archive**.
   f. Choisissez le fichier compressé qui contient les rapports et cliquez sur **Terminer**.
2. Editez les rapports que vous voulez migrer vers 3.9.
   a. Dans l'arborescence du **Navigateur**, renommez le dossier **ITNM** sous le projet que vous avez créé à l'étape 1 en `ressources`.
   b. Définissez la bibliothèque de rapports pour le rapport.
      1) Cliquez sur **Fenêtre** > **Préférences**.
      2) Dans l'arborescence du côté gauche, cliquez sur **Conception de rapport** > **Ressource**.
      3) Accédez au répertoire où se trouve le fichier `.rptlibrary`, par exemple C:/nom_utilisateur/espace_travail/Rapports ANZ/ressources/itnm/lib/, et cliquez sur OK.
   c. Dans l'onglet **Outline**, double-cliquez sur chacune des sources de données sous **itnm_data_source.rptlibrary** > **Sources de données** et modifiez les

sources de données pour les faire pointer vers l'ordinateur ou la base de données que vous voulez utiliser pour tester vos rapports dans le concepteur BIRT.

d. Résolvez les erreurs dans les rapports montrées par le concepteur BIRT.

3. Pour importer les rapports dans Tivoli Common Reporting, exécutez une commande similaire à celle-ci :

   ```
   NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
   nom_fichier_rapport -reportSetBase ensemble_rapports_destination
   -resourceDir ITNM39 -username nom_utilisateur_admin -password
   mot_de_passe_admin
   ```

   Où

   - *nom_fichier_rapport* est le nom de fichier du rapport à déplacer.
   - *ensemble_rapports_destination* est l'ensemble de rapports 3.9 où vous voulez que le rapport soit déplacé. Valeurs possibles :
     - "/content/package[@name='Network Manager']/folder[@name='Asset Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Current Status Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Views Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Path View Reports']"
     - "/content/package[@name='Network Manager']/ folder[@name='Performance Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Summary Reports']"
     - "/content/package[@name='Network Manager']/ folder[@name='Troubleshooting Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Utility Reports']"
   - *nom_utilisateur_admin* est le nom d'utilisateur d'un administrateur Tivoli Integrated Portal.
   - *mot_de_passe_admin* est le mot de passe de l'administrateur.

   La commande suivante déplace un rapport 3.7 nommé itnm_usa_vlan_summary vers l'ensemble de rapports "Network Technology Reports" :

   ```
   NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
   itnm_usa_vlan_summary.rptdesign -reportSetBase "/content/
   package[@name='Network Manager']/folder[@name='Network Technology
   Reports']" -resourceDir ITNM39 -username tipadmin -password netcool
   ```

4. Examinez les rapports que vous avez déplacés dans un ensemble de rapports 3.9. Si un rapport utilise la base de données ncmonitor ou ncpolldata, vérifiez les commandes SQL par rapport à des commandes similaires dans les rapports 3.9 par défaut. Les schémas de base de données peuvent avoir changé.

   Important : Les paramètres sauvegardés avec les rapports ne sont pas conservés.

Importation de données d'interface graphique V3.8

Après l'installation de Network Manager V3.9, vous pouvez importer vos données d'interface graphique de la version 3.8.

Avant de pouvoir importer des données d'interface graphique, vous devez exporter les données à partir de votre installation précédente V3.8 et installer la version 3.9.

Pour importer les données d'interface graphique, procédez comme suit :

1. Connectez-vous au serveur sur lequel les composants d'interface graphique de votre système V3.8 précédent sont installés.
2. Copiez le fichier d'exportation `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip` sur le serveur où vous avez installé les composants de l'interface graphique de Network Manager V3.9.
3. Sur votre nouvelle installation, accédez à l'emplacement du package d'installation.

   Remarque : Le serveur Tivoli Integrated Portal doit être en cours d'exécution lors de l'importation des données de l'interface graphique.
4. Exécutez le script d'importation de données d'interface graphique via une des méthodes suivantes :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, démarrez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Postinstallation**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Importer des données d'interface graphique Network Manager**.
   - Pour exécuter le script à partir de la ligne de commande, accédez au sous-répertoire `scripts` et, selon votre système d'exploitation, exécutez la commande UNIX **nmGuiImport** ou Windows **nmGuiImport.bat** comme suit :

     ```
     nmGuiImport | bat -u nom utilisateur administrateur TIP -p
     mot de passe pour administrateur
     TIP -
     f chemin vers fichier .zip d'exportation des données d'interface graphique -
     d emplacement de
     l'installation TIP
     ```

     Remarque : Si les valeurs ne sont pas fournies, vous êtes invité à les entrer. Si l'emplacement de l'installation Tivoli Integrated Portal n'est pas fourni, la variable d'environnement `TIPHOME` est utilisée. Si `TIPHOME` n'existe pas, vous êtes invité à entrer un emplacement.

Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

Les données d'interface graphique exportées sont importées dans la nouvelle installation.

Le processus d'importation crée ses propres fichiers journaux dans les répertoires suivants :

- `TIPHOME/profiles/TIPProfile/logs/upgrade.log`
- `TIPHOME/profiles/TIPProfile/logs/tipcli.log`
- `NCHOME/log/install/itnm_gui_migration.log`

Remarque : Le fichier `itnm_gui_migration.log` est un fichier de rapport de migration qui fournit des informations sur les fichiers importés, sauvegardés et pour lesquels une procédure de réconciliation manuelle est requise sur le nouveau système.

Après l'importation de vos données d'interface graphique précédentes, il peut être nécessaire de définir manuellement certains paramètres sur le nouveau système. Le processus d'exportation/importation indique pour quels fichiers une attention particulière est requise ainsi qu'une édition manuelle afin de mener à terme le processus de migration et de mise à niveau.

Importation de données d'interface graphique V3.8 - étapes manuelles

En raison des modifications du produit, vous devez migrer manuellement des paramètres de configuration d'interface graphique vers le nouveau système. Consultez les tâches suivantes pour déterminer les ajustements manuels supplémentaires à apporter à votre nouveau système.

Assurez-vous que vous avez effectué une collecte et une exportation de données d'interface graphique sur le système précédent et que vous avez importé les données d'interface graphique vers la nouvelle installation.

Pour vérifier que tous les paramètres d'interface graphique sont migrés :

1. Connectez-vous à la nouvelle installation.
2. Vous devez synchroniser manuellement les fichiers Tivoli Integrated Portal répertoriés dans `ITNMHOME/profiles/TIPProfile/etc/tnm/migration` et `ITNMHOME/profiles/TIPProfile/etc/tnm/*/migration`. Les fichiers archivés sont sauvegardés par le processus d'exportation-importation.
3. Utilisez le fichier de rapport de migration `NCHOME/log/install/itnm_gui_migration.log` pour identifier les fichiers qu'il convient de modifier manuellement pour qu'ils soient utilisés sur le nouveau système.
4. Les outils WebTool personnalisés sous `NCHOME/precision/scripts/webtools` ne sont pas migrés. Vous devez les sauvegarder manuellement dans l'installation précédente et les réimplanter sur le nouveau système. Un exemple de personnalisation de ce type est les paramètres à lancer dans TADDM.
5. Pour conserver des rapports nouveaux ou personnalisés de votre installation précédente, vous devez effectuer des étapes de configuration supplémentaires.

Tâches associées:

«Configuration de Network Manager pour le démarrage de IBM Tivoli Application Dependency Discovery Manager», à la page 218
Facultatif : pour autoriser les opérateurs réseau à lancer l'interface utilisateur graphique IBM Tivoli Application Dependency Discovery Manager à partir de Network Manager, vous devez ajouter les options de menu TADDM dans Network Manager.

Migration des rapports version 3.8

Si vous avez modifié ou créé des rapports dans Network Manager 3.8, vous devez les migrer manuellement.

Avant d'effectuer cette tâche, vous devez d'abord importer les données d'interface graphique 3.8, qui comprennent les rapports.

Le script d'importation des données d'interface graphique 3.8, **nmGuiImport**, place tous les rapports 3.8 personnalisés dans l'ensemble de rapports **Produits Tivoli** > **Rapports ITNM**. Pour migrer des rapports 3.8 personnalisés, procédez selon les étapes suivantes :

1. Connectez-vous à Network Manager 3.9 et cliquez sur **Génération de rapports** > **Génération de rapports communs** > **Produits Tivoli** > **Rapports ITNM**.
   - Si cet ensemble de rapports ne contient aucun rapport nouveau ou personnalisé, vous ne devez pas effectuer cette tâche. Vous pouvez supprimer l'ensemble de rapports **Produits Tivoli** > **Rapports ITNM**.
   - Si l'ensemble de rapports contient des rapports nouveaux ou personnalisés, choisissez les rapports que vous voulez migrer vers la version 3.9.
2. Sur le serveur où Tivoli Common Reporting est installé, accédez au répertoire où se trouvent les conceptions des rapports personnalisés 3.8 importés : `NCHOME/../tipv2Components/TCRComponent/data/design`.
3. Pour déplacer un rapport du groupe 3.8 vers un groupe de rapports 3.9, exécutez une commande similaire à la suivante :

   ```
   NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
   nom_fichier_rapport -reportSetBase ensemble_rapports_destination
   -resourceDir ITNM39 -username nom_utilisateur_admin -password
   mot_de_passe_admin
   ```

   Où

   - *nom_fichier_rapport* est le nom de fichier du rapport à déplacer.
   - *ensemble_rapports_destination* est l'ensemble de rapports 3.9 où vous voulez que le rapport soit déplacé. Valeurs possibles :
     - "/content/package[@name='Network Manager']/folder[@name='Asset Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Current Status Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Views Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Path View Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Performance Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Summary Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Troubleshooting Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Utility Reports']"

- *nom_utilisateur_admin* est le nom d'utilisateur d'un administrateur Tivoli Integrated Portal.
- *mot_de_passe_admin* est le mot de passe de l'administrateur.

La commande suivante déplace un rapport 3.8 nommé itnm_usa_vlan_summary vers l'ensemble de rapports "Network Technology Reports" :

```
NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
itnm_usa_vlan_summary.rptdesign -reportSetBase "/content/
package[@name='Network Manager']/folder[@name='Network Technology
Reports']" -resourceDir ITNM39 -username tipadmin -password netcool
```

4. Examinez les rapports que vous avez déplacés dans un ensemble de rapports 3.9. Si un rapport utilise la base de données ncmonitor ou ncpolldata, vérifiez les commandes SQL par rapport à des commandes similaires dans les rapports 3.9 par défaut. Les schémas de base de données peuvent avoir changé.

   Important : Les paramètres sauvegardés avec les rapports ne sont pas conservés.

Tâches associées:

«Configuration des sources de données pour BIRT», à la page 278
Si vous utilisez des rapports basés sur le modèle de données BIRT, vous devez configurer des sources de données. Si vous utilisez également des rapports basés sur le modèle Cognos, vous devez configurer les sources de données Cognos séparément.

Identification des personnalisations de la base de données de topologiques NCIM

Les scripts de mise à niveau ne migrent pas les personnalisations effectuées dans le schéma de la base de données topologiques NCIM. Toutefois, Network Manager fournit un outil permettant d'identifier les personnalisations que vous avez effectuées dans la base de données précédente afin que vous puissiez les recréer dans la base de données de la nouvelle installation. Pour migrer les personnalisations NCIM, utilisez d'abord le script **ncp_ncim_diff.pl** pour identifier les différences entre le schéma de base de données de topologie NCIM de l'installation précédente et celui de la nouvelle installation, et mettre ensuite à jour manuellement le nouveau schéma de base de données de topologie NCIM avec ces modifications.

Vous devez installer la nouvelle base de données et exécuter les scripts de schéma de base de données de créationNetwork Manager pour configurer les tables et les schémas.

Avant d'exécuter le script **ncp_ncim_diff.pl**, assurez-vous que les fichiers `DbLogins.`*`DOMAIN`*`.cfg` provenant de l'installation précédente ont été migrés vers votre nouvelle installation. Le processus d'exportation-importation pour les données de personnalisation offre cette possibilité. Le fichier `DbLogins.`*`DOMAIN`*`.cfg` contient les options nécessaires pour la connexion à votre base de données NCIM.

Remarque : Le processus de migration combiné à une nouvelle reconnaissance du réseau renseigne la base de données. Si vous disposez de modifications personnalisées dans votre base de données précédente, il vous suffit d'exécuter le script **ncp_ncim_diff.pl**.

Pour comparer les schémas de base de données de topologie :

1. Connectez-vous à votre nouvelle installation Network Manager.
2. Accédez au répertoire suivant :
   - UNIX: UNIX: `$NCHOME/precision/scripts/perl/scripts`
   - Windows: Windows: `%NCHOME%\precision\scripts\perl\scripts`
3. Entrez la commande suivante : `./ncp_ncim_diff.pl -domain DOMAIN -password NCIM_database_password`

   où *DOMAIN* correspond au nom de domaine de votre installation Network Manager précédente pour laquelle vous souhaitez comparer la structure NCIM à celle du schéma de la nouvelle installation. Vous devez utiliser le fichier `DbLogins.DOMAIN.cfg` de votre installation précédente pour que le script se connecte à la base de données précédente et compare le schéma présent avec le schéma de la nouvelle installation. Voici un exemple de sortie de la commande pour un domaine appelé NCOMS.

```
67  NCIM tables and views found in Domain NCOMS
66  NCIM tables and views found in  Default NCIM structure for ITNM v3.9


*********************************************************
 Additional elements in Domain NCOMS

         Table CUSTOM

*********************************************************

1 differences found between  Domain NCOMS and  Default NCIM structure
for ITNM v3.9
```

4. Facultatif : Vous pouvez spécifier un nom de fichier dans lequel la sortie est sauvegardée avec un paramètre `-dumpToFile nom de fichier.xml` facultatif.

Tâches associées:

«Configuration d'une base de données topologiques», à la page 62
A part la base de données Informix par défaut, vous pouvez utiliser une base de données DB2, MySQL ou Oracle pour stocker votre topologie. A moins que vous n'installiez la base de données Informix par défaut livrée avec Network Manager, vous devez configurer une base de données existante ou en installer et configurer une nouvelle avant d'installer Network Manager.

Copie d'une installation version 3.9 existante

Vous pouvez copier les personnalisations et les données d'une installation existante de la version 3.9 vers une autre installation de la version 3.9.

Si vous souhaitez cloner ou migrer une installation de Network Manager vers Network Manager version 3.9 groupe de correctifs 5, vous devez tout d'abord mettre à jour les scripts d'importation et d'exportation suivants : `$NCHOME/precision/install/scripts/nmExport`, `$NCHOME/precision/install/scripts/nmImport` et `$NCHOME/scripts/upgrade/ITNMExportNetworkViews.pl`. Après avoir installé Network Manager groupe de correctifs 5, copiez les scripts `nmExport` et `nmImport` dans le répertoire `scripts` à l'emplacement dans lequel vous avez décompressé le fichier d'installation de la version principale de Network Manager. Sinon, si vous utilisez `ExportPackage.tar`, copiez les scripts dans le répertoire `scripts` de l'emplacement dans lequel vous avez décompressé le fichier `.tar`. Vous ne pouvez pas exécuter ces scripts à partir d'une installation existante ou d'une installation de groupe de correctifs. Copiez également le script `ITNMExportNetworkViews.pl` dans le répertoire `migration/bin/` au même emplacement.

L'utilisation des scripts d'exportation-importation fournis avec Network Manager vous permet de faire une copie d'une installation version 3.9 et de l'utiliser pour recréer la même configuration sur un autre système, de restaurer ultérieurement des paramètres ou de déplacer un système de test vers un environnement de production.

Pour copier une installation existante de la version 3.9, procédez comme suit :

1. Accédez au système source où se trouve l'installation de Network Manager dont vous voulez faire une copie. Si vous avez une configuration distribuée, vous devez accéder à chacun des systèmes pour collecter toutes les données.
2. Accédez là où vous avez extrait le package d'installation.
3. Exécutez le script d'exportation de données via une des méthodes suivantes :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, lancez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Préinstallation et migration**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Exporter les données Network Manager**.
   - Pour exécuter le script à partir de la ligne de commande, exécutez le script UNIX **nmExport** sous UNIX ou le script Windows **nmExport.bat** sous Windows à partir du sous-répertoire `scripts`.

   Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

   Fournissez des réponses aux invites. Le script d'exportation extrait les données et les enregistre dans un fichier d'exportation à un emplacement de votre choix (`.pkg` sur des systèmes UNIX ou `.zip` sur des systèmes Windows).

   Restriction : L'historique des données d'interrogation n'est pas déplacé lors de la copie entre des versions 3.9.
4. Exécutez le script d'exportation des données d'interface graphique via une des méthodes suivantes :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, lancez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Préinstallation et migration**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Exporter des données d'interface graphique Network Manager**.
   - Pour exécuter le script à partir de la ligne de commande, accédez au sous-répertoire `scripts` et, selon votre système d'exploitation, exécutez la commande UNIX **nmGuiExport** ou Windows **nmGuiExport.bat** comme suit :

     ```
     nmGuiExport | bat -u nom utilisateur administrateur TIP -p
     mot de passe pour administrateur
     TIP -d emplacement de l'installation TIP à migrer
     ```

     Remarque : Si les valeurs ne sont pas fournies, vous êtes invité à les entrer. Si l'emplacement de l'installation Tivoli Integrated Portal à migrer n'est pas fourni, la variable d'environnement `TIPHOME` est utilisée. Si `TIPHOME` n'existe pas, vous êtes invité à entrer un emplacement.

Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.

Les données d'interface graphique sont extraites et enregistrées dans le fichier d'exportation `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip`.

5. Connectez-vous à l'installation de Network Manager où vous voulez copier la configuration.
6. Sur votre nouvelle installation, assurez-vous que les composants centraux de Network Manager pour chaque domaine sont en cours d'exécution. Pour cela, utilisez l'interface graphique des services Windows sur les systèmes Windows ou bien la commande suivante sur les systèmes UNIX : **itnm_start** `ncp -domain` *DOMAINE*. Par exemple, pour démarrer le domaine `NCOMS`, entrez : `itnm_start ncp -domain NCOMS` . Ceci garantit que Network Manager est complètement initialisé et que les tables du domaine sont remplies. Vous devez à nouveau arrêter les composants centraux pour effectuer l'importation elle-même, comme décrit à l'étape suivante.
7. Arrêtez les composants centraux de Network Manager pour chaque domaine sur votre nouvelle installation à l'aide de l'interface graphique des services Windows sur les systèmes Windows ou bien à l'aide de la commande suivante sur les systèmes UNIX : **itnm_stop** `ncp -domain` *DOMAINE*. Par exemple, pour arrêter le domaine `NCOMS`, entrez : `itnm_stop ncp -domain NCOMS`

   Remarque : Si vous ne spécifiez pas un nom de domaine avec **itnm_stop**, il arrête le domaine par défaut créé lors de l'installation.
8. Exécutez le script d'importation de données via une des méthodes suivantes :
   - Pour exécuter le script à partir du tableau de bord du programme d'installation, démarrez le tableau de bord en exécutant le script UNIX **launchpad.sh** sous UNIX ou l'exécutable Windows **launchpad.exe** sous Windows, sélectionnez l'option **Postinstallation**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Importer les données Network Manager**.
   - Pour exécuter le script depuis la ligne de commande, lancez le script UNIX **nmImport** sous UNIX ou le script Windows **nmImport.bat** sous Windows à partir du sous-répertoire `scripts` du support d'installation.

   Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit.
9. Lorsque vous y êtes invité, indiquez le chemin du fichier `.pkg` ou `.zip` qui contient les données de personnalisation précédemment exportées.
10. Répondez aux différentes questions posées par le processus d'importation pour copier les données.

    Remarque : La question suivante requiert une attention particulière :

    ```
    Allocate new entityIds during import [ N ]
    ```

    Chaque périphérique du système a un élément `entityId`. Le processus d'importation peut conserver les éléments `entityId` ou en allouer de nouveaux. Si vous répondez `no`, chaque périphérique conserve l'élément `entityId` de l'installation précédente. Cela est nécessaire lorsque vous avez des liens vers des systèmes externes qui utilisent les données Network Manager, par exemple, Tivoli Data Warehouse.

    Si vous répondez `yes`, des éléments `entityId` sont alloués à des périphériques.

Pour conserver les éléments `entityId`, le systèmes cible doit être vide. Si le système cible n'est pas vide (par exemple suite à une reconnaissance ou une importation de données précédente), la conservation des élémentsentityId peut être une opération complexe suite à des conflits potentiels entre les éléments `entityId` existants et ceux importés, et les résultats peuvent être imprévisibles. Par conséquent, la fusion de données de domaine n'est pas prise en charge.

Avertissement : Si un domaine sur le système cible a le même nom que sur votre système précédent, vérifiez le domaine sur le système cible ne contient pas de données. Les noms de domaine ne peuvent pas être modifiés pendant le processus de migration.

Le processus d'importation crée ses propres fichiers journaux. Les journaux du processus d'importation sont enregistrés dans `NCHOME/log/precision` :

- `ITNMDataImport.log`
- `get_policies.`*`nom domaine`*`.log`
- `ITNMImportNetworkViews.log`

Le processus d'exportation/importation détecte et recrée automatiquement les domaines à partir d'une installation précédente. Le script d'importation détecte les domaines potentiels à partir du système précédent en fonction des fichiers de données. A l'aide du script **`domain_create.pl`**, le processus crée automatiquement les domaines sur la nouvelle installation en utilisant les noms de domaine du système précédent. Une fois que les domaines ont été créés, la topologie principale et les données de règle sont importées pour chacun d'entre eux.

Le script **`domain_create.pl`** crée les fichiers de configuration de la reconnaissance pour les nouveaux domaines dans `NCHOME/etc/precision` en utilisant les valeurs des fichiers de configuration du domaine par défaut. Le processus d'importation enregistre les fichiers importés dans le répertoire `NCHOME/etc/precision/migration` en tant que fichiers en lecture seule. Vous pouvez utiliser les fichiers importés pour mettre à jour manuellement les fichiers nouvellement créés dans `NCHOME/etc/precision`. Lors de la copie à partir d'une installation version 3.9 existante, les fichiers peuvent être copiés directement dans `NCHOME/etc/precision`, mais ils doivent recevoir des autorisations en écriture pour pouvoir être modifiés à partir de l'interface graphique de configuration de la reconnaissance.

11. Vérifiez s'il y a des fichiers dans le répertoire `NCHOME/etc/precision/migration`. Les modifications utilisateur apportées aux fichiers répertoriés ici doivent être examinées et appliquées à nouveau manuellement.
12. Exécutez le script d'importation de données d'interface graphique via une des méthodes suivantes :
    - Pour exécuter le script à partir du tableau de bord du programme d'installation, démarrez le tableau de bord en exécutant le script UNIX **`launchpad.sh`** sous UNIX ou l'exécutable Windows **`launchpad.exe`** sous Windows, sélectionnez l'option **Postinstallation**, développez la section **Mise à niveau à partir d'une version existante de Network Manager** et cliquez sur **Importer des données d'interface graphique Network Manager**.
    - Pour exécuter le script à partir de la ligne de commande, accédez au sous-répertoire `scripts` et, selon votre système d'exploitation, exécutez la commande UNIX **`nmGuiImport`** ou Windows **`nmGuiImport.bat`** comme suit :

```
nmGuiImport | bat -u nom utilisateur administrateur TIP -p
mot de passe pour administrateur
TIP -
f chemin vers fichier .zip d'exportation des données d'interface graphique -
d emplacement de
l'installation TIP
```

Remarque : Si les valeurs ne sont pas fournies, vous êtes invité à les entrer. Si l'emplacement de l'installation Tivoli Integrated Portal n'est pas fourni, la variable d'environnement TIPHOME est utilisée. Si TIPHOME n'existe pas, vous êtes invité à entrer un emplacement.

Remarque : Vous devez exécuter le script à l'aide du même utilisateur qui celui qui a installé le produit. Le serveur Tivoli Integrated Portal doit être en cours d'exécution lors de l'importation des données de l'interface graphique.

13. Vous devez synchroniser manuellement les fichiers Tivoli Integrated Portal répertoriés dans ITNMHOME/profiles/TIPProfile/etc/tnm/migration et ITNMHOME/profiles/TIPProfile/etc/tnm/*/migration. Les fichiers archivés sont sauvegardés par le processus d'exportation-importation.
14. Utilisez le fichier de rapport de migration NCHOME/log/install/itnm_gui_migration.log pour identifier les fichiers qu'il convient de modifier manuellement pour qu'ils soient utilisés sur le nouveau système.
15. Si vous avez apporté des personnalisations au schéma de la base de données topologiques NCIM sur le système à partir duquel vous faites la copie, procédez selon les étapes décrites dans «Identification des personnalisations de la base de données de topologiques NCIM», à la page 165.
16. Si vous avez modifié la configuration de la base de données utilisée pour Tivoli Common Reporting, ou défini une nouvelle base de données pour le système cible où le système cible est différent du système source, configurez les sources de données pour la génération de rapport en suivant les instructions de la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

    Remarque : Le schéma ncmonitor et le schéma d'interrogation étant les mêmes lors de la copie entre versions identiques, les rapports ne nécessitent pas de modification manuelle pour les modifications de schéma.
17. Arrêtez et démarrez Network Manager, y compris Tivoli Integrated Portal, comme décrit dans Démarrage et arrêt de Network Manager. Le domaine par défaut est démarré par le processus de démarrage, mais si vous avez plusieurs domaines, démarrez chacun de ceux-ci à l'aide de la commande **itnm_start** ncp -domain *DOMAINE*.

Transition depuis IBM Tivoli NetView

Comme Network Manager dispose de fonctions qui ne sont pas disponibles dans IBM Tivoli NetView, aucun chemin de migration automatique n'est pris en charge entre les deux produits. En fait, passez à Network Manager en installant le produit et en le configurant pour reconnaître et visualiser le réseau. Pour planifier la transition, Network Manager contient des scripts que vous pouvez utiliser pour extraire des données utiles de IBM Tivoli NetView.

Vous pouvez passer à Network Manager depuis IBM Tivoli NetView V7.1.4 et V7.1.5.

La procédure générale de la transition depuis IBM Tivoli NetView est la suivante :

1. Extrayez les données depuis IBM Tivoli NetView. Vous pouvez exécuter un script depuis l'interface de ligne de commande ou sélectionner une option dans le tableau de bord.
2. Installez Network Manager V3.9. Dans le programme d'installation, ignorez l'option **Définir l'emplacement de départ de la reconnaissance à partir de l'installation IBM Tivoli NetView**. Vous pouvez optimiser les résultats en planifiant la configuration de Network Manager en utilisant les données que vous avez extraites à l'étape 1.
3. Planifiez, puis exécutez la reconnaissance. Utilisez les données extraites pour vous aider.
4. A la fin de la reconnaissance, recréez les emplacements IBM Tivoli NetView dans les vues de réseau.
5. Désinstallez IBM Tivoli NetView. Pour plus d'informations, recherchez la rubrique relative à la *désinstallation du programme Tivoli NetView* sur http://www-01.ibm.com/support/knowledgecenter/SS3HLM_7.1.1.16/com.ibm.tivoli.tpm.osd.doc_7.1.1.16/welcome/osdlanding.html.

Tâches associées:

Chapitre 1, «Planification de l'installation», à la page 1
Consultez les remarques sur le déploiement et les exigences système relatives à Network Manager.

Extraction des données de IBM Tivoli NetView

Pour planifier la transition vers Network Manager, vous pouvez extraire des données réseau utiles de IBM Tivoli NetView. Vous pouvez utiliser la sortie du script pour configurer la reconnaissance réseau exécutée par Network Manager.

Vous pouvez extraire les données suivantes :

- Noms d'hôte et adresses IP de tous les noeuds reconnus
- Noeuds et leurs chaînes de communauté SNMP
- Noms de communauté
- Noeuds gérés
- Regroupements de périphériques (conteneurs d'emplacements)

Avant d'extraire les données :

- Vérifiez que le langage Perl est installé sur l'hôte.
- Pour le tableau de bord, vérifiez qu'un navigateur compatible est installé.

Un script d'extraction des données est inclus dans le package d'installation de Network Manager. Vous pouvez également exécuter le script dans le tableau de bord.

- Pour extraire les données en exécutant le script :
  1. Décompressez le package d'installation de Network Manager et accédez au répertoire `scripts`.
  2. Copiez le package `ExportPackage` vers un répertoire de travail sur l'installation IBM Tivoli NetView et décompressez-le.
  3. Exécutez le script **`exportNVData`**.
- Pour extraire les données en utilisant le tableau de bord, sélectionnez **Préinstallation & Migration** dans le menu, puis développez **Collecte de données IBM Tivoli NetView pour l'emplacement de départ de la reconnaissance** et cliquez sur **Extraire les données de migration NetView**.

Les données IBM Tivoli NetView sont extraites et enregistrées dans un package nvMigrationData.

Décompressez le package nvMigrationData et utiliser les données pour planifier la reconnaissance.

Référence associée:

«Navigateurs pris en charge pour le tableau de bord du programme d'installation», à la page 48
Pour exécuter le tableau de bord du programme d'installation, assurez-vous qu'un navigateur pris en charge est installé. Les navigateurs pris en charge ne sont pas nécessairement les mêmes que pour les applications Web.

Création de vues de réseau depuis le fichier IBM Tivoli NetView location.conf

Le fichier de configuration location.conf permet de créer des mappages de topologie pour les emplacements qui reposent sur des plages d'adresses IP définies. Network Manager peut utiliser un sous-ensemble de la syntaxe du fichier location.conf et les plages d'adresses IP définies dans le fichier pour répliquer les mappages de topologie dans des vues de réseau.

Pour plus d'informations sur le sous-ensemble de la syntaxe location.conf prise en charge par Network Manager, voir Création de vues filtrées par IP.

Vous pouvez exécuter un script de provisionnement automatique qui convertit le fichier location.conf en noeud de vue de réseau dynamique. Le noeud qui dispose de vues de réseau qui correspondent au contenu du fichier location.conf. Un domaine peut être défini. Les vues de réseau peuvent être affectées à des utilisateurs ou des groupes.

1. Copiez le fichier location.conf vers ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision.
2. Accédez à ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision/examples et copiez le fichier example_netview_migration.xml vers ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision.
3. Dans ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision, ouvrez la copie du fichier example_netview_migration.xml. Modifiez au minimum les paramètres suivants.

   accessID
   Définissez l'utilisateur ou le groupe qui doit accéder aux vues de réseau.

   domain
   Définissez le domaine dans lequel vous voulez ajouter les vues de réseau.

   netViewMigration file
   Définissez l'emplacement du fichier location.conf. Si le fichier ne se trouve pas dans ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision, définissez le chemin relatif du fichier.

   Voir «Exemple», à la page 173 pour un exemple de fichier.
4. Exécutez le script.

Toutes les 60 secondes, le système recherche dans le répertoire ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision les nouveaux scripts de provisionnement automatique. Lorsqu'un script est détecté, il est lu et traité, puis la vue dynamique est créée.

Exemple

L'exemple suivant génère la vue MigratedLocation.conf. En fonction des données dans le fichier ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision/location.conf, un groupe de vues de réseau est créé sous MigratedLocation.conf. La vue générée est affectée à l'utilisateur itnmadmin. Les vues sont créées dans le domaine NCOMS.

```
<autoProvision name="MigratedLocation.conf" domain="NCOMS" accessLevel="user"
accessId="itnmadmin">
        <netViewMigration file="location.conf" endNodes="true" connectivity=
"ipsubnets"/>
</autoProvision>
```

Chapitre 4. Configuration de Network Manager

Après l'installation de Network Manager, vous devez configurer Network Manager pour votre environnement et en fonction de vos exigences. Si votre environnement ou vos exigences changent ultérieurement ou si vous souhaitez intégrer Network Manager à d'autres produits, il peut être nécessaire d'effectuer des tâches de configuration supplémentaires.

Cliquez sur le lien suivant pour extraire des remarques techniques sur les problèmes de configuration connus dans la version 3.9 de Network Manager : http://www-01.ibm.com/support/search.wss?word=ow&wfield=configure+configuration+configuring&rs=3118&tc=SSSHRK&atrn=SWVersion&atrv=3.9&ibm-go.x=18&ibm-go.y=12

Configuration des intégrations à d'autres produits

Vous pouvez configurer Network Manager pour l'utiliser avec plusieurs produits Tivoli. Consultez les informations relatives aux tâches de configuration requises pour configurer les intégrations disponibles.

Référence associée:

«Configuration requise pour les autres produits», à la page 34
Vérifiez que la configuration requise des produits intégrés à Network Manager est respectée.

Configuration de Tivoli Netcool/OMNIbus pour une utilisation avec Network Manager

Si vous avez installé Tivoli Netcool/OMNIbus sans utiliser l'installation de Network Manager, vous devez effectuer un certain nombre de tâches de configuration.

Tivoli Netcool/OMNIbus gère les événements fournis par Network Manager et d'autres sources d'événement et peut également être utilisé en tant que source d'authentification. Pour accéder aux rubriques qui vous intéressent, consultez la section **Rubriques connexes**.

Pour utiliser Tivoli Netcool/OMNIbus, vous devez modifier une table dans le serveur ObjectServer. Si vous exécutez Network Manager dans une installation FIPS 140–2, vous devez effectuer des opérations de configuration supplémentaires dans l'environnement d'exécution de Tivoli Netcool/OMNIbus.

Pour des informations détaillées sur Tivoli Netcool/OMNIbus, y compris les considérations relatives à la configuration post installation et à FIPS 140–2, consultez le centre de documentation de Tivoli Netcool/OMNIbus à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Pour plus d'informations sur Tivoli Netcool/OMNIbus, y compris les considérations relatives à la configuration post installation et à FIPS 140–2, consultez les guides *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* et *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Tâches associées:

Modification des registres d'utilisateurs après l'installation

Ajout de serveurs ObjectServer en tant que registres d'utilisateurs

Utilisation de SSL pour la communication avec le serveur ObjectServer

«Configuration de VMM pour ObjectServer», à la page 234
Lorsque votre serveur Tivoli Netcool/OMNIbus ObjectServer est inclus dans un référentiel fédéré, utilisez le script fourni avec Tivoli Integrated Portal pour configurer l'adaptateur VMM (Virtual Member Manager) pour le serveur ObjectServer.

«Configuration de la reprise en ligne de la source de données pour l'interface graphique Web Tivoli Netcool/OMNIbus», à la page 342
Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation interface graphique Web.

Modification du mot de passe pour la connexion au serveur ObjectServer

Configuration des automatisations pour les événements affectés par un service

Fix Pack 4

Configurez les automatisations dans Tivoli Netcool/OMNIbus pour prendre en charge la génération d'événements affectés par un service (SAE). Les étapes de cette tâche sont différentes, en fonction de la complexité de l'installation de Tivoli Netcool/OMNIbus. Cette tâche est obligatoire si vous souhaitez configurer les reconnaissances interdomaine dans les environnements dans lesquels Tivoli Netcool/OMNIbus V7.3.1 ou version antérieure s'exécute.

Pour les installations complexes de Tivoli Netcool/OMNIbus, notamment avec des architecture à plusieurs niveaux, suivez les instructions du *guide des bonnes pratiques 'dTivoli Netcool/OMNIbus*, disponible à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices. Vérifiez notamment que les déclencheurs d'événements affectés par un service (SAE) ne s'exécutent que sur le serveur d'objets principal (ObjectServer) et sont désactivés sur tous les autres serveurs d'objets. Les déclencheurs d'événements fournis avec Network Manager sont configurés en vue d'être exécutés uniquement sur les serveurs d'objets d'agrégation principaux.

Effectuez les opérations suivantes pour configurer l'automatisation et le plug-in SAE sur la passerelle d'événement (**ncp_g_event**). Les étapes ci-après décrivent la configuration d'une architecture à plusieurs niveaux. Aucune configuration n'est requise pour les serveurs ObjectServer de la couche de collection. Si votre installation de Tivoli Netcool/OMNIbus ne s'exécute pas sur une architecture à plusieurs niveaux, seule l'étape 3 est obligatoire. Pour savoir comment arrêter et démarrer Network Manager, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

1. Connectez-vous à l'hôte sur lequel Tivoli Netcool/OMNIbus est installé.
2. Arrêtez les processus **ncp**.
3. Configurez les serveurs d'objets de couche agrégation :

a. Exécutez le script NCHOME/precision/scripts/drop_sae_automation.sql pour supprimer les tables existantes. Par exemple, pour le serveur ObjectServer AGG_A et l'utilisateur OMNIUser :

```
$NCHOME/omnibus/bin/nco_sql -server AGG_A -user OMNIUser -password
 mot_de_passe < $NCHOME/precison/scripts/drop_sae_automation.sql
```

b. Exécutez le script NCHOME/precision/scripts/create_sae_automation.sql pour installer le déclencheur d'événements affectés par un service (SAE) et ajoutez les tables, y compris la colonne NmosDomainName. Exemple :

```
$NCHOME/omnibus/bin/nco_sql -server AGG_A -user OMNIUser -password
 mot_de_passe < $NCHOME/precison/scripts/create_sae_automation.sql
```

c. Vérifiez que l'automatisation des événements affectés par un service (SAE) s'exécute uniquement sur le serveur d'objets principal de travail et non sur le serveur d'objets de secours. Editez le fichier create_sae_automation.sql et vérifiez ou ajoutez la ligne suivante :

```
WHEN get_prop_value('ActingPrimary') %= 'TRUE'
```

d. Dans les serveurs d'objets de la couche agrégation, activez les déclencheurs SAE. Utilisez la commande suivante :

```
ALTER TRIGGER GROUP sae SET ENABLED TRUE;
```

e. Mettez à jour le mappage des serveurs d'objets de la couche agrégation. Dans le fichier NCHOME/omnibus/etc/AGG_GATE.map, ajoutez des instructions CREATE pour les tables qui viennent d'être créées par le script create_sae_automation.sql à la fin du fichier.

L'instruction CREATE se présente comme l'exemple suivant. Copiez les définitions exactes de la table telles qu'elles sont indiquées dans le script afin d'éviter des erreurs.

```
CREATE MAPPING EntityServiceMap
(
 'NmosEntityId'  = '@NmosEntityId' ON INSERT ONLY,
 'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
 'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);

CREATE MAPPING ServiceDetailsMap
(
 'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
 'Type' = '@Type' ON INSERT ONLY,
 'Name' = '@Name' ON INSERT ONLY,
 'Customer' = '@Customer',
 'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
```

f. Mettez à jour la passerelle pour les serveurs d'objets d'agrégation. Editez le fichier NCHOME/omnibus/etc/AGG_GATE.tblrep.def et ajoutez les instructions REPLICATE suivantes pour les tables qui ont été créées par le script create_sae_automation.sql à la fin du fichier :

```
REPLICATE ALL FROM TABLE 'precision.entity_service'
       USING MAP 'EntityServiceMap'
       INTO 'precision.entity_service';

REPLICATE ALL FROM TABLE 'precision.service_details'
       USING MAP 'ServiceDetailsMap'
       INTO 'precision.service_details';
```

4. Configurez tout serveur d'objets ObjectServers de couche affichage. Voir les étapes 3a and 3b pour consulter des exemples montrant comment exécuter les scripts drop_sae_automation.sql et create_sae_automation.sql.

a. Exécutez le script NCHOME/precision/scripts/drop_sae_automation.sql pour supprimer les tables existantes.

b. Exécutez le script NCHOME/precision/scripts/create_sae_automation.sql pour installer le déclencheur d'événements affectés par un service (SAE) et ajoutez les tables, y compris la colonne NmosDomainName.

c. Dans les serveurs d'objets ObjectServers de la couche affichage, désactivez les déclencheurs SAE pour empêcher leur exécution dans la couche d'affichage. Utilisez la commande suivante :

```
ALTER TRIGGER GROUP sae SET ENABLED FALSE;
```

d. Vérifiez que les tables precision.entity_service et precision.service_details sur les serveurs d'objets de couche affichage possèdent le même schéma que les tables qui se trouvent sur les serveurs d'objets de couche agrégation.

e. Mettez à jour le mappage pour la couche d'affichage ObjectServers. Editez les fichiers NCHOME/omnibus/etc/A_TO_D_GATE.map et ajoutez des instructions CREATE pour les tables qui ont été créées par le script create_sae_automation.sql à la fin du fichier. Ce mappage doit être identique au mappage sur la passerelle de couche agrégation. Si vous modifiez le mappage ultérieurement sur la passerelle bidirectionnelle pour les serveurs d'objets de couche agrégation, vous devez répliquer ces modifications ici.

```
CREATE MAPPING EntityServiceMap
(
'NmosEntityId' = '@NmosEntityId' ON INSERT ONLY,
'ServiceEntityId' = '@ServiceEntityId ON INSERT ONLY,
'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
CREATE MAPPING ServiceDetailsMap
(
'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
'Type' = '@Type' ON INSERT ONLY,
'Name' = '@Name' ON INSERT ONLY,
'Customer' = '@Customer',
'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
```

f. Mettez à jour la passerelle pour les serveurs d'objets de couche affichage. Editez le fichier NCHOME/omnibus/etc/A_TO_D_GATE.tblrep.def et ajoutez les instructions REPLICATE ci-dessous pour les tables qui ont été créées par le script create_sae_automation.sql à la fin du fichier. Ce mappage doit être identique au mappage sur la passerelle de couche agrégation. Si vous modifiez le mappage ultérieurement sur la passerelle bidirectionnelle pour les serveurs d'objets de couche agrégation, vous devez répliquer ces modifications ici.

```
REPLICATE ALL FROM TABLE 'precision.entity_service'
USING MAP 'EntityServiceMap'
INTO 'precision.entity_service';

REPLICATE ALL FROM TABLE 'precision.service_details'
USING MAP 'ServiceDetailsMap'
INTO 'precision.service_details';
```

5. Supprimez tous les événements Network Manager précédents de la table alerts.status sur les serveurs d'objets. Utilisez la commande SQL appropriée pour supprimer les événements. Pour plus d'informations, reportez-vous à la documentation Tivoli Netcool/OMNIbus à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_7.4.0/com.ibm.netcool_OMNIbus.doc_7.4.0/omnibus/wip/admin/concept/omn_adm_sql_objservsqlcommands.html.
6. Redémarrez les passerelles de serveur d'objets.
7. Redémarrez les processus **ncp**.

Modification du nom de la source de données de l'interface graphique Web Tivoli Netcool/OMNIbus

Pour vous connecter à une autre source de données interface graphique Web que celle indiquée lors de l'installation, modifiez le nom de source de données.

Pour vous connecter à une autre source de données que celle indiquée lors de l'installation :

1. Modifiez le fichier `NCHOME/etc/precision/ModelNcimDb.cfg`.
2. Définissez la propriété m_WebTopDataSource en lui attribuant le nom de la nouvelle source de données.
3. Relancez le processus ncp_model.

Sources de données de l'interface graphique Web Tivoli Netcool/OMNIbus :

Une source de données désigne un serveur ObjectServer ou une paire de reprise en ligne ObjectServer utilisée par interface graphique Web pour des informations d'événements.

L'interface graphique Web Tivoli Netcool/OMNIbus était appelée Netcool/Webtop dans les versions 2.2 et antérieures. Certains déploiements contiennent de nombreux serveurs ObjectServers, et l'interface graphique Web peut contenir des événements provenant de divers serveurs ObjectServer. Lors de l'installation, vous ne pouvez configurer interface graphique Web que pour une seule source de données. Après l'installation, il se peut que vous ayez besoin de modifier cette source de données ou d'ajouter de nouvelles sources.

Sources de données et topologie de réseau

Pour afficher l'état des unités, les vues de réseau et de tronçon font correspondre l'enregistrement de topologie d'une unité avec tous les événements relatifs à cette unité. Pour effectuer cette corrélation, les applications Web doivent avoir accès au nom de chaque source de données utilisée par l'interface graphique Web.

Sources de données et base de données NCIM

Les informations sur les sources de données de l'interface graphique Web sont stockées dans la table ncim.domainMgr de la base de données topologiques NCIM.

Pour plus d'informations sur la configuration des sources de données de l'interface graphique Web, voir *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*.

Configuration des types d'événement de topologie pour la liste des événements actifs

Pour que vous puissiez intégrer les vues de topologie et les vues de liste des événements actifs filtrées, le nom et le type de la vue doivent correspondre. Si vous changez les valeurs par défaut dans la liste des événements actifs, vous devez configurer le nom et le type dans Network Manager.

Dans une vue de liste des événements actifs filtrée, vous pouvez configurer le nom et le type de la vue. Si vous changez le nom et le type de la vue et remplacez les valeurs par défaut `Default` et `global`, la liste des événements actifs ne peut pas communiquer avec les Vues de réseau et les outils accessibles via un clic avec le bouton droit de la souris.

Si les valeurs par défaut ont été changées, vous devez changer les valeurs sur le serveur Network Manager pour qu'elles correspondent.

Pour éditer le nom et le type de la vue utilisés pour la communication avec la liste des événements actifs, procédez comme suit :

1. Sauvegardez et éditez le fichier `topoviz.properties`.
2. Changez les valeurs des propriétés suivantes :

```
# AEL view descriptions.
topoviz.webtop.view.name=Default
topoviz.webtop.view.type=global
```

Ajout de zones d'événement

Pour utiliser Tivoli Netcool/OMNIbus version 7.1, vous devez ajouter des zones de base de données supplémentaires à la table alerts.status ainsi qu'à chaque fichier de mappe de passerelle Tivoli Netcool/OMNIbus.

Conseil : Cette tâche est inutile si vous utilisez Tivoli Netcool/OMNIbus version 7.2 ou suivante.

Les zones requises sont les suivantes :

NmosDomainName
Nom du domaine Network Manager gérant l'événement. Par défaut, cette zone n'est renseignée que pour les événements générés par les interrogations Network Manager. Pour renseigner cette zone pour d'autres sources d'événement telles que celles des analyses Tivoli Netcool/OMNIbus, vous devez modifier les fichiers de règle.

NmosEntityId
ID numérique unique identifiant l'entité de topologie à laquelle est associé l'événement. Cette zone est similaire à la zone NmosObjInst mais fournit des informations plus détaillées. Par exemple, elle peut inclure l'ID d'une interface d'un périphérique.

NmosManagedStatus
Statut géré de l'entité réseau pour laquelle l'événement a été mis au premier plan. Lorsqu'une entité réseau n'est pas gérée, les interrogations Network Manager sont interrompues et les événements des autres sources sont référencés comme non gérés. Cette zone permet de filtrer les événements des entités non gérées.

BSM_Identity
Identificateur unique de la ressource à partir de laquelle l'événement est émis et qui permet de corréler ce dernier à cette ressource dans IBM Tivoli Business Service Manager (TBSM).

NmosEventMap
Nom de la mappe d'événements et priorité facultative de l'événement, qui indique comment Network Manager doit traiter l'événement (par exemple, PrecisionMonitorEvent.910). Le numéro de priorité facultative peut être concaténé à la fin de la valeur, précédé d'un point (.). Si la priorité n'est pas spécifiée, la valeur 0 lui est affectée.

Remarque : Cette valeur peut être remplacée par une insertion explicite de la table config.precedence de la passerelle d'événements, qui fournit les mêmes données.

Pour ajouter ces zones à la table de base de données alert.status, exécutez le script SQL suivant pour chaque ObjectServer de votre déploiement :

- UNIX

```
$NCHOME/omnibus/bin/nco_sql -server nom_objectserver -user nom_utilisateur -password
mot_de_passe < $NCHOME/precision/scripts/ncp_configure_omnibus.sql
```

- Windows

```
"%NCHOME%\omnibus\bin\isql.bat" -S nom_objectserver -U nom_utilisateur -P
mot_de_passe -i
"%NCHOME%\precision\scripts\ncp_configure_omnibus.sql"
```

Pour plus d'informations sur l'administration Tivoli Netcool/OMNIbus, consultez le *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Installation et configuration d'analyses

Si vous n'avez pas installé Tivoli Netcool/OMNIbus en tant qu'élément de l'installation Network Manager, et que vous utilisez une installation Tivoli Netcool/OMNIbus existante, vous devez configurer certaines analyses.

Pour vérifier que votre installation Tivoli Netcool/OMNIbus reçoit des événements depuis le réseau, configurez les analyses Tivoli Netcool/OMNIbus correspondantes. Installez et configurez au moins l'analyse SNMP (ou analyse mttrapd). Vous pouvez utiliser le script **ConfigOMNI**. Pour plus d'informations, voir «Configuration d'une installation Tivoli Netcool/OMNIbus existante», à la page 57.

Pour plus d'informations sur l'installation et la configuration d'une sonde, consultez le guide de référence de la sonde appropriée dans le Centre de documentation à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/common/kc_welcome-444.html.

Installation de Knowledge Library

Si vous n'avez pas installé Tivoli Netcool/OMNIbus en tant qu'élément de l'installation Network Manager, et que vous utilisez une installation Tivoli Netcool/OMNIbus existante, vous devez installer Netcool/OMNIbus Knowledge Library.

Netcool/OMNIbus Knowledge Library est un ensemble de fichiers de règles écrits selon une valeur standard commune et disponibles via l'installation de Tivoli Netcool/OMNIbus. Vous pouvez utiliser le script **ConfigOMNI** pour installer la bibliothèque. Voir «Options de ligne de commande ConfigOMNI», à la page 60.

Pour plus d'informations, voir Netcool/OMNIbus Knowledge Library Release Notes.

Référence d'intégration Tivoli Netcool/OMNIbus

Consultez les informations sur les paramètres pour une interaction supplémentaire entre Network Manager et Tivoli Netcool/OMNIbus.

catégories d'événement Network Manager :

Les événements émis par Network Manager sont classés en deux catégories : événements sur le réseau surveillé et événements sur les processus Network Manager.

Ces événements sont enregistrés sur le serveur ObjectServer Tivoli Netcool/OMNIbus. Sonde pour Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) permet de traiter et de transmettre les données d'événement à la table alerts.status du serveur ObjectServer.

La figure suivante présente le flux d'événements entre Network Manager et le serveur ObjectServer.

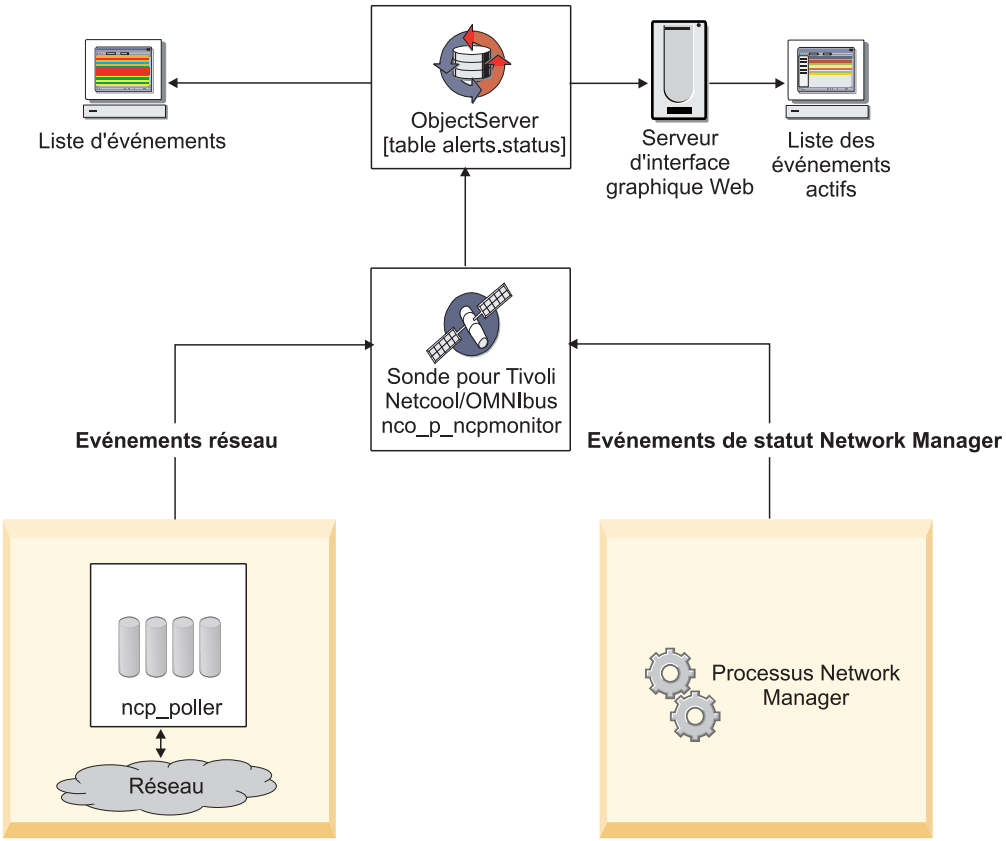

Figure 9. Flux des événements entre Network Manager etTivoli Netcool/OMNIbus

Evénements réseau Network Manager :

Le moteur d'interrogation, **ncp_poller**, génère des événements sur l'état du réseau. Ces événements permettent d'identifier les problèmes réseau et sont configurables à l'aide de l'interface graphique d'interrogation de réseau (sélectionnez **Administration** > **Réseau** > **Interrogation de réseau**). Ces événements sont appelés événements réseau et ont la valeur `ITNM Monitor` pour la zone alerts.status AlertGroup.

Chaque événement réseau est émis sur une seule entité, telle une interface ou un boîtier. Les données d'événement dépendent du type d'interrogation. Lorsque les événements réseau sont transmis à ObjectServer pour être insérés dans la table alerts.status, une valeur AlertGroup égale à `ITNM Monitor` leur est affectée.

Un ensemble d'identificateurs illimité est disponible pour les événements réseau. La valeur EventID de `NmosSnmpPollFail` de la table alerts.status est allouée aux événements générés lors de l'échec d'une interrogation SNMP.

Les événements réseau du serveur ObjectServer sont transmis à Network Manager via la passerelle d'événements pour effectuer un enrichissement d'événements, y compris l'analyse origine du problème.

Référence associée:

«Zones de la table alerts.status utilisées par Network Manager», à la page 196
La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Evénements d'état Network Manager :

Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Lorsque ces événements de statut sont transmis à ObjectServer pour être insérés dans la table alerts.status, une valeur AlertGroup égale à `ITNM Status` leur est affectée.

Types d'événements de statut

Un ensemble d'identificateurs d'état est utilisé pour identifier les événements de statut Network Manager par type. La liste suivante identifie les valeurs EventId qui sont insérées dans la table alerts.status et décrit comment chaque événement de statut leur étant associé est généré.

ItnmDatabaseConnection
Ce type d'événement est généré pour indiquer la perte de connexion à NCIM. Cet événement est généré par l'unité d'exécution d'interrogation de statut géré dans le processus **`ncp_model`**. L'émission de cet événement dépend de la période configurée dans l'intervalle d'interrogation de statut géré du modèle. Un problème est émis lorsque la connexion est perdue et un événement de résolution correspondant est émis lors de la restauration de la connexion ou au démarrage afin que toute erreur provenant d'opérations précédentes soit supprimée. Ce type d'événement permet l'utilisation du domaine de sauvegarde lorsque la reprise en ligne est configurée. Le processus de domaine virtuel réagit à cet événement, comme cela est défini dans le filtre pour NCIM dans le fichier `NCHOME/etc/precision/VirtualDomainSchema.cfg`.

ItnmDiscoAgentStatus
Ce type d'événement est généré par le processus **`ncp_disco`** lorsqu'un agent de reconnaissance passe à un nouvel état. A la fin d'une reconnaissance, un événement d'information est transmis à ObjectServer, pour chaque agent utilisé au cours de la reconnaissance.

Vous pouvez utiliser ces informations pour identifier l'état de chaque agent. Dans la table alerts.status, la zone LocalPriObj est utilisée pour stocker le nom de l'agent.

Les événements liés aux agents de reconnaissance dans ObjectServer sont écrasés lorsqu'une autre reconnaissance est exécutée.

ItnmDiscoFinderStatus

Ce type d'événement est généré par le processus **ncp_disco** lorsqu'un outil de recherche de reconnaissance passe à un nouvel état. A la fin d'une reconnaissance, un événement d'information est transmis à ObjectServer, pour chaque outil de recherche utilisé au cours de la reconnaissance.

Vous pouvez utiliser ces informations pour identifier quels outils de recherche sont exécutés et quel est leur état. Dans la table alerts.status, la zone LocalPriObj est utilisée pour stocker le nom de l'outil de recherche.

Les événements liés aux outils de recherche de reconnaissance dans ObjectServer sont écrasés lorsqu'une autre reconnaissance est exécutée.

ItnmDiscoPhase

Ce type d'événement est généré par le processus **ncp_disco** lorsque le processus de reconnaissance passe à une nouvelle phase. A la fin de la reconnaissance, cinq événements d'information doivent être générés dans ObjectServer pour afficher les transitions en boucle de la phase 0 (veille) aux phases 1, 2 et 3 (collecte des données) à la phase -1 (traitement des données). Un événement est généré pour chacun des changements de phase suivants dans le cadre d'une reconnaissance unique :

- 0 à 1
- 1 à 2
- 2 à 3
- 3 à -1
- -1 à 0

Vous pouvez utiliser ces informations pour déterminer la durée de chaque phase. Dans la table alerts.status, la zone LocalPriObj est utilisée pour stocker la phase dans laquelle entre la reconnaissance et la zone LocalSecObj sert à stocker la phase précédente de la reconnaissance.

Conseil : Les valeurs de chaîne des phases sont également affichées dans le fichier journal de reconnaissance lorsque le processus **ncp_disco** est exécuté en mode débogage.

Les événements liés aux phases de la reconnaissance dans ObjectServer sont écrasés lorsqu'une autre reconnaissance est exécutée.

ItnmDiscoStitcherStatus

Le processus de reconnaissance est composé d'une étape de collecte et d'une étape de traitement des données, pendant lesquelles la topologie est créée. Les événements ItnmDiscoStitcherStatus sont générés par le moteur de reconnaissance, **ncp_disco**, lorsqu'une phase majeure est atteinte dans l'étape de traitement des données. A la fin d'une reconnaissance, un événement d'information est transmis à ObjectServer, pour chaque programme stitcher de reconnaissance principal utilisé au cours de la reconnaissance.

Vous pouvez utiliser ces informations pour identifier à quelle étape le traitement de la reconnaissance se trouve. Dans la table alerts.status, la zone LocalPriObj est utilisée pour stocker le nom du programme stitcher correspondant à cette étape.

Les événements ItnmDiscoStitcherStatus se produisent lors de l'exécution des programmes stitcher suivants :

- BuildFinalEntityTable
- BuildContainment

- BuildLayers
- MergeLayers
- PostLayerProcessing

Les événements suivants se produisent lors de l'étape de création de la topologie au cours de l'exécution des programmes stitcher ci-dessous.

- CreateScratchTopology
- PostScratchProcessing
- SendTopologyToModel

Les événements liés aux programmes stitcher de reconnaissance dans ObjectServer sont écrasés lorsqu'une autre reconnaissance est exécutée.

ItnmEntityCreation

S'il est configuré dans le fichier `$NCHOME/etc/precision/ModelSchema.cfg`, ce type d'événement d'information est généré par le processus **ncp_model**, pour chaque nouvelle entité de boîtier ou d'interface IP (EntityType = 1) insérée dans la base de données NCIM.

Vous pouvez configurer le fichier `ModelSchema.cfg` en affectant la valeur 1 à la colonne RaiseEntityEvent dans l'instruction INSERT pour la table model.config. Par exemple :

```
create table model.config
(
LingerTime int not null primary key,          // default value 3 (discoveries)
RaiseEntityEvent int type boolean not null,   // default value 0 ( off )
DiscoveryUpdateMode int not null,             // default value 0 - full discovery,
                                              //               1 - partial
unique(LingerTime)
);
insert into model.config values (3, 1, 0);
```

Remarque : Pour que les modifications apportées à la configuration soient appliquées et que les événements soient activés, le processus **ncp_model** doit être redémarré. Le processus lit les paramètres de configuration au moment du démarrage.

ItnmEntityDeletion

S'il est configuré dans le fichier `$NCHOME/etc/precision/ModelSchema.cfg`, ce type d'événement d'information est généré par le processus **ncp_model**, pour chaque entité de boîtier ou d'interface IP (EntityType = 1) supprimée de la base de données NCIM.

Vous pouvez configurer le fichier `ModelSchema.cfg` en affectant la valeur 1 à la colonne RaiseEntityEvent dans l'instruction INSERT pour la table model.config, comme décrit précédemment pour l'ID d'événement ItnmEntityCreation.

ItnmFailover

Ce type d'événement est généré par le processus **ncp_virtualdomain** lorsqu'un domaine Network Manager d'une paire de reprise en ligne effectue une reprise en ligne ou une reprise par restauration.

Un événement de problème est généré lorsqu'une reprise en ligne est effectuée et un événement de résolution est généré lorsqu'une reprise par restauration est effectuée.

Dans la table alerts.status, la description de la zone Récapitulatif indique si le domaine est un domaine principal ou de secours et s'il est actif ou en veille.

ItnmFailoverConnection

Ce type d'événement est généré par le processus **ncp_virtualdomain** pour

indiquer le moment où le domaine de secours d'une paire de reprise en ligne se connecte ou se déconnecte du domaine principal.

Lorsque Network Manager est exécuté en mode de reprise en ligne, un événement de résolution est généré lorsque les domaines principal et de secours configurent leur connexion socket TCP. Cette connexion est requise pour transférer les mises à jour de topologie depuis le domaine principal car le processus de reconnaissance (**ncp_disco**) ne s'exécute pas dans le domaine de secours. Si la connexion est perdue ultérieurement, un événement de problème est généré.

Remarque : L'état de la connexion ne détermine pas le déclenchement de la reprise en ligne. Cette dernière est déclenchée uniquement lorsque des événements de vérification d'intégrité sont transférés (via ObjectServer) d'un domaine à l'autre, à condition qu'une connexion socket ait été configurée à un moment donné.

ItnmHealthChk

Les événements de vérification d'intégrité gouvernent la reprise en ligne de Network Manager. Chaque domaine de la paire de reprise en ligne génère des événements de résolution de la vérification d'intégrité tant que ce domaine est intègre (en bonne santé).

Les événements de problème de vérification d'intégrité pour un domaine peuvent être générés de deux manières :

- Par le domaine local, lorsqu'il détecte une reprise en ligne de l'un de ses processus, tel que configuré dans le fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg`.
- Par le domaine distant lorsqu'un domaine détecte qu'un autre domaine n'a pas généré d'événement de résolution de vérification d'intégrité dans le temps imparti et qu'un événement de problème de vérification d'intégrité synthétique est généré au nom du domaine distant.

Lorsqu'un événement de problème de vérification d'intégrité est généré pour le domaine principal, une reprise en ligne est lancée et le domaine de secours devient actif.

Auparavant, une valeur EventID égale à NcpHealthChk était affectée aux événements de vérification d'intégrité. Pour la compatibilité avec les versions antérieures de Network Manager, vous pouvez remplacer ItnmHealthChk par NcpHealthChk dans le fichier de règles d'analyse.

Remarque : Les événements de vérification d'intégrité sont gérés par la passerelle d'événements Network Manager qui requiert que la valeur Noeud corresponde au domaine auquel l'événement fait référence. Il n'est pas nécessaire qu'il s'agisse du domaine générant l'événement puisqu'un domaine peut générer des événements d'échec au nom de l'autre domaine.

ItnmMaintenanceState

S'il est configuré dans le fichier `$NCHOME/etc/precision/ModelSchema.cfg`, ce type d'événement est généré par le gestionnaire de topologie, **ncp_model**, pour les modifications d'état de maintenance apportées à un boîtier ou à une interface IP.

Vous pouvez configurer `ModelSchema.cfg` en affectant la valeur `1` à la colonne RaiseEntityEvent dans l'instruction INSERT pour la table model.config, comme décrit précédemment pour l'événement ItnmEntityCreation.

Un événement de problème est généré lorsqu'une entité de boîtier ou d'interface IP est en maintenance et un événement de résolution est généré lorsque l'entité n'est plus en maintenance.

Remarque : Un événement d'interface individuel est envoyé uniquement si la modification ne s'applique pas au niveau du boîtier. Lorsqu'un périphérique est modifié, un événement de boîtier et une série d'événements d'interface ne sont pas générés collectivement.

ItnmServiceState

Ce type d'événement est généré lorsqu'un processus démarre ou se termine. Il indique si le démarrage ou l'arrêt d'un processus n'a pas abouti au cours de l'exécution. (Il faut noter que les événements de statut de processus ne sont pas générés lorsque les processus sont stoppés lorsque le système est arrêté.)

Un événement de résolution est généré lorsque la commande **ncp_ctrl** démarre un processus. Si le démarrage d'un processus échoue ou si il s'arrête au cours de l'exécution, un événement de problème est généré.

Dans la table alerts.status, la description de la zone Récapitulatif comporte le nom du processus, l'identificateur de produit et mentionne si le processus :

- a démarré (et s'il s'est correctement initialisé),
- s'est arrêté (c'est-à-dire si il a été supprimé de la table de base de données **ncp_ctrl** appelée services.inTray),
- est terminé (c'est-à-dire s'il s'est arrêté mais sera redémarré par la commande **ncp_ctrl**),
- n'a pas pu démarrer,
- a échoué mais ne sera pas redémarré (c'est-à-dire s'il s'est arrêté et que le nombre de tentatives configuré pour ce processus a été dépassé).

ItnmTopologyUpdated

Ce type d'événement d'information est généré par le processus **ncp_model** lorsque la mise à jour de la base de données de topologie NCIM est terminée à la fin du cycle de reconnaissance. Cette information est utile si vous avez l'intention de programmer l'exécution de scripts ou de programmes après la mise à jour de la base de données NCIM.

Remarque : Si l'option de retour est activée, ou si des commandes PING sont envoyées à de grands sous-réseaux, il peut y avoir plusieurs cycles de reconnaissance et donc plusieurs événements de ce type (un événement par cycle de reconnaissance). Pour déterminer si la reconnaissance est finalement terminée, la requête OQL suivante peut être envoyée au service Outil de recherche PING :

```
select * from pingFinder.status where m_Completed <> 1;
```

Cette requête recherche tous les sous-réseaux vers lesquels l'outil de recherche PING continue à envoyer des commandes PING. Si aucun balayage PING n'est encore en cours et que la reconnaissance est en phase 0, cela signifie que la reconnaissance est terminée.

Concepts associés:

«A propos de la reprise en ligne», à la page 308
Dans votre environnement Network Manager, une architecture de reprise en ligne peut être utilisée pour configurer votre système pour une haute disponibilité, en minimisant l'impact d'un incident matériel ou réseau.

Tâches associées:

«Activation de la reprise en ligne», à la page 308
Vous pouvez activer la reprise en ligne dans votre environnement Network Manager afin de garantir que les différents composants sont en cours d'exécution et disponibles.

Référence associée:

«Zones de la table alerts.status utilisées par Network Manager», à la page 196
La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Configuration de la Sonde pour Tivoli Netcool/OMNIbus :

La Sonde pour Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) acquiert et traite les événements générés par les processus et les interrogations Network Manager et transmet ces événements au serveur ObjectServer.

La Sonde pour Tivoli Netcool/OMNIbus est installée dans le répertoire `$NCHOME/probes/arch`, où *arch* représente un répertoire de système d'exploitation. Vous pouvez configurer la sonde en utilisant ses fichiers de configuration, qui sont présentés ci-dessus.

- Fichier de propriétés : `nco_p_ncpmonitor.props`
- Fichier de règles : `nco_p_ncpmonitor.rules`

Remarque : Le fichier exécutable (ou commande **nco_p_ncpmonitor**) pour la sonde est également installé dans le répertoire `$NCHOME/probes/arch`. Toutefois, la sonde est configurée pour s'exécuter par défaut sous le contrôleur de processus de domaine. De plus, la commande **nco_p_ncpmonitor** doit être exécutée uniquement à des fins de traitement des incidents.

Les événements émis dans Network Manager sont spécifiques au domaine. Lorsque Network Manager s'exécute en mode de reprise en ligne, la sonde utilise par défaut le nom de domaine virtuel, à condition que le nom soit configuré dans le fichier `$NCHOME/etc/precision/ConfigItnm.cfg`.

Pour plus d'informations sur les concepts de sonde, voir le document *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation Tivoli Netcool/OMNIbus à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Tâches associées:

«Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg», à la page 345
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

A propos du fichier nco_p_ncpmonitor.props :

Le fichier `$NCHOME/probes/arch/nco_p_ncpmonitor.props` définit l'environnement dans lequel s'exécute le programme Sonde pour Tivoli Netcool/OMNIbus.

Le fichier de propriétés est constitué de paires nom-valeur séparées par un signe deux-points. Le fichier de propriétés par défaut répertorie un sous-ensemble de propriétés prises en charge par l'analyse. Ces propriétés sont mises en commentaire à l'aide d'un signe numéro (#) placé en début de ligne. L'ensemble standard de propriétés d'analyse communes, applicables pour la version de Tivoli Netcool/OMNIbus en cours d'exécution, peut être spécifié pour le programme Sonde pour Tivoli Netcool/OMNIbus, le cas échéant.

Une pratique suggérée pour la modification des valeurs par défaut des propriétés consiste à ajouter une ligne nom-valeur pour chaque propriété requise au bas du fichier. Pour spécifier une propriété, vérifiez que la ligne n'est pas mise en commentaire et modifiez ensuite la valeur comme il convient. Les valeurs de chaîne doivent être placées entre guillemets ; ce n'est pas nécessaire pour les autres types de valeur. Par exemple :

```
Server            :    "VIRTUAL"
RulesFile         :    "$NCHOME/probes/solaris2/nco_p_ncpmonitor.rules"
Buffering         :    1
BufferSize        :    15
```

Pour le traitement des incidents, vous pouvez configurer les propriétés d'analyse à partir de la ligne de commande en exécutant la commande **nco_p_ncpmonitor** avec les options de ligne de commande appropriées.

Pour plus d'informations sur les propriétés communes des analyses, voir *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation de Tivoli Netcool/OMNIbus à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

A propos du fichier nco_p_ncpmonitor.rules :

Le fichier `$NCHOME/probes/arch/nco_p_ncpmonitor.rules` définit comment la Sonde pour Tivoli Netcool/OMNIbus doit traiter les données d'événement Network Manager pour créer un événement Tivoli Netcool/OMNIbus porteur de sens.

Référence de configuration nco_p_ncpmonitor.rules :

Le fichier de règles mappe les données d'événement Network Manager vers les zones ObjectServer et peut être utilisé pour personnaliser le comportement de la sonde. Pour la configuration du fichier de règles, il est nécessaire de maîtriser la syntaxe des règles de sonde Tivoli Netcool/OMNIbus.

La sonde utilise des jetons et des éléments et applique des règles pour transformer les données source d'événement Network Manager en un format connu du serveur ObjectServer. Les données source d'événement brutes sont converties en jetons, qui sont ensuite analysés en éléments. Le fichier de règles permet d'effectuer le traitement conditionnel des éléments puis de mapper ces derniers vers les zones alerts.status du serveur ObjectServer. Dans le fichier de règles, les éléments sont identifiés par le symbole $ et les zones alerts.status par le symbole @. La configuration du fichier de règles mappe les éléments vers des zones, comme cela est présenté dans le code exemple suivant :

```
@Summary=$Description
```

Dans cet exemple, @Summary identifie la zone alerts.status et $Description identifie la zone d'entrée Network Manager.

Lorsque la zone ExtraInfo de Network Manager est utilisée avec des zones imbriquées pour enregistrer des données supplémentaires sur des entités (par exemple, ExtraInfo->ifIndex), ces zones sont disponibles au format suivant dans le fichier de règles :

```
$ExtraInfo_variable
```

où *variable* représente une variable MIB (Management Information Base), telle ifIndex ou d'autres données (par exemple, des noms de colonne dans des tables NCIM). Les variables MIB sont spécifiées à la fois en minuscules et majuscules et les autres données en majuscules. Par exemple :

```
$ExtraInfo_ifIndex
$ExtraInfo_MONITOREDENTITYID
```

Pour configurer le fichier de règles pour la Sonde pour Tivoli Netcool/OMNIbus, il est nécessaire de connaître :

- les données source d'événement Network Manager disponibles pour être utilisées dans le fichier de règles de sonde
- l'ensemble de zones alerts.status pouvant être chargées avec les données d'événement de Network Manager
- le mappage des données entre Network Manager et les zones alerts.status

Pour plus d'informations sur la syntaxe utilisée dans les fichiers de règles de sonde, voir le document *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* dans le centre de documentation Tivoli Netcool/OMNIbus à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Exemple de traitement de fichier de règles :

Cet exemple présente comment les données source de Network Manager sont traitées par le fichier de règles afin de générer les données de sortie insérées dans la table alerts.status.

L'exemple de code suivant présente un enregistrement de données d'événement Network Manager transmis à la Sonde pour Tivoli Netcool/OMNIbus pour traitement. Dans cet enregistrement, un événement de résolution a été créé lors du démarrage du processus **ncp_store** par **ncp_ctrl**.

```
{
 EventName='ItnmServiceState';
 Severity=1;
 EntityName='BACKUP';
 Description='ncp_store process [15299] has started';
 ExtraInfo={
  EVENTTYPE=2;
  SOURCE='ncp_ctrl';
  ALERTGROUP='ITNM Status';
  EVENTMAP='ItnmStatus';
  SERVICE='ncp_store';
  PID=15299;
  };
}
```

L'extrait suivant du fichier de règles de sonde présente la syntaxe utilisée pour le traitement et le mappage de ces zones d'entrée vers des zones alerts.status :

```
...
    #
    # populate some standard fields
    #
    @Severity = $Severity
    @Summary = $Description
    @EventId = $EventName
    @Type = $ExtraInfo_EVENTTYPE
    @AlertGroup = $ExtraInfo_ALERTGROUP
    @NmosEventMap = $ExtraInfo_EVENTMAP
    @Agent = $ExtraInfo_SOURCE

    if (exists($ExtraInfo_ACCESSIPADDRESS))
    {
        @Node = $ExtraInfo_ACCESSIPADDRESS
    }
    else
    {
        @Node = $EntityName
    }

    #
    # Stamp the event with the name of its originating domain
    #
    @NmosDomainName = $Domain
    @Manager = "ITNM"
    @Class = 8000

    #
    # populate fields for RCA
    #
    @LocalNodeAlias = @Node

...

    #
    # Now set the AlertKey and Identifier
    #
    if (match(@AlertGroup, "ITNM Status"))
    {
        switch ($EventName)
        {
            case ...
...
            case "ItnmServiceState":
                @LocalPriObj = $ExtraInfo_SERVICE
...
            case ...
....
        }
    }

    #
    # Both the Identifier and the AlertKey contain the domain name. This ensures
    # that in a multi-domain setup, events are handled on a per-domain basis
    #

    #
    # Include the LocalPriObj in the AlertKey or the link-downs on
    # all interfaces will cleared by a link-up on any interface
    #
    @AlertKey = $EntityName + @LocalPriObj + "->" + $EventName + @NmosDomainName

    #
    # Set up deduplication identifier and include the LocalPriObj
    # so we can correctly handle de-duplication of events raised on interfaces
    #
    @Identifier = $EntityName + @LocalPriObj + "->" + $EventName + @Type + @NmosDomainName
}
```

Une fois le traitement du fichier de règles terminé, les données de sortie transmises au serveur ObjectServer ont la forme suivante :

```
CMonitorProbeApp::ProcessStatusEvent
{
 AlertGroup='ITNM Status';
 EventId='ItnmServiceState';
 Type=2;
```

```
 Severity=1;
 Summary='ncp_store process [15299] has started';
 Node='BACKUP';
 NmosDomainName='PRIMARY';
 LocalNodeAlias='BACKUP';
 LocalPriObj='ncp_store';
 LocalRootObj='';
 RemoteNodeAlias='';
 AlertKey='BACKUPncp_store->ItnmServiceStateVIRTUAL';
 Identifier='BACKUPncp_store->ItnmServiceState2VIRTUAL';
 Class=8000;
 Agent='ncp_ctrl';
 LastOccurrence=1267122089;
}
```

En fonction du traitement du fichier de règles présenté dans cet exemple, vous pouvez voir que les zones d'entrée Network Manager sont associées aux zones alerts.status de la manière suivante :

Zone Network Manager	Zone de la table alerts.status
EventName	EventId
Severity	Severity
EntityName	Node
Description	Summary
ExtraInfo->EVENTTYPE	Type
ExtraInfo->SOURCE	Agent
ExtraInfo->ALERTGROUP	AlertGroup
ExtraInfo->EVENTMAP	NmosEventMap
ExtraInfo->SERVICE	LocalPriObj

Référence associée:

«Zones de la table alerts.status utilisées par Network Manager», à la page 196
La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Zones des données d'événement Network Manager :

Lorsque des événements sont générés dans Network Manager, les données associées sont insérées dans un certain nombre de zones (ou colonnes) dans les tables Network Manager. Bien que chaque événement n'utilise qu'un sous-ensemble des zones possibles, un certain nombre de zones sont communes à tous les types d'événement.

Le tableau suivant répertorie tous les noms des zones Network Manager pouvant être utilisées dans le fichier de règles d'analyse et décrit les données d'événement stockées dans chaque zone. Il identifie également les zones Network Manager communes à tous les événements et donc toujours disponibles dans le fichier de règles.

Tableau 16. Zones Network Manager qui renseignent les événements

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
Description	Courte description de l'événement.	Oui

Tableau 16. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
Domaine	Domaine en cours. Si Network Manager est configuré pour le mode de reprise en ligne, cela correspond au domaine principal.	Oui (à condition que le fichier de mappe ne soit pas modifié)
EntityName	Pour les événements de réseau, il s'agit de la zone entityName de la table entityData NCIM pour l'entité par rapport à laquelle l'événement est émis. En ce qui concerne les événements de statut, il s'agit toujours du nom du domaine à propos duquel l'événement est généré.	Oui
EventName	Identificateur de l'événement. Par exemple, ItnmDiscoPhase.	Oui
ExtraInfo_ACCESSIPADDRESS	Si l'entité de noeud principal ou d'interface identifiée par la zone d'entrée EntityName comporte une adresse IP accessible directement (zone accessIPAddress provenant des tables de l'interface ou du boîtier NCIM), elle est indiquée ici. Applicable aux événements de réseau uniquement.	Non
ExtraInfo_AGENT	Agent responsable d'un événement d'agent de reconnaissance (ItnmDiscoAgentStatus).	Oui (pour les événements ItnmDiscoAgentStatus)
ExtraInfo_ALERTGROUP	Groupe d'alerte de l'événement. En ce qui concerne les événements de statut Network Manager, le groupe d'alerte est `ITNM Status` et en ce qui concerne les événements de réseau, la valeur est `ITNM Monitor`.	Oui
ExtraInfo_ENTITYCLASS	Nom de classe affecté à l'entité, tel qu'identifié dans les tables NCIM entityClass et classMembers.	Oui (pour les événements de réseau et ItnmEntityCreation)
ExtraInfo_ENTITYTYPE	Type de l'entité, tel que défini dans la table NCIM entityType.	Oui (pour les événements de réseau)
ExtraInfo_LocalPriObj	Fournit une valeur pour la zone LocalPriObj dans l'enregistrement alerts.status. Cette zone a la même valeur que la zone dépréciée ExtraInfo_EventSnmpIndex, sauf qu'elle est précédée par l'identificateur pour l'entité MIB interrogée ; par exemple ifEntry, bgpPeerEntry.	Oui (pour les événements de réseau)
ExtraInfo_EVENTTYPE	Type de l'événement émis par Network Manager. Les valeurs sont les suivantes : • 1 : Problème • 2 : Résolution • 13 : Information	Oui
ExtraInfo_FINDER	L'outil de recherche responsable de l'événement d'outil de recherche de reconnaissance (ItnmDiscoFinderStatus).	Oui (pour les événements ItnmDiscoFinderStatus)

Tableau 16. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
ExtraInfo_ifIndex	En ce qui concerne les événements émis par rapport à une interface comportant une valeur ifIndex dans la table d'interface NCIM, cette valeur est indiquée ici. Applicable uniquement aux événements de réseau par rapport aux interfaces.	Non
ExtraInfo_IFALIAS	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifAlias, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFDESCR	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifDescr, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFNAME	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la valeur ifName, si elle est connue. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_IFTYPESTRING	En ce qui concerne les événements émis par rapport aux interfaces, cette zone contient la représentation de chaîne de la valeur ifType. Applicable uniquement aux interrogations d'interface.	Non
ExtraInfo_MAINNODEADDRESS	Interface de gestion du noeud principal contenant l'entité, telle qu'identifiée par la zone accessIPAddress de la table de boîtier NCIM. Applicable uniquement aux événements de réseau et ItnmEntityCreation.	Oui (pour les événements de réseau)
ExtraInfo_MAINNODEENTITYID	La zone entityId de la table entityData NCIM pour le noeud principal, tel qu'identifié par la zone accessIPAddress de la table de boîtier NCIM. Applicable uniquement aux événements de réseau.	Oui (pour les événements de réseau)
ExtraInfo_MAINNODEENTITYNAME	Zone entityName de la table entityData NCIM pour le noeud principal, telle qu'identifiée dans NCIM. Applicable uniquement aux événements de réseau.	Oui (pour les événements de réseau)
ExtraInfo_MONITOREDENTITYID	Zone entityId de la table entityData NCIM pour l'entité par rapport à laquelle l'événement est émis. Applicable uniquement aux événements de réseau et ItnmEntityCreation.	Non
ExtraInfo_MONITOREDINSTID	Enregistrement contenu dans la table ncpolldata.monitoredInstance.	Non
ExtraInfo_NEWPHASE	Phase de reconnaissance qui a démarré. Applicable uniquement aux événements de phase de reconnaissance (ItnmDiscoPhase).	Oui (pour les événements de phase de reconnaissance)
ExtraInfo_OLDPHASE	Phase de reconnaissance terminée. Applicable uniquement aux événements de phase de reconnaissance (ItnmDiscoPhase).	Oui (pour les événements de phase de reconnaissance)
ExtraInfo_POLICYNAME	Nom de la règle d'interrogation ayant entraîné l'événement.	Oui (pour les événements de réseau)

Tableau 16. Zones Network Manager qui renseignent les événements (suite)

Nom de zone Network Manager	Contenu de zone	Toujours disponible ?
ExtraInfo_PID	ID de processus du service Network Manager affecté. Applicable uniquement aux événements ItnmServiceState.	Oui (pour les événements d'état de service)
ExtraInfo_REMOTEDOMAIN	Nom du domaine distant. Applicable uniquement aux événements ItnmFailoverConnection.	Oui (pour les événements de connexion de reprise en ligne)
ExtraInfo_sysContact	Si disponible, la valeur sysContact est fournie uniquement pour les événements ItnmEntityCreation.	Non
ExtraInfo_sysLocation	Si disponible, la valeur sysLocation est fournie uniquement pour les événements ItnmEntityCreation	Non
ExtraInfo_sysObjectId	Si disponible, la valeur sysObjectId est fournie uniquement pour les événements ItnmEntityCreation	Non
ExtraInfo_SERVICE	Nom du service Network Manager affecté. Applicable uniquement aux événements ItnmServiceState.	Oui (pour les événements d'état de service)
ExtraInfo_SNMPSTATUS	Code de statut SNMP numérique.	Oui (pour les événements NmosSnmpPollFail)
ExtraInfo_SNMPSTATUSSTRING	Indication lisible par l'utilisateur de l'état d'échec SNMP.	Oui (pour les événements NmosSnmpPollFail)
ExtraInfo_SOURCE	Nom du processus d'où provient l'événement.	Oui
ExtraInfo_STITCHER	Programme stitcher responsable d'un événement de programme stitcher de reconnaissance (ItnmDiscoStitcherStatus).	Oui (pour les événements ItnmDiscoStitcherStatus)
Gravité	Niveau de gravité de l'événement. La gravité est une valeur différente de zéro.	Oui

Référence associée:

«Evénements réseau Network Manager», à la page 182
Le moteur d'interrogation, **ncp_poller**, génère des événements sur l'état du réseau. Ces événements permettent d'identifier les problèmes réseau et sont configurables à l'aide de l'interface graphique d'interrogation de réseau (sélectionnez **Administration** > **Réseau** > **Interrogation de réseau**). Ces événements sont appelés événements réseau et ont la valeur `ITNM Monitor` pour la zone alerts.status AlertGroup.

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Zones de la table alerts.status utilisées par Network Manager :

La table alerts.status d'ObjectServer contient les informations d'état sur les problèmes détectés par les sondes.

Un sous-ensemble des zones standard de la table alerts.status est rempli avec les données d'événement Network Manager. De plus, un ensemble de zones dédiées de la table alerts.status est réservé pour conserver les données spécifiques à Network Manager. Les noms de ces zones dédiées sont identifiés à l'aide du préfixe `Nmos`.

Le tableau suivant décrit les zones de la table alerts.status qui sont remplies par les zones Network Manager. Des valeurs par défaut sont affectées à certaines de ces zones à partir du fichier de règles d'analyse (évitez de les modifier).

Tableau 17. Zones de la table alerts.status utilisées par Network Manager

Zone de la table alerts.status	**Type de données**	**Description**	**Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles**
Agent	varchar(64)	Nom du processus qui a été généré l'événement. Vous pouvez utiliser cette zone pour filtrer une liste d'événements actifs afin de n'afficher que les événements d'un type donné ; par exemple, uniquement les événements de reconnaissance (avec la valeur ncp_disco).	ExtraInfo_SOURCE
AlertGroup	varchar(255)	Utilisée pour regrouper les événements par type. Les valeurs fournies par défaut à partir des événements Network Manager sont soit `ITNM Monitor` pour les événements liés au réseau, soit `ITNM Status` pour les événements de statut.	ExtraInfo_ALERTGROUP
AlertKey	varchar(255)	Chaîne de texte concaténant différents éléments relatifs à l'événement. Ces éléments peuvent inclure l'ID de l'événement, le domaine, la phase et le nom du processus. Cette zone permet de faire correspondre les événements de problème et de résolution.	Cette valeur est générée à partir des informations saisies pour veiller à ce que les événements de problème et de résolution soit correctement appariés au sein d'ObjectServer.
Class	entier	Classe d'alerte affectée à la Sonde pour Tivoli Netcool/OMNIbus.	La valeur `8000` est réservée aux événements générés par Network Manager.
EventId	varchar(255)	Type de l'événement (par exemple, SNMPTRAP-linkDown). La passerelle d'événements utilise cette valeur pour rechercher le mappage d'événement et pour déterminer la priorité des événements.	EventName
ExpireTime	entier	Date d'expiration de l'événement dans la base de données. Cette zone n'est pas utilisée par Network Manager pour le moment.	
FirstOccurrence	heure	Horodatage correspondant à la première occurrence de l'événement.	

Tableau 17. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
Identifier	varchar(255)	Valeur unique pour chaque type d'événement sur une entité donnée (par exemple, un événement LinkDown pour une interface de périphérique spécifique). Cet identificateur contrôle le dédoublonnage.	Cette valeur est générée à partir des informations saisies pour veiller à ce que les événements d'ObjectServer soient dédoublonnés de manière appropriée. Dans le fichier de règles, l'identification est construit sous la forme de valeurs de zone concaténées.
LastOccurrence	heure	Horodatage correspondant à la dernière occurrence de l'événement.	
LocalNodeAlias	varchar(64)	Adresse IP ou DNS du périphérique. Cette valeur fait généralement référence au boîtier, mais dans le cas précis des événements pingFails, elle peut correspondre à l'interface.	Pour les événements de réseau, cette zone a la même valeur que la zone Node. Aucune valeur n'est définie pour les événements de statut afin qu'ils ne soient pas retransmis à Network Manager via la passerelle d'événements.
LocalPriObj	varchar(255)	Entité spécifique pour laquelle l'événement est généré (par exemple, valeur de la zone ifIndex, ifDescr ou ifPhysAddress).	ExtraInfo_AGENT ou ExtraInfo_FINDER ou ExtraInfo_ifIndex ou ExtraInfo_NEWPHASE ou ExtraInfo_SERVICE ou ExtraInfo_STITCHER La valeur ExtraInfo_ifIndex est affichée à l'aide de la syntaxe `ifEntry.<ifIndex>` ; par exemple `ifEntry.12`.
LocalRootObj	varchar(255)	Conteneur de l'entité référencée dans la zone LocalPriObj. Il n'est pas nécessaire que ce soit le boîtier, mais il peut s'agir, par exemple, d'un emplacement du boîtier. Le boîtier peut être identifié à l'aide de la zone LocalNodeAlias.	
LocalSecObj	varchar(255)	Objet secondaire référencé par l'événement.	ExtraInfo_OLDPHASE
Manager	varchar(64)	Nom descriptif qui identifie le système ayant transmis les événements.	La valeur `ITNM` est utilisée pour les événements générés par Network Manager version 3.8 ou toute version ultérieure. La valeur `Omnibus` est utilisée pour les versions antérieures.
NmosCauseType	entier	Etat de l'événement. Cette zone est remplie par la passerelle NMOS. Les valeurs possibles sont les suivantes : • 0 : Inconnu • 1 : Origine du problème • 2 : Symptôme	

Tableau 17. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
NmosDomainName	varchar(64)	Nom du domaine réseau Network Manager qui a signalé l'événement. Le nom du domaine principal est utilisé en mode de reprise en ligne. Par défaut, cette zone est remplie uniquement pour les événements générés par Network Manager. Pour remplir cette zone pour d'autres sources d'événement, celles des autres sondes par exemple, vous devez modifier les fichiers de règles pour ces sondes. Cette zone est remplie par la passerelle d'événements si un événement correspond à une entité dans un domaine.	Domain
NmosEntityId	integer	ID objet unique qui identifie l'entité topologique à laquelle l'événement est associé. Cette zone est identique à la zone NmosObjInst mais contient davantage d'informations. Par exemple, elle peut inclure l'ID d'une interface dans un périphérique. Pour les événements générés par le moteur d'interrogation, la zone NmosEntityId est remplie dans le fichier de règles d'analyse. Pour tous les autres événements, cette zone est remplie par la passerelle lorsqu'une entité est identifiée.	ExtraInfo_MONITOREDENTITYID
NmosEventMap	varchar(64)	Nom de la mappe d'événements et priorité facultative de l'événement, qui indique comment Network Manager doit traiter l'événement (par exemple, PrecisionMonitorEvent.910). Le numéro de priorité facultative peut être concaténé à la fin de la valeur, précédé d'un point (.). Si la priorité n'est pas spécifiée, la valeur 0 lui est affectée. **Remarque :** Cette valeur peut être remplacée par une insertion explicite de la table config.precedence de la passerelle d'événements, qui fournit les mêmes données.	

Tableau 17. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
NmosManagedStatus	integer	Statut géré de l'entité réseau pour laquelle l'événement a été généré. Lorsqu'une entité réseau n'est pas gérée, les interrogations Network Manager sont suspendues et les événements provenant d'autres sources sont marqués comme non gérés. Cette zone vous permet de filtrer des événements à partir d'entités non gérées. Les valeurs possibles pour cette zone sont les suivantes : • 0 : Gérée • 1 : Non gérée par l'opérateur • 2 : Non gérée par le système • 3 : Hors de portée	
NmosObjInst	entier	ID objet unique qui identifie l'entité de boîtier topologique à laquelle l'événement est associé. Cette zone est remplie par la passerelle NMOS. **Conseil :** Cette zone peut être utilisée pour détecter si l'événement a été transmis pour enrichissement.	
NmosSerial	entier	Numéro de série de l'événement qui a supprimé l'événement en cours. Cette zone est remplie par la passerelle NMOS.	
Node	varchar(64)	Périphérique associé à la génération de l'événement. Si un événement est généré depuis une entité ayant une adresse IP accessible, cette adresse est utilisée. Sinon, la valeur entityName de la base de données NCIM est utilisée. Par défaut, la zone Node a la même valeur que la zone LocalNodeAlias.	ExtraInfo_ACCESSIPADDRESS ou EntityName La valeur EntityName est mappée vers la zone Node uniquement si la zone de saisie ExtraInfo_ACCESSIPADDRESS est vide.
NodeAlias	varchar(64)	Adresse IP du noeud principal, si disponible.	ExtraInfo_MAINNODEADDRESS
RemoteNodeAlias	varchar(64)	Adresse réseau d'un noeud distant, si pertinent. Par exemple : • Une valeur vide (si une interface est défaillante) • Une adresse voisine (si une interface connectée est défaillante) • Le poste d'interrogation (pour un événement d'échec de commande PING)	

Tableau 17. Zones de la table alerts.status utilisées par Network Manager (suite)

Zone de la table alerts.status	Type de données	Description	Nom de la zone Network Manager/Valeur par défaut dans le fichier de règles
Serial	incr	ID unique par événement par instance de serveur ObjectServer. Lorsque des serveurs ObjectServer principal et de secours sont configurés, ces serveurs auront des numéros de série différents pour le même événement.	
ServerName	varchar(64)	Nom du serveur ObjectServer à l'origine de l'événement.	
ServerSerial	entier	Numéro de série de l'événement sur le serveur ObjectServer d'origine. Lorsque des serveurs ObjectServer principal et de secours sont configurés, ces serveurs auront des numéros de série différents pour le même événement. Si l'événement provient du serveur ObjectServer en cours, la valeur de la zone ServerSerial est la même que celle de la zone Serial.	
Severity	entier	Niveau de gravité de l'événement stockés dans ObjectServer. Les valeurs par défaut sont les suivantes : • 0 : Effacer (VERT) • 1 : Non déterminé (VIOLET) • 2 : Avertissement (BLEU) • 3 : Mineur (JAUNE) • 4 : Majeur (ORANGE) • 5 : Critique (ROUGE)	Severity
StateChange	heure	Horodatage correspondant à la dernière modification de l'événement. Cette zone peut être utilisée pour déterminer si un processus a modifié un événement après qu'il a été ajouté à ObjectServer.	
Summary	varchar(255)	Description textuelle de l'événement.	Description
Tally	entier	Comptage du nombre d'occurrences d'un événement. Cette valeur est affichée dans la colonne Nombre de la liste d'événements ou de la liste d'événements actifs, et dans la colonne Occurred de la table mojo.events.	
Type	entier	Type de l'alerte. Les valeurs pertinentes pour Network Manager sont les suivantes : • 1 : Problème • 2 : Résolution • 13 : Information	ExtraInfo_EVENTTYPE

Pour plus d'informations sur la table alerts.status, consultez le manuel *IBM Tivoli Netcool/OMNIbus Administration Guide* dans le centre de documentation Tivoli Netcool/OMNIbus, à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Référence associée:

«Evénements réseau Network Manager», à la page 182
Le moteur d'interrogation, **ncp_poller**, génère des événements sur l'état du réseau. Ces événements permettent d'identifier les problèmes réseau et sont configurables à l'aide de l'interface graphique d'interrogation de réseau (sélectionnez **Administration** > **Réseau** > **Interrogation de réseau**). Ces événements sont appelés événements réseau et ont la valeur `ITNM Monitor` pour la zone alerts.status AlertGroup.

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Automatisations Tivoli Netcool/OMNIbus ajoutées par Network Manager :

Network Manager fournit de nombreuses automatisations Tivoli Netcool/OMNIbus. Chaque automatisation réalise différentes tâches dans l'installation de Network Manager.

Pour activer une automatisation, utilisez l'interface graphique d'administration Tivoli Netcool/OMNIbus.

Le tableau ci-dessous décrit les automatisations Tivoli Netcool/OMNIbus installées par Network Manager.

Tableau 18. Automatisations Tivoli Netcool/OMNIbus ajoutées par Network Manager

Automatisation	Description	Ajoutée pendant l'installation ?	Etat par défaut
severity_from_ causetype	Définit la gravité des événements dans la table ObjectServer alerts.status en fonction de la valeur de NmosCauseType, une zone énumérée qui contient les résultats des calculs Network Manager RCA (Root Cause Analysis). Les valeurs possibles de la zone NmosCauseType sont : • 0 - Inconnu • 1 - Origine du problème • 2 - Symptôme	Oui	Activé

Tableau 18. Automatisations Tivoli Netcool/OMNIbus ajoutées par Network Manager (suite)

Automatisation	Description	Ajoutée pendant l'installation ?	Etat par défaut
suppress_cross_ domain_connections	Supprime les événements des unités connectées lorsque l'unité connectée se trouve dans un domaine différent. Cette automatisation est déclenchée lorsqu'un événement est mis à jour par la passerelle d'événements. **Restriction :** Network Manager modèle uniquement des connexions via les domaines réseau dans les réseaux MPLS entre les unités PE et CE, et dans les réseaux BGP entre les homologues BGP. Pour que l'automatisation fonctionne, les deux unités réseau doivent être connectées à la couche 3 sur un sous-réseau /30 (un sous-réseau de seulement deux hôtes). Chaque unité doit également être reconnue dans un domaine réseau différent et l'existence de son unité associée doit avoir été induite pendant la reconnaissance. Ceci signifie que dans chaque domaine une unité CE induite ou une entité homologue BGP induite doit avoir été créée.	Oui	Désactivé
update_service_ affecting_events	Génère des événements affectés par un service (SAE) lorsqu'elle rencontre des événements réseau sur des entités de support de service. Après chaque reconnaissance, les plug-in SAE de la passerelle d'événements analysent la topologie mise à jour et mettent à jour le serveur ObjectServer avec la liste des entités prenant en charge des services. Ces informations activent l'automatisation pour générer des événements affectés par un service lorsqu'elles rencontrent des événements réseau sur des entités de support de service.	Non	Non applicable

Configuration de l'intégration avec Netcool Configuration Manager

Pour ajouter des capacités de configuration réseau et de gestion des règles à votre solution de gestion réseau, configurez Network Manager et Tivoli Netcool/OMNIbus afin de fonctionner avec IBM Tivoli Netcool Configuration Manager.

Vous pouvez configurer l'intégration entre Network Manager, Tivoli Netcool/OMNIbus et Netcool Configuration Manager. Pour plus d'informations, accédez à la page http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome, sélectionnez votre version de Netcool Configuration Manager et consultez les rubriques *Intégration de Netcool Configuration Manager avec Network Manager et Tivoli Netcool/OMNIbus*. Vous pouvez également télécharger la version PDF, intitulée *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Exportation de données de reconnaissance vers CCMDB, TADDM, et TBSM

Configurez et utilisez l'adaptateur de bibliothèque de reconnaissance (DLA) pour collecter des données sur les ressources et relations réseau à partir de Network Manager en vue de leur importation dans d'autres systèmes.

L'adaptateur DLA collecte des données sur Network Manager et crée des livres de bibliothèque de reconnaissance XML (également appelés langage IML ou livres IdML) contenant des données sur les ressources découvertes et leurs relations connues par le système. Les livres sont conformes à Tivoli Common Data Model (CDM) version 2.10.10. Pour plus d'informations sur Tivoli CDM, voir http://www.redbooks.ibm.com/abstracts/redp4389.html.

Les livres de la bibliothèque de reconnaissance peuvent être importés dans d'autres systèmes dans lesquels se trouve l'outil Library Reader de reconnaissance. Le DLA prend en charge IPv4 ou IPv6.

L'adaptateur de bibliothèque de reconnaissance est installé par défaut avec Network Manager sur le serveur de l'interface graphique dans le répertoire suivant : `$NCHOME/precision/adapters/ncp_dla`.

Pré-requis pour l'utilisation

Avant de configurer et utiliser l'adaptateur de bibliothèque de reconnaissance (DLA), vérifiez que les pré-requis sont respectés.

- Une reconnaissance réseauNetwork Manager a été effectuée avec succès et la base de données Network Connectivity and Inventory Model (NCIM) a été remplie.
- Le DLA utilise par défaut le pool de connexions du serveur d'interface graphique. Si vous souhaitez utiliser une autre base de données NCIM que celle fournie lors de l'installation, vous devez disposer des droits d'accès pour cette base de données NCIM.
- Vous devez savoir comment est déployé le produit avec lequel vous souhaitez effectuer l'intégration.
  - Pour plus d'informations sur IBM Tivoli Application Dependency Discovery Manager, voir le centre de documentation à l'adresse Web suivante :

    http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.2.0/welcome_page/kc_welcome-444.html
  - Pour plus d'informations sur IBM Tivoli Business Service Manager, voir le centre de documentation à l'adresse Web suivante :

    http://www-01.ibm.com/support/knowledgecenter/SS3HLM_7.1.1.16/com.ibm.tivoli.tpm.osd.doc_7.1.1.16/welcome/osdlanding.html
  - Pour plus d'informations sur IBM Tivoli Change and Configuration Management Database , voir le centre de documentation à l'adresse Web suivante :

    http://www-01.ibm.com/support/knowledgecenter/SSBH2C_7.2.2/com.ibm.isdm_7.2.2.doc/isdm_homepage.html

Configuration de l'adaptateur de bibliothèque de reconnaissance

L'adaptateur de bibliothèque de reconnaissance (DLA) requiert un fichier de propriétés de configuration pour déterminer la source de données à laquelle se connecter, le domaine à analyser, le répertoire cible pour les livres de bibliothèque de reconnaissance et les paramètres de connexion.

Vous devez configurer les propriétés de l'adaptateur de bibliothèque de reconnaissance si vous disposez d'un serveur d'interface graphique distinct ou si vous souhaitez utiliser cet adaptateur avec une instance NCIM différente de celle par défaut fournie lors de l'installation.

Un fichier de configuration `ncp_dla.properties` préconfiguré est fourni dans le répertoire d'installation de l'adaptateur de bibliothèque de reconnaissance dans `$NCHOME/precision/adapters/ncp_dla`. La présence de 'XXXXXX' ou <'word'> dans le fichier de configuration indique que le paramètre doit être défini par l'utilisateur. Ce fichier de configuration fournit des valeurs par défaut utiles pour la plupart des options. Veillez cependant à les remplacer par les valeurs appropriées pour votre environnement.

Windows Spécifiez les répertoires sur des systèmes Windows à l'aide de deux délimiteurs de chemin d'accès, par exemple `C:\\temp`.

Remarque : Par défaut, les paramètres d'accès NCIM requis pour l'utilisation de l'adaptateur de bibliothèque de reconnaissance sont dérivés du pool d'accès d'interface graphique Network Manager. Cette option est définie par le paramètre **`ncp.dla.datasource.autoConnect`**, où la valeur par défaut est «true». Si vous définissez cette valeur sur «false,» vous devez indiquer des valeurs pour les paramètres répertoriés à l'étape 6, à la page 205. La définition du mode de connexion manuel à la base de données NCIM est utile lorsque l'accès au pool de connexion est impossible ou si vous voulez utiliser une instance NCIM différente de celle fournie par défaut au cours de l'installation.

1. Accédez au fichier `$NCHOME/precision/adapters/ncp_dla` et copiez le fichier `ncp_dla.properties` vers une version spécifique du domaine en ajoutant son nom au nom du domaine, par exemple, `ncp_dla.properties.NCOMS`.
2. Indiquez le nom de domaine Network Manager en attribuant une valeur à la propriété **`ncp.dla.precisionDomain`**. Le nom de domaine par défaut est «NCOMS.»
3. Facultatif : Vous pouvez définir le chemin d'accès à un répertoire temporaire devant être utilisé par l'adaptateur de bibliothèque de reconnaissance lors de la génération de la sortie si vous ne voulez pas que celui-ci utilise le répertoire temporaire par défaut du système d'exploitation. Utilisez le paramètre **`ncp.dla.scratchDirectory`** pour définir le chemin d'accès complet à un répertoire temporaire inscriptible, par exemple **`ncp.dla.scratchDirectory=/opt/space/temp`**.
4. Facultatif : Vous pouvez définir les objets CDM pour lesquels vous voulez que des données soient générées. Utilisez le paramètre **`ncp.dla.generationFilter`** pour spécifier les valeurs dans la liste des valeurs séparées par une virgule. Les valeurs possibles sont les suivantes :
   - `ComputerSystem` - génère les données suivantes pour les périphériques :
     - ComputerSystem
     - SnmpSystemGroup
     - OperatingSystem
     - IpInterface pour IpDevice, périphériques sans accès SNMP

- Routeur
- Pont

- Mise en réseau - génère les données suivantes pour les réseaux :
  - L2Interface
  - IpInterface
  - IpV4Address
  - IpV6Address
  - IpNetwork
- Physique - génère les données suivantes pour les classes physiques :
  - PowerSupply
  - Ventilateur
  - Boîtier
  - Détecteur
  - PhysicalPackage
  - Carte
  - Fix Pack 5 Carte fille

Par exemple, pour générer des données liées à la connectivité réseau et système, ajoutez les valeurs suivantes au paramètre :

```
ncp_dla.generationFilter=ComputerSystem,Networking
```

5. Facultatif : Vous pouvez définir l'adresse URL à utiliser pour le lancement contextuel dans d'autres systèmes. Définissez le paramètre **ncp.dla.contextualLaunchURL** à la valeur de topologie dans laquelle vous voulez effectuer le lancement et spécifiez le nom d'hôte et le port pour le serveur de topologie Topoviz. L'option par défaut consiste à effectuer le lancement dans la vue Tronçon. Par exemple, pour configurer le lancement contextuel dans le navigateur de structure :

   ```
   ncp.dla.contextualLaunchURL=https://nom_hôte:16316/ibm/console/
   ncp_structureview/Launch.do?entityId=
   ```

6. Facultatif : Si vous remplacez la valeur de **ncp.dla.datasource.autoConnect** par «false,» spécifiez les détails d'accès RDBMS en modifiant les paramètres suivants qui définissent la base de données à laquelle se connecte l'adaptateur de bibliothèque de reconnaissance pour générer les manuels de la bibliothèque de reconnaissance :

   ncp.dla.datasource.type
   Spécifiez le type de système de gestion de base de données relationnelle ; le type par défaut est DB2 :

   - DB2 `DB2`
   - MySQL `MySQL`
   - Oracle `Oracle`
   - IDS `Informix`

   ncp.dla.datasource.driver
   Indiquez le pilote JDBC à utiliser :

   - DB2 `com.ibm.db2.jcc.DB2Driver`
   - MySQL `com.mysql.jdbc.Driver`
   - Oracle `oracle.jdbc.driver.OracleDriver`
   - IDS `com.informix.jdbc.IfxDriver`

ncp.dla.datasource.url
Indiquez l'adresse URL JDBC de connexion à la base de données NCIM :

- DB2 `jdbc:db2://nom_hôte:numéro_port/nom_base_de_données`
- MySQL `jdbc:mysql://nom_hôte:numéro_port/nom_base_de_données`
- Oracle `jdbc:oracle:thin:@nom_hôte:numéro_port/nom_base_de_données` où *nom_base_de_données*est l'identificateur système Oracle (SID) se référant à l'instance de base de données Oracle en cours d'exécution sur le serveur.
- IDS `jdbc:informix-sqli://nom_hôte:numéro_port/nom_base_de_données`

ncp.dla.datasource.schema
Nom du schéma de base de données, généralement «ncim»

ncp.dla.datasource.username
Nom d'utilisateur de la base de données, généralement «ncim»

ncp.dla.datasource.password
Mot de passe utilisateur de la base de données

ncp.dla.datasource.encrypted
Indique si le mot de passe de base de données est codé [true|false]

Si la valeur définie est true, vous devez indiquer une valeur valide pour `ncp.dla.datasource.keyFile` et utiliser le mot de passe codé référencé dans votre fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`.

ncp.dla.datasource.keyFile
Indiquez le nom et le chemin d'accès complet du fichier de clé cryptographique utilisé dans le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`.

ncp.dla.datasource.loginTimeout
Délai d'attente de connexion, correspondant par défaut à 5 secondes

7. Facultatif : Vous pouvez limiter la portée de la collecte des données à une ou plusieurs vues de réseau en définissant le paramètre **ncp.dla.network.view** de sorte qu'il filtre les données des vues de réseau sélectionnées uniquement. Par le biais des opérateurs SQL standard, définissez un segment SQL qui est ajouté à la zone **networkView.name** au cours de la requête de l'adaptateur de bibliothèque de reconnaissance. Le paramètre doit avoir une valeur commençant par l'un des opérateurs SQL suivants :
   - =
   - <>
   - !=
   - IN
   - NOT IN
   - LIKE
   - NOT LIKE

   Par exemple, la requête suivante définit la portée afin que seule la vue de réseau `Réseaux BGP` soit utilisée pour la portée de la collecte des données :

   ```
   ncp.dla.network.view=='BGP Networks'
   ```

Remarque : L'adaptateur de bibliothèque de reconnaissance ne prend pas en charge les guillemets. Tous les éléments situés après le signe égal dans l'exemple précédent font partie de la valeur définie, même le second signe égal (=).

Un autre exemple est celui dans lequel la portée de la collecte de données est définie comme étant n'importe quelle vue de réseau contenant le nom `Cisco` (remarquez l'utilisation du caractère générique SQL %) :

```
ncp.dla.network.view=LIKE 'Cisco%'
```

8. Indiquez la façon dont les livres de la bibliothèque de reconnaissance générés par l'adaptateur de bibliothèque de reconnaissance doivent être transférés en définissant le paramètre suivant :

   ncp.dla.datasink.type
   Méthode de transfert des livres de la bibliothèque de reconnaissance. Les options sont les suivantes :

   FILE Les livres de la bibliothèque de reconnaissance sont copiés en local dans le répertoire cible `/opt/IBM/tivoli/netcool/var/precision/ccmdb`. Si vous définissez cette option, ignorez l'étape 9 et passez à l'étape 10, à la page 208.

   FTP Les livres de la bibliothèque de reconnaissance sont transférés vers un serveur distant par FTP. Si vous définissez cette option, vous devez effectuer l'étape 9

   ncp.dla.datasink.targetDirectory
   Répertoire cible des fichiers des livres de la bibliothèque de reconnaissance

   Remarque : Si vous exécutez l'adaptateur de bibliothèque de reconnaissance (DLA) sur un serveur autre que le serveur d'interface graphique et souhaitez placer les livres générés sur ce serveur, vous pouvez spécifier les paramètres de connexion dans le fichier `ncp_dla.properties` en supprimant la mise en commentaire et en modifiant les paramètres autour de **`ncp.dla.datasink.targetDirectory`**.

9. Facultatif : Si vous avez défini l'option `FTP` pour la propriété **`ncp.dla.datasink.type`**, ajoutez les paramètres suivants :

   ncp.dla.datasink.server
   Adresse IP ou nom d'hôte du serveur FTP distant.

   ncp.dla.datasink.port
   Port TCP à utiliser (par défaut le 21)

   ncp.dla.datasink.binary
   Indique si des transferts FTP binaires doivent être utilisés [true|false]

   ncp.dla.datasink.passive
   Indique si des transferts FTP passifs doivent être effectués [true|false]

   ncp.dla.datasink.username
   Nom d'utilisateur FTP à utiliser

   ncp.dla.datasink.password
   Mot de passe utilisateur FTP à utiliser

   ncp.dla.datasink.encrypted
   Indique si le mot de passe FTP est codé [true|false]

   ncp.dla.datasink.keyFile
   Indiquez le nom et le chemin d'accès complet du fichier de clé

cryptographique utilisé dans le fichier $ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties.

10. Indiquez le niveau de débogage de l'adaptateur de bibliothèque de reconnaissance en attribuant une valeur à la propriété **log4j.rootLogger**. La valeur par défaut est FATAL et celles autorisées sont les suivantes :
    - DEBOG
    - INFO
    - WARN
    - ERROR
    - IRRECUPERABLE
11. Indiquez le nom et le chemin d'accès complet du fichier journal de l'adaptateur de bibliothèque de reconnaissance en définissant une valeur pour la propriété **log4j.appender.FILE.file**. Le nom par défaut est dla.log. Le fichier journal est écrit dans le répertoire d'installation de l'adaptateur de bibliothèque de reconnaissance.
12. Facultatif : La propriété obsolète **ncp.dla.validateComputerSystemFqdn** indique s'il convient de valider les noms des entités reconnues par Network Manager en tant que noms de domaine qualifiés complets.

    ATTENTION :
    Ne modifiez pas la valeur. Cette propriété est obsolète et n'est plus utilisée dans Network Manager versions 3.9 et suivante.
    Cette propriété peut prendre l'une des valeurs suivantes :

    True Il s'agit de la valeur par défaut. Les noms d'entité sont validés. L'adaptateur de bibliothèque de reconnaissance ajoute les attributs Fqdn aux instances ComputerSystem uniquement si le nom de périphérique est un nom de domaine qualifié complet valide.

    False Aucune validation n'est effectuée. L'adaptateur de bibliothèque de reconnaissance ajoute les attributs Fqdn aux instances ComputerSystem indépendamment du fait que le nom de périphérique soit un nom de domaine qualifié complet valide.
13. Créez une copie du fichier de configuration modifié, avec le nom de votre choix.
14. Créez une copie de la configuration pour chaque domaine Network Manager pour lequel vous souhaitez créer des livres de bibliothèque de reconnaissance.

    A faire : Créez un fichier de configuration pour chaque domaine Network Manager pour lequel vous voulez générer des manuels de la bibliothèque de reconnaissance et ajoutez le nom de ce fichier au nom du domaine (ncp_dla.properties.NCOMS, par exemple).

Pour démarrer les interfaces graphiques IBM Tivoli Application Dependency Discovery Manager à partir de Network Manager, procédez aux tâches de configuration supplémentaires afin d'ajouter une option de menu dans les interfaces graphiques Network Manager et le rapport d'inventaire Network Manager JSP dans TADDM.

Référence associée:

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur ITNM Status pour la zone alerts.status AlertGroup.

Création d'un manuel de la bibliothèque de reconnaissance

Pour créer un manuel de la bibliothèque de reconnaissance, exécutez l'adaptateur DLA avec le fichier de propriétés DLA approprié.

Avant d'exécuter DLA, le fichier de propriétés doit être correctement configuré.

DLA possède deux modes de fonctionnement :

Mode principal
Génère des manuels de la bibliothèque de reconnaissance en interrogeant la base de données NCIM pour les domaines identifiés dans le fichier de configuration indiqué.

Mode importation
Permet l'importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM, afin d'ouvrir l'interface utilisateur TADDM à partir de Network Manager.

1. Accédez au répertoire d'installation DLA sur le serveur des composants de l'interface graphique de Network Manager ; le répertoire par défaut est `$NCHOME/precision/adapters/ncp_dla`.
2. Exécutez l'adaptateur DLA et référencez le fichier de propriétés DLA approprié pour votre domaine afin de créer un manuel de la bibliothèque de reconnaissance :
   - UNIX `./ncp_dla.sh ncp_dla.properties.`*`nom_domaine`*
   - Windows `ncp_dla.bat ncp_dla.properties.`*`nom_domaine`*

   Pour obtenir un exemple d'exécution de la commande et de réponse système, voir «Exemple».

Exemple

L'exemple suivant présente la manière dont il faut exécuter DLA, ainsi que la réponse du système :

```
[root@sacramento test]# ./ncp_dla.sh ncp_dla.properties.NCOMS
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2011 By IBM Corporation.  All Rights Reserved.
See product license for details.

[IDML Generation Mode]
Initializing...
WARNING: user.install.root not defined, using /opt/IBM/tivoli/netcool
/precision/profiles/TIPProfile
Loading properties from /opt/IBM/tivoli/netcool/precision/profiles
/TIPProfile/etc/tnm/tnm.properties
ConnectionPool 'READ' Initialised
JDBC Driver: com.mysql.jdbc.Driver
JDBC URL   : jdbc:mysql://sacramento:3306/ncim?characterEncoding=UTF-8
Working on domain 'NCOMS'...
Processing 161 valid device(s)
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to
'/opt/dla/test/ITNMIP.sacramento.beach.tcr.com.2008-09-12T0192.168.34.909Z.
refresh.xml'
... Shutting down...
Finished.
```

Tâches associées:

«Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel», à la page 216
Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

Optimisation de l'exportation de données

Pour proposer un ensemble de ressources et de relations plus facilement utilisables à d'autres systèmes que Network Manager, vous pouvez optimiser l'exportation et la collecte de données DLA. L'optimisation de l'exportation de données Network Manager permet à TADDM et à d'autres utilisateurs de livre de bibliothèque de reconnaissance (IdML) d'importer uniquement les ressources et les relations requises pour générer le lien approprié entre les ressources généralement gérées. De plus, le fait de disposer uniquement des données requises peut de manière significative faciliter le processus d'exportation et d'importation.

Pour configurer une collecte et une exportation de données optimisées, procédez comme suit :

1. Reconnaissez le réseau à l'aide de Network Manager, comme cela est décrit dans Reconnaissance du réseau.
2. Exécutez l'utilitaire de balisage **itnmTagNetworkEdgeEntities.pl** pour identifier les entités de type réseau, comme cela est décrit dans «Identification des entités de périphérie du réseau».
3. Créez une vue réseau filtrée qui affiche uniquement la périphérie du réseau, comme cela est décrit dans «Création d'une vue de réseau filtrée pour la périphérie du réseau», à la page 212.
4. Modifiez le fichier de propriétés DLA `ncp_dla.properties.`*`nom_domaine`* afin d'inclure le nom de la vue réseau filtrée que vous avez créée et pour vous assurer que vous avez défini le paramètre **ncp.dla.generationFilter**, comme cela est décrit dans «Modification du fichier de propriétés DLA pour les entités de périphérie», à la page 213.
5. Exécutez l'adaptateur pour créer le livre de bibliothèque de reconnaissance, comme cela est décrit dans «Création d'un manuel de bibliothèque de reconnaissance pour les données de périphérie de réseau», à la page 214.

Identification des entités de périphérie du réseau :

Employez l'utilitaire **itnmTagNetworkEdgeEntities.pl** pour baliser les entités non reconnues, telles les ports et les interfaces, comme étant à la périphérie du réseau. Dans la plupart des cas, vous pouvez exécuter l'utilitaire pour baliser automatiquement les entités considérées comme étant à la périphérie du réseau. Cet utilitaire identifie ensuite les noeuds finaux, tels les hôtes et les serveurs qui fournissent ou utilisent des services.

Vérifiez que Network Manager a reconnu votre réseau. Les noeuds finaux doivent être reconnus avant que nous ne puissiez utiliser l'option `-autoEndNodeTags` avec l'utilitaire **itnmTagNetworkEdgeEntities.pl**.

Pour exécuter l'utilitaire afin de baliser automatiquement les entités considérées comme étant à la périphérie du réseau dans un domaine :

1. Accédez au répertoire `NHCOME/precision/scripts/perl/scripts`.
2. Exécutez **itnmTagNetworkEdgeEntities.pl** avec l'option de ligne de commande `-autoEndNodeTags` pour le domaine dans lequel les entités doivent être balisées. Inclut automatiquement les noeuds finaux, les routeurs et les commutateurs

directement connectés aux noeuds finaux. Par exemple, pour automatiquement baliser les interfaces considérées comme étant à la périphérie du réseau dans le domaine NCOMS, entrez :

- UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`
- Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`

3. Facultatif : Vous pouvez utiliser l'option `-includeNextHop` avec l'option `-autoEndNodeTags` pour accéder à un niveau suivant dans les entités de périphérie. L'utilisation de l'option `-includeNextHop` inclut automatiquement les entités de périphérie incluses lors de l'utilisation exclusive de l'option `-autoEndNodeTags`, plus tout routeur ou commutateur directement connecté aux entités de périphérie. Par exemple, pour automatiquement baliser de telles interfaces, entrez :

   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags -includeNextHop`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags -includeNextHop`

4. Facultatif : Vous pouvez également déterminer quels périphériques doivent être considérés comme unité de périphérie en fonction du nombre de connexions du périphérique. Utilisez l'option `-autoDegreeTags` pour baliser les périphériques comme étant à la périphérie du réseau s'ils ont plusieurs connexions. Si vous utilisez uniquement l'option `-autoDegreeTags`, tous les périphériques avec une connexion sont considérés par défaut comme étant à la périphérie du réseau.

   Si vous souhaitez spécifier un grand nombre de connexions, utilisez l'option `-autoDegreeTags` avec l'option `-degree` *n* où *n* correspond au nombre maximal de connexions. Par exemple, l'exécution de la commande suivante balise tous les périphériques ayant au maximum deux connexions :

   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoDegreeTags -degree 2`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoDegreeTags -degree 2`

   Remarque : L'option `-autoDegreeTags` ne peut pas être utilisée avec l'option `-autoEndNodeTags`. Le mode d'option `-autoDegreeTags` permet d'inclure des périphériques comme partie de la périphérie du réseau et qui ne sont pas considérés comme des périphériques de noeud final par l'option `-autoEndNodeTags`. Il permet également de filtrer et d'identifier les périphériques qui ont un nombre spécifique maximal de connexions.

5. Facultatif : Vous pouvez ensuite affiner le balisage en définissant un nombre d'options, telles l'exclusion ou l'inclusion de périphériques spécifiques pour le balisage ou l'inclusion de périphériques n'ayant plus d'accès SNMP mais ayant des connexions de couche 2. Pour plus d'informations sur toutes les options disponibles, consultez l'aide sur l'utilitaire en entrant :

   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -help`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -help`

L'utilitaire ajoute un attribut ExtraInfo->m_NetworkEdge=1 dans la base de données OQL master.entityByName et stocke un enregistrement entityDetails associé dans la base de données NCIM.

Vous pouvez maintenant créer une vue réseau filtrée qui affiche uniquement la périphérie de votre réseau.

Création d'une vue de réseau filtrée pour la périphérie du réseau :

Créez une vue réseau filtrée qui affiche uniquement la périphérie du réseau dans le domaine en fonction du balisage effectué par l'utilitaire **itnmTagNetworkEdgeEntities.pl**.

Conseil : Vous pouvez également utiliser la vue de réseau filtrée pour visualiser et surveiller la périphérie de votre réseau et pour voir quelles données sont exportées via l'adaptateur DLA.

Pour créer une vue filtrée de la périphérie de votre réseau, procédez comme suit :

1. Cliquez sur **Disponibilité** > **Disponibilité du réseau** > **Vues de réseau**. Cliquez sur **Nouvelle vue**  .
2. Renseignez l'onglet **Général**, comme suit :

   Nom Entrez le nom de la vue de réseau, vue dynamique ou du conteneur de la vue de réseau.

   Important : Il est recommandé d'utiliser des noms de vue de réseau contenant uniquement des caractères latins. Les noms de vues de réseau contenant des caractères non latins (par exemple, des caractères cyrilliques) ne sont pas pris en charge vu qu'ils ne peuvent pas être importés et exportés lors de la migration vers une nouvelle version de Network Manager.

   Parent Sélectionnez le noeud dans lequel la vue apparaît dans la hiérarchie de l'arborescence de navigation. Pour afficher la vue sur le niveau supérieur, sélectionnez `AUCUN`.

   Type Sélectionnez `Filtrée`.

   Présentation
   Sélectionnez une présentation `Orthogonale`, `Circulaire`, `Symétrique`, `Hiérarchique` ou `Tabulaire`.

   Icône de mappe
   Si vous souhaitez représenter la vue par une icône différente de l'icône de nuage par défaut, cliquez sur **Parcourir**  pour rechercher une icône.

   Icône d'arbre
   Si vous souhaitez représenter la vue par une icône différente de l'icône de nuage par défaut, cliquez sur **Parcourir**  pour rechercher une icône.

Image d'arrière-plan

Cliquez sur **Parcourir**  pour rechercher une image à utiliser en arrière-plan dans la vue.

Style d'arrière-plan
Indiquez si l'image en arrière-plan doit être centrée ou en mosaïque.

Statut de la ligne
Spécifiez comment les lignes qui représentent les liens entre les unités doivent être rendues.

Vous pouvez sélectionner de ne pas afficher de statut ou d'afficher le statut par défaut du système. Les lignes peuvent également être colorées en fonction de l'événement AEL associé avec la gravité la plus élevée, et peuvent apparaître avec une icône de gravité supplémentaire.

3. Configurez le filtre de la manière suivante :
   a. Cliquez sur l'onglet **Filtre**.
   b. Dans la liste **Domaine**, sélectionnez le domaine dans lequel vous avez exécuté l'utilitaire de balisage.
   c. Dans la colonne **Table**, sélectionnez l'attribut entityDetails
   d. Dans la colonne **Filtre**, entrez `keyName = 'NetworkEdge' and keyValue = '1'`.
4. Attribuez à l'option **Noeud finaux** la valeur `Inclusion`
5. Attribuez à l'option **Connectivité** la valeur `Couche 2`.
6. Cliquez sur **OK** puis sur **Sauvegarder**.

Vous devez maintenant inclure le nom de cette vue réseau dans le fichier de propriétés DLA pour le domaine.

Modification du fichier de propriétés DLA pour les entités de périphérie :

Modifiez le fichier `ncp_dla.properties` pour le domaine afin d'inclure le nom de la vue réseau filtrée créée et pour vous assurer que vous avez configuré les paramètres de génération de données appropriés.

Pour modifier le fichier, procédez comme suit :

1. Accédez au fichier de configuration `ncp_dla.properties` par défaut dans le répertoire d'installation DLA `$NCHOME/precision/adapters/ncp_dla`, ou à l'emplacement où se trouve votre fichier de propriétés DLA pour le domaine.
2. Ouvre le fichier `ncp_dla.properties.`*`nom_domaine`*.
3. Recherchez le paramètre **`ncp.dla.network.view`** et ajoutez le nom de la vue réseau filtrée créée. Par exemple, la vue filtrée appelée “Edge” doit être ajoutée à cette propriété, de la manière suivante : `ncp.dla.network.view=='Edge'`

   Remarque : L'utilisation du signe de double égalité (`==`) en tant qu'opérateur relationnel est intentionnelle.
4. Attribuez au paramètre **`ncp.dla.generationFilter`** la valeur `ComputerSystem` et `Networking`. Spécifiez les valeurs dans une liste dont chaque élément est séparé par une virgule, de la manière suivante :

   ```
   ncp_dla.generationFilter=ComputerSystem,Networking
   ```
5. Sauvegardez et fermez le fichier.

Vous pouvez maintenant exécuter l'adaptateur DLA avec le fichier de propriétés DLA mis à jour pour exporter un sous-ensemble des données réseau Network Manager.

Tâches associées:

«Configuration de l'adaptateur de bibliothèque de reconnaissance», à la page 204
L'adaptateur de bibliothèque de reconnaissance (DLA) requiert un fichier de propriétés de configuration pour déterminer la source de données à laquelle se connecter, le domaine à analyser, le répertoire cible pour les livres de bibliothèque de reconnaissance et les paramètres de connexion.

Création d'un manuel de bibliothèque de reconnaissance pour les données de périphérie de réseau :

Vous pouvez utiliser l'adaptateur de bibliothèque de reconnaissance (DLA) pour créer le manuel de bibliothèque de reconnaissance contenant uniquement les données pour vos entités réseau.

Assurez-vous d'avoir modifié le fichier `ncp_dla.properties` pour le domaine afin d'inclure le nom de la vue réseau filtrée contenant les entités réseau.

Pour créer un manuel DLA contenant des données réseau, procédez comme suit :

1. Accédez au répertoire d'installation DLA sur le serveur des composants de l'interface graphique de Network Manager ; le répertoire par défaut est `$NCHOME/precision/adapters/ncp_dla`.
2. Exécutez l'adaptateur DLA pour générer le fichier XML de manuel avec les données sur les entités réseau balisées :
   - UNIX `./ncp_dla.sh ncp_dla.properties.`*`nom_domaine`*
   - Windows `ncp_dla.bat ncp_dla.properties.`*`nom_domaine`*

   Par exemple, pour exécuter l'adaptateur pour le domaine appelé NCOMS, entrez la commande suivante : `./ncp_dla.sh ncp_dla.properties.NCOMS`

L'exemple suivant présente la réponse système pour l'exécution de l'adaptateur pour le domaine NCOMS :

```
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2011 By IBM Corporation.  All Rights Reserved.  See product
license for details.

[IDML Generation Mode]
Initializing...
Will use the following Network View(s) filter : ='FILTER'
Working on ITNM domain 'NCOMS'...
Processing 1148 IP Network(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 772 ComputerSystem(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 1 Topology(s)...
Processing 2535 Connection(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to '/opt/netcool/itnm39017/netcool/var/precision/ccmdb
/ITNMIP39.9.180.209.195.2010-10-05T13.33.37.314Z.refresh.xml'...
Shutting down...
Finished.
```

Le résultat est un fichier XML qui contient les périphériques inclus dans la vue réseau filtrée précédemment créée et spécifiée dans le fichier `ncp_dla.properties` pour le domaine. Le contenu du fichier XML dépend de la configuration du fichier de propriétés DLA.

Le fichier XML contient des segments CDM (Common Data Model) qui décrivent comment les périphériques sont connectés du point de vue d'une interface ou d'un port Network Manager spécifique. Le processus supprime les éléments en double et normalise les détails de connexion. Pour plus d'informations sur les segments, consultez la documentation Tivoli Common Data Model (CDM) disponible à l'adressehttp://www.redbooks.ibm.com/abstracts/redp4389.html.

Les exemples suivants présentent des parties de la sortie de fichier XML. L'interface choisie pour être l'identité de segment est mise en évidence en gras, notamment chaque instance dans laquelle elle est référencée.

- Exemple de connexion point à multipoint du point de vue de l'interface choisie pour être le point de démarrage d'un segment :

```
<cdm:net.Segment id="SegmentVia_359525_L2Interface" >
                <cdm:Name>Layer 2 Segment via 359525_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:359525_L2Interface
</cdm:ManagedSystemName>
 </cdm:net.Segment>
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="359525_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358156_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404607_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358221_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358185_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404595_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358107_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="357775_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358232_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404589_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358300_L2Interface" />
```

- Exemple d'une connexion point à point simple :

```
<cdm:net.Segment id="SegmentVia_355664_L2Interface" >
                <cdm:Name>Layer 2 Segment via 355664_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:355664_L2Interface
</cdm:ManagedSystemName>
</cdm:net.Segment>
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="355664_L2Interface" />
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="357336_L2Interface" />
```

Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel

Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

En plus de pouvoir lancer l'interface graphique de IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, vous pouvez également configurer TADDM pour lancer l'interface graphique de Network Manager.

Pour charger les manuels de bibliothèque de reconnaissance dans TADDM et configurer le lancement contextuel bidirectionnel, procédez comme suit :

1. Créez un livre de bibliothèque de reconnaissance.
2. Si nécessaire, transférez le fichier de livre de bibliothèque de reconnaissance sur votre serveur TADDM.
3. En tant qu'utilisateur TADDM, exécutez le processus de chargement en bloc pour importer le livre de bibliothèque de reconnaissance. Par exemple :

   ```
   user@host% cd $COLLATION_HOME/bin
   user@host% ./loadidml.sh -f chemin complet et nom complet du fichier de livre de la bibliothèque de reconnaissance
   ```

   Avertissement : Vous devez entrer le chemin complet vers le fichier des livres de la bibliothèque de reconnaissance, ainsi que son nom de fichier complet seulement si le livre se trouve dans un autre répertoire.
4. Importez les identificateur globaux uniques (GUID) de TADDM dans la base de données NCIM (voir les tâches connexes plus loin dans cette section).

Tâches associées:

«Création d'un manuel de la bibliothèque de reconnaissance», à la page 209
Pour créer un manuel de la bibliothèque de reconnaissance, exécutez l'adaptateur DLA avec le fichier de propriétés DLA approprié.

«Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM», à la page 219
Facultatif : Pour permettre aux utilisateurs d'ouvrir l'interface graphique de IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, importez les identificateurs globaux uniques de TADDM dans la table entityGUIDCache de la base de données NCIM (Network Connectivity and Inventory Model).

Configuration de IBM Tivoli Application Dependency Discovery Manager pour démarrer Network Manager

Facultatif : pour afficher un récapitulatif des ressources que Network Manager exporte vers IBM Tivoli Application Dependency Discovery Manager et, à partir de là, ouvrir Network Manager, vous devez ajouter un rapport JSP.

Important : Si vous utilisez une version antérieure d'TADDM que la version 7.2.1 Fix Pack 1, suivez ces instructions pour installer et configurer le rapport JSP. Par contre, si vous utilisez la version 7.2.1 Fix Pack 1 ou une version ultérieure, ignorez ces étapes. Dans la version 7.2.1 Fix Pack 1 ou ultérieure, le rapport destiné à afficher l'inventaire Network Manager et à fournir le lancement en contexte d'Network Manager est installé (ou mis à jour s'il existe déjà) lors de l'installation de TADDM. Pour plus d'informations, reportez-vous à la documentation de TADDM à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.2.1/com.ibm.taddm.doc_721/welcome_page/kc_welcome-444.html.

Pour utiliser le rapport JSP fourni, les fichiers doivent être copiés à l'emplacement correct sur votre serveur TADDM.

1. Connectez-vous au serveur TADDM.
2. Vérifiez que la variable d'environnement $COLLATION_HOME est définie correctement.
3. Copiez le fichier *répertoire_install_dla*/integration/itnm_inventory.jsp du serveur des composants de l'interface graphique Network Manager dans le répertoire $COLLATION_HOME/deploy-tomcat/reports/WEB-INF/view sur le serveur TADDM.
4. Copiez les deux fichiers GIF (tivoli.gif et ibm_logo.gif) dans le répertoire *répertoire_install_dla*/integration/itnm_images à partir du serveur des composants de l'interface graphique Network Manager vers le répertoire $COLLATION_HOME/deploy-tomcat/images sur le serveur TADDM.
5. Arrêtez votre serveur TADDM.
6. Modifiez le fichier $COLLATION_HOME/etc/cdm/xml/reports.xml en ajoutant la section suivante avant de fermer la balise </beans> :

```
<bean class="com.collation.cdm.reports.viewer.JspReportViewer"
id="ITNMInventoryReport">

<property name="reportGroup">
  <value>Inventory Reports
</value>
 </property>

<property name="reportName">
  <value>ITNM IP Inventory Report
</value>
 </property>
 <!-- START NON-TRANSLATABLE -->
 <property name="jsp">
  <value>/WEB-INF/view/itnm_inventory.jsp</value>
 </property>
 <!-- END NON-TRANSLATABLE -->
</bean>
```

7. Redémarrez votre serveur TADDM.

Le rapport d'inventaire de Network Manager s'affiche dans la console du gestionnaire de domaine TADDM. Il est constitué des sections suivantes :

- Server Summary : cette section comporte des informations sur les instances installées du produit Network Manager, notamment les versions de Network Manager installées, les adresses d'hôte des serveurs sur lesquels Network Manager est installé, et les adresses URL permettant d'accéder à l'interface graphique de Network Manager.
- Resource Summary : cette section répertorie toutes les ressources Network Manager qui sont liées au système informatique (ComputerSystem), notamment des informations sur leur adresse IP, le fabricant, le type de ressource (par exemple routeur) et l'identificateur unique dans la base de données de Network Manager.

Configuration de Network Manager pour le démarrage de IBM Tivoli Application Dependency Discovery Manager

Facultatif : pour autoriser les opérateurs réseau à lancer l'interface utilisateur graphique IBM Tivoli Application Dependency Discovery Manager à partir de Network Manager, vous devez ajouter les options de menu TADDM dans Network Manager.

Les étapes suivantes supposent que l'adaptateur de bibliothèque de reconnaissance (DLA) est installé sur le même serveur que Tivoli Integrated Portal et les composants de l'interface graphique de Network Manager. Si le DLA est installé à un autre emplacement, copiez le répertoire d'installation correspondant ainsi que son contenu sur le serveur où Tivoli Integrated Portal et les composants de l'interface graphique de Network Manager sont installés.

Pour plus d'informations sur la relation entre IBM Tivoli Application Dependency Discovery Manager et IBM Tivoli Change and Configuration Management Database , consultez le centre de documentation à l'adresse Web suivante et recherchez "CCMDB overview" ("présentation de CCMDB") : http://www-01.ibm.com/support/knowledgecenter/SSBH2C_7.2.2/com.ibm.isdm_7.2.2.doc/isdm_homepage.html

1. Configurez les points d'origine à partir du menu lors de l'installation TADDM :
   a. Accédez au répertoire `ITNMHOME/profiles/TIPProfile/etc/tnm/tools/`.
   b. Modifiez les fichiers suivants :
      - `ncp_wt_ccmdb_details.xml`
      - `ncp_wt_ccmdb_history.xml`
   c. Définissez les paramètres suivants :

      TADDM_HOST
      Adresse IP ou nom d'hôte de votre serveur TADDM.

      TADDM_PORT
      Port TCP sur lequel votre serveur TADDM est en mode écoute. Par défaut, il s'agit du port 9430. Cette valeur ne doit être modifiée que si un autre numéro de port a été indiqué lors de l'installation de TADDM.

      TADDM_USER
      Nom d'utilisateur à utiliser pour accéder au serveur TADDM.

      TADDM_PASSWORD
      Mot de passe associé au paramètre **`TADDM_USER`**.
   d. Facultatif : Pour configurer le démarrage de TADDM dans la même fenêtre que Network Manager, modifiez la zone `target` de la propriété `url` dans chaque fichier de définition d'outil. Par défaut, TADDM démarre dans une nouvelle fenêtre. Par exemple, pour afficher les caractéristiques CCMDB dans la même fenêtre, définissez la propriété du fichier `ncp_wt_ccmdb_details.xml` de la façon suivante :
      ```
      target="ccmdbDetails'"
      ```
2. Vérifiez que le sous-menu TADDM a été ajouté dans Network Manager :
   a. Connectez-vous à Network Manager.
   b. Sélectionnez **Disponibilité du réseau** > **Vues de réseau**
   c. Sélectionnez une vue de réseau, puis cliquez avec le bouton droit de la souris sur un périphérique.

Dans le menu contextuel, les éléments de menu TADDM suivants doivent apparaître sous **Lancer sur...** > **TADDM/CCDMB** :

Détails d'affichage

View History (Historique des vues)

Remarque : L'application des modifications peut prendre plusieurs minutes. Si cela prend plus de 5 minutes, déconnectez-vous, relancez votre navigateur et reconnectez-vous.

Vous devez maintenant importer les GUID TADDM dans la base de données NCIM.

Tâches associées:

«Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM»
Facultatif : Pour permettre aux utilisateurs d'ouvrir l'interface graphique de IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, importez les identificateurs globaux uniques de TADDM dans la table entityGUIDCache de la base de données NCIM (Network Connectivity and Inventory Model).

Importation d'identificateurs globaux uniques IBM Tivoli Application Dependency Discovery Manager dans la base de données NCIM

Facultatif : Pour permettre aux utilisateurs d'ouvrir l'interface graphique de IBM Tivoli Application Dependency Discovery Manager depuis Network Manager, importez les identificateurs globaux uniques de TADDM dans la table entityGUIDCache de la base de données NCIM (Network Connectivity and Inventory Model).

1. Exécutez l'adaptateur de bibliothèque de reconnaissance de sorte que les ressources et relations de Network Manager soient importées dans TADDM.
2. Connectez-vous au serveur où vos composants de l'interface graphique de Network Manager sont installés, et copiez le répertoire d'intégration DLA et son contenu de `ITNMHOME/adapters/ncp_dla/integration` vers votre serveur TADDM (par exemple `$COLLATION_HOME/sdk/dla/integration`). Assurez-vous que les autorisations sont définies de façon telle que l'utilisateur TADDM puisse accéder aux fichiers.
3. Sur le serveur TADDM, accédez au répertoire où vous avez copié les fichiers.
4. En tant qu'utilisateur TADDM, utilisez l'interface de programme d'application de TADDM pour demander au CCMDB des données de système informatique et transmettre les résultats à un fichier XML appelé `itnm_guids.xml`. Par exemple :

   ```
   user@host% $COLLATION_HOME/sdk/bin/api.sh -u nom_utilisateur -p motdepasse find
   ComputerSystem > itnm_guids.xml
   ```

5. Vérifiez que les fichiers `itnm_guids.xsl` et `itnm_guids.xml` existent dans le répertoire actuel.
6. En tant qu'utilisateur TADDM, utilisez le processeur XLST pour extraire les ID et les identificateurs uniques globaux des entités et les transmettre à un fichier CSV appelé `itnm_guids.csv`. Par exemple :

   ```
   user@host% $COLLATION_HOME/sdk/bin/xslt.sh -XSL ./itnm_guids.xsl >
   itnm_guids.csv
   ```

7. Recopiez le fichier `itnm_guids.csv` vers le serveur d'interface graphique Network Manager dans le répertoire de base ou dans le répertoire `ITNMHOME/adapters/ncp_dla`.

8. Exécutez l'adaptateur de bibliothèque de reconnaissance en mode d'importation pour importer les fichiers CSV dans la base de données NCIM de Network Manager. Voir «Exemple» pour un exemple présentant comment passer en mode d'importation et les réponses du système.

Exemple

L'exemple suivant présente comment exécuter l'adaptateur de bibliothèque de reconnaissance en mode d'importation et comment le système répond.

```
user@host% cd /opt/IBM/DiscoveryLibrary/ITNM
user@host% [./ncp_dla.sh | ncp_dla.bat ] -import
-file integration/itnm_guids.csv ncp_dla.properties.MYSQL
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2007 By IBM Corporation.  All Rights Reserved.
See product license for details.

[GUID Import Mode]
Initializing...
Importing GUIDs from 'integration/itnm_guids.csv'
Imported 15 GUID(s) into NCIM.
Shutting down...
Finished.
user@host%
```

Tâches associées:

«Chargement des manuels de bibliothèque de reconnaissance et activation du lancement bidirectionnel», à la page 216
Vous devez charger le manuel de bibliothèque de reconnaissance (IdML) dans TADDM pour rendre les informations du manuel disponibles pour TADDM. L'importation du manuel active également le lancement contextuel bidirectionnel.

Intégration à TBSM

Network Manager est par défaut intégré à IBM Tivoli Business Service Manager utilisant la Sonde pour Tivoli Netcool/OMNIbus (nco_p_ncpmonitor). Cette sonde fournit à IBM Tivoli Business Service Manager des jetons BSM_Identity pour Network Manager.

IBM Tivoli Network Manager IP Edition et IBM Tivoli Business Service Manager doivent être installés et configurés.

Le jeton BSM_Identity est utilisé par défaut par TBSM pourassocier les événements aux ressources. En utilisant l'adaptateur de bibliothèque de reconnaissance (DLA) deNetwork Manager, TBSM détecte les ressources de Network Manager. La zone BSM_Identity est ajoutée à Network Manager en fonction du paramètre suivant dans le fichier `$NCHOME/probes/arch/nco_p_ncpmonitor.rules` :

```
@BSM_Identity = "ITNMIP:" + $ExtraInfo_MONITOREDENTITYID + "&domain=" + $Domain
```

Référence associée:

«Pré-requis pour l'utilisation», à la page 203
Avant de configurer et utiliser l'adaptateur de bibliothèque de reconnaissance (DLA), vérifiez que les pré-requis sont respectés.

Configuration de Tivoli Integrated Portal

Une fois l'installation terminée, il se peut que vous deviez configurer la connexion unique ou la sécurité Tivoli Integrated Portal.

Configuration des registres centraux d'utilisateurs

Après l'installation, vous pouvez configurer un registre d'utilisateurs central pour la gestion et l'authentification des utilisateurs. Vous pouvez configurer un serveur LDAP ou un registre Tivoli Netcool/OMNIbus ObjectServer (ou les deux).

Remarque : Lorsque vous ajoutez un nouvel utilisateur, vous devez vérifier que l'ID utilisateur que vous spécifiez n'existe pas déjà dans les référentiels d'utilisateurs pour éviter des difficultés lorsque le nouvel utilisateur essaye de se connecter.

Dans un environnement réseau qui inclut un registre d'utilisateurs sur un serveur LDAP ou Tivoli Netcool/OMNIbus ObjectServer, vous pouvez configurer Network Manager pour utiliser l'un ou l'autre type ou les deux.

Avant de configurer un registre d'utilisateurs, vérifiez que le ou les registres d'utilisateurs que vous envisagez d'identifier sont démarrés et accessibles à partir de l'ordinateur sur lequel vous avez installé Network Manager.

Avertissement : Lorsque Network Manager est configuré avec plusieurs référentiels d'utilisateurs centraux, vous ne pouvez pas vous connecter si un référentiel d'utilisateurs distant devient inaccessible depuis Network Manager, même si votre identifiant d'utilisateur existe dans un des autres référentiels. Si vous avez besoin d'un accès dans cette situation, vous devez exécuter des commandes WebSphere Application Server pour permettre l'accès lorsque tous les référentiels sont disponibles, sans quoi les référentiels fédérés ne fonctionneront pas correctement. Pour plus d'informations, reportez-vous aux liens suivants :

- http://www-01.ibm.com/support/docview.wss?uid=swg1PK78677
- http://www-01.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.web20fep.multiplatform.doc/info/ae/ae/rxml_atidmgrrealmconfig.html

Ajout d'un référentiel LDAP externe :

Après l'installation, vous pouvez ajouter un serveur IBM Tivoli Directory Server ou un serveur Microsoft Active Directory Server comme référentiel LDAP pour Network Manager.

Pour ajouter un nouveau référentiel LDAP :

1. Connectez-vous à Network Manager.
2. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
3. Dans la console d'administration WebSphere Application Server sélectionnez **Paramètres** > **Global security** (sécurité globale).
4. Dans la liste **Available realm definitions** (Définitions de domaines disponibles), sélectionnez **Federated repositories** (Référentiels fédérés) et cliquez sur **Configurer**.
5. Dans la zone Related Items (Articles liés), cliquez sur **Manage repositories (Gestion des référentiels)** puis sur **Ajouter** pour ajouter un nouveau référentiel LDAP.

6. Dans la zone **Repository identifier** (identificateur de référentiel), spécifiez un identificateur unique pour le référentiel. L'identificateur identifie de façon unique le référentiel dans la cellule, par exemple, `LDAP1`.
7. Dans la liste **Directory type** (Type d'annuaire), sélectionnez le type de serveur LDAP. Le type de serveur LDAP détermine les filtres par défaut utilisés par WebSphere Application Server.

   Remarque : Les utilisateurs d'IBM Tivoli Directory Server peuvent choisir IBM Tivoli Directory Server ou SecureWay comme type d'annuaire. Pour de meilleures performances, utilisez le type d'annuaire IBM Tivoli Directory Server.
8. Dans la zone **Primary host name** (nom d'hôte principal), entrez le nom de système hôte qualifié complet du serveur LDAP principal. Le nom de l'hôte principal et le nom distinctif ne doivent comporter aucun espace. Vous pouvez entrer l'adresse IP ou le nom DNS (Domain Name System).
9. Dans la zone **Port**, entrez le port serveur de l'annuaire LDAP.

   Le nom d'hôte et le numéro de port représentent le domaine pour ce serveur LDAP dans une cellule dont les noeuds sont de versions différentes. Si des serveurs dans différentes cellules communiquent les uns avec les autres en utilisant des jetons LTPA (Lightweight Third Party Authentication), ces domaines doivent correspondre exactement dans toutes les cellules.

   Remarque :

   La valeur du port par défaut est `389`, ce qui n'est pas un port de connexion SSL (Secure Sockets Layer). Utilisez le port `636` pour une connexion SSL. Sur certains serveurs LDAP, vous pouvez spécifier un port différent. Si vous ne savez pas quel port utiliser, contactez votre administrateur de serveur LDAP.
10. Facultatif : Dans les zones **Bind distinguished name** (nom distinctif de liaison) et **Bind password** (mot de passe de liaison), entrez le nom distinctif de liaison (DN) (par exemple, `cn=root`) et le mot de passe.

    Remarque : Le nom distinctif de liaison est nécessaire pour les opérations d'écriture ou pour obtenir les informations d'utilisateur ou de groupe si les liaisons anonymes ne sont pas possibles sur le serveur LDAP. Dans la plupart des cas, un nom distinctif de liaison et un mot de passe de liaison sont nécessaires, sauf lorsqu'une liaison anonyme peut satisfaire toutes les fonctions requises. Si le serveur LDAP est configuré pour utiliser les liaisons anonymes, laissez ces zones vides.
11. Facultatif : Dans la zone **Login properties** (Propriétés de connexion), entrez les noms de propriété utilisés pour la connexion à WebSphere Application Server. Cette zone accepte plusieurs propriétés de connexion, séparées par un point virgule (`;`). Par exemple, `cn`.
12. Facultatif : Dans la liste **Certificate mapping** (Mappage de certificats), sélectionnez un mode de mappage de certificat. Vous pouvez utiliser les certificats X.590 pour l'authentification utilisateur lorsque LDAP est sélectionné comme référentiel.

    Remarque : La zone **Certificate mapping** est utilisée pour indiquer si les certificats X.509 doivent être mappés dans un répertoire LDAP par `EXACT_DN` (nom distinctif exact) ou par `CERTIFICATE_FILTER` (filtre de certificat). Si vous sélectionnez `EXACT_DN`, le nom distinctif du certificat doit correspondre à l'entrée utilisateur du serveur LDAP, notamment la casse et les espaces.
13. Cliquez sur **OK**.

14. Dans la zone Messages en haut de la page Global security (Sécurité globale), cliquez sur le lien **Enregistrer** et quittez la console WebSphere Application Server.

Configurez Tivoli Integrated Portal Server pour communiquer avec un référentiel LDAP externe.

Configuration d'un référentiel LDAP externe :

Vous pouvez configurer le Tivoli Integrated Portal Server pour communiquer avec un référentiel LDAP externe.

Pour configurer un serveur d'applications pour communiquer avec un référentiel LDAP externe :

1. Connectez-vous à Network Manager.
2. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
3. Dans la console d'administration WebSphere Application Server sélectionnez **Paramètres** > **Global security** (sécurité globale).
4. Dans la liste **Available realm definitions** (Définitions de domaines disponibles), sélectionnez **Federated repositories** (Référentiels fédérés) et cliquez sur **Configurer**.
5. Pour ajouter une entrée au domaine de base :
   a. Cliquez sur **Add Base entry to Realm (Ajouter une entrée de base au domaine)**.
   b. Indiquez le nom distinctif d'une entrée de base afin d'identifier de manière unique cet ensemble d'entrées dans le domaine. Cette entrée de base doit identifier de manière unique le référentiel externe dans le domaine.

      Remarque : Si le domaine comporte plusieurs référentiels, utilisez la zone Nom distinctif pour définir un nom distinctif supplémentaire qui identifiera de manière unique cet ensemble d'entrées dans le domaine. Par exemple, les référentiels LDAP1 et LDAP2 peuvent utiliser tous les deux `o=ibm,c=us` comme entrée de base dans le référentiel. Par conséquent, `o=ibm,c=us` est utilisé pour LDAP1 et `o=ibm2,c=us` pour LDAP2. Le nom distinctif spécifié dans cette zone renvoie au nom distinctif LDAP de l'entrée de base au sein du référentiel (comme `o=ibm,c=us b`). L'entrée de base indique le point de départ pour les recherches au sein du serveur de répertoires LDAP (comme `o=ibm,c=us c`).
   c. Cliquez sur **OK**.
   d. Dans la zone Messages en haut de la page Global security (Sécurité globale), cliquez sur le lien **Enregistrer** et quittez la console WebSphere Application Server.
6. Dans la console d'administration WebSphere Application Server sélectionnez **Paramètres** > **Global security** (sécurité globale).
7. Dans la liste **Available realm definitions** (Définitions de domaine disponibles), sélectionnez **Federated repositories** (Référentiels fédérés) et cliquez sur **Set as current** (Définir comme actif) pour marquer le référentiel fédéré comme le domaine actif.
8. Arrêtez et redémarrez Tivoli Integrated Portal Server :
   a. Dans le répertoire *rép_base_tip*`/profiles/TIPProfile/bin`, en fonction de votre système d'exploitation, entrez l'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 *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'une des commandes suivantes :

- Windows `startServer.bat server1`
- UNIX Linux `startServer.sh server1`

9. Vérifiez que le référentiel fédéré est correctement configuré :
   a. Dans le panneau de navigation portail, cliquez sur **Users and Groups (Utilisateurs et groupes)** > **Manage Users (Gérer les utilisateurs)**.
   b. Sélectionnez **User ID (ID utilisateur)** dans la liste **Search by (Rechercher par)**.
   c. Cliquez sur **Rechercher** pour rechercher des utilisateurs dans le référentiel fédéré.
   d. Vérifiez que la liste inclut à la fois des utilisateurs du référentiel LDAP et du registre de fichiers local.

   Sur Tivoli Integrated Portal Server, LDAP les utilisateurs sont analysés uniquement par l'attribut `userid` (ID utilisateur). Lorsque les utilisateurs sont importés dans LDAP en utilisant un fichier LDIF (LDAP Data Interchange Format), une classe auxiliaire de type `eperson` et un attribut `uid` sont ajoutés à l'identifiant utilisateur LDAP. Ceci s'impose uniquement si vous voulez explorer le référentiel LDAP en utilisant VMM à partir du serveur.

Pour pouvoir créer ou gérer des utilisateurs surla portail qui sont définis dans votre référentiel LDAP, dans la console d'administration WebSphere Application Server, spécifiez les types d'entités pris en charge.

Gestion des utilisateurs LDAP sur la console :

Pour créer ou gérer sur la portail des utilisateurs qui sont définis dans votre référentiel LDAP, dans la console d'administration WebSphere Application Server, spécifiez les types d'entités pris en charge.

Pour créer ou gérer des utilisateurs LDAP sur la portail :

1. Connectez-vous à Network Manager.
2. Dans le panneau de navigation, cliquez sur **Paramètres** > **Console d'administration Websphere** et sur **Lancer la console d'administration Websphere**.
3. Dans la console d'administration WebSphere Application Server sélectionnez **Paramètres** > **Global security** (sécurité globale).
4. Dans la liste **Available realm definitions** (Définitions de domaines disponibles), sélectionnez **Federated repositories** (Référentiels fédérés) et cliquez sur **Configurer**.
5. Dans la zone Additional Properties (Propriétés supplémentaires), cliquez sur **Supported entity types** (Types d'entité pris en charge).
6. Dans la colonne Entity type (Type d'entité), cliquez sur le lien **Groupe** pour afficher sa page de propriétés.

7. Dans la zone **Base entry for the default parent** (Entrée de base pour le parent par défaut), spécifiez une entrée de base pertinente pour votre configuration LDAP par exemple, `o=ibm,c=us`.
8. Dans la zone **Relative Distinguished Name properties** (Propriétés de nom distinctif relatif), spécifiez la même valeur que pour la zone **Base entry for the default parent**, par exemple, `o=ibm,c=us`.
9. Cliquez sur **OK** pour revenir à la page des types d'entités pris en charge.
10. Editez les entités **OrgContainer** et **PersonAccount** en spécifiant les mêmes valeurs que pour l'entité **Group** (par exemple, `o=ibm,c=us`).
11. Dans la zone Messages en haut de la page Global security (Sécurité globale), cliquez sur le lien **Enregistrer** et quittez la console WebSphere Application Server.
12. Pour que les changements soient pris en compte, arrêtez et redémarrez Tivoli Integrated Portal Server.
13. Arrêtez et redémarrez Tivoli Integrated Portal Server :
    a. Dans le répertoire *rép_base_tip*`/profiles/TIPProfile/bin`, en fonction de votre système d'exploitation, entrez l'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 *rép_base_tip*`/profiles/TIPProfile/bin`, en fonction de votre système d'exploitation, entrez l'une des commandes suivantes :
       - Windows `startServer.bat server1`
       - UNIX Linux `startServer.sh server1`

Vous pouvez maintenant gérer les utilisateurs du référentiel LDAP sur la portail via les options de menu **Utilisateurs et groupes** > **Gérer les utilisateurs**.

Remarque : Lorsque vous ajoutez un nouvel utilisateur, vous devez vérifier que l'ID utilisateur que vous spécifiez n'existe pas déjà dans les référentiels d'utilisateurs pour éviter des difficultés lorsque le nouvel utilisateur essaye de se connecter.

Restriction : Vous ne pouvez actuellement pas mettre à jour via le portlet **Utilisateurs et groupes** > **Gérer les utilisateurs** les ID utilisateurs qui ont été créés dans les référentiels Microsoft Active Directory.

Configuration d'une connexion SSL sur un serveur LDAP :

Si votre implémentation de Network Manager utilise un référentiel d'utilisateurs LDAP externe, tel que Microsoft Active Directory, vous pouvez la configurer pour communiquer via un canal SSL sécurisé.

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 Tivoli Integrated Portal Server.

Procédez comme suit pour configurer Tivoli Integrated Portal Server 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.

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 **Security (Sécurité)** > **SSL certificate and key management (Certificat SSL et gestion des clés)**.
   b. Dans la zone Related Items (Articles liés), cliquez sur le lien **Key stores and certificates (Fichiers de clés et certificats)** et dans le tableau, cliquez sur le lien **NodeDefaultTrustStore**.
   c. Dans la zone Additional Properties (Propriétés supplémentaires), cliquez sur le lien **Signer certificates (Certificats de signataires)** puis sur le bouton **Retrieve from port (Extraire depuis le port)**.
   d. 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 **Retrieve signer information (Extraire certificats de signataires)** puis sur **OK**.
3. Procédez comme suit pour activer les communications SSL sur votre serveur LDAP :
   a. Dans le panneau de navigation, cliquez sur **Security (Securité)** > **Secure administration, application, and infrastructure (Administration, applications et infrastructure sécurisées)**.
   b. Sélectionnez **Federated repositories (Référentiels fédérés)** dans la liste **Available realm definitions (Définitions de domaines disponibles)** puis cliquez sur **Configure (Configurer)**.
   c. Sélectionnez votre serveur LDAP dans la liste déroulante **Repository (Référentiel)**.
   d. Cochez la case **Require SSL communications (Communications SSL requises)** et sélectionnez l'option **Centrally managed (Géré de manière centrale)**.
   e. Cliquez sur **OK**.
4. Pour que les modifications soient prises en compte, enregistrez celles-ci puis arrêtez et redémarrez toutes les instances de Tivoli Integrated Portal Server.

Si vous souhaitez activer la fonction de connexion 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.

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 Tivoli Integrated Portal Server.

Suivez les étapes ci-après pour configurer un canal sécurisé pour les communications entre le Tivoli Integrated Portal Server et le serveur ObjectServer.

1. Récupérez les informations de certificat ObjectServer, comme suit :
   a. Dans le panneau de navigation Tivoli Integrated Portal, cliquez sur **Security (Sécurité)** > **SSL certificate and key management (Certificat SSL et gestion des clés)**.
   b. Sur la page SSL certificate and key management (Certificat SSL et gestion de clés), cliquez sur **Key stores and certificates (Fichiers de clés et certificats)** et, sur la page affichée, cliquez sur **NodeDefaultTrustStore**.
   c. Sur la page NodeDefaultTrustStore page, cliquez sur **Signer certificates (Certificats de signataires)** et, sur la page qui s'affiche, cliquez sur **Retrieve from port (Extraire depuis le port)**.
   d. Dans les zones correspondantes, entrez les valeurs d'**Hôte**, de **Port** et d'**Alias** pour le serveur ObjectServer et cliquez sur **Retrieve signer information (Extraire les informations de 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.
2. Ouvrez le fichier *rép_base_tip*/profiles/TIPProfile/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
3. Arrêtez et redémarrez Tivoli Integrated Portal Server :
   a. Dans le répertoire *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'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 *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'une des commandes suivantes :

- Windows `startServer.bat server1`
- UNIX Linux `startServer.sh server1`

Connexion unique

La fonction de connexion unique (SSO) des produits Tivoli vous permet de vous connecter à une application Tivoli puis d'accéder à d'autres applications Web Tivoli ou compatibles Web sans qu'une nouvelle soumission de vos données d'identification utilisateur soit nécessaire.

Le référentiel pour les ID utilisateur peut être le registre Tivoli Netcool/OMNIbus ObjectServer ou un registre LDAP (Lightweight Directory Access Protocol) (LDAP). L'utilisateur se connecte à l'une des applications participantes et à ce moment-là, ses données d'identification sont authentifiées au niveau d'un référentiel central. Une fois ces données authentifiées en un point centralisé, l'utilisateur peut passer d'une application à une autre pour visualiser les données connexes ou exécuter des actions. La connexion unique est possible entre applications déployées vers des serveurs Tivoli Integrated Portal sur plusieurs machines.

La fonction SSO exige que les produits impliqués utilisent le protocole LTPA (Lightweight Third Party Authentication) (LTPA) comme mécanisme d'authentification. Une fois cette fonction activée, un cookie contenant le jeton LTPA est créé et inséré dans la réponse HTTP. Lorsque l'utilisateur accède à d'autres ressources Web (portlets) dans tout autre processus du serveur d'applications relevant du même domaine du système de nom de domaine (DNS - Domain Name Service), 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, vous devez partager les clés LTPA et le registre d'utilisateurs entre ces cellules pour que la connexion unique fonctionne. Les noms de domaine sur chaque système dans le domaine SSO sont sensibles à la casse et doivent correspondre exactement. Reportez-vous à la rubrique Managing LTPA keys from multiple WebSphere Application Server cells dans le centre de documentation de WebSphere Application Server.

Configuration de la connexion unique (SSO) :

Suivez les instructions ci-après pour la prise en charge de la connexion unique et pour la configuration d'un référentiel fédéré.

La configuration de la connexion unique est nécessaire avant intégration de produits déployés sur plusieurs serveurs. Toutes les instances du Tivoli Integrated Portal Server doivent pointer sur le registre d'utilisateurs central (serveur 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.

Pour configurer les fonctionnalités du référentiel fédéré WebSphere pour le serveur LDAP :

1. Connectez-vous à la console d'administration.
2. Dans la zone **Authentification**, développez **Web Security (Sécurité Web)** et cliquez sur **Single sign-on (Connexion unique)**.
3. Si la connexion unique est désactivée, cliquez sur l'option **Activée**.
4. S'il est prévu que toutes les demandes utilisent HTTPS, cliquez sur **Requires SSL (Nécessite SSL)**.
5. Dans la zone Nom de domaine, entrez les noms qualifiés complets des domaines pour lesquels la connexion unique est effective. Si le nom de domaine n'est pas qualifié complet, Tivoli Integrated Portal Server ne définit pas de valeur de nom de domaine pour le cookie **LtpaToken** et la connexion unique n'est valide que pour le serveur qui a créé le cookie. Pour que la connexion unique fonctionne entre différentes applications Tivoli, les serveurs de ces applications doivent être installés dans le même domaine (utilisez le même nom de domaine).
6. 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.
7. 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.
8. Cliquez sur **OK** pour enregistrer vos modifications, puis arrêtez et redémarrez toutes les instances Tivoli Integrated Portal Server.

Remarque : Lorsque vous lancez Network Manager, vous devez utiliser une adresse URL au format protocole://hôte.domaine:port /*. Si vous n'utilisez pas de nom de domaine qualifié complet, Network Manager ne peut pas utiliser la connexion unique entre les produits Tivoli.

Protection du fichier de clés du coffre

Afin que la clé de chiffrement du mot de passe administrateur reste sûre, faites en sorte que le fichier de clés du coffre soit strictement limité aux accès en lecture seule.

Pour que les applications Tivoli Integrated Portal s'exécutent correctement, l'ID administrateur Tivoli Integrated Portal créé lors de l'installation (ID par défaut = **tipadmin**) doit pouvoir accéder au fichier de clés du coffre.

La clé du coffre est une clé qui est utilisée pour chiffrer le mot de passe administrateur indiqué lors de l'installation et qui est stockée en local pour les applications Tivoli Integrated Portal. Suivez les étapes ci-après pour restreindre les accès au fichier.

1. Sur l'ordinateur sur lequel serveur d'applications est installé, ouvrez le répertoire *rép_base_tip*/_uninst/TIPInstall21.
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.

Sous Windows, par exemple, les attributs d'accès pour le répertoire TIPInstall21 sont déjà définis en lecture seule, cependant les attributs associés au fichier `.vault.key` sont définis sur lecture seule et masqué.

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.

Après installation de Network Manager 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.

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 :

1. Accédez au répertoire suivant : *`rép_base_tip`*`/profiles/TIPProfile/config/cells/TIPCell/applications`.
2. A partir de cet emplacement, recherchez les fichiers `web.xml` dans les répertoires suivants :
   - Pour l'archive d'application Web de Integrated Solutions Console : `isclite.ear/deployments/isclite/isclite.war/WEB-INF`
   - Pour Tivoli Common Reporting : `tcr.ear/deployments/tcr/rptviewer_v1.2.0.war/WEB-INF`
   - Pour l'archive d'application Web de Tivoli Common Reporting : `isclite.ear/deployments/isclite/rptwebui_v1.2.0.war/WEB-INF`
   - Pour l'archive d'application Web Tivoli Integrated Portal Charts Web : `isclite.ear/deployments/isclite/TIPChartPortlet.war/WEB-INF`
   - Pour l'archive d'application Web Tivoli Integrated Portal Change Password : `isclite.ear/deployments/isclite/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. Arrêtez et redémarrez le serveur d'applications.

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>
```

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 Tivoli Integrated Portal sur le port HTTP.

https://<*nom_hôte*>:16311/ibm/console
: Utilisez le port sécurisé HTTPS pour vous connecter à Tivoli Integrated Portal.

Remarque : Si vous souhaitez utiliser une connexion unique (SSO), vous devez utiliser le nom de domaine qualifié complet de l'hôte Tivoli Integrated Portal.

Activation de FIPS

Vous pouvez configurer Tivoli Integrated Portal Server pour utiliser les fichiers Federal Information Processing Standard Java Secure Socket Extension.

Suivez les étapes ci-après pour activer la norme FIPS 140–2 sur Tivoli Integrated Portal Server.

1. Configurez le serveur d'applications pour l'utilisation de la norme FIPS.
   a. Dans la portail, cliquez sur **Security (Sécurité)>SSL certificate and key management (Certificat SSL et gestion des clés)**.
   b. Sélectionnez l'option **Use the United States Federal Information Processing Standard (FIPS) algorithms (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.
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 *rép_install*/profiles/TIPProfile/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 *rép_install*/profiles/TIPProfile/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 *rép_install*/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 renumérotez les 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 : ouvrez le navigateur et cliquez sur **Outils > Options Internet**. Dans l'onglet **Avancés**, sélectionnez l'option **TLS 1.0**.
b. Firefox : TLS 1.0 est activé par défaut.

6. Exportez les clés 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 **Paramètres** > **Global security** (sécurité globale).
   c. Sur la page Sécurité globale, dans la zone Authentification, cliquez sur le lien **LTPA**.
   d. Sous **Ouverture d'une session intercellulaire**, spécifiez un fichier de clés et indiquez un nom et un mot de passe pour le fichier qui contiendra les clés LTPA exportées.
   e. Cliquez sur **Exporter les clés**.
7. Reconfigurez toute application utilisant les clés LTPA Tivoli Integrated Portal Server : pour reconfigurer le service de connexion unique Tivoli avec les clés LTPA mises à jour, exécutez ce script : *rép_base_tip*`/profiles/TIPProfile/bin/setAuthnSvcLTPAKeys.jacl`.
   a. Accédez au répertoire *rép_base_tip*`/profiles/TIPProfile/bin/`
   b. Démarrez le Tivoli Integrated Portal Server :
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`
   c. Exécutez la commande :

      `wsadmin -username` *admin_tip* `-password` *mot_de_passe_admin_tip* `-f setAuthnSvcLTPAKeys.jacl` *chemin_fichier_clés_exporté mot_de_passe_clés*

      Où :

      chemin_fichier_clés_exporté est le nom et le chemin d'accès complet du fichier de clés qui a été exporté.

      mot_de_passe_clés est le mot de passe qui a été utilisé pour exporter la clé.
8. Pour SSO, activez les FIPS pour tous les autres serveurs d'applications, puis importez les clés LTPA mises à jour à partir du premier serveur dans ces serveurs :
   a. Copiez le fichier de clés LTPA configuré à l'étape 4 vers un autre ordinateur du 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 **Paramètres** > **Global security** (sécurité globale).
   d. Sur la page Sécurité globale, dans la zone Authentification, 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 **Importer les clés**.
9. Exécutez la commande ConfigureCLI :

Windows *rép_base_tip*\bin\tipcli.bat ConfigureCLI --useFIPS true

Linux UNIX *rép_base_tip*/bin/tipcli.sh ConfigureCLI --useFIPS true

Le fichier *rép_base_tip*/java/jre/lib/security/java.security du kit de développement de logiciels IBM se présente comme suit lorsque IBMJCEFIPS est activé.

```
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 de la valeur du délai d'attente pour le jeton LPTA

Vous pouvez configurer la valeur du délai d'attente pour le jeton LTPA (Lightweight Third Party Authentication) (LTPA) pour Tivoli Integrated Portal sur la console WebSphere Application Server.

Tivoli Integrated Portal est activé pour la connexion unique.

Le délai d'attente par défaut pour un jeton LTPA est de 120 minutes. Un dépassement du délai d'attente LTPA a pour effet de vous déconnecter de Tivoli Integrated Portal et peut également afficher un message d'authentification si la première requête après le dépassement du délai d'attente est une requête AJAX provenant d'un portlet. Pour configurer le délai d'attente du jeton LTPA :

1. Dans le panneau de navigation Tivoli Integrated Portal cliquez sur **Paramètres** > **Console d'administration WebSphere**.
2. Cliquez sur **Lancer la Console d'administration WebSphere** pour démarrer la console WebSphere Application Server.
3. Dans le panneau de navigation WebSphere Application Server, cliquez sur **Security** > **Global security**.
4. Dans la zone Authentification de la page Global security, cliquez sur le lien **LTPA**.
5. Dans la zone du délai d'attente LTPA de la page LTPA, éditez la valeur du délai d'attente LTPA et cliquez sur **OK**.
6. Dans la zone Messages en haut de la page Global security (Sécurité globale), cliquez sur le lien **Enregistrer** et quittez la console WebSphere Application Server.

Dans un environnement à équilibrage de charge, vous devez définir la valeur du délai d'attente du jeton LTPA sur chaque instance de Tivoli Integrated Portal Server.

Configuration de VMM pour ObjectServer

Lorsque vous installez Tivoli Netcool/OMNIbus à l'aide du programme d'installation Network Manager et que vous utilisez le serveur d'objets pour l'authentification d'utilisateur, le programme d'installation configure l'adaptateur de gestionnaire de membre virtuel pour le serveur d'objets. A défaut, configurez le gestionnaire de membre virtuel manuellement lorsque vous souhaitez utiliser le serveur d'objets pour l'authentification d'utilisateur.

Conservez les informations ObjectServer suivantes à portée de main : nom et mot de passe d'administrateur, adresse IP et numéro de port. Si vous utilisez un deuxième serveur ObjectServer pour la prise en charge du basculement, vous devez disposer de l'adresse IP et du numéro de port. Le serveur ObjectServer doit être en cours d'exécution au moment de l'installation de Network Manager, car le processus d'installation tente de s'y connecter.

Le script part du principe que le répertoire d'installation `tip` est le répertoire parent et que les noms de profil et de cellule sont TIPProfile et TIPCell. Exécutez le script de configuration VMM sur chaque ordinateur intégrant le serveur d'applications.

1. Accédez au répertoire *rép_base_tip*`/bin`. Ce répertoire comporte un script à exécuter :
   - Windows `confvmm4ncos.bat`
   - Linux `confvmm4ncos.sh`
   - UNIX `confvmm4ncos.sh`
2. Entrez la commande suivante à l'invite de commande : `confvmm4ncos utilisateur mot_de_passe adresse port [adresse2 port2]`où
   a. `utilisateur` représente l'ID d'un utilisateur disposant de droits d'administration pour ce serveur ObjectServer
   b. `mot_de_passe` représente le mot de passe pour l'ID utilisateur
   c. `adresse` représente l'adresse IP du serveur ObjectServer
   d. `port` représente le numéro du port utilisé par le serveur ObjectServer
   e. Facultatif : `adresse2` et `port2` représentent l'adresse et le numéro de port du serveur ObjectServer de basculement éventuellement installé

L'adaptateur VMM est configuré pour le serveur ObjectServer. Par la suite, chaque fois qu'il est nécessaire d'accéder au registre d'utilisateurs, l'adaptateur VMM est appelé pour la transmission de ces informations.

Modification du registre de sécurité par défaut

Le registre de sécurité par défaut peut être défini au moment de l'installation. Procédez de la manière suivante pour modifier le registre par défaut après l'installation.

Ces étapes nécessitent que votre ID utilisateur vous fasse bénéficier du rôle de l'administrateur et que vous connaissiez la valeur de l'entrée de base de votre référentiel. Pour LDAP ou Microsoft Active Directory, il s'agit généralement d'une chaîne telle que `ou=company,dc=country,dc=region`. Pour le serveur ObjectServer, l'entrée de base est `o=netcoolObjectServerRepository`.

Si vous n'avez pas sélectionné de registre utilisateur par défaut pendant l'installation, ou si vous voulez modifier la valeur par défaut sur un registre différent, procédez de la manière suivante.

1. Si cela n'est déjà fait, connectez-vous à la console d'administration. Votre ID doit avoir le rôle de l'administrateur.
2. Cliquez sur **Sécurité** > **Administration, applications et infrastructure sécurisées**.
3. Dans la zone réservée aux référentiels de comptes utilisateur, sélectionnez **Référentiels fédérés** pour les Définitions de domaines disponibles, puis cliquez sur **Configurer**.
4. Cliquez sur **Types d'entité pris en charge** sous **Propriétés supplémentaires**.
5. Cliquez sur le type d'entité puis éditez l'**Entrée de base du parent par défaut** et les **Propriétés du nom distinctif relatif**.
6. Cliquez sur **OK** pour enregistrer vos modifications puis répétez l'étape précédente pour configurer tout autre type d'entité. Pour Microsoft Active Directory, les types d'entité (PersonAccount, Group et OrgContainer) doivent être configurés avec un DN de base et le RDN pour PersonAccount doit être `cn` au lieu de `uid`.
7. Arrêtez et redémarrez Tivoli Integrated Portal Server :
   a. Dans le répertoire *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'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 *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'une des commandes suivantes :
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`

Intégration à IBM Tivoli Monitoring

Vous pouvez installer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition pour contrôler l'état de santé de votre installation Network Manager. IBM Tivoli Monitoring est inclus dans le package Network Manager.

Vous devez avoir installé Network Manager avant d'installer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

Restriction : UNIX Le tableau de bord ouvre des fenêtres xterm pour exécuter des scripts d'interpréteur de commandes destinés à la migration et à l'installation de IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. Si vous souhaitez coller des caractères non-ASCII entre les fenêtres xterm (démarrées par le programme d'installation) et d'autres fenêtres, définissez un environnement local se terminant par UTF-8 avant d'exécuter le tableau de bord. Utilisez une commande identique à la suivante : `export LANG=fr_FR.UTF-8`.

Pour installer IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, procédez comme suit :

1. Sur le serveur où les composants centraux de Network Manager sont installés, exécutez le script d'installation d'IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
   - Pour exécuter le script d'installation à l'aide du tableau de bord, démarrez ce dernier à l'aide du script **`launchpad.sh`** sous UNIX ou l'exécutable

launchpad.exe sous Windows et cliquez sur **Postinstallation** > **Installation de l'agent de surveillance** > **Démarrer l'installation de l'agent ITM**.

- Pour exécuter le script d'installation à l'aide de la ligne de commande, exécutez le script `ITMagent\WINDOWS\setup.exe` (sous Windows) ou le script `ITMagent/install.sh` (sous UNIX) à partir du répertoire `scripts` du support d'installation.

2. Pour connaître les procédures d'installation, consultez le manuel *IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition User's Guide*.

Configuration de l'intégration à IBM Systems Director

Vous pouvez configurer Network Manager pour l'utiliser avec IBM Systems Director. Après la configuration de l'intégration, vous pouvez lancer IBM Systems Director à partir de l'interface graphique de Network Manager et effectuer différentes tâches sur le périphérique sélectionné dans IBM Systems Director.

Présentation de l'intégration à IBM Systems Director

IBM Systems Director fournit des vues consolidées de vos systèmes gérés ainsi qu'un ensemble de tâches pour la gestion des systèmes comprenant notamment la reconnaissance, l'inventaire, la configuration, la santé système, la surveillance, la notification d'événements et l'automatisation des systèmes gérés. Une fois l'intégration configurée, vous pouvez ouvrir des tâches IBM Systems Director à partir de l'interface graphique Network Manager à l'aide du menu contextuel.

Vous pouvez lancer IBM Systems Director pour gérer des ressources de votre réseau en cliquant avec le bouton droit de la souris sur une unité dans n'importe quelle vue de topologie Network Manager et en sélectionnant l'option de menu **Lancer sur** > **Director**, puis en sélectionnant la tâche que vous souhaitez ouvrir dans IBM Systems Director.

Les fonctions IBM Systems Director que vous pouvez lancer pour une unité depuis Network Manager dépendent des informations partagées relatives à l'unité reconnue dans les deux produits. La liste suivante identifie toutes les tâches IBM Systems Director disponibles lorsque le lancement se fait depuis Network Manager :

- Statut actif
- Configurer l'accès
- Configuration actuelle
- Créer un groupe
- Problèmes de conformité
- Gestionnaire de configuration
- Plans de configuration
- Règle de conformité
- Modèles de configuration
- Commande distribuée
- Historique de déploiement
- Journal des événements
- Gestion des fichiers
- Diagnostics réseau
- Parcourir les ressources : Topologie de base
- Parcourir les ressources : Topologie de virtualisation
- Récapitulatif des performances

- Demander l'accès
- Ligne de commande éloignée
- Vérifier la connexion
- Afficher et collecter l'inventaire
- Parcourir les ressources : Vue des propriétés

Remarque : La liste des fonctions pouvant être lancées à partir du menu contextuel de Network Manager varie et peut être un sous-ensemble de la liste précédente.

Pour plus d'informations sur les fonctions ouvertes dans IBM Systems Director et une aide relative à leur utilisation, cliquez sur le bouton d'aide de la page IBM Systems Director ouverte.

Sinon, accédez au centre de documentation IBM Systems Director à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSAV7B_621/com.ibm.director.main.helps.doc/fqm0_main.html?cp=SSAV7B_621%2F2 et recherchez le nom sur lequel vous avez cliqué dans l'option de menu contextuel (par exemple, "Configurer l'accès").

Architecture de l'intégration

L'intégration entre Network Manager et IBM Systems Director requiert l'exécution d'un processus d'adaptateur Java basé sur les paramètres définis dans le fichier de configuration `itnmSystemsDirector.properties`.

Le fichier de configuration est installé par défaut avec Network Manager sur le serveur d'interface graphique, et se trouve dans le répertoire `NCHOME/precision/adapters/itnm_systemsDirectorLiC`.

Le processus d'adaptateur Java communique avec le serveur IBM Systems Director à l'aide du protocole HTTPS pour associer des ressources IBM Systems Director et des points d'origine à des unités reconnues par Network Manager pour le domaine défini dans le fichier de propriétés. L'adaptateur détermine l'ensemble de points d'origine IBM Systems Director associés à une unité Network Manager et stocke ces derniers dans la table LiCmapping NCIM. La table LiCmapping décrit la ressource IBM Systems Director, l'adresse URL du point d'origine et le nom de menu de chaque tâche que vous pouvez exécuter sur une unité Network Manager.

Restriction : Pour que l'intégration aboutisse, Network Manager et IBM Systems Director doivent reconnaître et gérer les mêmes ressources.

Téléchargement et installation d'IBM Systems Director

Vous devez disposer d'une installation d'IBM Systems Director en cours d'exécution avant de configurer l'intégration avec Network Manager.

Pour obtenir IBM Systems Director, procédez comme suit :

1. Accédez à http://www.ibm.com/systems/management/director/downloads/
2. Accédez à l'onglet **Management servers** et téléchargez IBM Systems Director version 6.2 ou version ultérieure.
3. Accédez au centre de documentation IBM Systems Director à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSAV7B_621/com.ibm.director.main.helps.doc/fqm0_main.html?cp=SSAV7B_621%2F2,

développez "IBM Systems Director V6.2.1", puis consultez les rubriques relatives à la planification et à l'installation.

4. Suivez les instructions fournies pour planifier l'installation d'IBM Systems Director et effectuer cette dernière.

Configuration de l'intégration à IBM Systems Director

Effectuez les tâches suivantes pour configurer l'intégration entre Network Manager et IBM Systems Director.

Préparation du fichier de propriétés :

Pour configurer l'intégration, vous devez créer une copie du fichier `itnmSystemsDirector.properties` pour chaque domaine Network Manager dans lequel exécuter les tâches IBM Systems Director.

Créez une copie du fichier de propriétés pour le domaine dans lequel vous envisagez d'exécuter l'adaptateur :

1. Accédez au répertoire `NCHOME/precision/adapters/itnm_systemsDirectorLiC`. Le fichier de configuration est installé par défaut avec Network Manager sur le serveur de l'interface graphique.
2. Effectuez une copie du fichier `itnmSystemsDirector.properties` et ajoutez à la fin du nom de fichier le nom du domaine pour lequel définir l'intégration.

   Par exemple, pour créer une copie du fichier de propriétés pour le domaine NCOMS, entrez la commande suivante sur les systèmes d'exploitation UNIX :

   ```
   cp itnmSystemsDirector.properties itnmSystemsDirector.properties.NCOMS
   ```

   Cette commande permet de créer une copie du fichier de propriétés et d'ajouter NCOMS à la fin du fichier.
3. Utilisez la copie du fichier pour configurer l'intégration, comme cela est décrit dans les tâches suivantes.

Exportation et importation du certificat SSL :

Le processus d'adaptateur Java qui communique entre Network Manager et IBM Systems Director requiert la configuration d'une connexion sécurisée. Vous devez importer le certificat SSL à partir du serveur IBM Systems Director dans le fichier de clés utilisé par le processus Java Network Manager exécutant l'adaptateur.

Pour obtenir le certificat, vous devez l'exporter à partir d'IBM Systems Director puis l'importer dans Network Manager :

1. Connectez-vous au serveur IBM Systems Director.
2. Exportez le certificat à l'aide de la commande **`keytool -export`** :

   ```
   /opt/ibm/director/jre/bin/keytool -export -alias lwiks -keystore
   /opt/ibm/director/lwi/security/keystore/ibmjsse2.jks -file
   directorcert.arm
   ```
3. Copiez le fichier `directorcert.arm` dans le serveur Network Manager où va s'exécuter l'adaptateur. Par exemple, `/tmp/directorcert.arm`.
4. Importez le fichier `directorcert.arm` dans le fichier de clés local à l'aide de la commande **`keytool -import`** :

   ```
   keytool -import -alias directorcert -file /chemin du fichier/
   directorcert.arm -keystore TIPHOME/java/jre/lib/security/cacerts
   ```

   Remarque : Le mot de passe par défaut est `changeit`.

   Vous trouverez ci-dessous un exemple d'importation de certificat :

```
/opt/IBM/tivoli/tip/java/bin/keytool -import -alias directorcert -file
/tmp/directorcert.arm -keystore /opt/IBM/tivoli/tip/java/jre/lib/
security/cacerts
```

Configuration des propriétés de connexion :

Modifiez la copie du fichier `itnmSystemsDirector.properties` afin de spécifier les propriétés de connexion pour l'adaptateur associant Network Manager et IBM Systems Director.

Assurez-vous d'avoir créé une copie du fichier `itnmSystemsDirector.properties` et d'avoir ajouté le nom de fichier à la fin du nom du domaine pour lequel vous souhaitez configurer l'intégration avec IBM Systems Director, par exemple, `itnmSystemsDirector.properties.NCOMS`.

Pour configurer les propriétés de connexion, procédez comme suit :

1. Ouvrez le fichier de propriétés `itnmSystemsDirector.properties.`*`nom du domaine`*.
2. Modifiez les valeurs suivantes pour configurer la connexion :
   a. Définissez le paramètre **`itnm.integration.ibm.SystemsDirector.cryptographicKeyFile`** afin de faire référence au fichier de clés cryptographiques Network Manager ou au fichier de clés généré à l'aide de l'option **`./itnm_systemsDirectorLiC.sh`** `-generate -keyfile` *nom fichier*.

      Par exemple, définissez le chemin de la manière suivante pour utiliser le fichier de clés par défaut :

      ```
      itnm.integration.ibm.SystemsDirector.cryptographicKeyFile=/opt/IBM/
      tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

   b. Définissez le paramètre **`itnm.integration.ibm.SystemsDirector.server`** afin de référencer l'adresse IP ou le nom d'hôte du serveur IBM Systems Director. Par exemple :

      ```
      itnm.integration.ibm.SystemsDirector.server=192.0.2.24
      ```

   c. Définissez le paramètre **`itnm.integration.ibm.SystemsDirector.port`** en fonction du numéro de port sur lequel le serveur IBM Systems Director écoute. Par exemple :

      ```
      itnm.integration.ibm.SystemsDirector.port=4495
      ```

      Remarque : Le port par défaut est 8422.

   d. Définissez le paramètre **`itnm.integration.ibm.SystemsDirector.userName`** afin qu'il référence le nom d'utilisateur IBM Systems Director. Par exemple :

      ```
      itnm.integration.ibm.SystemsDirector.userName=root
      ```

3. Chiffrez et définissez le mot de passe pour l'utilisateur IBM Systems Director :
   a. Accédez au répertoire `NCHOME/precision/adapters/itnm_systemsDirectorLiC`.
   b. Exécutez la commande suivante en utilisant le mot de passe pour l'utilisateur IBM Systems Director défini dans le paramètre **`itnm.integration.ibm.SystemsDirector.userName`** : `./itnm_systemsDirectorLiC.sh -encrypt` *`mot de passe`* `-keyfile` */`chemin complet du fichier de clés cryptographiques`/`chemin complet du fichier de clés cryptographiques`*`.key`. Cette commande créé une chaîne de texte chiffrée pour le mot de passe.

Par exemple, pour chiffrer le mot de passe Network1 à l'aide du fichier de clés par défaut, entrez :

```
./itnm_systemsDirectorLiC.sh -encrypt Network1 -keyfile
/opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
encryption/keys/crypt.key
```

jR/CjUmgRaYRF64Dsf37FGJvxDxqmxcE3XybALZ7THo= constitue un exemple de sortie du processus de chiffrement.

c. Définissez le paramètre **itnm.integration.ibm.SystemsDirector.password** afin de référencer le mot de passe chiffré de l'utilisateur.

Par exemple, pour utiliser le mot de passe chiffré de l'étape précédente, entrez :

```
itnm.integration.ibm.SystemsDirector.password=
jR/CjUmgRaYRF64Dsf37FGJvxDxqmxcE3XybALZ7THo=
```

4. Définissez le paramètre **itnm.integration.ibm.SystemsDirector.jreKeyStoreFile** pour référencer l'emplacement du fichier de clés Network Manager dans lequel vous avez importé le certificat SSL. Par exemple :

```
itnm.integration.ibm.SystemsDirector.jreKeyStoreFile=/opt/IBM/tivoli/tip/
java/jre/lib/security/cacerts
```

5. Chiffrez et définissez le mot de passe du fichier de clés :
   a. Accédez au répertoire NCHOME/precision/adapters/itnm_systemsDirectorLiC.
   b. Exécutez la commande suivante en utilisant le mot de passe pour le fichier de clés : ./itnm_systemsDirectorLiC.sh -encrypt *mot de passe* -keyfile */chemin complet du fichier de clés cryptographiques/nom du fichier de clés cryptographiques*.key. Cette commande créé une chaîne de texte chiffrée pour le mot de passe.

      Par exemple, pour chiffrer le mot de passe Crypto1 à l'aide du fichier de clés par défaut, entrez :

      ```
      ./itnm_systemsDirectorLiC.sh -encrypt Crypto1 -keyfile
      /opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

      i/y7aYCV5looIK3eRoYEPWJvxDxqmxcE3XybALZ7THo= constitue un exemple de sortie du processus de chiffrement.

   c. Définissez le paramètre **itnm.integration.ibm.SystemsDirector.jreKeyStorePassword** afin de référencer le mot de passe chiffré pour le fichier de clés.

      Par exemple, pour utiliser le mot de passe chiffré de l'étape précédente, entrez :

      ```
      itnm.integration.ibm.SystemsDirector.jreKeyStorePassword=
      i/y7aYCV5looIK3eRoYEPWJvxDxqmxcE3XybALZ7THo=
      ```

6. Enregistrez le fichier de propriétés.

Vous pouvez spécifier des paramètres facultatifs supplémentaires dans le fichier itnmSystemsDirector.properties pour l'adaptateur.

Tâches associées:

«Paramètres d'adaptateur supplémentaires», à la page 242
En dehors de la définition des propriétés de connexion, vous pouvez modifier les paramètres par défaut qui contrôlent les caractéristiques de journalisation et de comportement supplémentaires de l'adaptateur. Modifiez la copie du fichier itnmSystemsDirector.properties pour l'adaptateur liant le domaine Network Manager et IBM Systems Director.

Configuration de la connexion à NCIM :

Vous pouvez configurer les paramètres de connexion à la base de données NCIM où l'adaptateur insère dans la table LiCmapping des données provenant d'IBM Systems Director. Si la chaîne **itnm.integration.ibm.SystemsDirector.itnmDatabaseUseConnectionPool** a la valeur `true`, les paramètres par défaut de NCIM sont utilisés et il n'est pas nécessaire de configurer les propriétés de base de données.

Le seul paramètre obligatoire est **itnmDomain** qui doit être spécifié (voir la première étape).

Pour définir les propriétés de connexion pour la base de données NCIM, procédez comme suit :

1. Dans la propriété **itnm.integration.ibm.SystemsDirector.itnmDomain**, spécifiez le domaine Network Manager dans lequel s'exécute l'adaptateur. Par exemple :
   `itnm.integration.ibm.SystemsDirector.itnmDomain=NCOMS`
2. Facultatif : Si vous ne souhaitez pas utiliser les paramètres par défaut et que l'élément **itnm.integration.ibm.SystemsDirector.itnmDatabaseUseConnectionPool** a la valeur `false`, vous pouvez spécifier d'autres propriétés de base de données devant être utilisées par l'adaptateur :
   a. Retirez le caractère de hachage au début de la ligne et définissez la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabaseType** en lui attribuant le type de base de données à utiliser. Les valeurs prises en charge sont `DB2`, `Oracle`, `MySQL` et `Informix`.
   b. Retirez le caractère de hachage au début de la ligne et définissez la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabaseDriver** en lui attribuant l'URL du pilote JDBC qui spécifie le type de pilote JDBC à utiliser. Utilisez une des valeurs suivantes en fonction de la base de données sélectionnée :
      - Pour DB2 : `com.ibm.db2.jcc.DB2Driver`
      - Pour Oracle : `oracle.jdbc.driver.OracleDriver`
      - Pour MySQL : `com.mysql.jdbc.Driver`
      - Pour Informix : `com.informix.jdbc.IfxDriver`
   c. Retirez le caractère de hachage au début de la ligne et définissez la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabaseURL** en lui attribuant l'URL JDBC pour la connexion à la base de données NCIM. Utilisez une des syntaxes suivantes en fonction de la base de données sélectionnée :
      - Pour DB2 : `jdbc:db2://`*`nom_hôte`*`:`*`numéro_port`*`/`*`nom_base_de_données`*
      - Pour Oracle : `jdbc:oracle:thin:@`*`nom_hôte`*`:`*`numéro_port`*`:`*`nom_base_de_données`*
      - Pour MySQL : `jdbc:mysql://`*`nom_hôte`*`:`*`numéro_port`*`/`*`nom_base_de_données`*
      - Pour Informix : `jdbc:informix-sqli://`*`nom_hôte`*`:`*`numéro_port`*`/`*`nom_base_de_données`*`:INFORMIXSERVER=`*`nom_serveur`*

      Conseil : Ce paramètre dépend de la base de données utilisée. Consultez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties` pour obtenir des informations sur la base de données utilisée et obtenir de l'aide en matière de définition de l'URL spécifique à la plateforme.

L'exemple suivant présente les paramètres pour une base de données Informix :

```
# itnm.integration.ibm.SystemsDirector.itnmDatabaseType=Informix
# itnm.integration.ibm.SystemsDirector.itnmDatabaseDriver=
com.informix.jdbc.IfxDriver
# itnm.integration.ibm.SystemsDirector.itnmDatabaseURL=
jdbc:informix-sqli://abc123.ibm.com:9995/ncimdb:INFORMIXSERVER=inst1
```

3. Facultatif : Définissez la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName** afin de référencer le nom d'utilisateur de base de données NCIM. Par exemple :

   ```
   itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName=root
   ```

4. Facultatif : Chiffrez et définissez le mot de passe pour l'utilisateur NCIM :
   a. Accédez au répertoire NCHOME/precision/adapters/itnm_systemsDirectorLiC.
   b. Exécutez la commande suivante en utilisant le mot de passe pour l'utilisateur NCIM défini dans la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName** : ./itnm_systemsDirectorLiC.sh -encrypt *mot de passe* -keyfile */chemin complet du fichier de clés cryptographiques/nom du fichier de clés cryptographiques*.key. Cette commande créé une chaîne de texte chiffrée pour le mot de passe.

      Par exemple, pour chiffrer le mot de passe Database1 à l'aide du fichier de clés par défaut, entrez :

      ```
      ./itnm_systemsDirectorLiC.sh -encrypt Database1 -keyfile
      /opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

      DvDlWqoRzRHAD9WpYzkI0mJvxDxqmxcE3XybALZ7THo= constitue un exemple de sortie du processus de chiffrement.
   c. Définissez la propriété **itnm.integration.ibm.SystemsDirector.itnmDatabasePassword** pour référencer le mot de passe chiffré. Par exemple :

      ```
      itnm.integration.ibm.SystemsDirector.itnmDatabasePassword=
      DvDlWqoRzRHAD9WpYzkI0mJvxDxqmxcE3XybALZ7THo=
      ```

5. Enregistrez le fichier de propriétés.

Paramètres d'adaptateur supplémentaires :

En dehors de la définition des propriétés de connexion, vous pouvez modifier les paramètres par défaut qui contrôlent les caractéristiques de journalisation et de comportement supplémentaires de l'adaptateur. Modifiez la copie du fichier itnmSystemsDirector.properties pour l'adaptateur liant le domaine Network Manager et IBM Systems Director.

Assurez-vous d'avoir modifié la copie du fichier itnmSystemsDirector.properties pour lequel vous avez configuré l'intégration.

Le fichier de configuration est installé par défaut avec Network Manager sur le serveur d'interface graphique et est disponible dans le répertoire NCHOME/precision/adapters/itnm_systemsDirectorLiC.

Pour modifier des caractéristiques supplémentaires de l'adaptateur, procédez comme suit :

1. Ouvrez le fichier de propriétés itnmSystemsDirector.properties.*nom du domaine*.

2. Modifiez les valeurs suivantes :
   a. Attribuez au paramètre **itnm.integration.ibm.SystemsDirector.connectTimeout** une valeur correspondant à la durée pendant laquelle l'adaptateur tente de se connecter au serveur IBM Systems Director. Si l'adaptateur ne peut pas se connecter une fois cette durée écoulée, une erreur est générée. La valeur est exprimée en millisecondes et la valeur par défaut est 60000 (60 secondes).
   b. Attribuez au paramètre **itnm.integration.ibm.SystemsDirector.readTimeout** la valeur correspondant à la durée d'attente avant que l'adaptateur ne lise des données à partir du serveur IBM Systems Director après s'y être connecté. Si l'adaptateur ne peut pas lire de données une fois cette durée écoulée, une erreur est générée. La valeur est exprimée en millisecondes et la valeur par défaut est 60000 (60 secondes).
   c. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.verifySSLHostNames** pour définir si l'adaptateur vérifie ou non le nom du serveur IBM Systems Director enregistré dans le certificat. La vérification est effectuée lorsque la valeur est `true`, elle n'est pas effectuée lorsque la valeur est `false`.
   d. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.usePasswordAuthentication** pour définir si l'authentification par mot de passe est utilisée ou non. L'authentification par mot de passe est activée si la valeur est `true`, elle est désactivée lorsque la valeur est `false`.
   e. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.ignoreIPAddress.n** pour indiquer à l'adaptateur d'ignorer les adresses IP spécifiques dans IBM Systems Director. Spécifiez plusieurs adresses IP en répétant ce paramètre et en incrémentant *n* de 1 chaque fois.

      Par exemple, pour faire en sorte que l'adaptateur ignore les adresses IP 192.0.2.12 et 192.0.2.24, ajoutez les lignes suivantes :

      ```
      itnm.integration.ibm.SystemsDirector.ignoreIPAddress.1=192.0.2.12
      itnm.integration.ibm.SystemsDirector.ignoreIPAddress.2=192.0.2.24
      ```

   f. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.ignoreHostName.n** pour indiquer à l'adaptateur d'ignorer des noms d'hôte spécifiques. Spécifiez plusieurs tâches en répétant ce paramètre et en incrémentant *n* de 1 chaque fois.

      Par exemple, pour faire en sorte que l'adaptateur ignore les noms d'hôte mymachine et ball.company.com, ajoutez les lignes suivantes :

      ```
      itnm.integration.ibm.SystemsDirector.ignoreHostName.1=mymachine
      itnm.integration.ibm.SystemsDirector.ignoreHostName.2=ball.company.com
      ```

   g. L'adaptateur crée une table dans NCIM associant des ressources IBM Systems Director à des périphériques détectés par Network Manager pour le domaine défini dans le fichier de propriétés. Vous pouvez remplacer les ressources IBM Systems Director individuelles par un mappage de périphérique Network Manager en spécifiant manuellement quel OID IBM Systems Director correspond à quel nom d'hôte ou adresse IP de noeud principal Network Manager. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.n** pour indiquer à l'adaptateur de remplacer l'association de ressource automatique. Spécifiez plusieurs adresses en répétant ce paramètre et en incrémentant *n* de 1 chaque fois. Le format est`mapOIDtoITNMIPAddressOrHostName.`*`n=oid:ipaddress`* ou `mapOIDtoITNMIPAddressOrHostName.`*`n+1=oid:hostname`*.

Par exemple, pour faire en sorte que l'adaptateur utilise l'OID 2292 et l'associe à l'adresse IP 192.0.2.12 ainsi que l'OID 2286 et l'associe au nom d'hôte mymachine, ajoutez les lignes suivantes :

```
itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.1=
2292:192.0.2.12
itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.1=
2286:mymachine
```

h. Vous pouvez définir l'adaptateur de telle sorte qu'il ignore des tâches IBM Systems Director spécifiques. Utilisez le paramètre **itnm.integration.ibm.SystemsDirector.ignoreTask.n** pour définir les tâches ignorées par l'adaptateur et qui ne sont pas disponibles pour s'exécuter sur un périphérique. Spécifiez plusieurs tâches en répétant ce paramètre et en incrémentant *n* de 1 chaque fois.

   Par exemple, pour faire en sorte que l'adaptateur ignore la tâche Diagnostics réseau, ajoutez la ligne suivante :

```
itnm.integration.ibm.SystemsDirector.ignoreTask.1=Network Diagnostics
```

3. Enregistrez le fichier de propriétés.

Vous pouvez également définir les propriétés de journalisation pour le processus d'adaptateur.

Tâches associées:

«Définition des propriétés de journalisation pour l'adaptateur»
Vous pouvez spécifier les propriétés de journalisation pour l'adaptateur utilisé afin de lier IBM Systems Director et Network Manager.

Définition des propriétés de journalisation pour l'adaptateur :

Vous pouvez spécifier les propriétés de journalisation pour l'adaptateur utilisé afin de lier IBM Systems Director et Network Manager.

Assurez-vous d'avoir modifié la copie du fichier `itnmSystemsDirector.properties` pour lequel vous avez configuré l'intégration.

Pour définir les propriétés de journalisation pour l'adaptateur, procédez comme suit :

1. Ouvrez le fichier de propriétés `itnmSystemsDirector.properties.`*nom du domaine*.
2. Modifiez les valeurs suivantes :
   a. Définissez le niveau de journalisation général à l'aide du paramètre **.level**. La valeur par défaut est `WARNING` et les niveaux suivants peuvent être définis :
      - `CONFIG` :

        Journalise tous les événements jusque et y compris les changements de configuration.
      - `INFO` :

        Journalise uniquement les changements d'état système. Il s'agit du paramètre par défaut.
      - `WARNING` :

        Journalise les erreurs système récupérables.
      - `SEVERE` :

        Journalise les erreurs système non récupérables.
      - `FINE` :

Niveau minimal de traçage. La majorité des traces de pile apparaissent déjà à ce niveau et sont écrites dans le fichier de trace. Ce dernier inclut également tous les messages de journal.

- `FINER` :

  Niveau moyen de traçage qui fournit des messages de débogage plus détaillés.

- `FINEST` :

  Niveau maximal de traçage qui fournit des informations techniques très détaillées.

b. Définissez le niveau de journalisation pour le gestionnaire de fichiers à l'aide du paramètre **java.util.logging.FileHandler.level**. Les niveaux possibles sont les mêmes que pour le paramètre **.level**.

c. En cas d'utilisation, définissez le niveau de journalisation pour le gestionnaire de console à l'aide du paramètre **java.util.logging.ConsoleHandler.level**. Les niveaux possibles sont les mêmes que pour le paramètre **.level**.

d. Modifiez l'emplacement de sauvegarde du fichier journal à l'aide du paramètre **java.util.logging.FileHandler.pattern**.

3. Enregistrez le fichier de propriétés.

La journalisation pour les processus d'adaptateur utilise la même logique qu'une autre journalisation dans Network Manager. Consultez les fichiers journaux pour détecter tout problème potentiel.

Exécution de l'adaptateur pour remplir NCIM

Après la définition des propriétés de l'adaptateur, vous devez exécuter l'adaptateur pour remplir la base de données NCIM avec les informations sur les ressources pouvant être gérées dans IBM Systems Director pour le domaine Network Manager défini dans le fichier de propriétés.

Assurez-vous d'avoir défini tous les paramètres requis dans le fichier de propriétés de l'adaptateur pour le domaine.

Pour exécuter l'adaptateur, procédez comme suit :

1. Accédez au répertoire `NCHOME/precision/adapters/itnm_systemsDirectorLiC`.
2. Exécutez l'adaptateur à l'aide de la commande **./itnm_systemsDirectorLiC.sh** et référencez le fichier de propriétés pour le domaine pour lequel vous configurez l'adaptateur.

   Par exemple, pour exécuter l'adaptateur pour le domaine NCOMS, entrez la commande suivante :

   ```
   ./itnm_systemsDirectorLiC.sh itnmSystemsDirector.properties.NCOMS
   ```

   En fonction des paramètres du fichier de propriétés, l'adaptateur remplit la table LiCmapping dans la base de données NCIM avec les informations de point de démarrage provenant d'IBM Systems Director.
3. Cliquez à l'aide du bouton droit sur les périphériques dans toute vue de topologie Network Manager après l'exécution de l'adaptateur. Plusieurs tâches IBM Systems Director sont disponibles pour être lancées à partir de Network Manager pour le périphérique si ce dernier est géré par les deux produits. La liste suivante identifie toutes les tâches IBM Systems Director disponibles lors du lancement à partir de Network Manager:

   - Statut actif

- Configurer l'accès
- Configuration actuelle
- Créer un groupe
- Problèmes de conformité
- Gestionnaire de configuration
- Plans de configuration
- Règle de conformité
- Modèles de configuration
- Commande distribuée
- Historique de déploiement
- Journal des événements
- Gestion des fichiers
- Diagnostics réseau
- Parcourir les ressources : Topologie de base
- Parcourir les ressources : Topologie de virtualisation
- Récapitulatif des performances
- Demander l'accès
- Ligne de commande éloignée
- Vérifier la connexion
- Afficher et collecter l'inventaire
- Parcourir les ressources : Vue des propriétés

Remarque : La liste des fonctions pouvant être lancées à partir du menu contextuel de Network Manager varie et peut être un sous-ensemble de la liste précédente.

Traitement des incidents liés à l'intégration à IBM Systems Director

Si le lancement en contexte à partir de Network Manager vers IBM Systems Director ne fonctionne pas, il peut être nécessaire de vérifier vos paramètres d'intégration IBM Systems Director.

Si l'intégration à IBM Systems Director ne fonctionne pas, il est possible que l'adaptateur ne fonctionne pas et ne charge pas les données de point de lancement dans la table LiCmapping.

Pour vérifier les paramètres d'intégration, procédez comme suit :

1. La première étape après une erreur consiste à vérifier tous les paramètres de configuration et à vérifier que Network Manager et IBM Systems Director gèrent le même ensemble de ressources.
2. Vérifiez les éléments suivants :

Option	Description
Le certificat SSL n'a pas été importé à partir d'IBM Systems Director dans Network Manager.	Exportez le certificat puis importez-le dans Network Manager, comme cela est décrit dans «Exportation et importation du certificat SSL», à la page 238.

Option	Description
La configuration IBM Systems Director n'est pas correcte.	Assurez-vous d'avoir correctement défini les propriétés de connexion à IBM Systems Director, comme cela est décrit dans «Configuration des propriétés de connexion» , à la page 239.
La configuration de base de données NCIM Network Manager n'est pas correcte.	Vérifiez les paramètres NCIM, comme cela est décrit dans «Configuration de la connexion à NCIM», à la page 241.
Il existe un pare-feu bloquant l'accès à l'API IBM Systems Director.	Vérifiez vos paramètres de pare-feu et permettez l'accès à l'hôte IBM Systems Director.
Le domaine Network Manager spécifié n'a pas de périphérique géré par IBM Systems Director.	Assurez-vous que les mêmes périphériques sont reconnus par les deux produits.
Le serveur IBM Systems Director n'est pas en cours d'exécution.	Assurez-vous que le serveur IBM Systems Director est en cours d'exécution et que vous pouvez vous connecter. Pour plus d'informations sur IBM Systems Director, consultez le centre de documentation à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSAV7B/welcome et recherchez "Management server and agent commands."
La base de données NCIM Network Manager n'est pas en cours d'exécution.	Assurez-vous que tous les processus sont en cours d'exécution dans Network Manager, comme cela est décrit dans .
Les mots de passe spécifiés ont été chiffrés à l'aide d'un fichier de clés cryptographiques différent de celui spécifié dans le fichier de propriétés.	Assurez-vous de chiffrer les mots de passe avec le fichier référencé dans le fichier de propriétés de l'adaptateur, comme cela est décrit dans «Configuration des propriétés de connexion», à la page 239.

3. S'il est nécessaire d'avoir des informations plus détaillées pour comprendre la cause de l'erreur, attribuez la valeur FINEST au niveau de journalisation et consultez les messages d'erreur dans le fichier journal.

Tâches associées:

«Définition des propriétés de journalisation pour l'adaptateur», à la page 244
Vous pouvez spécifier les propriétés de journalisation pour l'adaptateur utilisé afin de lier IBM Systems Director et Network Manager.

Configuration de Network Manager pour les systèmes d'exploitation UNIX

Sur des systèmes d'exploitation UNIX, tels que Solaris et AIX, il peut être nécessaire d'effectuer des tâches de configuration supplémentaires avant d'utiliser le produit.

Configuration des autorisations d'utilisateur root/non root

Sous UNIX, si vous avez installé Network Manager en tant qu'utilisateur non root, vous devez effectuer une configuration supplémentaire.

Certains composants de Network Manager nécessitent des autorisations d'utilisateur root pour fonctionner. Vous devez effectuer différentes opérations si vous souhaitez exécuter Network Manager en tant qu'utilisateur root ou non root.

Installations en tant que superutilisateur et non superutilisateur

Sous UNIX, vous pouvez installer Network Manager en tant que superutilisateur ou en tant que non superutilisateur.

Si vous avez installé tout autre produit IBM Tivoli dans le même répertoire d'installation, vous devez installer Network Manager à l'aide du même identifiant utilisateur que celui utilisé pour les autres produits.

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Après l'installation, vous pouvez configurer les composants centraux de Network Manager pour qu'ils puissent être exécutés par un utilisateur différent. Par exemple, si vous avez installé le produit en tant que superutilisateur, vous pouvez configurer les composants centraux pour qu'ils puissent être exécutés par un non superutilisateur.

Restriction : Lorsque vous installez et exécutez Network Manager en tant que superutilisateur, des scripts qui redémarrent les processus Network Manager et Tivoli Netcool/OMNIbus lorsque le serveur est réamorcé sont également installés. Lorsque Network Manager est installé et exécuté en tant qu'utilisateur non root, les processus Network Manager et Tivoli Netcool/OMNIbus ne sont pas redémarrés automatiquement lorsque le serveur est réamorcé.

Restriction : AIX Si vous installez les composants de base de Network Manager en tant qu'utilisateur non superutilisateur sur AIX, et que vous employez DB2 comme base de données topologiques NCIM, vous devez effectuer certaines tâches de configuration supplémentaires et vous assurer que seule la bibliothèque client DB2 est active sur le serveur DB2. La présence de plusieurs clients DB2 actifs sur le serveur peut entraîner des problèmes et n'est pas prise en charge.

Restriction : IBM Tivoli Business Service Manager doit être exécuté en tant qu'utilisateur non root. Lorsque Network Manager et IBM Tivoli Business Service Manager sont installés sur le même serveur, assurez-vous d'installer et d'exécuter les deux en tant qu'utilisateur non root.

En raison de ces restrictions, vous ne pouvez pas exécuter les composants centraux Network Manager et IBM Tivoli Business Service Manager sur le même serveur AIX si vous utilisez DB2 pour la base de données topologiques NCIM.

Configuration des composants centraux pour une exécution en tant qu'utilisateur root

Sous UNIX, si vous avez installé Network Manager en tant qu'utilisateur non root, vous devez procéder à une configuration supplémentaire pour exécuter les composants centraux en tant qu'utilisateur root.

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Vous devez exécuter un script mettant à jour les droits d'accès aux fichiers afin de garantir l'accès de l'utilisateur root à tous les fichiers requis.

Si vous avez installé Network Manager en tant qu'utilisateur root, aucune configuration n'est nécessaire pour exécuter les composants centraux en tant qu'utilisateur root.

1. Connectez-vous au serveur où les composants centraux de Network Manager sont installés. Connectez-vous en tant qu'utilisateur root.
2. Exécutez le script à partir du tableau de bord du programme d'installation ou de la ligne de commande :

Option	Description
A partir du tableau de bord	1. Accédez au répertoire dans lequel vous avez extrait le package d'installation de Network Manager. 2. Démarrez le tableau de bord en tant qu'utilisateur root en utilisant la commande **./launchpad.sh**. 3. Sélectionnez le menu de post-installation. 4. Développez **Tâches de post-installation non racine (UNIX uniquement)** et cliquez sur **Exécuter IBM Tivoli Network Manager IP Edition 3.9 en tant que racine**.
A partir de la ligne de commande	1. Accédez au répertoire `NCHOME/precision/scripts`. 2. Exécutez le script `setup_run_as_root.sh`.

Configuration des composants centraux pour une exécution en tant que non superutilisateur

Sous UNIX, si vous avez installé Network Manager en tant que non superutilisateur et que vous souhaitez autoriser les droits utilisateur permettant d'exécuter les composants centraux, vous devez vous connecter en tant que superutilisateur et procéder à une configuration supplémentaire.

Avertissement : Procédez à des installations et exécutions en tant que non superutilisateur uniquement sur des serveurs sur lesquels seuls les utilisateurs de confiance sont autorisés à se connecter.

Les applications Web Network Manager doivent toujours être exécutées par l'utilisateur ayant installé le produit.

Pour accorder ces droits à un non superutilisateur, vous devez exécuter un script. Il est impossible d'installer et d'exécuter Network Manager sans se connecter en

tant que superutilisateur. Vous devez au minimum vous connecter temporairement en tant que superutilisateur pour exécuter le script.

Important : Sur les systèmes d'exploitation Linux pour s390 et s390x, vous devez installer le logiciel GSKit avant d'exécuter le script setuid.

Effectuez les étapes de configuration suivantes pour exécuter les composants centraux en tant qu'utilisateur non root :

1. Connectez-vous en tant qu'utilisateur root.
2. Exécutez le script à partir du tableau de bord du programme d'installation ou de la ligne de commande :

Option	Description
A partir du tableau de bord	1. Accédez au répertoire dans lequel vous avez extrait le package d'installation Network Manager. 2. Démarrez le tableau de bord en tant qu'utilisateur root en utilisant la commande **./launchpad.sh**. 3. Sélectionnez le menu de post-installation. 4. Développez **Tâches de post-installation non racine (UNIX uniquement)** et cliquez sur **Exécuter IBM Tivoli Network Manager IP Edition 3.9 en tant qu'utilisateur de l'installation**.
A partir de la ligne de commande	1. Accédez au répertoire `NCHOME/precision/scripts`. 2. Exécutez le script `setup_run_as_setuid_root.sh`.

3. Facultatif : Si vous souhaitez exécuter la sonde mttrapd (également appelée sonde SNMP) en tant qu'utilisateur non root, procédez à une configuration supplémentaire :
   - Configurez la sonde pour qu'elle s'exécute en tant qu'utilisateur non root à l'aide des instructions de la section *Running the mttrapd probe as suid root (Exécution de la sonde mttrapd en tant que suid root)* dans *IBM Tivoli Netcool/OMNIbus Probe for SNMP Reference Guide*.
   - AIX Sous AIX, vous devez également suivre les instructions fournies à l'URL suivante : http://www.ibm.com/support/docview.wss?uid=swg21296292.

     Important : Notez que ces instructions impliquant la copie de bibliothèques Sybase dans le répertoire `/usr/lib`, cette opération peut affecter le fonctionnement des installations de Sybase se trouvant sur le même serveur que la sonde mttrapd.

Une fois le script exécuté, l'utilisateur ayant installé Network Manager peut se connecter et exécuter les composants centraux de Network Manager.

Installation de GSKit sous AIX :

Avant de configurer les composants centraux à exécuter en tant qu'utilisateur non root sous AIX, vous devez installer la trousse GSKit (IBM Global Secure ToolKit).

Assurez-vous que vous disposez de la version 8.0.13.3, ou ultérieure, de la trousse GSKit. Ce logiciel de cryptographie IBM permet d'établir une communication SSL (Secure Socket Layer). Le kit GSKit est fourni avec le package d'installation de Network Manager.

Avant d'exécuter le script `setup_run_as_setuid_root.sh`, vous devez installer GSKit dans le répertoire `/usr/lib`. Un processus exécuté en tant que bit ID utilisateur n'utilise pas la variable d'environnement LIBPATH, et ne peut donc pas utiliser le GSKit lorsqu'il est installé dans un sous-répertoire de $NCHOME.

Pour installer GSKit sous AIX dans /usr/lib à l'aide de la commande **`installp`**, effectuez les tâches suivantes.

1. Connectez-vous en tant qu'utilisateur root.
2. Accédez au répertoire dans lequel vous avez extrait le package d'installation de Network Manager ou accédez à l'emplacement racine du support d'installation.
3. Ouvrez une invite de commande et entrez les commandes suivantes.

   ```
   installp -acgXd . GSKit8.gskcrypt32.ppc.rte
   installp -acgXd . GSKit8.gskssl32.ppc.rte
   ```

   Où `-a` correspond à l'application, `-c` correspond à la validation, `-g` installe et valide automatiquement tout progiciel requis, `-X` développe le système de fichier si nécessaire, et `-d` indique l'emplacement du support d'installation.

   Remarque : Les deux packages GSKit sont fournis dans le package d'installation de Network Manager et sont disponibles au plus haut niveau après extraction du package. Dans l'exemple précédent, la commande est exécutée depuis ce répertoire du plus haut niveau.

Installation et configuration d'Informix après une installation non root

Informix peut être installé uniquement par l'utilisateur root. Si vous avez installé Network Manager sans être utilisateur root et que vous souhaitez utiliser Informix en tant que base de donnés topologiques, vous devez vous connecter en tant que root après l'installation et installer Informix sur le système en utilisant les valeurs fournies lors de l'installation de Network Manager.

Vérifiez que l'installation de Network Manager a abouti. Consultez les fichiers journaux d'installation pour obtenir plus d'informations sur les tâches postérieures à l'installation requises pour l'installation de la base de données.

Pour configurer Informix après une installation non root :

1. Connectez-vous en tant que superutilisateur.
2. Vous pouvez utiliser l'interface graphique (tableau de bord) ou l'interface de ligne de commande :

Option	Description
Configuration d'Informix à l'aide de l'interface graphique (tableau de bord)	1. Accédez au répertoire dans lequel vous avez extrait le package d'installation Network Manager. 2. Démarrez le tableau de bord en tant que superutilisateur en utilisant la commande **./launchpad.sh**. 3. Sélectionnez le menu de post-installation. 4. Développez **Non-root postinstallation tasks (UNIX only) (Tâches de post-installation non racine (UNIX uniquement))** et cliquez sur **Finish installing Informix as topology database (Terminer l'installation d'Informix en tant que base de données de topologie)**. 5. Indiquez l'emplacement où vous avez installé Network Manager (valeur de la variable d'environnement $NCHOME) et attendez la fermeture de la fenêtre de commande. Cette opération peut durer quelques minutes.
Configuration d'Informix à l'aide de l'interface de ligne de commande	1. Accédez au répertoire `NCHOME/precision/install/scripts` 2. Exécutez la commande **install_ids_root.ksh** de la manière suivante : `./install_ids_root.ksh -f ../data/ids.properties` 3. Attendez la fin du script.

Remarque : Informix ne peut être lancé que par l'utilisateur root ou par l'administrateur de la base de données Informix. Si vous disposez d'une installation Network Manager avec Informix réalisée par un utilisateur non root et que vous devez redémarrez la base de données Informix pour une raison quelconque, vous devez vous connecter en tant qu'utilisateur root et exécuter la commande suivante sur les systèmes Linux et Solaris : `/etc/init.d/informix start|stop` ou la commande suivante sur les systèmes AIX : `/etc/rc.d/init.d/informix start|stop`. Vous pouvez également vous connecter en tant qu'administrateur de la base de données et exécutez la commande **onmode -ky** pour arrêter la base de données Informix, et la commande **oninit** pour démarrer la base de données.

Pour plus d'informations, accédez au centre de documentation IBM Informix 11.70 à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.70.0/com.ibm.welcome.doc/welcome.htm et recherchez *Administrator's Reference*.

Tâches associées:

«Affichage des journaux d'installation», à la page 123
L'affichage des journaux d'installation peut être utile à des fins de dépannage.

Configuration d'Informix à distance pour la génération de rapports

Si l'installation est effectuée par un utilisateur non-root et que vous installez Informix sur un autre serveur que le serveur sur lequel les composants d'interface graphique sont installés, vous devez installer le logiciel Informix IConnect en tant qu'utilisateur root sur le serveur de composants d'interface graphique pour utiliser des rapports Cognos.

Pour installer Informix IConnect :

1. Connectez-vous au serveur en tant qu'utilisateur root sur lequel vous avez installé les composants d'interface graphique (serveur Tivoli Integrated Portal, par exemple).
2. Installez IConnect à l'aide de l'interface graphique (tableau de bord) ou de l'interface de ligne de commande :

Option	Description
Installez Informix IConnect à l'aide de l'interface graphique (tableau de bord)	1. Accédez au répertoire dans lequel vous avez extrait le package d'installation de Network Manager. 2. Démarrez le tableau de bord en tant qu'utilisateur root en utilisant la commande **./launchpad.sh**. 3. Sélectionnez le menu de post-installation. 4. Développez **Tâches de post-installation non racine (UNIX uniquement)** et cliquez sur **Installer Informix IConnect**. 5. Indiquez l'emplacement où vous avez installé Network Manager (valeur de la variable d'environnement $NCHOME) et attendez la fermeture de la fenêtre de commande. Cette opération peut durer quelques minutes.
Installez Informix IConnect à l'aide de l'interface de ligne de commande	1. Créez l'utilisateur et le groupe `informix`. Reportez-vous aux instructions spécifiques à la plateforme concernée dans la rubrique *Création du groupe informix et de l'utilisateur informix* dans le centre de documentation Informix à l'URL suivante :http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.50.0/com.ibm.start.doc/welcome.htm 2. Accédez au répertoire dans lequel vous avez extrait le package d'installation de Network Manager. 3. Accédez au répertoire suivant : `scripts` 4. Exécutez la commande d'installation comme suit : `./installConnect` 5. Suivez les invites pour une installation standard dans `NCHOME/platform/$ARCH/informix`.

Configuration d'autorisations pour les outils Web sous Solaris 10

Sous Solaris 10, vous devez définir l'autorisation net_rawaccess pour garantir que tous les outils Web fonctionnent correctement.

Ces paramètres de chemin de bibliothèque et d'autorisations affectent principalement la capacité d'un utilisateur non root à exécuter l'outil Web de routage avancé.

1. En tant qu'utilisateur root, entrez la commande `ppriv` pour afficher les permissions. Voici un exemple de sortie dans lequel l'autorisation net_rawaccess n'est pas définie.

```
flags = <none>
E: all
I: basic
P: all
L: all
```

2. Exécutez la commande usermod pour définir l'autorisation net_rawaccess. Par exemple, la commande suivante définit l'autorisation net_rawaccess pour l'utilisateur itnmuser.

```
usermod -K defaultpriv=basic,net_rawaccess itnmuser
```

Configuration d'interfaces graphiques

Vous pouvez changer l'apparence et la fonctionnalité des vues panoramiques, mettre à jour des informations MIB et configurer la présentation des événements à partir d'unités non gérées.

Administration du client TopoViz

Il est possible de personnaliser les opérations du client TopoViz. Cela inclut notamment les paramètres d'affichage, les icônes de périphériques par exemple, la fréquence des mises à jour de la topologie, et les paramètres d'alerte.

Modification des délais d'expiration de Tivoli Integrated Portal

Lorsque vous travaillez dans Tivoli Integrated Portal, votre session d'interface graphique est sujette aux délais d'expiration. Vous pouvez modifier les paramètres de délai d'expiration.

Tivoli Integrated Portal fournit les paramètres de délai d'expiration par défaut suivants :

Délai d'invalidation
Si un utilisateur est connecté à Network Manager à l'aide de Tivoli Integrated Portal et qu'il ferme la fenêtre Tivoli Integrated Portal, la session utilisateur expire automatiquement après 30 minutes.

Délai d'expiration de l'authentification LPTA (Lightweight Third Party Authentication)
Lorsqu'un utilisateur est connecté depuis 24 heures, la session de connexion de Tivoli Integrated Portal est fermée automatiquement et l'utilisateur est obligé de se reconnecter.

Modification du paramètre du délai d'invalidation :

Si un utilisateur est connecté à Network Manager en utilisant Tivoli Integrated Portal et qu'il ferme la fenêtre de Tivoli Integrated Portal, la session utilisateur expire par défaut après 30 minutes. C'est ce qu'on appelle le délai d'invalidation. Vous pouvez modifier le paramètre de délai d'invalidation.

Pour modifier le paramètre du délai d'invalidation :

1. Connectez-vous au serveur sur lequel les composants d'interface graphique Network Manager sont installés et modifiez le fichier suivant :
   - UNIX `$TIPHOME/profiles/TIPProfile/config/cells/TIPCell/applications/isclite.ear/deployments/isclite/deployment.xml`
   - Windows `%TIPHOME%\profiles\TIPProfile\config\cells\TIPCell\applications\isclite.ear\deployments\isclite\deployment.xml`
2. Dans ce fichier, recherchez la valeur `invalidationTimeout`. Par défaut, cette valeur est définie sur 30 minutes.
3. Définissez `invalidationTimeout` à la valeur requise, en minutes.
4. Sauvegardez le fichier `deployment.xml`.

Modification du paramètre du délai d'expiration de l'authentification LTPA (Lightweight Third Party Authentication) :

Lorsqu'un utilisateur est connecté depuis un certain temps, par défaut 24 heures, la session de connexion de Tivoli Integrated Portal est fermée automatiquement et l'utilisateur est obligé de se reconnecter. C'est ce qu'on appelle le délai d'expiration de l'authentification LPTA (Lightweight Third Party Authentication). Vous pouvez modifier le paramètre du délai d'expiration LPTA.

Pour modifier le paramètre du délai d'expiration LPTA :

1. Cliquez sur **Sécurité** > **Administration, applications et infrastructure sécurisées**.
2. Dans la fenêtre Administration, applications et infrastructure sécurisées, cliquez sur **Mécanismes et expiration d'authentification**.
3. Définissez la **Timeout value for forwarded credentials between servers** (Valeur du délai d'attente pour des justificatifs de réacheminement entre des serveurs) de votre choix. La valeur par défaut est de 1440 minutes (24 heures).
4. Cliquez sur **OK**.

Fonctionnalités du client TopoViz

Ces informations présentent les fonctionnalités du client TopoViz pouvant être personnalisées.

Icônes TopoViz :

Dans une mappe topologique, les icônes représentent des types de périphériques ou d'éléments de réseau. Vous pouvez personnaliser ces icônes.

Vous pouvez personnaliser les icônes suivantes :

- icônes de périphériques
- icônes d'arborescence et de mappe

La figure suivante montre une représentation des icônes d'arborescence et de mappe :

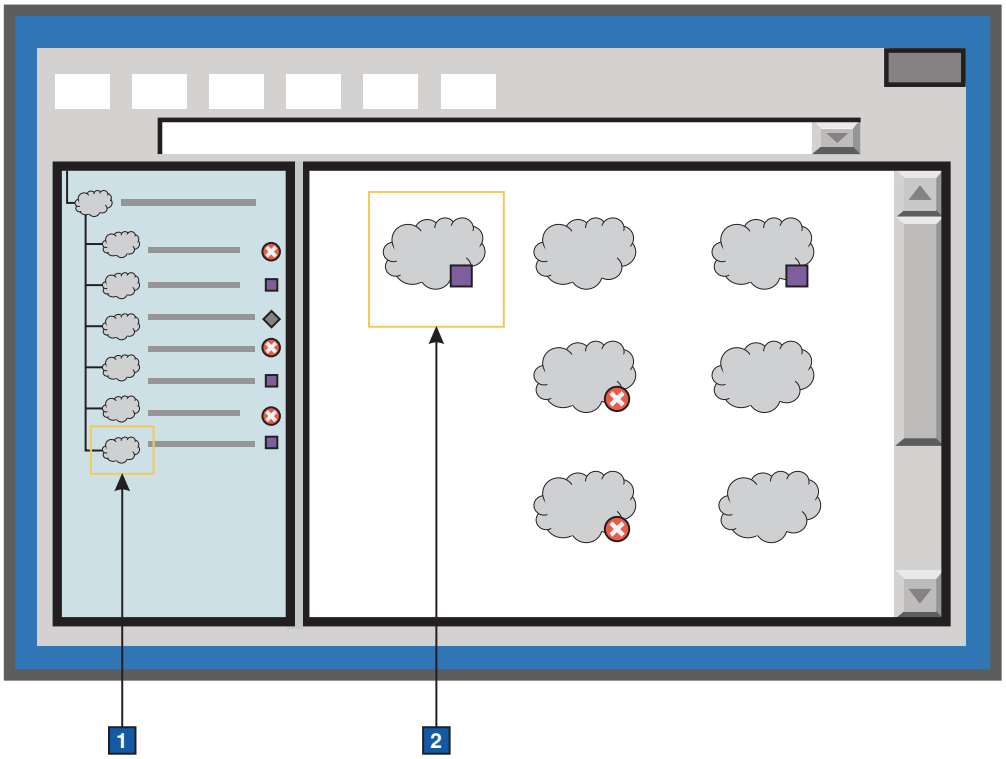

Figure 10. Icônes d'arborescence et de mappe

1 icône arborescence
Utilisée pour représenter les vues dans le Panneau de navigation. Les icônes de mappe et d'arborescence sont en forme de nuage. Les opérateurs réseau peuvent personnaliser ces icônes lorsqu'is définissent une nouvelle vue de réseau dans l'interface graphique des vues de réseau. Pour ce faire, ils doivent en choisir dans une liste d'icônes prédéfinies.

2 icônes de mappe
Utilisées pour représenter les vues dans le Panneau d'affichage de topologie.

Tâches associées:

«Ajout d'icônes», à la page 258
Mettez à la disposition des opérateurs réseau des icônes personnalisées supplémentaires ; ils pourront ainsi utiliser d'autres icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Référence associée:

«Configuration de l'affichage des informations supplémentaires associées à un périphérique», à la page 262
Les informations telles que les statuts d'alerte et l'état de maintenance d'un périphérique sont affichées dans un cadre coloré, autour du périphérique. Vous pouvez configurer les couleurs, les icônes et le positionnement des éléments utilisés pour afficher ces informations.

Types de classes de périphérique :

Toutes les classes de périphérique sont automatiquement catégorisées par *type de classe*. Dans les mappes topologiques, chaque type de classe est représenté par une icône différente, ce qui n'est pas le cas pour les classes de périphérique.

Les types de classe sont stockées dans la base de données de topologie NCIM, dans la zone Typeclasse de la table Typeentité.

Les différents types de classe sont :

- Central
- Noeud d'extrémité
- Périphérique réseau
- Routeur
- Commutateur

Tous les types de classe sont constitués de classes de périphériques. Par exemple, le type de classe Périphérique réseau contient les classes de périphériques Alcatel et Cisco.

Infobulles de périphériques :

Les infobulles de périphériques apparaissent lorsque vous passez la souris sur les périphériques dans les mappes topologiques.

Les infobulles de périphérique sont définis par des entrées HTML dans le fichier de configuration `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` sur le serveur où les composants de l'interface graphique de Network Manager sont installés. Vous pouvez spécifier le contenu des infobulles associées aux périphériques, aux sous-réseaux et aux liens.

Les modifications du fichier `topoviz.properties` sont surveillées toutes les 60 secondes, pour que Topoviz détecte automatiquement ces modifications.

Entrées du fichier topoviz.properties contrôlant les infobulles de périphériques

Les paramètres de contrôle par défaut des infobulles de périphérique sont les suivants :

`topoviz.tooltip.`*`élément_mappe`*`.`*`Typeentité`*`=`*`instruction_HTML`*

Où :

élément_mappe
Prend l'une des valeurs suivantes :

- `périphérique` : Pour une infobulle de boîtier (périphérique de noeud principal) ou de sous-réseau
- `lien`: pour une infobulle de lien

Typeentité
Numéro de type d'entité d'un périphérique, sous-réseau, ou lien. Il prend l'une des valeurs suivantes :

- `1`: pour une infobulle de boîtier (périphérique de noeud principal)
- `15`: pour une infobulle de sous-réseau
- `2`: pour une infobulle de lien

instruction_HTML
Tout code HTML valide utilisé pour définir le contenu et le format de l'infobulle.

Pour insérer la valeur à partir d'une zone d'une base de données topologiques NCIM, utilisez la syntaxe suivante : {*table.zone*}

Exemple

L'exemple d'instruction suivant définit une infobulle :

```
topoviz.tootip.device.1=<b>{entity.displayLabel}</b><br><b>sysDescr</b> 
{chassis.sysDescr}<br><b>sysContact</b> {chassis.sysContact}
```

Modification des icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau

Vous pouvez modifier les icônes représentant les classes de périphériques, les types de classes, les arborescences, et les mappes pour qu'elles soient plus facilement reconnaissables pour les utilisateurs lorsque ces derniers affichent les mappes topologiques dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Ajout d'icônes :

Mettez à la disposition des opérateurs réseau des icônes personnalisées supplémentaires ; ils pourront ainsi utiliser d'autres icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Pour mettre à la disposition des opérateurs réseau des icônes d'arborescence et de mappe personnalisées :

1. Créez votre icône. Pour un meilleur résultat, utilisez l'un des formats suivants :
   - Pour une icône d'arborescence : image PNG, GIF ou JPG de 16 pixels sur 16
   - Pour une icône de mappe : image PNG, GIF, JPG, ou SVG de toute taille.

   Il vous suffit de fournir une image, car Topoviz la met à la bonne échelle.
2. Copiez l'icône vers le répertoire `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/` se trouvant sur le serveur où les applications Web sont installées.

Concepts associés:

«Icônes TopoViz», à la page 255
Dans une mappe topologique, les icônes représentent des types de périphériques ou d'éléments de réseau. Vous pouvez personnaliser ces icônes.

Affectation d'icônes aux périphériques :

Vous pouvez modifier les icônes de périphériques et d'autres entités utilisées dans les mappes de topologie affichées dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Affectation d'icônes aux classes d'unités :

Pour représenter différentes classes d'unités à l'aide de différentes icônes, affectez une icône particulière à chaque classe d'unités. Cela permet aux opérateurs de distinguer les classes d'unités dans les mappes topologiques (par exemple, unités Cisco et Alcatel).

Assurez-vous que des icônes personnalisées sont disponibles, en ajoutant des icônes, comme décrit dans le lien associé.

Pour affecter une icône personnalisée à une classe d'unités :

1. Affectez l'icône préalablement préparée à un type de classe en modifiant une ligne qui décrit l'icône dans le fichier `topoviz.properties`, comme suit :
   a. Modifiez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
   b. Recherchez la section qui spécifie des noms d'icônes pour des types de périphérique.
   c. Modifiez la ligne de code appropriée comme suit :

      `topoviz.deviceicon.`*`classname=kkkkkkkkkkkkkkkkkkkiconname.extension`*

      Où
      - *classname* est le nom de la classe d'unités. Elle doit correspondre au paramètre `active object` dans le fichier AOC qui définit la classe. Les fichiers AOC sont contenus dans le répertoire `$NCHOME/precision/aoc/`.
      - *iconname* est le nom de votre icône.
      - *extension* est l'extension de fichier.
2. Sauvegardez le fichier `topoviz.properties`.

Tâches associées:

«Ajout d'icônes», à la page 258
Mettez à la disposition des opérateurs réseau des icônes personnalisées supplémentaires ; ils pourront ainsi utiliser d'autres icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Affectation d'icônes aux types d'entité :

Certaines entités réseau qui s'affichent dans l'interface graphique ne sont pas des périphériques et, par conséquent, ne disposent pas d'un nom de classe associé. Afin de pouvoir afficher une icône pour ces entités dans l'interface graphique, vous pouvez associer une icône au type d'entité associé à une icône.

Assurez-vous que des icônes personnalisées sont disponibles en ajoutant des icônes comme décrit dans le lien associé.

Pour affecter une icône personnalisée à un type d'entité :

1. Affectez l'icône préalablement préparée à un type de classe en ajoutant une ligne qui décrit l'icône dans le fichier `topoviz.properties`, comme suit :
   a. Modifiez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
   b. Recherchez la section qui spécifie des noms d'icônes pour des types de périphérique.
   c. Ajoutez la ligne de code appropriée comme suit :

      `topoviz.image.`*`type_entité=nom_icône.extension`*

      Où

- *type_entité* est le type d'entité. Ceci doit correspondre exactement au nom du type d'entité comme indiqué dans la table `entityType` NCIM. Pour plus d'informations sur la table `entityType`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données topologiques*.
- *iconname* est le nom de votre icône.
- *extension* est l'extension de fichier.

2. Sauvegardez le fichier `topoviz.properties`.

Tâches associées:

«Ajout d'icônes», à la page 258
Mettez à la disposition des opérateurs réseau des icônes personnalisées supplémentaires ; ils pourront ainsi utiliser d'autres icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Affectation d'icônes aux types de classe :

Modifiez les icônes utilisées pour représenter les types de classe facilite l'identification des types de classe dans les mappes topologiques pour les opérateurs réseau. Les types de classe regroupent plusieurs classes. Par exemple, une icône unique peut représenter le type de classe CiscoSwitch, où le type de classe CiscoSwitch regroupe plusieurs icônes de classe CiscoSwitch.

Assurez-vous que des icônes personnalisées sont disponibles, en ajoutant des icônes, comme décrit dans le lien associé.

Pour affecter une icône personnalisée à un type de classe :

1. Identifiez les classes qui constituent votre type de classe. Par exemple, si vous souhaitez une seule icône pour tous les commutateurs Cisco (type de classe commutateur Cisco), identifiez chacun des fichiers AOC qui représentent des classes de commutateur Cisco individuelles.
2. Accédez au répertoire qui contient les fichiers AOC (Active Object Class). Les fichiers AOC définissent les classes de périphérique.

   ```
   cd $NCHOME/precision/aoc/
   ```

3. Pour chaque fichier AOC de votre type de classe, modifiez le paramètre `visual_icon` comme suit :

   ```
   visual_icon = type_classe;
   ```

   Par exemple, dans chaque fichier AOC de commutateur Cisco, modifiez le paramètre `visual_icon` comme suit :

   ```
   visual_icon = CiscoSwitch;
   ```

   Après avoir modifié les fichiers AOC, redémarrez le processus **`ncp_class`**. Une fois **`ncp_class`** redémarré et en cours d'exécution, redémarrez le processus **`ncp_model`**.
4. Affectez l'icône préalablement préparée à un type de classe. Par exemple, si vous voulez utiliser une icône unique pour représenter tous les commutateurs Cisco (type de classe commutateur Cisco), modifiez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`, recherchez la section indiquant les noms des icônes pour les types de périphériques et modifiez la ligne de code appropriée comme suit :

   ```
   topoviz.image.CiscoSwitch=mon_icône.svg
   ```

   Où *mon_icône* est le nom du fichier de l'icône personnalisée pour le type de classe commutateur Cisco.

5. Sauvegardez le fichier topoviz.properties.

Tâches associées:

«Ajout d'icônes», à la page 258
Mettez à la disposition des opérateurs réseau des icônes personnalisées supplémentaires ; ils pourront ainsi utiliser d'autres icônes dans les interfaces graphiques Vues de réseau et Vue tronçon de réseau.

Configuration des mises à jour et de la présentation de la mappe topologique

Vous pouvez modifier la manière dont les unités et le statut d'alerte sont affichés dans les mappes topologiques. Vous pouvez également modifier la fréquence des mises à jour de la topologie et du statut d'alerte.

Apparence des noeuds et des lignes dans les mappes topologiques :

Par défaut, les noeuds, qui représentent par exemple des périphériques et d'autres entités du réseau, apparaissent toujours devant les lignes montrant les connexions entre les noeuds. Vous pouvez modifier ce paramètre par défaut, mais cela peut rendre difficile la visualisation et l'interaction avec les noeuds.

Par défaut, les noeuds recouvrent les lignes dans une mappe topologique. Le paramètre qui contrôle cette option se trouve dans le fichier suivant : $ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties. Pour trouver ce paramètre, recherchez la section concernée qui commence par le commentaire # Specifies whether nodes are drawn before edges.

```
# Specifies whether nodes are drawn before edges
#    true => Edges overlay nodes
#    false => Nodes overlay edges
topoviz.graph.nodesBeforeEdges=false
```

Par défaut, le paramètre topoviz.graph.nodesBeforeEdges est défini à false, ce qui signifie que les noeuds recouvrent toujours les lignes dans une mappe topologique.

Modification de la fréquence des contrôles de mise à jour de topologie :

TopoViz contrôle régulièrement si la topologie affichée dans une vue de réseau a été mise à jour. Pour modifier la fréquence, modifiez la valeur topoviz.topologyupdateperiod dans le fichier topoviz.properties.

Les nouveaux noeuds apparaissent automatiquement dans les mappes topologiques ; ils sont mis en évidence par des indicateurs.

La fréquence par défaut est 3600 secondes (60 minutes). Vous pouvez la modifier par toute valeur en secondes. Si vous définissez la valeur topoviz.topologyupdateperiod à 0, Topoviz arrête de contrôler les mises à jour de la topologie.

Pour modifier la fréquence des contrôles :

1. Ouvrez le fichier de configuration ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties et identifiez la ligne suivante :

   ```
   topoviz.topologyupdateperiod=3600
   ```

2. Modifiez la fréquence à la valeur voulue, en secondes. Sauvegardez puis fermez le fichier topoviz.properties.

Configuration de l'affichage des informations supplémentaires associées à un périphérique :

Les informations telles que les statuts d'alerte et l'état de maintenance d'un périphérique sont affichées dans un cadre coloré, autour du périphérique. Vous pouvez configurer les couleurs, les icônes et le positionnement des éléments utilisés pour afficher ces informations.

Vous contrôlez l'affichage d'informations supplémentaires associées à un périphérique à l'aide des paramètres des fichiers suivants :

- `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`
- `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`

Les paramètres que vous pouvez configurer à l'aide de ces fichiers sont les suivants :

Statut géré de périphérique
Icônes qui affichent le statut non géré et partiellement non géré, position et taille des icônes.

Indication de périphériques ajoutés manuellement
Icône indiquant qu'il s'agit d'un périphérique ajouté manuellement, position et taille de l'icône.

Statut d'alerte de périphérique
Indique s'il convient d'afficher une icône de statut d'alerte, et dans l'affirmative, position de l'icône de statut d'alerte.

Cadre autour du périphérique
Arrondi des angles du cadre autour du périphérique, hauteur et largeur du cadre.

Texte du libellé du périphérique
Police, taille de police et style de police du texte du libellé du périphérique.

Exemple

La figure suivante montre la représentation d'un périphérique ajouté manuellement en mode non géré.

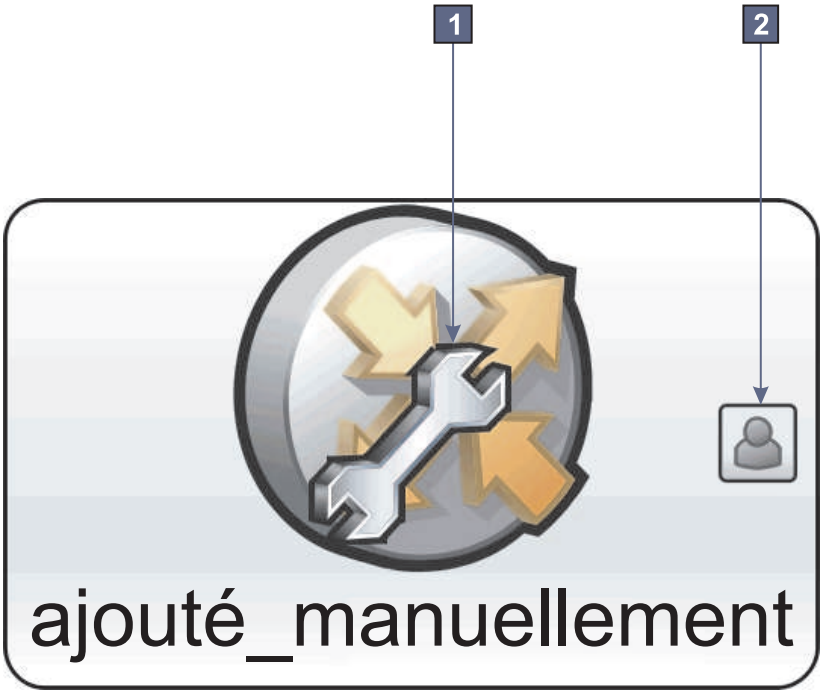

Figure 11. Représentation d'un périphérique ajouté manuellement en mode non géré

Configurez les paramètres des icônes de statut non géré et de périphérique ajouté manuellement comme suit :

1 Icône de statut non géré, position et taille

Les paramètres sont spécifiés dans le fichier `topoviz.properties`. Pour localiser ces paramètres, recherchez la section correspondante qui commence par le commentaire `# Overlay definitions.`.

```
1]    # Overlay definitions.
2]    topoviz.overlay.image.UNMANAGED=unmanaged.svg
3]    topoviz.overlay.position.UNMANAGED=C
4]    topoviz.overlay.size.UNMANAGED=25
5]    topoviz.overlay.image.PARTIALMANAGED=partial_managed.svg
6]    topoviz.overlay.position.PARTIALMANAGED=C
7]    topoviz.overlay.size.PARTIALMANAGED=25
```

Tableau 19. Description des paramètres pour les icônes de statut non géré

Ligne	Description
2	Indique l'icône à utiliser pour indiquer un statut non géré.
3	Indique la position de l'icône de statut non géré. La lettre C signifie centré.
4	Indique la taille de l'icône de statut non géré. Le nombre est une valeur relative.
5	Indique l'icône à utiliser pour indiquer un statut partiellement non géré.
6	Indique la position de l'icône de statut partiellement non géré. La lettre C signifie centré.
7	Indique la taille de l'icône de statut partiellement non géré. Le nombre est une valeur relative.

2 Icône de périphérique ajouté manuellement, position et taille

Les paramètres sont spécifiés dans le fichier `topoviz.properties`. Pour localiser ces paramètres, recherchez la section correspondante qui commence par le commentaire `# Overlay definitions.`.

```
1]    # Overlay definitions - Manual device
2]    topoviz.overlay.image.MANUAL=manualoverlay.svg
3]    topoviz.overlay.position.MANUAL=E
4]    topoviz.overlay.size.MANUAL=10
5]    topoviz.overlay.xoffset.MANUAL=-2
```

Tableau 20. Description des paramètres de l'icône de statut de périphérique ajouté manuellement

Ligne	Description
2	Indique l'icône à utiliser pour indiquer un périphérique ajouté manuellement.
3	Indique la position de l'icône de périphérique ajouté manuellement. La lettre E signifie aligné à droite.
4	Indique la taille de l'icône de périphérique ajouté manuellement. Le nombre est une valeur relative.
5	Indique le décalage sur l'axe des X de l'icône. Le positionnement d'alignement à droite, en ligne 2, place l'icône de sorte qu'elle touche le cadre entourant le périphérique. La valeur de décalage -2 déplace légèrement l'icône vers la gauche de sorte qu'elle se trouve juste à l'intérieur du cadre.

Exemple

La figure suivante montre la représentation d'un périphérique avec une alerte critique associée.

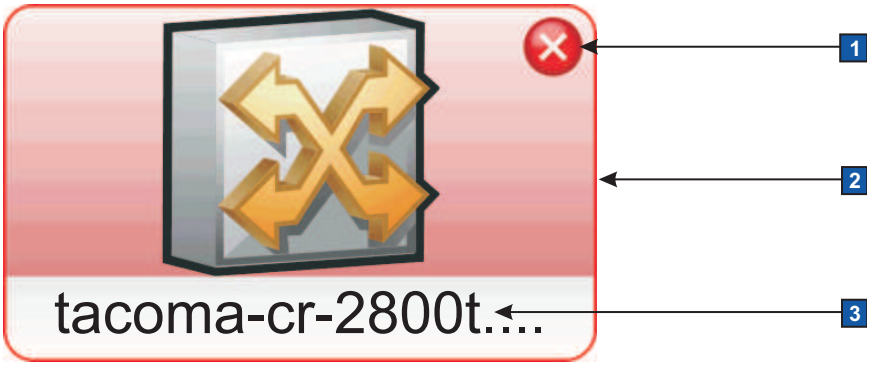

Figure 12. Représentation d'un affichage de périphérique, montrant une alerte critique associée

Configurez les paramètres pour l'icône de statut d'alerte, le cadre de périphérique et le texte de libellé de périphérique comme suit :

1 Icône de statut d'alerte

Les paramètres qui contrôlent si et où il convient d'afficher les icônes de statut d'alerte dans les mappes topologiques sont les suivants. Certains paramètres se trouvent dans le fichier `topoviz.properties` et d'autres sont dans le fichier `status.properties`.

Afficher les icônes de statut d'alerte dans les mappes topologiques

Le paramètre du fichier `status.properties` qui commande au système d'afficher le statut d'alerte est défini `status.enabled=true`.

Position

Le paramètre du fichier `topoviz.properties` qui spécifie la position de l'icône du statut d'alerte est `topoviz.status.position=NE`. Il commande au système de placer l'icône de statut d'alerte dans l'angle supérieur droit du cadre contenant le périphérique.

2 Cadre du périphérique

Les paramètres sont spécifiés dans le fichier `topoviz.properties`. Pour

localiser ces paramètres, recherchez les sections commençant par les commentaires `# Node dimensions` et `# Corner arc`.

```
1]    # Node dimensions (not used in legacy mode).
2]    topoviz.node.height=60
3]    topoviz.node.width=100
4]
5]    # Node resizability
6]    # Options: LOCKED (Fixed height and width)
7]    #   TIGHT_HEIGHT (Fixed height, variable width)
8]    topoviz.node.resizeability=TIGHT_HEIGHT
9]
10]   # Corner arc (not used in legacy mode).
11]   topoviz.node.arc=10
```

Tableau 21. Description des paramètres du cadre du périphérique

Ligne	Description
2	Indique la hauteur du cadre.
3	Indique la largeur du cadre. **Remarque :** Le texte du libellé de périphérique ne revient pas à la ligne, par conséquent si vous souhaitez afficher tout le texte du libellé de périphérique, vous devez augmenter cette valeur de largeur ou réduire la taille de police du texte à l'aide du paramètre **topoviz.node.fontsize**.
8	Indique comment les paramètres **topoviz.node.height** et **topoviz.node.width** sont traités. La valeur par défaut est `TIGHT_HEIGHT`. Lorsque l'option `LOCKED` est utilisée, cela signifie que les valeurs définies dans les paramètres **topoviz.node.height** et **topoviz.node.width** sont utilisés pour le cadre du périphérique. L'utilisation de l'option `TIGHT_HEIGHT` gère le paramètre **topoviz.node.height**, mais pas le paramètre **topoviz.node.width**, ce qui signifie que le cadre du périphérique est élargi automatiquement pour s'adapter au libellé du périphérique, tout en maintenant une largeur minimale.
11	Indique l'arrondi des angles du cadre. Plus la valeur est élevée, plus les angles sont arrondis.

3 Libellé de périphérique

Les paramètres sont spécifiés dans le fichier `topoviz.properties`. Pour localiser ces paramètres, recherchez la section correspondante qui commence par le commentaire `# Font settings.`.

```
1]    # Font settings
2]    topoviz.node.font=Arial,Helvetica
3]    topoviz.node.fontsize=10
4]    topoviz.node.fontstyle=0
```

Tableau 22. Description des paramètres du texte de libellé de périphérique

Ligne	Description
2	Indique la police à utiliser pour le texte de libellé de périphérique.
3	Indique la taille de police à utiliser pour le texte de libellé de périphérique.
4	Indique le style de police à utiliser pour le texte de libellé de périphérique.

Concepts associés:

«Icônes TopoViz», à la page 255
Dans une mappe topologique, les icônes représentent des types de périphériques ou d'éléments de réseau. Vous pouvez personnaliser ces icônes.

Tâches associées:

«Changement des paramètres d'alerte», à la page 267
Si nécessaire, vous pouvez changer les paramètres relatifs aux alertes. Vous pouvez modifier la fréquence des mises à jour des informations sur la gravité de l'alerte, remplacer les icônes par défaut représentant la gravité de l'alerte, configure le mode d'extraction du statut d'alerte et configurer d'autres paramètres d'alerte.

Configuration de la position des noeuds dans les vues de réseau après la reconnaissance :

Vous pouvez configurer la façon dont les noeuds reconnus et existants doivent être positionnés dans les vues de réseau après une reconnaissance du réseau.

Par défaut, le client TopoViz change la présentation d'une mappe de vue de réseau si de nouveaux noeuds reconnus sont ajoutés à la mappe. La position des noeuds existants n'est pas garantie lorsque la présentation de la mappe est mise à jour, car la présentation est régie par des facteurs tels que les informations de connectivité obtenues au cours de la reconnaissance.

Pour changer le comportement par défaut et configurer Network Manager afin de conserver la position des noeuds existants et séparer visuellement les nouveaux noeuds des noeuds déjà présents dans les vues de réseau, éditez les paramètres ci-après.

Remarque : Ce comportement est mieux adapté à la **présentation symétrique**. D'autres options de présentation prennent d'autres facteurs en compte, qui peuvent avoir un impact sur la position des noeuds existants. Par exemple, la **disposition circulaire** met l'accent sur la présentation des noeuds sous forme de disposition circulaire plutôt que sur la conservation de la position des noeuds, alors que les dispositions **hiérarchique** et **orthogonale** mettent l'accent sur le routage des connexions entre les noeuds à l'aide de lignes orthogonales plutôt que sur la conservation de la position exacte des noeuds.

1. Accédez au répertoire `NCHOME/precision/profiles/TIPProfile/etc/tnm` et ouvrez le fichier `topoviz.properties`.
2. Localisez le paramètre **`topoviz.node.freezeold`** et changez la valeur en définissant `true` (la valeur par défaut est `false`).

   Le paramètre `true` conserve la position des noeuds existants, alors que les nouveaux noeuds sont placés sur une ligne au début de la mappe, séparant clairement les nouveaux noeuds des noeuds non ajoutés lors de la dernière reconnaissance. Les nouveaux noeuds sont placés sur une ou plusieurs lignes au début de la mappe avec un espacement horizontal et vertical de 20 pixels par défaut.
3. Déconnectez-vous de l'interface graphique de Network Manager et redémarrez le navigateur. Cette étape est nécessaire pour que le paramètre `true` prenne effet.
4. Facultatif : Vous pouvez ajuster plus en détail le positionnement des nouveaux noeuds avec les paramètres suivants dans le fichier `topoviz.properties` :
   - Vous pouvez définir si les nouveaux noeuds doivent être placés au début ou à la fin de la mappe avec le paramètre **`topoviz.node.new.placement`**. Le paramètre par défaut est `top` ; remplacez-le par `bottom` pour que les nouveaux noeuds soient placés à la fin de la mappe de vue de réseau.
   - Vous pouvez définir l'espacement horizontal entre les nouveaux noeuds en pixels avec le paramètre **`topoviz.node.new.spacing.horizontal`**. Le paramètre par défaut est `20` pixels ; remplacez-le par un nombre de pixels différent afin de rapprocher ou d'éloigner horizontalement les nouveaux noeuds les uns par rapport aux autres.
   - Vous pouvez définir l'espacement vertical entre les nouveaux noeuds en pixels avec le paramètre **`topoviz.node.new.spacing.vertical`**. Le paramètre par défaut est `20` pixels ; remplacez-le par un nombre de pixels différent afin de rapprocher ou d'éloigner verticalement les nouveaux noeuds les uns par rapport aux autres.

Remarque : Tous les paramètres supplémentaires présentés dans cette étape ne sont appliqués que si le paramètre **topoviz.node.freezeold** a pour valeur `true`.

Changement des paramètres d'alerte :

Si nécessaire, vous pouvez changer les paramètres relatifs aux alertes. Vous pouvez modifier la fréquence des mises à jour des informations sur la gravité de l'alerte, remplacer les icônes par défaut représentant la gravité de l'alerte, configure le mode d'extraction du statut d'alerte et configurer d'autres paramètres d'alerte.

Référence associée:

«Configuration de l'affichage des informations supplémentaires associées à un périphérique», à la page 262
Les informations telles que les statuts d'alerte et l'état de maintenance d'un périphérique sont affichées dans un cadre coloré, autour du périphérique. Vous pouvez configurer les couleurs, les icônes et le positionnement des éléments utilisés pour afficher ces informations.

Modification de la fréquence de mise à jour de la gravité d'alerte :

Si nécessaire, modifiez la fréquence de mise à jour des informations sur la gravité d'alerte sur interface graphique Web Tivoli Netcool/OMNIbus.

Pour modifier la fréquence de mise à jour de la gravité d'alerte :

1. Sur le serveur sur lequel les applications Web sont installées, ouvrez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`.
2. Effectuez les modifications suivantes :
   - Pour modifier la fréquence des mises à jour d'alerte de gravité dans l'arborescence de vue de réseau, modifiez la valeur de la propriété `status.tree.updateperiod`. La valeur est affichée en secondes. Par exemple :
     ```
     status.tree.updateperiod=60
     ```
   - Pour modifier la fréquence des mises à jour d'alerte de gravité dans la mappe topologique, modifiez la valeur de la propriété `status.map.updateperiod`. La valeur est affichée en secondes. Par exemple :
     ```
     status.map.updateperiod=60
     ```
3. Sauvegardez et fermez le fichier.

Modification des icônes des niveaux de gravité d'alerte :

Vous pouvez modifier les icônes de statut d'alerte utilisées pour représenter les niveaux de gravité d'alerte dans l'arborescence de vue de réseau, la mappe topologique et la présentation tabulaire de la topologie.

Modification des icônes des niveaux de gravité d'alerte dans l'arborescence de vue de réseau et la mappe topologique :

Si vous souhaitez que des icônes de statut d'alerte différentes représentent les niveaux de gravité d'alerte dans l'arborescence de vue de réseau et la mappe topologique, remplacez les icônes par défaut.

Les formats requis pour les icônes de remplacement sont les suivants :

- Pour l'arborescence des vues de réseau : GIF ou PNG.
- Pour la mappe topologique : GIF, PNG ou SVG.

GIF ou SVG.

Pour remplacer une icône par défaut :

1. Créez l'image de l'icône de sécurité que vous souhaitez remplacer et copiez-la dans ITNMHOME/profiles/TIPProfile/etc/tnm/resource/.
2. Ouvrez le fichier ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties et procédez aux modifications suivantes.
   a. Dans la section Tree status images des fichiers, associez la propriété correspondant au niveau de gravité requis à la nouvelle image. Par exemple, pour remplacer le fichier par défaut critical.gif pour le niveau de gravité 5 avec votre propre image :

      status.tree.image.5=status/<*nom de fichier de la nouvelle icône "critique"*>.gif
   b. Dans la section Map status images des fichiers, associez la propriété correspondant au niveau de gravité requis à la nouvelle image. Par exemple, pour remplacer le fichier par défaut critical.gif pour le niveau de gravité 5 avec votre propre image :

      status.map.image.5=status/<*nom de fichier de la nouvelle icône "critique"*>.gif
3. Répétez la procédure pour chaque icône par défaut à remplacer.
4. Sauvegardez et fermez le fichier.

Modification des icônes des niveaux de gravité d'alerte dans la présentation tabulaire de la mappe topologique :

Si vous souhaitez que des icônes de statut d'alerte différentes représentent les niveaux de gravité d'alerte dans l'option de présentation tabulaire de la mappe topologique, remplacez les icônes par défaut.

Les formats requis pour les icônes de remplacement de la vue de la table de la mappe topologique sont GIF ou PNG.

Pour remplacer une icône par défaut :

1. Créez l'image de l'icône de sécurité que vous souhaitez remplacer et copiez-la dans ITNMHOME/profiles/TIPProfile/etc/tnm/resource/.
2. Ouvrez le fichier ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties et, dans la section Net View Table status images, associez la propriété correspondant au niveau de gravité requis à la nouvelle image. Par exemple, pour remplacer le fichier par défaut ac16_critical04_24.gif de niveau de gravité 5 par votre propre image :

   status.table.image.5=status/<*filename for new critical icon*>.gif
3. Répétez la procédure pour chaque icône par défaut à remplacer.
4. Sauvegardez et fermez le fichier.

Configuration de filtres de liste des événements actifs pour l'arborescence des vues de réseau :

Lorsque vous cliquez sur une icône de statut d'alerte dans l'arborescence des vues de réseau, une liste des événements actifs filtrée s'affiche. Vous pouvez configurer l'arborescence des vues de réseau afin de définir ces filtres à la demande, ce qui permet d'utiliser une quantité inférieure de mémoire.

La configuration de filtres de liste des événements actifs à définir pour toutes les vues de réseau de l'arborescence des vues de réseau consomme une quantité élevée de mémoire, particulièrement si les arborescences de navigation sont profondes et très structurées et comportent un nombre élevé de vues parent, ce qui peut entraîner des problèmes de performance.

Vous pouvez configurer l'arborescence des vues de réseau afin de définir des filtres de liste des événements actifs pour la vue de réseau affichée seulement. La définition de filtres à la demande utilise une quantité inférieure de mémoire. Par défaut, le filtrage à la demande est désactivé et des filtres sont créés pour toutes les vues lorsque l'arborescence des vues de réseau est affichée.

Des filtres sont toujours créés pour les noeuds feuille dans l'arborescence des vues de réseau. Les noeuds feuille sont des vues de réseau (et non des conteneurs) qui ne contiennent pas eux-mêmes d'autres vues de réseau. Le statut d'alerte agrégé est affiché pour tous les noeuds de l'arborescence des vues de réseau, que les filtres de liste des événements actifs à la demande soient activés ou non.

Pour configurer des filtres de liste des événements actifs à la demande dans l'arborescence des vues de réseau, procédez comme suit :

1. Sur le serveur sur lequel les applications Web sont installées, sauvegardez et éditez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`.
2. Effectuez les modifications suivantes :
   - Pour activer les filtres de liste des événements actifs à la demande dans l'arborescence des vues de réseau, remplacez la valeur de la propriété status.tree.filterael par false. Les filtres de liste des événements actifs ne sont créés que si vous ouvrez une vue de réseau. Lorsque vous ouvrez une liste des événements actifs depuis une vue de réseau parent dans l'arborescence des vues de réseau qui n'a pas été ouverte dans le panneau d'affichage de la topologie, la liste des événements actifs répertorie des événements pour tous les périphériques. Si vous cliquez sur la vue de réseau, puis lancez une liste des événements actifs depuis cette vue, la liste des événements actifs est filtrée et n'affiche que les événements relatifs aux périphériques de cette vue.
   - Pour désactiver les filtres de liste des événements actifs à la demande dans l'arborescence des vues de réseau, remplacez la valeur de la propriété status.tree.filterael par true. Des filtres de liste des événements actifs sont créés pour chaque vue à l'avance. Lorsque vous ouvrez une liste des événements actifs depuis une vue de réseau, la liste des événements actifs est filtrée et n'affiche que les événements relatifs aux périphériques de cette vue.
3. Sauvegardez et fermez le fichier.

Paramètres du statut d'alerte :

Les paramètres de statut d'alerte déterminent si les périphériques sont affichés dans les mappes topologiques, comment ils s'affichent, et la fréquence de mise à jour des paramètres.

Les paramètres de statut d'alerte figurent dans le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`. Le tableau suivant décrit les propriétés. Lorsque plusieurs propriétés contrôlent une valeur pour chaque gravité d'alerte, une seule propriété avec un astérisque (*) est indiquée. Par exemple, **`status.color.background.*`** correspond aux propriétés **`status.color.background.unknown`**, **`status.color.background.nonw`** et **`status.color.background.0`** à **`status.color.background.5`**.

Tableau 23. Paramètres du statut d'alerte

Paramètre	Description
`status.color.background.*`	Indique la couleur du statut d'arrière-plan pour chaque gravité.

Tableau 23. Paramètres du statut d'alerte (suite)

Paramètre	Description
status.color.foreground.*	Indique la couleur du libellé de périphérique pour chaque gravité.
status.enabled	Indique si le statut du périphérique est affiché ou non dans les mappes topologiques.

status.globalfilter	Filtres certaines alertes de l'affichage du statut des périphériques dans la mappe topologique. Cette propriété effectue un filtrage sur la table `alerts.status` du serveur ObjectServer.
	
	L'exemple suivant empêche les événements d'échec PING d'affecter le statut affiché des périphériques dans la topologie :
	`status.globalfilter=EventId<>' NmosPingFail'`
	
	L'exemple suivant affiche le statut des périphériques des vues de topologie auxquels sont associés des événements marqués par `EventId ='NmosPingFail'` :
	`viewsstatus.globalfilter=EventId= 'NmosPingFail'`
	
	L'exemple suivant affiche le statut des périphériques des vues de topologie auxquels sont associés des événements marqués par une gravité (`Severity`) mineure (`Minor`), majeure (`Major`) ou critique (`Critical`) :
	`status.globalfilter=Severity>2`

status.hopview.linestyle	Indique si le statut d'alerte doit s'afficher sur les liens entre les noeuds dans la Vue Tronçon.
status.map.updateperiod	Indique comment le système met à jour les paramètres de statut d'alerte dans les mappes de topologie.
status.map.maxnodes	Indique le nombre maximal de noeuds pour lequel le statut d'alerte peut s'afficher dans une mappe de topologie unique.
status.map.image.*	Indique les icônes utilisées pour représenter le statut d'alerte d'un périphérique dans la mappe topologique. Pour changer ces icônes, créez un fichier `.gif` ou `.svg` avec un nom approprié et sauvegardez-le dans `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
status.map.image.size.*	Indique la taille des icônes représentant le statut d'alerte de périphérique dans les mappes topologiques.

Tableau 23. Paramètres du statut d'alerte (suite)

Paramètre	Description
status.map.image.xoffset.* **status.map.image.yoffset.***	Indique le décalage sur l'axe des X et des Y de l'icône. Le positionnement NE (nord-est) spécifié dans le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` place l'icône de sorte qu'elle touche le cadre entourant le périphérique. Les valeurs de décalage déplacent l'icône vers le bas à gauche de sorte qu'elle se trouve à l'intérieur du cadre.
status.map.topcolor.saturation.* **status.map.bottomcolor.saturation.*** **status.map.topcolor.brightness.*** **status.map.bottomcolor.brightness.***	Indique les commandes d'ajustement de la saturation et de la brillance qui contrôlent le gradient de la couleur d'état d'arrière-plan pour chaque niveau de gravité d'alerte.
status.netview.linestyle	Indique si le statut d'alerte doit s'afficher sur les liens entre les noeuds dans les Vues de réseau.
status.none.enabled	Indique si le statut None du périphérique est représenté de la même façon que le statut effacer. **Conseil :** Le statut None signifie qu'aucun événement n'a été reçu pour le périphérique. Le statut effacer signifie que les événements antérieurs de gravité 1 ou plus sont effacés du périphérique.
status.pathview.linestyle	Indique si le statut d'alerte doit s'afficher sur les liens entre les noeuds dans la Vue Tronçon. S'applique également à TE MPLS et Chemins IP.
status.registration.devicealert	Définissez cette propriété sur `true` pour inclure des alertes à partir des unités dans le statut d'alerte des vues qui sont basées sur les composants de périphérique. Par exemple, si vous avez une vue MPLS comprenant uniquement des interfaces, vous pouvez vouloir exclure des alertes à partir du boîtier des unités contenant ces interfaces. Pour exclure les alertes des noeuds principaux, définissez cette propriété sur `false`.
status.table.image.*	Indique les icônes utilisées pour représenter le statut d'alerte d'un périphérique dans la mappe topologique en mode de présentation tabulaire. Pour changer ces icônes, créez un fichier `.gif` ou `.svg` avec un nom approprié et sauvegardez-le dans `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
status.table.image.sortUp **status.table.image.sortDown**	Indique comment trier les icônes de gravité d'alerte dans la mappe de topologie en mode de présentation tabulaire.

Tableau 23. Paramètres du statut d'alerte (suite)

Paramètre	Description
status.tree.filterael	Pour activer les filtres de liste des événements actifs (AEL) à la demande dans l'arborescence des vues de réseau, remplacez la valeur de la propriété **status.tree.filterael** par `false`. Lorsque vous ouvrez une liste des événements actifs depuis une vue de réseau parent dans l'arborescence des vues de réseau qui n'a pas été ouverte dans le panneau d'affichage de la topologie, la liste des événements actifs répertorie des événements pour tous les périphériques. Si vous cliquez sur la vue de réseau, puis lancez une liste des événements actifs depuis cette vue, la liste des événements actifs est filtrée et n'affiche que les événements relatifs aux périphériques de cette vue. L'activation des filtres à la demande utilise une quantité inférieure de mémoire. Pour désactiver les filtres de liste des événements actifs à la demande dans l'arborescence des vues de réseau, remplacez la valeur de la propriété **status.tree.filterael** par `true`. Lorsque vous ouvrez une liste des événements actifs depuis une vue de réseau, la liste des événements actifs est filtrée et n'affiche que les événements relatifs aux périphériques de cette vue.
status.tree.updateperiod	Indique la fréquence de mise à jour des paramètres de statut d'alerte dans le panneau de navigation Vues de réseau et Navigateur de structure.
status.tree.image.*	Indique les icônes utilisées pour représenter le statut d'alerte d'un périphérique dans l'arborescence d'une vue de réseau. Pour changer ces icônes, créez un fichier `.gif` ou `.svg` avec un nom approprié et sauvegardez-le dans `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.

Configuration de la différenciation visuelle entre des unités ajoutées manuellement et des unités reconnues :

Vous pouvez configurer les vues topologiques pour mettre en évidence des unités ajoutées manuellement dans la mappe topologique à l'aide d'une icône de recouvrement.

Pour configurer le système pour mettre en évidence des unités ajoutées manuellement :

1. Modifiez le fichier suivant : `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
2. Dans ce fichier, recherchez la valeur `topoviz.topologymanagement.differentiate_manual`.

- `topoviz.topologymanagement.differentiate_manual=true` : configure des unités et connexions ajoutées manuellement à différencier des unités et connexions reconnues.
- `topoviz.topologymanagement.differentiate_manual=false` : les unités et connexions ajoutées manuellement ne sont pas différenciées des unités et connexions reconnues.

Par défaut, cette valeur est définie sur `true`.

3. Si le paramètre est `topoviz.topologymanagement.differentiate_manual=true`, vérifiez la configuration de l'image de recouvrement pour la différenciation des noeuds ajoutés manuellement.

```
# Overlay definitions - Manual device
topoviz.overlay.image.MANUAL=manualoverlay.svg
topoviz.overlay.position.MANUAL=E
topoviz.overlay.size.MANUAL=10
topoviz.overlay.xoffset.MANUAL=-2
```

Ce fragment de configuration contient les paramètres suivants :

- L'image de recouvrement utilisée est intitulée `manualoverlay.svg`. Ce fichier se trouve dans `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`. Vous pouvez modifier l'image de recouvrement utilisée en copiant une autre icône .svg dans `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/manualoverlay.svg`.
- Par défaut, l'icône s'affiche à droite (E signifie Est) de l'unité ajoutée manuellement. Les autres options sont N, S, O, NE, NO, SO, SE et C (pour centré sur l'unité).

4. Sauvegardez le fichier `topoviz.properties`.

Passage en mode de visualisation version 3.8 :

Les icônes de topologie, ainsi que leur présentation, ont changé dans la version 3.9 par rapport aux versions précédentes. Utilisez ces informations si vous voulez repasser en mode version 3.8 de présentation de la topologie.

Pour repasser en mode de présentation de topologie version 3.8, modifiez les fichiers de configuration suivants :

- `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`
- `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`

1. Ouvrez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
2. Recherchez le texte `legacy`.
3. A chaque fois que le texte `legacy` est trouvé, suivez les instructions figurant dans les commentaires.
4. Sauvegardez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
5. Ouvrez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`.
6. Recherchez le texte `legacy`.
7. A chaque fois que le texte `legacy` est trouvé, suivez les instructions figurant dans les commentaires.
8. Sauvegardez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`.

Chargement des informations MIB mises à jour

Pour garantir que le navigateur de la base d'informations de gestion (MIB) contient les informations MIB les plus récentes, chargez les informations MIB mises à jour en exécutant l'application de ligne de commande **ncp_mib**.

Vous ne devez exécuter l'application de ligne de commande ncp_mib que lorsque de nouvelles informations MIB sont ajoutées au répertoire NCHOME/precision/mibs. Celle-ci est exécutée une fois lors de l'installation, donc si vous n'ajoutez pas de nouvelles informations MIB, vous ne devez pas l'exécuter à nouveau.

Important : Vous devez exécuter ncp_mib si vous effectuez une migration de données vers une nouvelle version de Network Manager et que vous avez copié des MIB personnalisés dans le cadre de cette migration de données. Si vous l'omettez, des processus (tels que l'auxiliaire SNMP, ncp_dh_snmp) ne seront pas lancés au démarrage de Network Manager.

Important : Toutes les bases d'informations de gestion (MIB) doivent être valides pour pouvoir faire l'objet d'une analyse syntaxique correcte. La commande ncp_mib distingue les majuscules des minuscules et requière une extension en .mib (et non .MIB). Le préfixe peut être une association entre majuscules et minuscules.

Une fois exécuté, **ncp_mib** remplit le schéma ncmib dans la base de données NCIM pour fournir un lieu de stockage central de toutes les informations MIB pouvant faire l'objet d'une requête par Network Manager. Le schéma ncmib de la base de données NCIM est défini dans le répertoire NCHOME/etc/precision/MibDbLogin.cfg. La valeur par défaut est MIB.

Il n'existe qu'un seul processus **ncp_mib** pour tous les domaines. Par conséquent, il n'existe pas d'option -domain pour **ncp_mib**. De même, cette commande ne dispose pas de dépendances de processus.

Dans une installation répartie, ncp_mib est installé sur le serveur Tivoli Integrated Portal, c'est-à-dire sur le même serveur que les applications Web Network Manager.

Si votre base de données MIB est endommagée ou si vous voulez importer une nouvelle MIB en conflit avec l'une de celles importées précédemment, notez les différentes options de ligne de commande en exécutant **ncp_mib -help**. Pour plus d'informations sur l'option de ligne de commande ncp_mib, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Conseil : Si vous n'êtes pas certain du résultat, exécutez **ncp_mib** à l'aide de l'option **-dryrun**. Vous pouvez voir les résultats mais la base de données ne sera pas modifiée.

Pour mettre à jour les informations MIB, suivez la procédure suivante sur le serveur sur lequel Tivoli Integrated Portal est installé.

1. Copiez tous les nouveaux fichiers MIB vers le répertoire NCHOME/precision/mibss.
2. Assurez-vous que les autorisations d'accès à la base de données sont correctes.

   Les seuls paramètres de configuration requis pour l'application de ligne de commande ncp_mib sont les autorisations d'accès à la base de données NCIM. Ils sont stockées dans un fichier de configuration, NCHOME/etc/precision/

`MibDbLogin.cfg`. Notez qu'en raison du fait que **ncp_mib** dépend du domaine, ce fichier ne dispose pas de variantes spécifiques au domaine comme les autres fichiers de configuration.

3. Démarrez le processus **ncp_mib** en émettant la commande **ncp_mib**.

Pour vérifier que le chargement d'une MIB a abouti, recherchez dans la table de base de données ncmib.mib_modules en entrant la commande suivante à partir de l'invite de la base de données NCIM (cet exemple part du principe que NCIM s'exécute sur MySQL) :

```
mysql> select * from ncmib.mib_modules where moduleName ='RFC1213-MIB';
```

Si les MIB sont chargées, une table contenant un nom de module RFC1213-MIB s'affiche.

Vous pouvez également vérifier que les MIB sont chargées en exécutant la commande **ncp_mib** avec l'option `-messagelevel info`. Un message similaire au message suivant vous informe que les MIB sont en cours de traitement :

```
09/10/08 12:41:08: Information: I-MIB-001-013: [1096571552t]
Resolving references for module 'RFC1213-MIB'
```

Lorsque le traitement est terminé, un message indique que les MIB ont été validées dans la base de données.

Conseil : Pour obtenir des informations sur l'utilisation du navigateur MIB SNMP et la création de graphiques à l'aide des variables MIB, consultez le guide *IBM Tivoli Network Manager IP Edition - Guide de traitement des incidents liés au réseau*.

Configuration de la présentation d'événements d'unités non gérées

Vous pouvez configurer la façon dont les événements d'unités non gérées (unités qui ne sont pas interrogées par Network Manager) sont présentés aux opérateurs de réseau.

Pour configurer la présentation d'événements non gérés par Network Manager dans la **Liste des événements actifs**, réalisez l'une des actions suivantes :

- Elimination par filtrage des événements non gérés de sorte qu'ils n'apparaissent pas dans la **Liste des événements actifs**, ou balisage de ces événements dans la **Liste des événements actifs** pour que vous sachiez qu'ils proviennent d'unités non gérées.
- Balisage de ces événements dans la **Liste des événements actifs** pour que l'opérateur de réseau sache qu'ils proviennent d'unités non gérées. Dans ce cas, la zone NmosManagedStatus associée à un événement non géré dans la **Liste des événements actifs** affiche la valeur 1 (Opérateur non géré) ou 2 (Système non géré).

Les analyses Tivoli Netcool/OMNIbus et les sources d'événements d'autres systèmes de gestion de réseau peuvent générer des événements sur des unités ou des interfaces signalées comme non gérées dans Network Manager. En général, une unité non gérée est signalée comme non gérée car elle est en cours de maintenance et peut, par conséquent, générer des événements réseau inutiles. Les rubriques suivantes expliquent comment gérer les événements réseau d'une unité non gérée.

A faire : Les unités non gérées s'affichent sur la mappe de réseau à l'aide d'icônes superposées en forme de clé à double extrémité. Les unités partiellement non gérées (unités dans lesquelles seules certaines interfaces ne sont pas gérées) s'affichent sur la mappe de réseau à l'aide d'icônes superposées en forme de clé à une seule extrémité.

Elimination par filtrage des événements d'unités non gérées

Vous pouvez filtrer des événements d'unités non gérées pour qu'ils n'apparaissent pas dans la **Liste des événements actifs**.

1. Dans la **Liste des événements actifs**, sélectionnez le **Générateur de filtre**.
2. Créez un nouveau filtre ou éditer le filtre existant pour éliminer par filtrage tous les événements où la zone NmosManagedStatus est égale à 1 (opérateur non géré) ou 2 (système non géré).

Une fois que vous avez terminé cette opération et appliqué le filtre à la **Liste des événements actifs**, les événements d'unités non gérées n'apparaissent plus dans la **Liste des événements actifs**.

Marquage des événements pour les unités non gérées

Vous pouvez marquer les événements dans la **Liste des événements actifs** afin de savoir qu'ils proviennent d'unités non gérées.

1. Dans la **Liste des événements actifs**, sélectionnez le **View Builder (Générateur de vues)**.
2. Créez une vue ou modifiez une vue existante pour afficher la zone NmosManagedStatus associée à un événement. Cette zone affiche l'état géré l'unité ou de l'interface associée à l'événement. Pour les unités non gérées, cette zone affiche la valeur 1 (non gérée par l'opérateur) ou 2 (non gérée par le système).

Une fois que vous avez terminé cette opération et appliqué la vue à la **Liste des événements actifs**, chaque événement de la **Liste des événements actifs** affiche l'état géré de l'unité ou de l'interface réseau associée.

Configuration de Tivoli Common Reporting

Network Manager utilise Tivoli Common Reporting comme outil de production de rapports. Effectuez les tâches suivantes pour configurer Tivoli Common Reporting en vue de l'exécution des rapports Network Manager.

Restriction : Vous pouvez choisir de configurer Tivoli Common Reporting 2.x sur votre machine locale, mais notez que Tivoli Common Reporting 2.x ne prend pas en charge Internet Explorer version 10 ou 11. Par conséquent, vous ne pouvez pas utiliser la fonction de génération de rapports si vous utilisez Internet Explorer 10 ou 11 pour l'interface graphique de Network Manager. Vous pouvez aussi installer Tivoli Common Reporting 3.1 à distance : Tivoli Common Reporting 3.1 fonctionne avec tous les navigateurs.

Restriction : Tivoli Common Reporting 3.1 est disponible uniquement pour les utilisateurs de Netcool Operations Insight.

Configuration de Tivoli Common Reporting 2.x

Exécutez ces tâches pour configurer Tivoli Common Reporting 2.x. Notez que Tivoli Common Reporting 2.x ne prend pas en charge Internet Explorer version 10 ou 11. Par conséquent, vous ne pouvez pas utiliser la fonction de génération de rapports si vous utilisez Internet Explorer 10 ou 11 pour l'interface graphique de Network Manager.

Configuration de rapports pour des installations existantes

Vous pouvez configurer les rapports de gestion de réseau fournis par Network Manager en vue de leur utilisation avec Tivoli Common Reporting.

Pour que vous puissiez activer des rapports de gestion de réseau, Tivoli Common Reporting doit être installé. Si vous avez installé des composants d'interface graphique Network Manager sur une machine sur laquelle Tivoli Common Reporting est déjà installé, il n'est pas nécessaire d'effectuer ces opérations.

Pour configurer des rapports de gestion de réseau :

1. Connectez-vous à la machine sur laquelle les composants d'interface graphique Network Manager et Tivoli Common Reporting sont installés.
2. Exécutez le script pour configurer des rapports de gestion de réseau à partir du tableau de bord du programme d'installation ou depuis la ligne de commande :

Option	Description
A partir du tableau de bord	1. Accédez au répertoire dans lequel vous avez extrait le package d'installation de Network Manager. 2. Démarrez le tableau de bord en tant que l'utilisateur ayant installé Network Manager à l'aide de la commande **`./launchpad.sh`**. 3. Sélectionnez le menu de post-installation. 4. Développez **Installer les rapports Network Manager à utiliser avec TCR** et cliquez sur **Installer les rapports Network Manager**.
A partir de la ligne de commande	1. Placez-vous dans le répertoire `NCHOME/precision/products/tnm/bin`. 2. Exécutez le script `configTCR.sh -d` *`mot_de_passe_base_de_données_NCIM`* `-p` *`mot_de_passe_administrateur_TIP`* `-i install`. 3. Oracle Lorsque vous utilisez une configuration Oracle RAC ou un nom de service pour vous connecter à la base de données, ajoutez aussi l'option `-s` *`nom_service_Oracle`* afin de définir l'adresse URL JDBC pour l'accès à la base de données. L'option `-s` est requise afin de configurer la source de données BIRT pour l'accès à la base de données à l'aide du nom de service. **Remarque :** Vous devez utiliser la ligne de commande dans ces cas. Le tableau de bord ne propose pas l'option permettant d'utiliser la valeur `-s`.

Configuration des sources de données pour BIRT

Fix Pack 5

Si vous utilisez des rapports basés sur le modèle de données BIRT, vous devez configurer des sources de données. Si vous utilisez également des rapports basés sur le modèle Cognos, vous devez configurer les sources de données Cognos séparément.

Si vous n'utilisez pas Tivoli Data Warehouse, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM.

Si vous utilisez Tivoli Data Warehouse, configurez les sources de données `NCIM` et `PARAMETERS` de telle sorte qu'elles pointent vers la base de données NCIM, et `NCPOLLDATA` de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse. Obtenez les détails relatifs à la connexion et à la base de données auprès de l'administrateur de base de données avant de commencer cette procédure.

Conseil : La documentation de référence de chaque rapport vous indique si le rapport emploie le modèle de données BIRT ou Cognos.

Pour configurer les sources de données de tous les rapports basés sur le modèle de données BIRT, procédez comme indiqué ci-après.

1. Si Tivoli Common Reporting est installé sur le même serveur que Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script `configTCR.sh` avec une commande similaire à la commande suivante : UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d motdepasse_bdd_NCIM
    -p motdepasse_administrateur_TIP
   ```

   Le tableau suivant décrit les options de ligne de commande :

Tableau 24. Options de ligne de commande pour configTCR

Option de ligne de commande	Description
`-d`	Mot de passe du nom d'utilisateur de la base de données NCIM, sur la machine locale ou sur un hôte distant.
`-p`	Mot de passe de l'administrateur de Tivoli Integrated Portal.
`-i` *install*	Indique que les rapports de gestion de réseau sont installés. Vous devez utiliser le paramètre **`install`** dans tous les cas après l'option `-i`.
Oracle `-s` *nom_service_Oracle*	Lorsque vous utilisez une configuration Oracle RAC ou un nom de service pour vous connecter à la base de données, utilisez cette option suivie du *nom_service_Oracle* afin de définir l'adresse URL JDBC d'accès à la base de données. L'option `-s` est requise afin de configurer la source de données BIRT pour l'accès à la base de données à l'aide du nom de service.

Tableau 24. Options de ligne de commande pour configTCR (suite)

Option de ligne de commande	Description
`-t` *chemin_TIPHOME*	Si TIPHOME n'est pas configuré ou si vous n'avez pas exécuté le script env.sh, vous pouvez définir l'emplacement auquel l'instance Tivoli Integrated Portal est installée.
`-r` *chemin_package_rapports*	Si, dans votre installation Network Manager, le package de rapports se trouve dans un emplacement autre que l'emplacement par défaut, vous pouvez définir l'emplacement dans lequel le package utilise cette option.
`-u` *nom_utilisateur_NCPOLLDATA*	Dans certaines bases de données, comme Oracle, les noms d'utilisateur peuvent être différents pour la base de données NCIM et la base de données NCPOLLDATA. Vous devez spécifier les deux noms d'utilisateur s'ils sont différents. Utilisez cette option pour indiquer le nom d'utilisateur NCPOLLDATA.
`-v` *mot_de_passe_NCPOLLDATA*	Si vous définissez le nom d'utilisateur NCPOLLDATA, vous devez définir son mot de passe avec cette option.
`-e` *nom_utilisateur_NCIM*	Dans certaines bases de données, comme Oracle, les noms d'utilisateur peuvent être différents pour la base de données NCIM et la base de données NCPOLLDATA. Vous devez spécifier les deux noms d'utilisateur s'ils sont différents. Utilisez cette option pour indiquer le nom d'utilisateur NCIM. L'option `-d` définit le mot de passe pour cet utilisateur.

2. Si Tivoli Common Reporting est installé sur un serveur différent de celui de Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script `configRemoteTCR.sh` avec une commande similaire à la commande suivante : UNIX

```
$NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -b nom_bdd
-d motdepasse_NCIM -e nom_utilisateur_NCIM -h
nom_hôte_bdd  [-i install] -j nom_utilisateur_admin_tip
 -n port_bdd -p motdepasse_admin_tip
[-r répertoire_packages] [-s nom_service_Oracle]
 -t $REP_PRINCIPAL_TIP -z type_bdd
```

   Restriction : Le script `configRemoteTCR.sh` est disponible dans Network Manager à partir de la version 3.9 groupe de correctifs 5.

   Le tableau suivant décrit les options de ligne de commande pour le script **`configRemoteTCR`**.

Tableau 25. Options de ligne de commande pour configRemoteTCR

Option de ligne de commande	Description
`-b` *nom_bdd*	Nom de la base de données DB2 NCIM ou nom du service Oracle NCIM

Tableau 25. Options de ligne de commande pour configRemoteTCR (suite)

Option de ligne de commande	Description
`-d` *motdepasse_NCIM*	Mot de passe du nom d'utilisateur de la base de données NCIM. La base de données NCIM peut être installée sur le serveur local ou sur un hôte distant.
`-e` *nom_utilisateur_NCIM*	Dans certaines bases de données, comme Oracle, les noms d'utilisateur peuvent être différents pour la base de données NCIM et la base de données NCPOLLDATA. Vous devez spécifier les deux noms d'utilisateur s'ils sont différents. Utilisez cette option pour indiquer le nom d'utilisateur NCIM. L'option `-d` définit le mot de passe pour cet utilisateur.
`-h` *nom_hôte_bdd*	Nom d'hôte de la base de données NCIM
`-i` *install*	Indique que les rapports de gestion de réseau sont installés. Vous devez utiliser le paramètre **`install`** dans tous les cas après l'option `-i`.
`-j` *nom_utilisateur_admin_Jazz_SM*	Nom d'utilisateur de l'administrateur Jazz for Service Management
`-n` *port_bdd*	Port de la base de données NCIM
`-p` *motdepasse_admin_Jazz_SM*	Mot de passe de l'administrateur de Tivoli Integrated Portal.
`-r` *chemin_package_rapports*	Si, dans votre installation Network Manager, le package de rapports se trouve dans un emplacement autre que l'emplacement par défaut, vous pouvez définir l'emplacement dans lequel le package utilise cette option.
Oracle `-s` *nom_service_Oracle*	Lorsque vous utilisez une configuration Oracle RAC ou un nom de service pour vous connecter à la base de données, utilisez cette option suivie du *nom_service_Oracle* afin de définir l'adresse URL JDBC d'accès à la base de données. L'option `-s` est requise afin de configurer la source de données BIRT pour l'accès à la base de données avec le nom de service.
`-t` *Rép_principal_JazzSM*	Emplacement d'installation de Jazz for Service Management.
`-z` *type_bdd*	Type du serveur de base de données. Peut être `db2`, `informix` ou `oracle`.

3. Si vous utilisez Tivoli Data Warehouse, configurez les sources de données `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données Tivoli Data Warehouse.
   a. Accédez au répertoire suivant (le chemin ci-dessous est l'emplacement par défaut) : `/opt/IBM/tivoli/tipv2Components/TCRComponent/bin`.
   b. Exécutez la commande : UNIX

```
trcmd.sh -modify -dataSources -reports -username nom_utilisateur_tip -password
mot_de_passe_tip -dataSource name=nom_source_données -setDatasource odaURL=
URL_base_de_données_JDBC odaDriverClass=classe_pilote_JDBC
odaUser=utilisateur_base_de_données odaPassword=mot_de_passe_utilisateur_
base_de_données
```

Windows

```
trcmd.bat -modify -dataSources -reports -username nom_utilisateur_tip -password
mot_de_passe_tip -dataSource name=nom_source_données -setDatasource odaURL=
URL_base_de_données_JDBC odaDriverClass=classe_pilote_JDBC
odaUser=utilisateur_base_de_données odaPassword=mot_de_passe_utilisateur_
base_de_données
```

Remplacez les variables dans la commande à l'aide des définitions suivantes :

- *nom_utilisateur_tip* est le nom d'utilisateur de l'administrateur Tivoli Integrated Portal (par exemple, `tipadmin`).
- *mot_de_passe_tip* est le mot de passe de cet utilisateur.
- *nom_source_données* est le nom de la source de données que vous désirez configurer. Utilisez NCPOLLDATA pour configurer la connexion à Tivoli Data Warehouse. Les autres valeurs admises sont :
  - NCIM pour les rapports utilisant des informations de topologie.
  - PARAMETERS pour les rapports utilisant la base de données NCPOLLDATA ou le schéma NCPOLLDATA pour des paramètres de rapport.
- *URL_base_de_données_JDBC* est l'adresse URL de la base de données JDBC. L'adresse URL dépend de la plateforme et des autres variables. Pour construire l'adresse URL, reportez-vous à la liste suivante :
-

  JDBC URL

  IDS **Informix**

  ```
  jdbc:informix-sqli://nom_hôte:port/nom_bdd
  :INFORMIXSERVER=serveur;
  DELIMIDENT=Y;IFX_LOCK_MODE_WAIT=-1
  ```

  Oracle **Oracle**

  ```
  jdbc:oracle:thin:@nom_hôte:port:nom_bdd
  ```

  MySQL **MySQL**

  ```
  jdbc:mysql://nom_hôte:port/nom_bdd
  ```

  DB2 **DB2**

  ```
  "jdbc:db2://nom_hôte:port/
  nom_bdd:currentSchema=NCIM;"
  ```

  A l'aide des valeurs suivantes :

  nom_hôte
  Nom de l'hôte sur lequel la base de données NCIM ou TDW est installée.

  port Port sur lequel se connecter à la base de données NCIM ou TDW. La valeur par défaut pour les bases de données DB2 est 50000, pour les bases de données Oracle 1521, pour les bases de données Informix 9088, et pour MySQL 3306.

nom_bdd
Par défaut, le nom de la base de données NCIM est `ncim`. Le nom par défaut de la base de données TDW est WAREHOUS.

serveur
Nom du serveur Informix.

Les exemples suivants montrent les adresses URL de connexion JDBC pour chacune des différentes plateformes de base de données.

IDS **Informix**

jdbc:informix-sqli://192.168.1.2:9088/
itnm:INFORMIXSERVER=demo_on;
DELIMIDENT=Y; IFX_LOCK_MODE_WAIT=-1

Cet exemple d'adresse URL se connecte à une base de données Informix avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 9088. Il s'agit du port par défaut pour Informix.
- Le nom de la base de données Informix est itnm.
- Le nom de l'instance de serveur Informix est demo_on.

Oracle **Oracle**

jdbc:oracle:thin:192.168.1.2:1521:itnm

Cet exemple d'adresse URL se connecte à une base de données Oracle avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 1521. Il s'agit du port par défaut pour Oracle.
- Le nom de la base de données Oracle est itnm.

MySQL **MySQL**

jdbc:mysql://192.168.1.2:3306/ncim

Cet exemple d'adresse URL se connecte à une base de données MySQL avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 3306. Il s'agit du port par défaut pour MySQL.
- Le nom du schéma de la base de données topologiques est ncim.

DB2 **DB2**

jdbc:db2://192.168.1.2:50000/itnm:NCIM

Cet exemple d'adresse URL se connecte à une base de données DB2 avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 50000. Il s'agit du port par défaut pour DB2.

- Le nom de la base de données DB2 est itnm.
- Le nom du schéma de la base de données topologiques est NCIM.

- *classe_pilote_jdbc* est le nom de classe du pilote JDBC. Les valeurs suivantes représentent les noms de classe des différentes plateformes.
-

  Pilote JDBC

  IDS **Informix**
  `com.informix.jdbc.IfxDriver`

  Oracle **Oracle**
  `oracle.jdbc.driver.OracleDriver`

  MySQL **MySQL**
  `com.mysql.jdbc.Driver`

  DB2 **DB2**
  `com.ibm.db2.jcc.DB2Driver`

- *utilisateur_base_de_données* est le nom d'un utilisateur disposant de droits en lecture dans la base de données cible.
- *mot_de_passe_utilisateur_base_de_données* est le mot de passe de cet utilisateur.

Exemples de commande pour la définition de la source de données NCPOLLDATA sur Tivoli Data Warehouse

Exemple de commande DB2

La commande suivante permet de configurer la source de données NCPOLLDATA pour la production de rapports d'historique de telle sorte qu'elle utilise Tivoli Data Warehouse exécuté sur DB2.

```
trcmd.sh -modify
-dataSources -reports -username tipadmin -password netc00l
-dataSource name=NCPOLLDATA -setDatasource "odaURL=jdbc:db2://
myserver.abc.com:50000
/ITNM:currentSchema=NCPOLLDATA;"
"odaDriverClass=com.ibm.db2.jcc.DB2Driver"
odaUser=ncim odaPassword=ncim
```

Exemple de commande Oracle

La commande suivante permet de configurer la source de données NCPOLLDATA pour la production de rapports d'historique de telle sorte qu'elle utilise Tivoli Data Warehouse exécuté sur Oracle.

```
trcmd.sh -modify
-dataSources -reports -username tipadmin -password admin
-dataSource name=NCPOLLDATA -setDatasource "odaURL=jdbc:thin://
myserver.abc.com:1521/WAREHOUS"
"odaDriverClass=oracle.jdbc.driver.OracleDriver" odaUser=itmuser
odaPassword=itmuser
```

Tâches associées:

«Migration des rapports version 3.8», à la page 164
Si vous avez modifié ou créé des rapports dans Network Manager 3.8, vous devez les migrer manuellement.

Migration du magasin de contenu Cognos de Derby vers DB2 ou Oracle

La base de données Content Store utilisée par Cognos est adaptée à des fins de démonstration mais ne peut pas être utilisée comme base de données Content Store dans un environnement de production. Si vous utilisez des rapports de gestion du réseau avec Tivoli Common Reporting, vous pouvez migrer la base de données Content Store de la base de données Derby par défaut vers DB2 ou Oracle. Network Manager utilise la base de données configurée dans Tivoli Common Reporting comme base de données Content Store Cognos. Si vous avez déjà changé votre configuration Tivoli Common Reporting en vue de l'utilisation d'une base de données autre que la base de données Derby par défaut, il n'est pas nécessaire d'effectuer cette tâche.

Pour plus d'informations sur la base de données Derby par défaut et les autres bases de données Content Store pour Tivoli Common Reporting, voir la note technique suivante : http://www-01.ibm.com/support/docview.wss?uid=swg21609287.

Vous devez réaliser les étapes suivantes pour passer de DB2 ou Oracle pour la base de données Cognos Content Store, que vous installiez Network Manager sur un serveur sur lequel sont déjà installés les composants d'interface graphique Tivoli Common Reporting ou que vous installiez Tivoli Common Reporting sur un serveur avec une interface graphique Network Manager existante et les composants Tivoli Integrated Portal déjà installés. En effet, toute installation de Tivoli Common Reporting utilise Derby par défaut et vous devez passer à DB2 ou Oracle manuellement.

Pour migrer la base de données Cognos Content Store de la base de données Derby par défaut vers DB2 ou Oracle, procédez comme suit : suivez bien chaque étape à moins qu'il ne soit précisé que cette dernière est spécifique à une base de données, auquel cas, ne suivez que les étapes de la base de données de votre choix.

1. Connectez-vous à l'interface graphique de Network Manager en tant qu'utilisateur itnmadmin et exportez les données de la base de données Content Store comme indiqué dans http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.1.doc/inst_cr_winux_id3024c8bi_CreateAnExportDeploymentSpecif.html.

   Remarque : Lorsque vous cliquez sur **Sélectionner Content Store dans son ensemble** pour exporter la totalité du magasin de contenu, veillez à sélectionner les informations de compte utilisateur.
2. Créez la base de données de votre magasin de contenu Cognos. Suivez les étapes correspondant à votre type de base de données :

Option	Description
Pour utiliser DB2 pour votre magasin de contenu Cognos :	DB2 1. Connectez-vous en tant qu'utilisateur ayant créé la base de données Network Manager. Dans cet exemple, 'db2inst1' : `su - db2inst1` 2. Sourcez les variables d'environnement DB2 : `. sqllib/db2profile` 3. Créez la base de données Cognos à l'aide du script Network Manager en appelant l'utilisateur de base de données, dans ce cas 'ncim' : a. Accédez à `$NCHOME/precision/scripts/sql/db2`. b. Entrez `./create_db2_cognos_database.sh` *`nom_base_de_données nom_utilisateur`*, où *nom_base_de_données* est le nom requis de la base de données Content Store Cognos et *nom_utilisateur* l'utilisateur DB2 qui est utilisé pour la connexion à la base de données. Par exemple, pour créer une base de données appelée ITNMCM pour l'utilisateur DB2 ncim, entrez `./create_db2_cognos_database.sh ITNMCM ncim`. **Remarque :** Si votre base de données DB2 se trouve sur un autre serveur que Network Manager, copiez le script sur le serveur sur lequel se trouve votre base de données, puis exécutez le script.
Pour utiliser Oracle pour votre magasin de contenu Cognos :	Oracle Créez une base de données Oracle destinés aux rapports Cognos avec le jeu de caractères AL32UTF8 ou AL32UTF16, comme décrit dans la page Cognos "Instructions pour la création du magasin de contenu". **Remarque :** A ce stade, vous avez seulement besoin de créer la base de données. Le schéma de base de données sera créé ultérieurement, au démarrage de Cognos.

La page Cognos "Instructions pour la création du magasin de contenu" se trouve à l'adresse suivante : http://www.ibm.com/support/knowledgecenter/SSEP7J_10.1.0/com.ibm.swg.im.cognos.inst_cr_winux.10.1.0.doc/inst_cr_winux_id2792CreatetheContentStore.html

3. En tant qu'utilisateur ayant installé Network Manager, configurez l'accès à la source de données Content Store à l'aide du script Network Manager suivant :
   a. Sourcez les variables d'environnement :
      `. /opt/IBM/tivoli/netcool/env.sh`

b. Accédez à $NCHOME/precision/products/tnm/bin.

c. Entrez ./modify_cognos_cm -filename *chemin d'accès complet vers le fichier* -dbname *nom_base_de_données ou instance_SID_Oracle ou nom_service_Oracle (Oracle RAC seulement)* -dbport *numéro_port* -dbhost *nom_hôte* -dbtype db2 -username *nom_utilisateur* -password *mot_de_passe* .

DB2 Par exemple, utilisez une ligne de commande similaire à la suivante pour DB2 : UNIX

```
$NCHOME/precision/products/tnm/bin/modify_cognos_cm -filename
répertoire_installation_TCR/cognos/configuration/cogstartup.xml
 -dbname ITNMCM -dbport 50000 -dbhost abc
 -dbtype db2 -username db2inst1 -password password
```

Oracle Par exemple, utilisez une ligne de commande similaire à la suivante pour Oracle : UNIX

```
$NCHOME/precision/products/tnm/bin/modify_cognos_cm -filename
répertoire_installation_TCR/cognos/configuration/cogstartup.xml
 -dbname ITNM411 -dbport 1521 -dbhost abc
 -dbtype oracle -username oracleadmin -password password
```

d. Oracle Lorsque vous utilisez une configuration Oracle RAC ou un nom de service pour vous connecter à la base de données, utilisez le script **./tcr_cogconfig.sh** dans $NCHOME/../tipv2Components/TCRComponent/cognos/bin pour créer une source de données de base de données Oracle avancée. Utilisez une chaîne de connexion similaire à la chaîne suivante : (description=(address=(host=myhost)(protocol=tcp)(port=1521)(connect_data=(service_name=(orcl)))))

Pour plus d'informations sur la configuration de source de données, voir http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.0.doc/inst_cr_winux_id7376UninstallCognosContentDatabase.html.

4. Oracle Si vous utilisez Oracle comme gestionnaire de contenu, éditez le fichier ci-après. Cette opération est requise pour résoudre un problème connu : ojdbc6.jar n'est pas chargé par Cognos.

a. Ouvrez le fichier $NCHOME/../tipv2Components/TCRComponent/cognos/bin64/cogconfig.sh pour l'éditer.

b. Recherchez la chaîne suivante : CLASSPATH=.:../bin/cclcfgmcf_mcf.jar:cogconfig.jar

c. Ajoutez ce qui suit à la fin : :../webapps/p2pd/WEB-INF/lib/ojdbc6.jar

L'exemple suivant montre la chaîne CLASSPATH avec l'ajout à la fin :

```
CLASSPATH=.:../bin/cclcfgmcf_mcf.jar:cogconfig.jar:../bin/
cogconfigi.jar:../bin/dom4j.jar:../bin/xercesImpl.jar:../bin/xml-
apis.jar:../bin/cclcfgmcf.jar:../bin/cclcfgapi.jar:../bin/
jcam_crypto.jar:../bin/i18nj.jar:../bin/icu4j.jar:../bin/commons-
httpclient.jar:../bin/commons-logging.jar:../bin/CognosIPF.jar:../bin/
log4j-1.2.8.jar:../bin/jcam_jni.jar:../bin/jaxp.jar:../bin/
jdxslt.jar:../bin/ant.jar:../bin/jcam_config_test.jar:../bin/
cclcoreutil.jar:../bin/CognosCCL4J.jar:../webapps/p2pd/WEB-INF/lib/
ojdbc6.jar
```

5. En tant qu'utilisateur ayant installé Network Manager, redémarrez le serveur Tivoli Integrated Portal : accédez à $NCHOME/precision/bin et lancez les commandes **itnm_stop tip** puis **itnm_start tip**.

Remarque : Si vos variables d'environnement sont définies, vous pouvez exécuter les commandes d'arrêt et de démarrage à partir d'un répertoire.

6. Importez la base de données Content Store comme décrit dans http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.ug_cra.8.4.1.doc/ug_cra_i_ImportData.html.

   Notez ce qui suit pour la procédure d'importation :

   a. Dans la zone **Archive de déploiement**, sélectionnez l'archive vous avez précédemment créée pendant la procédure d'exportation.
   b. Lorsque vous sélectionnez les options souhaitées, veillez à sélectionner **Les rapports doivent être mis à niveau** comme choix de résolution de conflit.

7. Après la migration du magasin de contenu Cognos, désinstallez la base de données de contenu Derby, comme indiqué dans la rubrique *Uninstall Cognos Content Database* du document IBM Cognos 8 Business Intelligence Installation and Configuration Guide 8.4.0, dans le centre de documentation IBM Cognos : http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.0.doc/inst_cr_winux_id7376UninstallCognosContentDatabase.html

   Important : Notez ce qui suit pour la procédure de désinstallation Derby : si Tivoli Common Reporting est utilisé, la commande est **`tcr_cogconfig.sh`** (au lieu de **`cogconfig.sh`**).

Configuration de NCIM pour Tivoli Common Reporting

Si vous souhaitez utiliser Informix, MySQL ou Oracle en tant que base de données NCIM, vous devez configurer les bases de données pour pouvoir utiliser des rapports Tivoli Common Reporting.

Configurez les bases de données Informix, MySQL ou Oracle après avoir installé Network Manager. Si vous voulez utiliser DB2 en tant que base de données NCIM, vous devez configurer DB2 avant d'installer Network Manager.

Tâches associées:

«Configuration d'une base de données topologiques», à la page 62
A part la base de données Informix par défaut, vous pouvez utiliser une base de données DB2, MySQL ou Oracle pour stocker votre topologie. A moins que vous n'installiez la base de données Informix par défaut livrée avec Network Manager, vous devez configurer une base de données existante ou en installer et configurer une nouvelle avant d'installer Network Manager.

Configuration de la base de données Informix pour Tivoli Common Reporting sous Windows :

Si vous utilisez Informix sous Windows, vous devez effectuer certaines tâches de configuration avant de pouvoir utiliser les rapports Tivoli Common Reporting.

Installez Network Manager et la base de données Informix.

Pour configurer Informix pour Tivoli Common Reporting, procédez comme suit.

1. Ouvrez le fichier `C:\Program Files (x86)\IBM\Informix\Client-SDK\bin\setnet32.exe`. Un panneau de configuration s'affiche pour la base de données Informix.
2. Cliquez sur l'onglet **Environment**.
3. Sélectionnez la variable **DELIMIDENT** et attribuez-lui la valeur `Y`.
4. Sélectionnez la variable **DBDATE** et attribuez-lui la valeur `Y4MD-`.

5. Cliquez sur l'onglet **Server Information**.
6. Sélectionnez le serveur **ITNM**.

Configuration de la base de données Informix pour Tivoli Common Reporting sur Unix :

Si vous utilisez Informix sous Unix, vous devez effectuer certaines tâches de configuration avant d'utiliser des rapports Tivoli Common Reporting.

Installez Network Manager et la base de données Informix.

Pour configurer Informix pour Tivoli Common Reporting, procédez comme suit.

1. Créez le fichier `odbcinst.ini` dans le répertoire `%NCHOME%/etc/`.
2. Modifiez le fichier afin d'inclure les informations de configuration pour la base de données Informix.

   L'exemple suivant est pour la version Linux du fichier `odbcinst.ini` d'Informix.

```
[ODBC Drivers]
IBM INFORMIX ODBC DRIVER=Installed
[IBM INFORMIX ODBC DRIVER]
Driver=/opt/IBM/tivoli/netcool/platform/linux2x86/informix/lib/cli/
iclit09b.so
Setup=/opt/IBM/tivoli/netcool/platform/linux2x86/informix/lib/cli/
iclit09b.so
smProcessPerConnect = Y
FileUsage           = 0
SQLLevel            = 1
```

Configuration de la base de données MySQL pour Tivoli Common Reporting sur Unix :

Si vous utilisez MySQL en tant que base de données topologiques sur des plateformes UNIX, vous devez configurer la base de données avant de pouvoir utiliser des rapports Tivoli Common Reporting.

Installez Network Manager et la base de données MySQL.

Pour configurer MySQL pour Tivoli Common Reporting, procédez comme suit :

1. Créez le fichier `odbcinst.ini` dans le répertoire `$NCHOME/etc/`.
2. Modifiez le fichier afin d'inclure les informations de configuration pour la base de données MySQL.

   L'exemple suivant concerne la version MySQL Solaris d'`odbcinst.ini`.

```
[ODBC Drivers]
MySQL=Installed
[MySQL]
Description      = ODBC for MySQL
Driver           = /opt/IBM/tivoli/netcool/platform/solaris2/mysql-connector
-odbc-5.1.6/lib/libmyodbc5-5.1.6.so
FileUsage        = 1
UsageCount       = 2
```

Configuration de la base de données Oracle pour Tivoli Common Reporting :

Si vous utilisez Oracle en tant que base de données topologiques, vous devez configurer la base de données avant de pouvoir utiliser des rapports Tivoli Common Reporting.

Installez Network Manager et la base de données Oracle.

Pour configurer Oracle pour Tivoli Common Reporting, procédez comme suit :

1. Créez ou éditez le fichier `tnsnames.ora` dans le répertoire suivant : `NCHOME/platform/linux2x86/oracleInstantClient11.1/network/admin`.
2. Modifiez le fichier afin d'inclure les informations de configuration pour la base de données Oracle. Spécifiez le nom de service, le port et l'hôte corrects.

   Pour l'accès à la base de données Oracle, configurez le fichier avec une insertion similaire à celle qui suit. Notez que cette insertion ne doit comprendre qu'une seule ligne :

   ```
   orcl = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
   (HOST = p6tpm06n)(PORT = 1521))) (CONNECT_DATA =
   (SID = orcl.london.company.com) )
   ```

   Remarque : Fix Pack 5 Si votre valeur SID Oracle n'est pas la même que votre valeur SERVICE_NAME, ou si vous accédez à la fonction RAC d'Oracle avec un nom d'accès client unique, vous devez utiliser la valeur SERVICE_NAME dans l'insertion à la place du SID. Exemple :

   ```
   orcl = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
   (HOST = p6tpm06n)(PORT = 1521))) (CONNECT_DATA =
   (SERVICE_NAME = orcl.london.company.com) )
   ```

   Important : Le nom de service (SERVICE_NAME) doit être un nom complet.

Configuration de Tivoli Common Reporting 3.1 sur un serveur distant

Pour pouvoir exécuter des rapports avec Tivoli Common Reporting 3.1, vous devez installer Tivoli Common Reporting 3.1 sur un serveur distinct et configurer une intégration à couplage lâche entre le serveur Network Manager et le serveur Tivoli Common Reporting.

Restriction : Tivoli Common Reporting 3.1 est disponible uniquement pour les utilisateurs de Netcool Operations Insight.

architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager

Ces informations permettent de comprendre comment intégrer Tivoli Common Reporting 3.1 d'un serveur distinct sur le serveur Network Manager.

La figure suivante présente l'architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager.

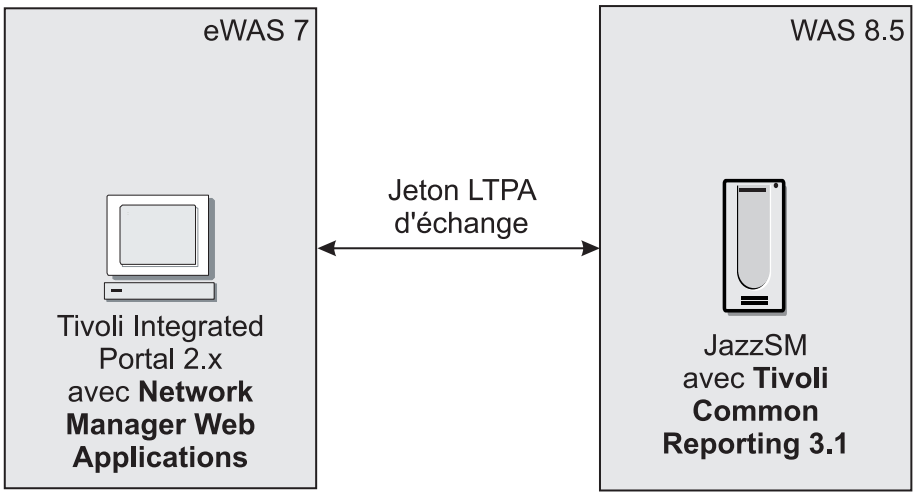

Figure 13. architecture de l'intégration de Tivoli Common Reporting 3.1 à Network Manager

Configuration requise pour le serveur Tivoli Common Reporting 3.1

Vous devez télécharger et installer le logiciel suivant sur le serveur Tivoli Common Reporting 3.1 :

- JazzSM
- WAS 8.5
- Tivoli Common Reporting 3.1.

Préparation du serveur Tivoli Common Reporting 3.1

Préparez le serveur Tivoli Common Reporting 3.1 en déployant des rapports sur ce dernier et en configurant les bases de données et les sources de données.

Déploiement des rapports : Fix Pack 5

Vous devez copier les rapports à partir du serveur Network Manager et les déployer sur le serveur Tivoli Common Reporting 3.1.

Pour configurer Tivoli Common Reporting, vous devez exécuter la commande Tivoli Common Reporting `trcmd.sh`. Vous devez suivre les procédures de configuration suivantes avant d'exécuter cette commande :

- Note technique : Une exception OutOfMemoryError se produit lors de l'exécution de la commande trcmd
- Entrée de blogue SMC : Le moteur BIRT TCR émet java.lang.StackOverflowError : une modification mineure a été effectuée à l'étape 6 de cette procédure. Au cours de cette étape, ajoutez la propriété suivante au fichier :

  ```
  osgi.nl=en_US
  ```

- Editez le script `/opt/IBM/JazzSM/reporting/bin/trcmd.sh` et modifiez la ligne suivante :

  ```
  # Store the location of the BIRT lib directory
  BIRT_LIB=${TCR_ADDONS_DIR}/birt/birt-runtime-2_2_2/ReportEngine/lib
  ```

  Modifiez la valeur de `BIRT_LIB` comme suit :

  ```
  BIRT_LIB=$TCR_HOME/lib/birt-runtime-2_2_2/ReportEngine/lib
  ```

Procédez comme suit :

1. Copiez les fichiers suivants vers un répertoire cible pratique sur le serveur Tivoli Common Reporting 3.1. Prenez note de l'emplacement du répertoire cible.
   - `$ITNMHOME/products/tnm /itnmreports.zip`
   - `$ITNMHOME/products/tnm /itnmcognos.zip`
   - `configRemoteTCR.sh`
2. DB2 Pour DB2 uniquement, copiez les fichiers suivants :
   - `/opt/IBM/JazzSM/lib/db2/db2jcc.jar` vers `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc_license_cu.jar` vers `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc_license_cu.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
3. Oracle Pour Oracle uniquement, copiez les fichiers suivants :
   - `$NCHOME/precision/products/tnm/lib/ojdbc6.jar` vers `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `$NCHOME/precision/products/tnm/lib/ojdbc6.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
4. Oracle Pour Oracle uniquement, vérifiez que l'utilisateur `ncpolldata` peut accéder au schéma `NCPOLLDATA`.
5. Informix Pour Informix uniquement, copiez les fichiers suivants :
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbc.jar` vers `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlang.jar` vers `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbc.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlang.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbcx.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlsupp.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxsqlj.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxtools.jar` vers `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
6. DB2 Sur le serveur Tivoli Common Reporting 3.1, localisez et exécutez le script `configRemoteTCR.sh`. Indiquez le chemin d'accès complet au package de rapports à l'aide de l'option `-r`. Exécutez le script une fois pour le package `itnmcognos10.zip` et une fois pour le package `itnmreports.zip`.

   Utilisez une commande similaire à l'exemple suivant : UNIX

```
$NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d nom_bdd -e
nom_utilisateur_NCIM -h nom_hôte_bdd  [-i install] -j
nom_utilisateur_admin_Jazz_SM -n port_bdd -p
motdepasse_admin_Jazz_SM [-r
répertoire_packages]
[-s nom_service_Oracle] -t
$Rép_principal_JazzSM -z
type_bdd
```

Les options diffèrent pour DB2, Oracle 11 et Oracle 12. Le tableau suivant décrit les options du script `configRemoteTCR` :

Tableau 26. Options de ligne de commande pour configRemoteTCR

Option de ligne de commande	Description
`-d` *nom_bdd* ou *nom_service*	Nom de la base de données DB2 NCIM ou nom du service Oracle NCIM
`-e` *nom_utilisateur_NCIM*	Dans certaines bases de données, comme Oracle, les noms d'utilisateur peuvent être différents pour la base de données NCIM et la base de données NCPOLLDATA. Vous devez spécifier les deux noms d'utilisateur s'ils sont différents. Utilisez cette option pour indiquer le nom d'utilisateur NCIM. L'option `-d` définit le mot de passe pour cet utilisateur.
`-h` *nom_hôte_bdd*	Nom d'hôte de la base de données NCIM
`-i` *install*	Indique que les rapports de gestion de réseau sont installés. Vous devez utiliser le paramètre **`install`** dans tous les cas après l'option `-i`.
`-j` *nom_utilisateur_admin_Jazz_SM*	Nom d'utilisateur de l'administrateur Jazz for Service Management
`-n` *port_bdd*	Port de la base de données NCIM
`-p` *motdepasse_admin_Jazz_SM*	Mot de passe de l'administrateur de Tivoli Integrated Portal
`-r` *chemin_package_rapports*	Si, dans votre installation Network Manager, le package de rapports se trouve dans un emplacement autre que l'emplacement par défaut, vous pouvez définir l'emplacement dans lequel le package utilise cette option.
Oracle `-s` *<SID_Oracle*	Définit le SID (Oracle System ID) de NCIM.
`-t` *Rép_principal_JazzSM*	Emplacement d'installation de Jazz for Service Management.
`-u`	Facultatif. Si un utilisateur spécifique a besoin d'un accès au schéma NCPOLLDATA, indiquez le nom d'utilisateur avec cette option. Le nom d'utilisateur par défaut est `ncpolldata`.
`-z` *type_bdd*	Type du serveur de base de données. Peut être `db2`, `informix` ou `oracle`.

7. Redémarrez le serveur Jazz for Service Management à l'aide des scripts `stopServer.sh` et `startServer.sh`. Par défaut, ces scripts se trouvent dans le répertoire `/opt/IBM/JazzSM/profile/bin/`.

Configuration des sources de données DB2 :

Pour configurer les sources de données DB2 sur le serveur Tivoli Common Reporting 3.1, effectuez les étapes de configuration suivantes.

Ajout de la prise en charge de DB2 :

Pour ajouter la prise en charge de DB2 sur le serveur Tivoli Common Reporting 3.1, suivez ces étapes de configuration.

Exécutez les tâches suivantes pour ajouter la prise en charge de DB2.

1. Installez le client DB2 sur le serveur Tivoli Common Reporting 3.1.
2. Exécutez les commandes suivantes pour cataloguer la base de données utilisée par les rapports.

   ```
   db2 CATALOG TCPIP NODE ITNMNODE REMOTE HOSTNAME SERVER PORT
   db2 CATALOG DATABASE DBNAME AT NODE ITNMNODE
   db2 TERMINATE
   ```

   Où :

   - *HOSTNAME* correspond au nom d'hôte du serveur de base de données topologiques NCIM Network Manager distant ou au nom d'hôte du serveur Network Manager, si la base de données topologiques NCIM y est installée.
   - *PORT* correspond au port de communication du serveur de base de données topologiques NCIM Network Manager distant ou au nom d'hôte du serveur Network Manager, si la base de données topologiques NCIM y est installée.
   - *DBNAME* correspond au nom de la base de données.
3. Définissez la variable d'environnement `LD_LIBRARY_PATH` pour permettre à Cognos d'accéder aux bibliothèques DB2 32 bits.

   ```
   Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$DB2HOME/sqllib/lib32
   ```
4. Copiez les fichiers JAR DB2 suivants à l'emplacement spécifié : Fichiers JAR :
   - db2jcc.jar
   - db2jcc_license_cu.jar

   Emplacement : `$TCRHOME/lib/birt-runtime-2_2_2/ReportEngine /plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/ drivers`

Configuration des sources de données DB2 pour Cognos :

Configurez les sources de données DB2 pour des rapports basés sur le modèle de données Cognos. Les sources de données DB2 pour les rapports basés sur le modèle de données BIRT doivent être configurées séparément.

Pour configurer les sources de données DB2 pour Cognos, exécutez la commande suivante pour chaque base de données, en remplaçant les paramètres appropriés pour chaque base de données :

```
$TCRHOME/bin/trcmd.sh -dataSource -add nom_source_données -dbType DB2 -dbname nom_bdd
-openSessionSql "SET CURRENT SCHEMA=nom_source_données" -dbLogin utilisateur_bdd
-dbPassword motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
```

Où les définitions ci-dessous s'appliquent à cette commande et aux commandes des étapes suivantes :

- *nom_source_données* correspond au nom de la source de données que vous ajoutez. Dans les commandes qui suivent, vous ajoutez les sources de données suivantes :
  - NCIM
  - NCPOLLDATA
  - PARAMETERS
  - NCPGUI
  - NCMONITOR
- *nom_bdd* est le nom de la base de données correspondant à la source de données que vous configurez.
- *utilisateur_bdd* correspond au nom d'utilisateur pour cette base de données.
- *motdepasse_bdd* correspond au mot de passe pour cette base de données.
- *nom_utilisateur* correspond au nom d'utilisateur de l'utilisateur administrateur WebSphere Application Server ; par défaut, il s'agit de smadmin.
- *mot_de_passe* correspond au mot de passe de l'utilisateur administrateur WebSphere Application Server.

1. Exécutez la commande suivante pour configurer la source de données NCIM :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCIM -dbType DB2
    -dbname nom_bdd -openSessionSql "SET CURRENT SCHEMA=NCIM"
   -dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username
   nom_utilisateur -password mot_de_passe -force
   ```

2. Exécutez la commande suivante pour configurer la source de données NCPOLLDATA :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPOLLDATA -dbType DB2 -dbname nom_bdd
   -openSessionSql "SET CURRENT SCHEMA=NCPOLLDATA" -dbLogin utilisateur_bdd
   -dbPassword motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
   ```

3. Exécutez la commande suivante pour configurer la source de données PARAMETERS :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add PARAMETERS -dbType DB2 -dbname nom_bdd
   -openSessionSql "SET CURRENT SCHEMA=NCPOLLDATA" -dbLogin utilisateur_bdd
   -dbPassword motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
   ```

4. Exécutez la commande suivante pour configurer la source de données NCPGUI :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPGUI -dbType DB2 -dbname nom_bdd
   -openSessionSql "SET CURRENT SCHEMA=NCPGUI" -dbLogin utilisateur_bdd
   -dbPassword motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
   ```

5. Exécutez la commande suivante pour configurer la source de données NCMONITOR :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCMONITOR -dbType DB2 -dbname nom_bdd
   -openSessionSql "SET CURRENT SCHEMA=NCMONITOR" -dbLogin utilisateur_bdd
   -dbPassword motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
   ```

Si vous utilisez Tivoli Data Warehouse, configurez la source de données NCPOLLDATA de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse.

1. Accédez au répertoire ci-après (le chemin suivant est l'emplacement par défaut) : /opt/IBM/JazzSM/reporting/bin/.
2. Exécutez la commande : UNIX

   ```
   trcmd.sh -dataSource -add nom_source_données -connectionString "^UserID:^?Password:;
   LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=000/
   0@COLSEQ=IBM_JD_CNX_STR:^UserID:^?Password:;
   LOCAL;JD-D2;URL==URL_bdd_JDBC odaDriverClass=classe_pilote_JDBC odaUser=
   utilisateur_bdd odaPassword=motdepasse_utilisateur_bdd;;DRIVER_NAME=com.ibm.db2.jcc.
   ```

```
DB2Driver" -openSessionSql "SET CURRENT SCHEMA =schema_name" -signonName
utilisateur_bdd -dbLogin utilisateur_bdd -dbPassword motdepasse_utilisateur_bdd
-username nom_utilisateur_jazz -password motdepasse_jazz -force
```

Windows

```
trcmd.bat -dataSource -add nom_source_données -connectionString "^UserID:^?Password:;
LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=0@0/0@COLSEQ=IBM_JD_CNX_STR:^UserID:^?Password:;
LOCAL;JD-D2;URL==URL_bdd_JDBC odaDriverClass=classe_pilote_JDBC odaUser=
utilisateur_bdd odaPassword=motdepasse_utilisateur_bdd;;DRIVER_NAME=com.ibm.db2.jcc.
DB2Driver" -openSessionSql "SET CURRENT SCHEMA =schema_name" -signonName
utilisateur_bdd -dbLogin utilisateur_bdd -dbPassword motdepasse_utilisateur_bdd
-username nom_utilisateur_jazz -password motdepasse_jazz -force
```

Remplacez les variables dans la commande à l'aide des définitions suivantes :

- *utilisateur_jazz* correspond au nom d'utilisateur de l'administrateur de Jazz for Service Management, par exemple, `smadmin`.
- *motdepasse_jazz* correspond au mot de passe de cet utilisateur.
- *nom_source_données* est le nom de la source de données que vous désirez configurer. Utilisez NCPOLLDATA pour configurer la connexion à Tivoli Data Warehouse.
- *nom_schéma* correspond au nom du schéma de base de données.
- *URL_base_de_données_JDBC* est l'adresse URL de la base de données JDBC. L'adresse URL dépend de la plateforme et des autres variables. Pour construire l'adresse URL, reportez-vous à la liste suivante :
- **JDBC URL**

  `"jdbc:db2://nom_hôte:port/nom_bdd:currentSchema=NCIM;"`

  A l'aide des valeurs suivantes :

  nom_hôte
  Nom de l'hôte sur lequel la base de données Tivoli Data Warehouse est installée.

  port
  Port à utiliser pour la connexion à la base de données Tivoli Data Warehouse. La valeur par défaut pour les bases de données DB2 est 50000.

  nom_bdd
  Le nom par défaut de la base de données Tivoli Data Warehouse est WAREHOUS.

  serveur
  Nom du serveur Informix.

  L'exemple suivant indique l'adresse URL de connexion JDBC pour DB2.

  DB2 **DB2**

  jdbc:db2://192.168.1.2:50000/itnm:NCIM

  Cet exemple d'adresse URL se connecte à une base de données DB2 avec les propriétés suivantes :

  – L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
  – La base de données s'exécute sur le port 50000. Il s'agit du port par défaut pour DB2.
  – Le nom de la base de données DB2 est itnm.
  – Le nom du schéma de la base de données topologiques est NCIM.
- *classe_pilote_jdbc* est le nom de classe du pilote JDBC. Les valeurs suivantes représentent les noms de classe des différentes plateformes.

- **Pilote JDBC**
  `com.ibm.db2.jcc.DB2Driver`
- *utilisateur_bdd* est le nom d'un utilisateur disposant de droits en lecture dans la base de données cible.
- *motdepasse_utilisateur_bdd* est le mot de passe de cet utilisateur.

Exemple de commande pour la définition de la source de données NCPOLLDATA sur Tivoli Data Warehouse

Exemple de commande DB2

La commande suivante définit la source de données NCPOLLDATA pour la production de rapports d'historique de telle sorte qu'elle utilise Tivoli Data Warehouse exécuté sur DB2 :

```
./trcmd.sh -dataSource -add NCPOLLDATA -connectionString "^UserID:^?Password:;
LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=0@0/
0@COLSEQ=IBM_JD_CNX_STR:^User ID:^?Password:;
LOCAL;JD-D2;URL=jdbc:db2://sqa03.hursley.ibm.com:50000/
Warehous:currentSchema=ITMUSER;;
DRIVER_NAME=com.ibm.db2.jcc.DB2Driver" -
openSessionSql "SET CURRENT SCHEMA =ITMUSER"
-signonName ncpolldata -dbLogin itmuser -dbPassword itmuser -username
smadmin -password netcool -force
```

Configuration des sources de données DB2 pour BIRT :

Si vous utilisez des rapports basés sur le modèle de données BIRT, vous devez configurer des sources de données. Si vous utilisez également des rapports basés sur le modèle Cognos, vous devez configurer les sources de données Cognos séparément.

Si vous n'utilisez pas Tivoli Data Warehouse, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM.

Si vous utilisez Tivoli Data Warehouse, configurez les sources de données `NCIM` et `PARAMETERS` de telle sorte qu'elles pointent vers la base de données NCIM, et `NCPOLLDATA` de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse. Obtenez les détails relatifs à la connexion et à la base de données auprès de l'administrateur de base de données avant de commencer cette procédure.

Conseil : La documentation de référence de chaque rapport vous indique si le rapport emploie le modèle de données BIRT ou Cognos.

Pour configurer les sources de données de tous les rapports basés sur le modèle de données BIRT, procédez comme indiqué ci-après.

1. Si Tivoli Common Reporting est installé sur le même serveur que Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script `configTCR.sh` avec une commande similaire à la commande suivante : UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d mot de passe_bd_NCIM
    -p mot de passe_administrateur_TIP
   ```
2. Si Tivoli Common Reporting est installé sur un serveur différent de celui de Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et

NCPOLLDATA de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script configRemoteTCR.sh avec une commande similaire à la commande suivante : UNIX

```
$NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d nom_bdd -e
nom_utilisateur_NCIM -h nom_hôte_bdd  [-i install] -j
nom_utilisateur_admin_Jazz_SM -n port_bdd -p
motdepasse_admin_Jazz_SM [-r
répertoire_packages]
[-s nom_service_Oracle] -t
$Rép_principal_JazzSM -z
type_bdd
```

Restriction : Le script configRemoteTCR.sh est disponible dans Network Manager à partir de la version 3.9 groupe de correctifs 5.

3. Si vous utilisez Tivoli Data Warehouse, configurez la source de données NCPOLLDATA de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse.
   a. Accédez au répertoire ci-après (le chemin suivant est l'emplacement par défaut) : /opt/IBM/JazzSM/reporting/bin/.
   b. Exécutez la commande : UNIX

```
trcmd.sh -modify -dataSources -reports
-reportName "/content/package[@name='NetworkManager']/
folder[@name='Performance Reports']/report
[@name='Historical SNMP  Trend Quick View Report']"
-username jazz_username -password jazz_password  -
dataSourcename=data_source_name
-setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Windows

```
trcmd.sh -modify -dataSources -reports
-reportName "/content/package[@name='NetworkManager']/
folder[@name='Performance Reports']/report
[@name='Historical SNMP  Trend Quick View Report']"
-username jazz_username -password jazz_password  -
dataSourcename=data_source_name
-setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Remplacez les variables dans la commande à l'aide des définitions suivantes :

- *utilisateur_jazz* correspond au nom d'utilisateur de l'administrateur de Jazz for Service Management, par exemple, smadmin.
- *motdepasse_jazz* correspond au mot de passe de cet utilisateur.
- *nom_source_données* est le nom de la source de données que vous désirez configurer. Utilisez NCPOLLDATA pour configurer la connexion à Tivoli Data Warehouse. Les autres valeurs admises sont :
  - NCIM pour les rapports utilisant des informations de topologie.
  - PARAMETERS pour les rapports utilisant la base de données NCPOLLDATA ou le schéma NCPOLLDATA pour des paramètres de rapport.
- *URL_base_de_données_JDBC* est l'adresse URL de la base de données JDBC. L'adresse URL dépend de la plateforme et des autres variables. Pour construire l'adresse URL, reportez-vous à la liste suivante :
-

JDBC URL

`"jdbc:db2://`*nom_hôte*`:`*port*`/`
nom_base_de_données`:currentSchema=NCIM;"`

A l'aide des valeurs suivantes :

nom_hôte
Nom de l'hôte sur lequel la base de données Tivoli Data Warehouse est installée.

port Port à utiliser pour la connexion à la base de données Tivoli Data Warehouse. La valeur par défaut pour les bases de données DB2 est 50000.

nom_base_de_données
Le nom par défaut de la base de données Tivoli Data Warehouse est WAREHOUS.

serveur
Nom du serveur Informix.

L'exemple suivant indique l'adresse URL de connexion JDBC pour DB2.

DB2 **DB2**

jdbc:db2://192.168.1.2:50000/itnm:NCIM

Cet exemple d'adresse URL se connecte à une base de données DB2 avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 50000. Il s'agit du port par défaut pour DB2.
- Le nom de la base de données DB2 est itnm.
- Le nom du schéma de la base de données topologiques est NCIM.

- *classe_pilote_jdbc* est le nom de classe du pilote JDBC. Les valeurs suivantes représentent les noms de classe des différentes plateformes.
-

  Pilote JDBC
  `com.ibm.db2.jcc.DB2Driver`
- *utilisateur_bdd* est le nom d'un utilisateur disposant de droits en lecture dans la base de données cible.
- *mot_de_passe_utilisateur_bdd* est le mot de passe de cet utilisateur.

Exemple de commande pour la définition de la source de données NCPOLLDATA sur Tivoli Data Warehouse

Exemple de commande DB2

La commande suivante permet de configurer la source de données NCPOLLDATA pour la production de rapports d'historique de telle sorte qu'elle utilise Tivoli Data Warehouse exécuté sur DB2.

```
trcmd.sh -modify
-dataSources -reports -reportName "/content/package
[@name='Network Manager']/folder[@name='Performance Reports']/report
[@name='Historical SNMP Trend Quick View Report']" -username
jazz_username
-password jazz_password -dataSource name=data_source_name
-setDatasource odaURL=JDBC_database_URL
```

```
odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Configuration des sources de données Oracle :

Pour configurer les sources de données Oracle sur le serveur Tivoli Common Reporting 3.1, effectuez les étapes de configuration suivantes.

Ajout de la prise en charge d'Oracle :

Pour ajouter la prise en charge d'Oracle sur le serveur Tivoli Common Reporting 3.1, suivez ces étapes de configuration.

Veillez à installer le client de base de données Oracle sur l'ordinateur où Tivoli Common Reporting 3.1 est installé.

Exécutez les tâches suivantes pour ajouter la prise en charge d'Oracle.

1. Copiez les bibliothèques 32 bits du client Oracle de l'emplacement suivant sur le serveur Network Manager vers la machine Tivoli Common Reporting 3.1.

   ```
   $NCHOME/platform/linux2x86/oracleInstantClient11.1
   ```

2. Définissez la variable d'environnement LD_LIBRARY_PATH pour permettre à Cognos d'accéder aux bibliothèques Oracle 32 bits.

   ```
   Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$NCHOME/platform/linux2x86/
   oracleInstantClient11.1
   ```

3. Créez ou éditez le fichier $ORACLE_HOME/network/admin/tnsnames.ora et ajoutez-y les lignes suivantes :

   ```
   DB_NAME =
       (DESCRIPTION =
      (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = HOSTNAME)(PORT = PORT)))
      (CONNECT_DATA = (SID = <DB_NAME>) )
   )
   ```

   Où :

   - *DBNAME* correspond au nom de la base de données.
   - *HOSTNAME* correspond au nom d'hôte du serveur de base de données topologiques NCIM Network Manager distant ou au nom d'hôte du serveur Network Manager, si la base de données topologiques NCIM y est installée.
   - *PORT* correspond au port de communication du serveur de base de données topologiques NCIM Network Manager distant ou au nom d'hôte du serveur Network Manager, si la base de données topologiques NCIM y est installée.

4. Copiez le fichier JAR Oracle suivant à l'emplacement spécifié : Fichier JAR :

   - ojdbc6.jar

   Emplacement : $TCRHOME/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/

Configuration des sources de données Oracle pour Cognos :

Configurez les sources de données Oracle pour les rapports basés sur le modèle de données Cognos. Les sources de données Oracle pour les rapports basés sur le modèle de données BIRT doivent être configurées séparément.

1. Pour configurer les sources de données Oracle pour Cognos, exécutez la commande suivante pour chaque base de données, en remplaçant les paramètres appropriés pour chaque base de données :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add nom_source_données -dbType ORACLE
   -dbname nom_bdd -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=
   nom_source_données" -dbLogin utilisateur_bdd -dbPassword
   motdepasse_bdd -username nom_utilisateur -password mot_de_passe -force
   ```

   Où les définitions ci-dessous s'appliquent à cette commande et aux commandes des étapes suivantes :

   - *nom_source_données* correspond au nom de la source de données que vous ajoutez. Dans les commandes qui suivent, vous ajoutez les sources de données suivantes :
     - NCIM
     - NCPOLLDATA
     - PARAMETERS
     - NCPGUI
     - NCMONITOR
   - *nom_bdd* est le nom de la base de données correspondant à la source de données que vous configurez.
   - *utilisateur_bdd* correspond au nom d'utilisateur pour cette base de données.
   - *motdepasse_bdd* correspond au mot de passe pour cette base de données.
   - *nom_utilisateur* correspond au nom d'utilisateur de l'utilisateur administrateur WebSphere Application Server ; par défaut, il s'agit de smadmin.
   - *mot_de_passe* correspond au mot de passe de l'utilisateur administrateur WebSphere Application Server.
2. Exécutez la commande suivante pour configurer la source de données NCIM :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCIM -dbType ORACLE
   -dbname nom_bdd -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA = NCIM"
   -dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username nom_utilisateur -password
   mot_de_passe -force
   ```
3. Exécutez la commande suivante pour configurer la source de données NCPOLLDATA :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPOLLDATA -dbType ORACLE
   -dbname nom_bdd -openSessionSql ALTER SESSION SET CURRENT_SCHEMA=NCPOLLDATA"
   -dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username nom_utilisateur
   -password mot_de_passe -force
   ```
4. Exécutez la commande suivante pour configurer la source de données PARAMETERS :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add PARAMETERS -dbType ORACLE
   -dbname nom_bdd -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCPOLLDATA"
   -dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username nom_utilisateur
   -password mot_de_passe -force
   ```
5. Exécutez la commande suivante pour configurer la source de données NCPGUI :

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPGUI -dbType ORACLE
   -dbname nom_bdd -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCPGUI"
   -dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username nom_utilisateur
   -password mot_de_passe -force
   ```

6. Exécutez la commande suivante pour configurer la source de données NCMONITOR :

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCMONITOR -dbType ORACLE
-dbname nom_bdd -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCMONITOR"
-dbLogin utilisateur_bdd -dbPassword motdepasse_bdd -username nom_utilisateur
-password mot_de_passe -force
```

7. Si vous utilisez Tivoli Data Warehouse, configurez la source de données NCPOLLDATA de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse.
   a. Accédez au répertoire ci-après (le chemin suivant est l'emplacement par défaut) : /opt/IBM/JazzSM/reporting/bin/.
   b. Exécutez la commande suivante : UNIX

```
trcmd.sh -dataSource -add nom_source_données -connectionString
 "^User ID:^?Password:;LOCAL;JD-OR;URL=URL_bdd_JDBC;DRIVER_NAME=
oracle.jdbc.driver.OracleDriver" -
openSessionSql "ALTER SESSION CURRENT_SCHEMA=schema_name"
 -signonName utilisateur_bdd  -dbLogin utilisateur_bdd
 -dbPassword motdepasse_utilisateur_bdd -username nom_utilisateur_jazz
-password motdepasse_jazz -force
```

Windows

```
trcmd.bat -dataSource -add nom_source_données -connectionString
"^User ID:^?Password:;LOCAL;JD-OR;URL=URL_bdd_JDBC;
DRIVER_NAME= oracle.jdbc.driver.OracleDriver"  -
openSessionSql " ALTER SESSION SET
CURRENT_SCHEMA=schema_name" -signonName utilisateur_bdd -
dbLogin utilisateur_bdd  -dbPassword
motdepasse_utilisateur_bdd -username nom_utilisateur_jazz -password
motdepasse_jazz -force
```

Remplacez les variables dans la commande à l'aide des définitions suivantes :

- *utilisateur_jazz* correspond au nom d'utilisateur de l'administrateur de Jazz for Service Management, par exemple, smadmin.
- *motdepasse_jazz* correspond au mot de passe de cet utilisateur.
- *nom_source_données* est le nom de la source de données que vous désirez configurer. Utilisez NCPOLLDATA pour configurer la connexion à Tivoli Data Warehouse.
- *nom_schéma* correspond au nom du schéma de base de données.
- *URL_bddd_JDBC* est l'adresse URL de la base de données JDBC. L'adresse URL dépend de la plateforme et des autres variables.

Voici un exemple d'URL JDBC : jdbc:oracle://*nom_hôte*:*port*/*nom_bdd*:currentSchema=NCIM;"

Où :

- *nom_hôte* correspond au nom de l'hôte sur lequel la base de données Tivoli Data Warehouse est installée.
- *port* correspond au port sur lequel établir la connexion à la base de données Tivoli Data Warehouse. La valeur par défaut pour les bases de données Oracle est 1521.
- *nom_bdd* correspond au nom de la base de données. Le nom par défaut de la base de données Tivoli Data Warehouse est WAREHOUS.
- *serveur* correspond au nom du serveur Informix.

classe_pilote_jdbc est le nom de classe du pilote JDBC. Les valeurs suivantes représentent les noms de classe des différentes plateformes.

- `oracle.jdbc.driver.OracleDriver`
- *utilisateur_bdd* est le nom d'un utilisateur disposant de droits en lecture dans la base de données cible.
- *motdepasse_utilisateur_bdd* est le mot de passe de cet utilisateur.

L'exemple suivant indique l'adresse URL de la connexion JDBC pour Oracle : `jdbc:oracle://192.168.1.2:1521/itnm:NCIM`

Cet exemple d'adresse URL se connecte à une base de données Oracle avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 1521. Il s'agit du port par défaut pour Oracle.
- Le nom de la base de données Oracle est itnm.
- Le nom du schéma de la base de données topologiques est NCIM.

Configuration des sources de données Oracle pour BIRT :

Si vous utilisez des rapports basés sur le modèle de données BIRT, vous devez configurer des sources de données. Si vous utilisez également des rapports basés sur le modèle Cognos, vous devez configurer les sources de données Cognos séparément.

Si vous n'utilisez pas Tivoli Data Warehouse, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM.

Si vous utilisez Tivoli Data Warehouse, configurez les sources de données `NCIM` et `PARAMETERS` de telle sorte qu'elles pointent vers la base de données NCIM, et `NCPOLLDATA` de telle sorte qu'elle pointe vers la base de données Tivoli Data Warehouse. Obtenez les détails relatifs à la connexion et à la base de données auprès de l'administrateur de base de données avant de commencer cette procédure.

Conseil : La documentation de référence de chaque rapport vous indique si le rapport emploie le modèle de données BIRT ou Cognos.

Pour configurer les sources de données de tous les rapports basés sur le modèle de données BIRT, procédez comme indiqué ci-après.

1. Si Tivoli Common Reporting est installé sur le même serveur que Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script `configTCR.sh` avec une commande similaire à la commande suivante : UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d mot de passe_bd_NCIM
    -p mot de passe_administrateur_TIP
   ```

2. Si Tivoli Common Reporting est installé sur un serveur différent de celui de Network Manager, configurez les sources de données `NCIM`, `PARAMETERS` et `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données NCIM. Exécutez le script `configRemoteTCR.sh` avec une commande similaire à la commande suivante : UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d nom_bdd -e
   nom_utilisateur_NCIM -h nom_hôte_bdd  [-i install] -j
   nom_utilisateur_admin_Jazz_SM -n port_bdd -p
   motdepasse_admin_Jazz_SM [-r
   ```

```
répertoire_packages]
[-s nom_service_Oracle] -t
$Rép_principal_JazzSM -z
type_bdd
```

Restriction : Le script `configRemoteTCR.sh` est disponible dans Network Manager à partir de la version 3.9 groupe de correctifs 5.

3. Si vous utilisez Tivoli Data Warehouse, configurez les sources de données `NCPOLLDATA` de telle sorte qu'elles pointent vers la base de données Tivoli Data Warehouse.
   a. Accédez au répertoire ci-après (le chemin suivant est l'emplacement par défaut) : `/opt/IBM/JazzSM/reporting/bin/`.
   b. Exécutez la commande : UNIX

```
trcmd.sh -modify -dataSources -reports
-reportName "/content/package[@name='NetworkManager']/
folder[@name='Performance Reports']/report
[@name='Historical SNMP  Trend Quick View Report']"
-username jazz_username -password jazz_password  -
dataSourcename=data_source_name
-setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Windows

```
trcmd.sh -modify -dataSources -reports
-reportName "/content/package[@name='NetworkManager']/
folder[@name='Performance Reports']/report
[@name='Historical SNMP  Trend Quick View Report']"
-username jazz_username -password jazz_password  -
dataSourcename=data_source_name
-setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Remplacez les variables dans la commande à l'aide des définitions suivantes :

- *nom_utilisateur_jazz* est le nom d'utilisateur de l'administrateur de Tivoli Integrated Portal, par exemple `smadmin`.
- *motdepasse_jazz* correspond au mot de passe de cet utilisateur.
- *nom_source_données* est le nom de la source de données que vous désirez configurer. Utilisez NCPOLLDATA pour configurer la connexion à Tivoli Data Warehouse. Les autres valeurs admises sont :
  - NCIM pour les rapports utilisant des informations de topologie.
  - PARAMETERS pour les rapports utilisant la base de données NCPOLLDATA ou le schéma NCPOLLDATA pour des paramètres de rapport.
- *URL_base_de_données_JDBC* est l'adresse URL de la base de données JDBC. L'adresse URL dépend de la plateforme et des autres variables. Pour construire l'adresse URL, reportez-vous à la liste suivante :
- **JDBC URL**

  `jdbc:oracle:thin:@`*`nom_hôte`*`:`*`port`*`:`*`nom_base_de_données`*

  A l'aide des valeurs suivantes :

  nom_hôte

  Nom de l'hôte sur lequel la base de données TDW est installée.

port Port auquel connecter la base de données TDW. La valeur par défaut pour les bases de données Oracle est 1521.

nom_base_de_données
Le nom par défaut de la base de données TDW est WAREHOUS.

serveur
Nom du serveur Informix.

L'exemple suivant indique l'adresse URL de connexion JDBC pour Oracle.

Oracle **Oracle**
jdbc:oracle:thin:192.168.1.2:1521:itnm

Cet exemple d'adresse URL se connecte à une base de données Oracle avec les propriétés suivantes :

- L'adresse IP de l'hôte serveur de la base de données est 192.168.1.2.
- La base de données s'exécute sur le port 1521. Il s'agit du port par défaut pour Oracle.
- Le nom de la base de données Oracle est itnm.

- *classe_pilote_jdbc* est le nom de classe du pilote JDBC. Les valeurs suivantes représentent les noms de classe des différentes plateformes.
-

Pilote JDBC
`oracle.jdbc.driver.OracleDriver`

- *utilisateur_base_de_données* est le nom d'un utilisateur disposant de droits en lecture dans la base de données cible.
- *mot_de_passe_utilisateur_base_de_données* est le mot de passe de cet utilisateur.

Exemple de commande pour la définition de la source de données NCPOLLDATA sur Tivoli Data Warehouse

Exemple de commande Oracle

La commande suivante permet de configurer la source de données NCPOLLDATA pour la production de rapports d'historique de telle sorte qu'elle utilise Tivoli Data Warehouse exécuté sur Oracle.

```
trcmd.sh -modify -dataSources -reports -reportName
"/content/package[@name='Network
Manager']/folder[@name='Performance Reports']/
report[@name='Historical SNMP
Trend Quick View Report']" -username jazz_username -password
jazz_password -dataSource name=data_source_name -setDatasource
odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Configuration de l'intégration entre Network Manager et Tivoli Common Reporting 3.1

Installez Tivoli Common Reporting 3.1 sur un serveur distinct, puis configurez l'intégration de sorte à pouvoir exécuter des rapports sur le serveur Tivoli Common Reporting directement à partir de l'interface graphique sur le serveur Network Manager.

Avant d'effectuer ces tâches de configuration, veillez à respecter les conditions suivantes :

- Les mêmes utilisateurs existent sur les serveurs Tivoli Integrated Portal et Tivoli Common Reporting. Cette condition est requise pour la connexion unique.
- Un certificat SSL valide est installé sur les serveurs Tivoli Integrated Portal et Tivoli Common Reporting. Cette condition est requise pour garantir que le contenu n'est pas bloqué, en particulier pour le contenu Tivoli Common Reporting 3.1 en cours d'affichage sur le serveur Tivoli Integrated Portal.
- Dans Internet Explorer, vérifiez que le serveur Tivoli Integrated Portal 3.1 est ajouté à la liste des sites Web à afficher dans l'affichage de compatibilité.

Configuration de l'échange de jeton LTPA :

Configurez l'échange de jeton LTPA (Lightweight Third Party Authentication) entre le serveur Tivoli Integrated Portal et le serveur Tivoli Common Reporting 3.1 pour éviter les invites de mot de passe lors de l'affichage de rapports dans Tivoli Common Reporting 3.1.

Procédez comme suit :

1. Sur le serveur Tivoli Integrated Portal, cliquez sur **Paramètres** > **WebSphere Administrative Console** dans le panneau de navigation de gauche pour accéder à WebSphere Administrative Console.
2. Exportez le jeton LTPA. Pour plus d'informations, consultez la rubrique "Gestion des clés LTPA à partir de plusieurs cellules WebSphere Application Server" dans la documentation WebSphere Application Server.
3. Sur le serveur Tivoli Common Reporting 3.1, cliquez sur **Console Settings** > **WebSphere Administrative Console** > dans la bande de navigation de gauche pour accéder à WebSphere Administrative Console.
4. Importez le jeton LTPA. Pour plus d'informations, consultez la rubrique "Gestion des clés LTPA à partir de plusieurs cellules WebSphere Application Server" dans la documentation WebSphere Application Server.

Réaffectation de rôles Tivoli Common Reporting :

Par défaut, Tivoli Integrated Portal contient un rôle prédéfini qui contrôle si les utilisateurs visualisent le point de lancement Tivoli Common Reporting 2.x dans la navigation Tivoli Integrated Portal. Vous devez supprimer ce rôle de tous les utilisateurs et de tous les groupes auxquels vous l'avez affecté sur le serveur Tivoli Integrated Portal, puis sur le serveur Tivoli Common Reporting 3.1, vous devez affecter ce rôle aux utilisateurs et aux groupes appropriés.

Procédez comme suit :

1. Dans le panneau de navigation de gauche Tivoli Integrated Portal, cliquez sur **Utilisateurs et groupes** > **Rôles**.
2. Identifiez le rôle tcrPortalOperator.
3. Supprimez-le de tous les utilisateurs et groupes auxquels il est affecté.

4. Supprimez le rôle.
5. Sur le serveur Tivoli Common Reporting 3.1, affectez ce rôle aux utilisateurs et aux groupes appropriés.

Configuration de l'interface utilisateur de telle sorte qu'elle pointe vers le système Tivoli Common Reporting 3.1 :

Vous devez créer une page Tivoli Integrated Portal afin d'y présenter les données de rapport issues du système Tivoli Common Reporting 3.1.

Procédez comme suit :

1. Dans le panneau de navigation de gauche Tivoli Integrated Portal, cliquez sur **Settings** > **Pages**.
2. Sur la page Pages, cliquez sur **New Page...**.
3. Sur la page Page Settings, attribuez un nom à la page et à son emplacement dans le panneau de navigation de gauche Tivoli Integrated Portal. Par exemple, vous pourriez nommer la page Common Reporting 3.1 et l'ajouter au noeud **Reporting**.
4. Cliquez sur **Page Layout** > **Freeform** et cliquez sur **OK**. Un nouvel onglet s'ouvre, dans lequel vous pouvez définir le contenu à inclure sur cette page.
5. Ajoutez un widget Web à la page. Pour ajouter le widget Web, dans le ruban des widgets situé dans la partie supérieure de la page, faites défiler l'écran vers la droite jusqu'à ce que l'icône du portlet **Web Widget** soit visible ; faites ensuite glisser l'icône du portlet **Web Widget** dans la zone de page principale.
6. Cliquez sur **Edit Options** > **Personalize**.
7. Dans la fenêtre Web Widget, procédez comme suit :
   - Entrez l'adresse URL suivante dans la zone de texte **Home Page** :
     `https://`*`nom_serveur_TCR`*`:16311/tarf/servlet/dispatch`, où *nom_serveur_TCR* correspond au nom de ressource du serveur Tivoli Common Reporting 3.1.
   - Décochez la case **Show a browser control toolbar**.
   - Les autres valeurs peuvent rester telles quelles.
8. Cliquez sur **OK**.
9. Enregistrez la page.

Configuration des rapports BIRT en vue du stockage des mots de passe de base de données à l'aide de JNDI

Pour des raison de conformité FIPS 140-2, vous pouvez configurer les rapports BIRT en vue du stockage des mots de passe NCIM à l'aide de l'interface JNDI (Java Naming and Directory Interface).

Pour configurer les rapports BIRT en vue du stockage des mots de passe NCIM à l'aide de JNDI, procédez comme suit :

Restriction : Le script `setupITNMDatasources.jy` fonctionne uniquement avec DB2 et Oracle.

1. 1. Supprimez les informations d'accès à la base de données des rapports Birt.
   a. Modifiez le fichier `$NCHOME/../tipv2Components/TCRComponent/data/resource/ITNM39/itnm/lib/itnm_data_source.rptlibrary`.

b. Supprimez les propriétés suivantes de chaque source de données : odaURL, odaUser et odaPassword. Les lignes à supprimer sont similaires au fragment de code suivant :

```
<property name="odaURL">jdbc:db2://nomhôte:port/nom_bd</property>
<property name="odaUser">root</property>
<encrypted-property name="odaPassword" encryptionID="base64">
motdepasse_chiffré</encrypted-property>
```

Remarque : Ne supprimez pas le propriété de source de données odaJndiName.

2. Exécutez le script setupITNMDatasources.jy pour créer les noms JNDI pour les sources de données.

Remarque : Tivoli Integrated Portal doit être en cours d'exécution pour que vous puissiez exécuter ce script.

Le script $NCHOME/precision/bin/setupITNMDatasources.jy définit deux ensembles de sources de données JNDI pour DB2 et Oracle, un pour NCIM et un pour NCPOLLDATA. Ces sources de données JNDI sont utilisées par les rapports BIRT. Le script setupITNMDatasources.jy est nécessaire dans les installations FIPS 140-2 pour lesquelles le mot de passe de base de données chiffré ne doit pas être stocké dans le fichier Tivoli Common Reporting rptlibrary.

La syntaxe d'exécution du script est la suivante :

```
/opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
 nom_util_tip -password motdepasse_tip -f setupITNMDatasources.jy
 -createDB2|-createOracle  all nom_util_bd motdepasse_util_bd
 nomhôte_serveur_bd nom_bd chemin_vers_db2_jdbc_jar
|chemin_vers_oracle_jdbc_jar port_bd
```

Voici un exemple pour une base de données DB2 : DB2

```
/opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
 tipadmin -password netcool -f setupITNMDatasources.jy
 -createDB2  all db2inst1 netcool db2hostserver.ibm.com ITNM
/opt/IBM/tivoli/tipv2Components/BIRTExtension/platform/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.1.r22x_v20070919/drivers 50000
```

Voici un exemple pour une base de données Oracle : DB2

```
/opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
 tipadmin -password netcool -f setupITNMDatasources.jy
 -createOracle  all ncim ncim oraclehostserver.ibm.com orcl
/opt/IBM/tivoli/tipv2Components/TCRComponent/lib/birt-runtime-2_2_2
/ReportEngine/plugins/
org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers 1521
```

Remarque : Pour modifier une source de données JNDI existante, vous devez préalablement la supprimer, puis la recréer. Vous devez par exemple effectuer cette opération lorsque le mot de passe de la base de données est modifié.

3. 3. Arrêtez puis redémarrez Tivoli Integrated Portal.

Script setupITNMDatasources

Utilisez le script `setupITNMDatasources` pour gérer les sources de données JNDI.

Exécution du script

Le script utilise la syntaxe suivante.

Restriction : Le script `setupITNMDatasources.jy` fonctionne uniquement avec DB2 et Oracle.

DB2

```
/opt/IBM/tivoli/tipv2/profiles/TIPProfile/bin/wsadmin.sh -lang jython -username
 tip_user_name -password tip_password -f
 setupITNMDatasources.jy [ -createDB2|-createOracle  all db_user_name
db_user_password db_server_hostname db_database_name
 path_to_db2_jdbc_jar|path_to_oracle_jdbc_jar db_port]
 [ -display ] [ -delete ]
```

Options de ligne de commande

Le tableau suivant décrit les options de ligne de commande du script `setupITNMDatasources`.

Tableau 27. Options de ligne de commande setupITNMDatasources

Option de ligne de commande	Description
`-createDB2`	Crée une source de données DB2.
`-createOracle`	Crée une source de données Oracle.
`-display`	Affiche toutes les sources de données en cours.
`-delete`	Supprime toutes les sources de données en cours.

Activation de la reprise en ligne

Vous pouvez activer la reprise en ligne dans votre environnement Network Manager afin de garantir que les différents composants sont en cours d'exécution et disponibles.

A propos de la reprise en ligne

Dans votre environnement Network Manager, une architecture de reprise en ligne peut être utilisée pour configurer votre système pour une haute disponibilité, en minimisant l'impact d'un incident matériel ou réseau.

La reprise en ligne peut être implémentée pour chacun des produits et composants suivants, qui peuvent être installés lorsque vous utilisez le programme d'installation de Network Manager :

- Les composants Network Manager centraux, notamment le composant d'analyse d'origine du problème, le moteur d'interrogation et la passerelle d'événements
- La base de données topologiques
- Tivoli Netcool/OMNIbus, y compris le serveur ObjectServer (pour la gestion des événements)
- Les applications Web Network Manager et l'interface graphique Web Tivoli Netcool/OMNIbus, qui sont installées dans l'infrastructure du serveur Tivoli Integrated Portal

Restriction : Network Manager ne prend pas en charge la fonction d'équilibrage de charge Tivoli Integrated Portal gérée par l'interface graphique Web Tivoli Netcool/OMNIbus.

Vous devez déterminer quels éléments doivent mettre en oeuvre une reprise en ligne, ainsi que le nombre d'ordinateurs requis pour la haute disponibilité.

A propos de la haute disponibilité de la base de données topologiques NCIM

Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

La haute disponibilité se réfère à un environnement informatique dans lequel les composants matériels et logiciels restent opérationnels pendant les indisponibilités planifiées (par exemple des opérations de maintenance régulières) et non planifiées (par exemple des pannes de matériel, de réseau ou de logiciel inattendues). La base de données topologiques NCIM est un composant qui doit rester opérationnel à tout moment.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Pour définir une configuration de reprise en ligne pour la base de données topologiques NCIM et ainsi fournir aux utilisateurs un environnement à haute disponibilité pour l'exécution d'applications de base de données et l'accès aux informations stockées dans la base de données topologiques NCIM, vous devez vous familiariser avec les tâches et les rubriques d'arrière-plan suivantes :

- Stratégies de haute disponibilité fournies par la base de données
- Architecture de reprise en ligne pour la base de données topologiques NCIM et les processus de base Network Manager
- Tâches liées à l'installation de la base de données

Haute disponibilité avec DB2

Vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 pour configurer la réplication des données depuis une base de données principale vers une base de données de secours. La base de données principale traite normalement l'intégralité ou la majorité de la charge de travail des applications, mais la base de données de secours peut s'occuper de la charge de travail si la base de données principale est défaillante ; ainsi, la base de données reste disponible dans les applications utilisateur. Dans un environnement

de reprise à haut niveau de disponibilité après incident (HADR) DB2, cette base de données secondaire est appelée base de données de secours.

Avec la fonction de reprise à haut niveau de disponibilité après incident (HADR), la fonction de redirection automatique du client (ACR) de DB2 permet la redirection des connexions client Network Manager vers le serveur NCIM principal approprié.

Vous pouvez utiliser IBM Tivoli System Automation for Multiplatforms (SA MP) pour promouvoir automatiquement un serveur DB2 de secours en serveur principal lorsque le serveur principal est défaillant.

Remarque : DB2 met à disposition les outils nécessaires à l'installation et à la configuration de la base de données topologiques NCIM (et des processus de base) en vue de l'utilisation de la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Pour des informations sur l'installation et la configuration de DB2, voir Informations connexes plus loin pour connaître les liens vers le centre de documentation DB2.

Fix Pack 5

Mise en cluster et haute disponibilité à l'aide d'Oracle RAC

Oracle fournit la fonction RAC (Real Application Clusters) pour la mise en cluster et la haute disponibilité dans les environnements de base de données Oracle. A l'aide d'Oracle RAC, vous pouvez créer une configuration de haute disponibilité pour votre base de données topologiques NCIM. Pour plus d'informations sur l'installation et la configuration d'Oracle RAC, voir Informations connexes plus loin pour un lien vers la documentation Oracle.

Architecture de reprise en ligne pour la base de données topologiques NCIM et les processus de base Network Manager

Vous pouvez implémenter la reprise en ligne des processus de base Network Manager en configurant des installations Network Manager principale et de secours qui s'exécutent sur des serveurs et dans des domaines différents. Les deux installations peuvent être connectées à un serveur d'objets Tivoli Netcool/OMNIbus unique ou à une paire virtuelle de serveurs d'objets. La reprise en ligne de Network Manager peut être implémentée avec ou sans la haute disponibilité de la base de données topologiques NCIM. Si vous choisissez d'implémenter la reprise en ligne avec la haute disponibilité de la base de données topologiques NCIM, appliquez la fonction de haute disponibilité mise à disposition par la base de données prise en charge. Par exemple, pour définir une configuration de reprise en ligne pour la base de données topologiques NCIM si vous utilisez une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) DB2. De même, si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) pour la reprise en ligne NCIM.

Tâches liées à l'installation de la base de données

Une base de données DB2 peut être installée et configurée par Network Manager. Pour utiliser une base de données DB2 ou Oracle indépendante, configurez-la conformément aux instructions de la rubrique «Configuration d'une base de données topologiques», à la page 62.

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Tâches associées:

«Installation et configuration de bases de données DB2 sous UNIX», à la page 67
Pour utiliser une base de données DB2 en tant que base de données topologique sous UNIX, vous devez installer DB2, configurer une instance et créer une base de données avant d'installer Network Manager.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Architectures de reprise en ligne

La reprise en ligne Network Manager est implémentée indépendamment de la reprise en ligne des produits et composants auxquels elle s'intègre. Avant la configuration de la reprise en ligne, vous devez comprendre les architectures de reprise en ligne pouvant être implémentées pour vous assurer de la haute disponibilité de votre installation Network Manager.

Une installation de reprise en ligne Network Manager contient des serveurs Network Manager principal et de secours sur lesquels les composants centraux sont installés. Si le serveur principal est défaillant en raison de problèmes liés aux matériels ou aux logiciels, le serveur de secours assume le rôle du serveur principal. Pour un environnement plus sûr, vous pouvez inclure une ou plusieurs configurations de reprise en ligne supplémentaires suivantes :

- ObjectServer Tivoli Netcool/OMNIbus principal et un autre de secours.
- Reprise en ligne de la source de données de l'interface graphique Web Tivoli Netcool/OMNIbus.

  Restriction : Network Manager ne prend pas en charge la fonction d'équilibrage de charge Tivoli Integrated Portal gérée par l'interface graphique Web Tivoli Netcool/OMNIbus.
- Configuration de la haute disponibilité d'une base de données topologiques NCIM

  Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication

de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Cette configuration de la haute disponibilité de la base de données topologiques NCIM permet de s'assurer que l'interrogation du réseau peut se poursuivre sur l'installation de secours et que les vues de topologie sont répliquées.

Pour parer aux incidents matériels ou logiciels, et pour une performance optimale de votre environnement, implémentez votre solution de reprise en ligne sur plusieurs ordinateurs.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Architecture de reprise du serveur ObjectServer

Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

Les composants de l'architecture sont disposés par couches : collecte, agrégation et affichage. La configuration de reprise en ligne de base est constituée d'un serveur ObjectServer principal et d'un serveur ObjectServer de sauvegarde reliés par une passerelle ObjectServer bidirectionnelle dans la couche agrégation, sans lien avec une couche collecte ou affichage. La conception modulaire de l'architecture à plusieurs niveaux signifie qu'un système peut être constitué au départ par une paire unique de serveurs ObjectServer d'agrégation, auxquels des composants de collecte ou d'affichage peuvent être ajoutés ultérieurement.

La figure suivante montre un exemple de la configuration de reprise en ligne de base dans la couche d'agrégation.

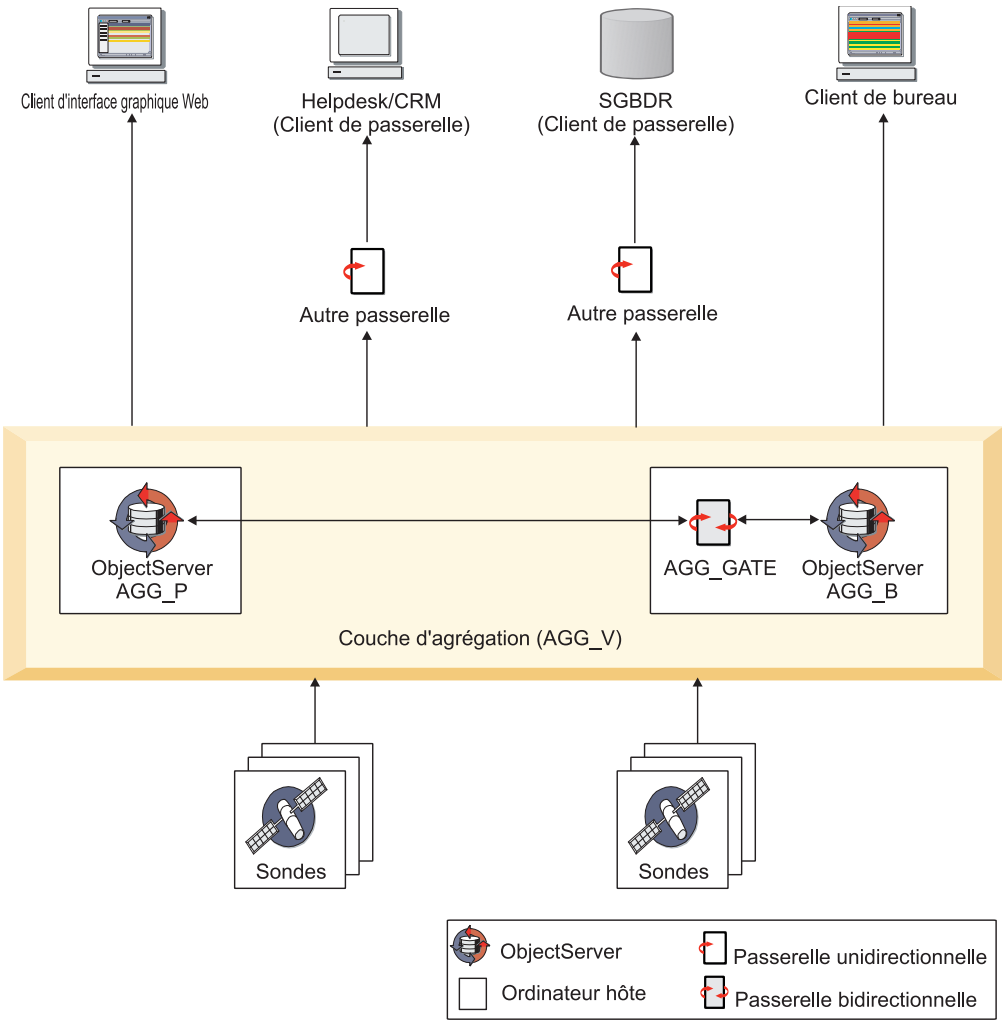

Figure 14. Architecture de reprise du serveur ObjectServer

Pour réduire l'impact de l'échec de l'ordinateur, l'ObjectServer principal (AGG_P) et l'ObjectServer de sauvegarde (AGG_B) s'exécutent sur deux ordinateurs distincts. La passerelle ObjectServer bidirectionnelle (AGG_GATE) s'exécute sur l'ObjectServer de sauvegarde et synchronise les serveurs d'objets. Les ObjectServer principal et de sauvegarde sont configurés en tant que paire d'agrégation virtuelle (AGG_V) auxquelles des analyses et d'autres clients tels la passerelle d'événements peuvent se connecter directement. Le concept de paire virtuelle contribue à faciliter une reprise en ligne transparente vers l'ObjectServer de sauvegarde en cas d'indisponibilité du serveur ObjectServer principal et la reprise par restauration lorsque l'ObjectServer principal est à nouveau actif. Dans la figure, les cibles exemple vers lesquelles les alertes peuvent être acheminées à partir de la couche agrégation sont également présentées.

Pour des informations complètes sur la configuration de la reprise en ligne d'un serveur ObjectServer dans les couches de collecte, d'agrégation et d'affichage de l'architecture à plusieurs niveaux, voir le document *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Tâches associées:

«Configuration de la reprise en ligne du serveur ObjectServer», à la page 337
La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

A propos des fichiers de configuration de reprise en ligne Tivoli Netcool/OMNIbus :

Tivoli Netcool/OMNIbus version 7.3 ou ultérieure fournit un ensemble de fichiers de configuration que vous pouvez appliquer aux serveurs ObjectServer et aux passerelles ObjectServer afin d'implémenter une architecture composée de plusieurs couches.

Ces fichiers sont disponibles dans le répertoire `$NCHOME/omnibus/extensions/multitier` et incluent :

- Les fichiers d'importation SQL pouvant être appliqués à chaque serveur ObjectServer, dans le but de mettre à jour le schéma de base de données avec la configuration requise. Par exemple, des colonnes supplémentaires, des conversions et des automatisations
- Les fichiers de passerelle ObjectServer pouvant être utilisés pour configurer les passerelles dans l'architecture

Important :

- Lors de l'utilisation des fichiers de configuration fournis dans Tivoli Netcool/OMNIbus version 7.3 ou ultérieure, vous devez vous conformer à la convention d'attribution de nom définie pour les composants de chaque couche de l'architecture composée de plusieurs couches. Pour implémenter la reprise en ligne dans la couche agrégation, utilisez les conventions de dénomination décrites dans figure 14, à la page 313, c'est-à-dire AGG_P pour le serveur ObjectServer principal, AGG_B pour le serveur ObjectServer de sauvegarde, AGG_V pour la paire virtuelle et AGG_GATE pour la passerelle ObjectServer bidirectionnelle.
- Dans les versions antérieures de Tivoli Netcool/OMNIbus, aucun fichier de configuration n'est fourni et la conformité à ces conventions de dénomination n'est pas obligatoire.

Pour plus d'informations sur les fichiers de configuration comportant plusieurs couches et les conventions de dénomination pour les composants de l'architecture comportant plusieurs couches, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Architecture de reprise en ligne Network Manager (processus centraux)

La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Lorsque vous vous connectez à un serveur Network Manager, le domaine associé sous lequel le processus s'exécute doit être identifié. Network Manager fournit un domaine virtuel pouvant être utilisé lors d'une exécution en mode de reprise en ligne. Toute connexion à ce domaine virtuel est routée vers l'installation de Network Manager qui s'exécute en tant que serveur principal dans l'architecture de reprise en ligne. Cette capacité de routage est fournie par le composant de domaine virtuel.

La figure suivante montre l'architecture de reprise en ligne de haut niveau pour les processus centraux de Network Manager qui sont configurés dans deux domaines distincts.

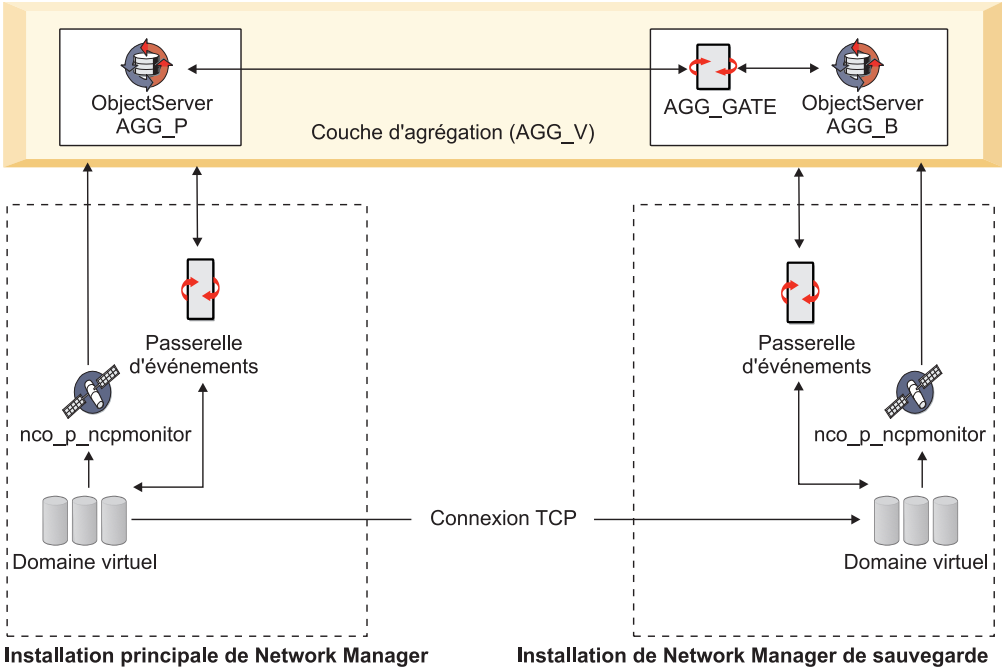

Figure 15. Network Managerarchitecture de reprise en ligne

Dans la figure, les deux installations principale et de secours se connectent à une paire virtuelle de serveurs d'objets.

Dans chaque domaine :

- Le composant de domaine virtuel (**ncp_virtualdomain**) gère la reprise en ligne et génère des événements de vérification d'intégrité pour indiquer si le domaine est en bonne santé.
- La Sonde pour Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) se connecte à la paire de serveurs d'objets virtuels et transfère les événements de vérification d'intégrité.

- La passerelle d'événement (**ncp_g_event**) se connecte à la paire de serveurs d'objets virtuels, lit tous les événements de vérification d'intégrité et transfère ensuite les événements au composant du domaine virtuel.

  Ces événements de vérification d'intégrité sont utilisés pour déclencher la reprise en ligne.

Une connexion de socket TCP est requise entre les processus de domaine virtuel pour copier des données du domaine principal vers le domaine de secours. Ceci garantit que la topologie est en synchronisation lorsque la reprise en ligne se produit.

Remarque : Si vous implémentez la reprise en ligne, vous devez veiller à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement pendant la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Implémentations NCIM pour la reprise en ligne

Vous pouvez configurer la reprise en ligne de Network Manager avec la fonction de haute disponibilité de la base de données topologiques NCIM. Cette configuration de reprise en ligne évite la perte de données en répliquant les modifications apportées aux données depuis la base de données topologiques NCIM source dans le domaine Network Manager principal dans une ou plusieurs bases de données topologiques NCIM cible dans le domaine Network Manager de secours. La base de données topologiques NCIM source est appelée base de données principale et la base de données topologiques NCIM cible est appelée base de données de secours. Cette approche supprime le point de défaillance unique car les domaines Network Manager principal et de secours se connectent tous les deux à la base de données qui sert de base de données principale.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, même si la haute disponibilité de la base de données est configurée. Par contre, la base de données est répliquée sur le serveur de base de données de secours.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Que la reprise en ligne soit configurée ou non avec ou sans la haute disponibilité de la base de données topologiques NCIM, les entités de la topologie sont stockées sous le nom du domaine principal et toutes les règles d'interrogation sont configurées pour le domaine principal. La table domainMgr ne comporte pas d'entrée pour le domaine de secours. En conséquence, la zone NmosDomainName d'un événement de la table alerts.status est toujours remplie avec le nom de domaine principal lorsque la reprise en ligne est configurée.

Remarque : Pour configurer la haute disponibilité de la base de données topologiques NCIM avec la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2, configurez l'environnement HADR en suivant les instructions qui figurent dans la documentation DB2. Voir la rubrique Informations connexes ultérieurement pour connaître les liens vers votre centre de documentation DB2. Vous effectuez ensuite des tâches afin de configurer Network Manager pour qu'il fonctionne avec la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Fix Pack 5 Si vous avez une base de données Oracle, configurez l'environnement Oracle RAC à l'aide des instructions fournies dans la documentation Oracle. Vois les liens connexes plus loin pour un lien vers la documentation Oracle. Vous effectuez ensuite des tâches afin de configurer Network Manager pour qu'il fonctionne dans l'environnement Oracle RAC.

Concepts associés:

«Architecture de reprise du serveur ObjectServer», à la page 312
Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

«Reprise en ligne sur l'installation de sauvegarde sans réplication NCIM», à la page 327
Cette configuration de reprise en ligne ne comprend pas de base de données topologiques NCIM sur l'installation de sauvegarde.

«Reprise en ligne sur l'installation de sauvegarde avec réplication NCIM», à la page 329
Cette configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde. Tous les processus de l'installation de sauvegarde pointent vers la base de données topologiques NCIM sur l'installation de sauvegarde.

Fix Pack 4 «Reprise en ligne sur l'installation de sauvegarde», à la page 332
Tous les processus de l'installation de sauvegarde pointent vers la base de données topologiques NCIM sur l'installation principale ; cette dernière peut être une base de données autonome ou une base de données configurée pour la haute disponibilité.

Fix Pack 4 «A propos de la haute disponibilité de la base de données topologiques NCIM», à la page 309
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Tâches associées:

«Configuration de la reprise en ligne des processus centraux de Network Manager» , à la page 345
Vous pouvez configurer la reprise en ligne des processus centraux de Network Manager à l'aide du fichier `$NCHOME/etc/precision/ConfigItnm.cfg` pour activer la reprise en ligne.

«Installation et configuration de bases de données DB2 sous UNIX», à la page 67
Pour utiliser une base de données DB2 en tant que base de données topologique sous UNIX, vous devez installer DB2, configurer une instance et créer une base de données avant d'installer Network Manager.

Fix Pack 4 «Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC», à la page 351
Vous pouvez configurer les processus principaux de Network Manager en vue de l'utilisation du catalogue DB2 et de l'interface graphique Network Manager pour qu'ils fonctionnent dans l'environnement de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Fix Pack 5 De la même manière, vous pouvez également configurer les processus principaux de Network Manager et l'interface graphique de Network Manager pour qu'ils fonctionnent dans l'environnement RAC (Real Application Clusters) d'Oracle.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Reprise en ligne de la source de données de l'interface graphique Web Tivoli Netcool/OMNIbus

L'interface graphique Web implémente la reprise en ligne de la source de données. Si des serveurs d'objets principal et de sauvegarde sont disponibles, vous pouvez configurer des connexions vers ces deux serveurs d'objets de sorte que si le serveur d'objets principal échoue, l'interface graphique Web procède à une reprise en ligne et utilise le serveur d'objets de sauvegarde comme source pour ses événements.

Concepts associés:

«Sources de données de l'interface graphique Web Tivoli Netcool/OMNIbus», à la page 179
Une source de données désigne un serveur ObjectServer ou une paire de reprise en ligne ObjectServer utilisée par interface graphique Web pour des informations d'événements.

Tâches associées:

«Configuration de la reprise en ligne de la source de données pour l'interface graphique Web Tivoli Netcool/OMNIbus», à la page 342
Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation interface graphique Web.

Allocation de serveur pour la reprise en ligne

Tout système principal doit être installé sur un hôte distinct d'un système de sauvegarde, de sorte que s'il tombe en panne, l'hôte de sauvegarde ne soit pas touché.

Dans l'idéal, le serveur d'objets principal, le serveur d'objets de sauvegarde, le serveur Network Manager principal, le serveur Network Manager de sauvegarde et le serveur Tivoli Integrated Portal devraient être installés sur des hôtes distincts. Toutefois, cela peut s'avérer ne pas être pratique.

Référence associée:

«Contraintes d'installation et de démarrage des composants», à la page 16
Certains composants doivent être installés et démarrés avant d'autres. Utilisez ces informations et les exemples d'installations pour comprendre l'ordre dans lequel vous devez installer et démarrer les composants.

Exemple d'hébergement de reprise en ligne sans haute disponibilité de la base de données topologiques NCIM :

Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne ne comprend pas de copie de la base de données topologiques NCIM sur l'installation de secours.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, mais dans une configuration de reprise en ligne sans haute disponibilité de la base de données topologiques NCIM, la base de données n'est pas répliquée sur un serveur de secours.

La figure suivante présente un exemple de serveur d'objets d'hébergement et une reprise en ligne Network Manager utilisant quatre machines hôtes.

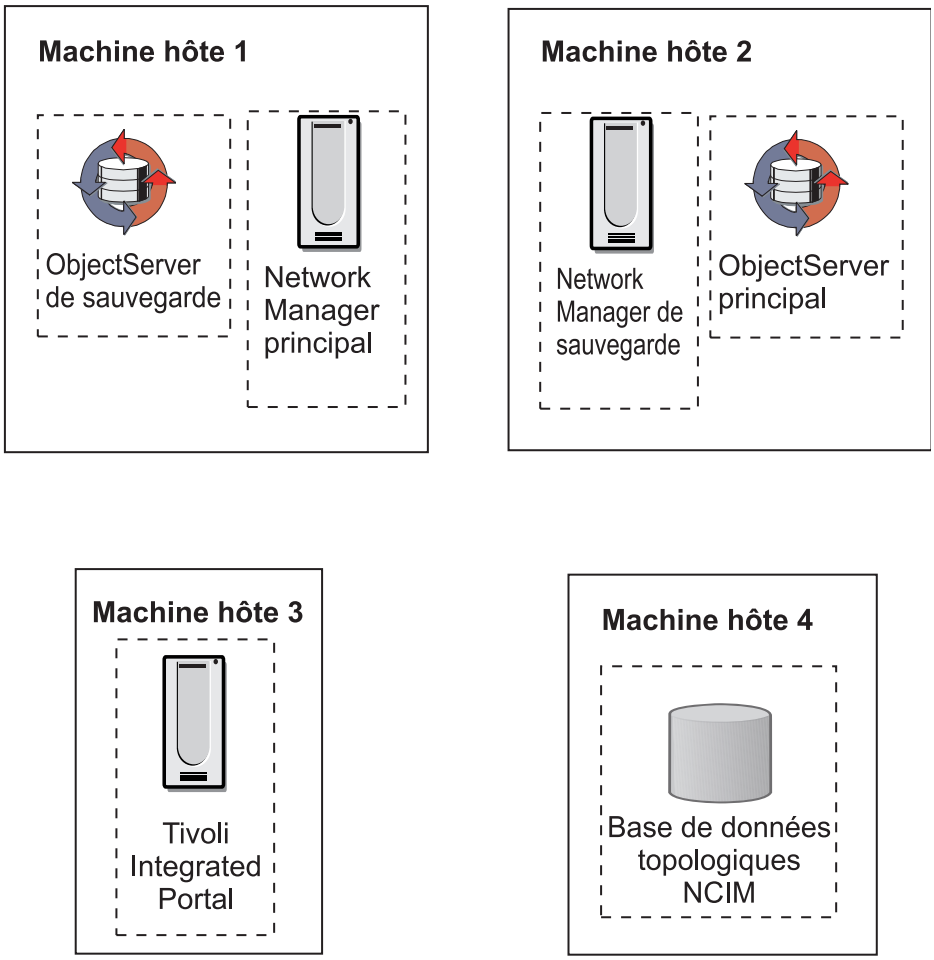

Figure 16. Exemple d'hébergement de reprise en ligne

Pour des questions de performance, la base de données topologiques NCIM doit être connectée au serveur Tivoli Integrated Portal via une liaison à large bande. Si la machine hôte 3 dispose de plusieurs unités centrales et de suffisamment de mémoire, vous pouvez y installer NCIM.

Installez les composants principaux sur les machines hôte 1 et 2 et installez les applications Web sur la machine hôte 3. Installez la base de données topologiques NCIM sur la machine hôte 4.

Remarque : Si vous implémentez la reprise en ligne sans réplication NCIM et que vous avez entré les noms de communauté SNMP à l'aide de l'interface graphique de la configuration de la reconnaissance, vous devez veillez à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement lors de la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Exemple d'hébergement de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM :

Il s'agit d'un exemple d'hébergement de reprise en ligne dans lequel la configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde.

Dans toute configuration de reprise en ligne, les domaines Network Manager principal et de secours se connectent à la même base de données, mais dans une configuration de reprise en ligne dans laquelle la haute disponibilité de la base de données est configurée, la base de données est répliquée sur le serveur de base de données de secours.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

La figure suivante présente un exemple de serveur d'objets d'hébergement et une reprise en ligne Network Manager utilisant cinq machines hôtes.

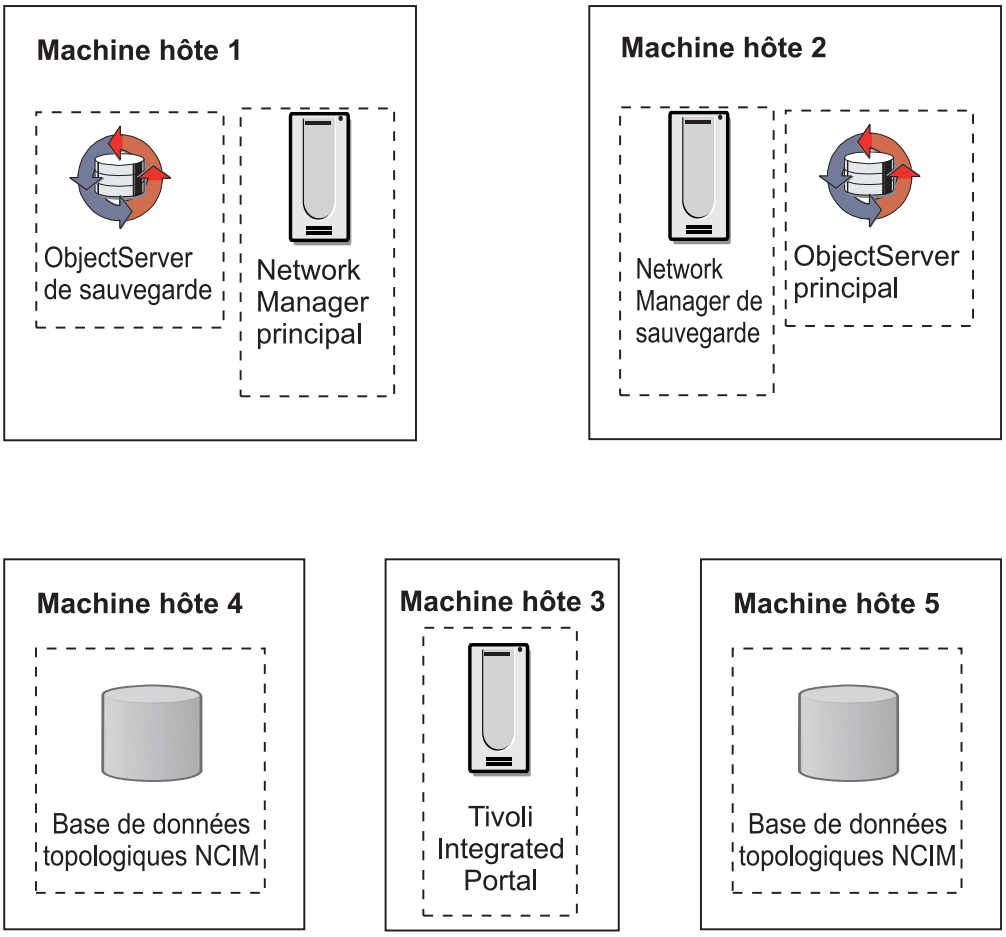

Figure 17. Exemple d'hébergement de reprise en ligne avec base de données topologiques NCIM de secours

Pour des questions de performance, la base de données topologiques NCIM doit être connectée au serveur Tivoli Integrated Portal via une liaison à large bande. Si la machine hôte 3 dispose de plusieurs unités centrales et de suffisamment de mémoire, vous pouvez y installer la base de données NCIM principale.

Installez les composants principaux sur les machines hôte 1 et 2 et installez les applications Web sur la machine hôte 3. Installez la base de données topologiques NCIM principale sur la machine hôte 4 et la base de données topologiques NCIM de secours sur la machine hôte 5.

Opération de reprise en ligne des processus centraux de Network Manager

La reprise en ligne des processus Network Manager centraux est gérée par le processus de domaine virtuel, **ncp_virtualdomain**. Utilisez ces informations pour comprendre comment la reprise en ligne et la reprise par restauration de Network Manager sont déclenchées.

Evénements de vérification d'intégrité et reprise en ligne

La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Dans l'environnement de reprise en ligne, tous les processus des domaines principal et de secours sont démarrés par le contrôleur de processus maître, **ncp_ctrl**. Dans chaque domaine, **ncp_ctrl** surveille aussi régulièrement les processus qu'il contrôle et stocke leur statut dans la table state.services. Le processus de domaine virtuel applique des filtres (qui sont définis dans la table state.filters) aux enregistrements d'états de certains des processus, et génère des événements de vérification d'intégrité pour indiquer si un domaine est en état d'intégrité. Les filtres sont appliqués à :

- **ncp_poller**, le moteur d'interrogation

  Plusieurs filtres peuvent être définis pour le moteur d'interrogation, un pour chaque interrogateur défini dans le fichier `CtrlServices.cfg`.
- **ncp_g_event**, la passerelle d'événements
- **ncp_model**, le gestionnaire de topologie

Des événements de vérification d'intégrité sont générés localement dans chaque domaine et peuvent également être générés à distance par un domaine au nom de l'autre domaine :

- Domaine local : si tous les enregistrements de statut passent les filtres, le serveur Network Manager est considéré comme intègre et le domaine virtuel génère un événement de résolution de vérification d'intégrité pour ce domaine. Chaque domaine indique à l'autre domaine qu'il est intègre en envoyant un événement de résolution qui est acheminé via le serveur d'objets. Un domaine s'attend à recevoir un événement de résolution à un intervalle configuré dans le fichier schéma du processus de domaine virtuel (`$NCHOME/etc/precision/VirtualDomainSchema.cfg`).

  Si un ou plusieurs filtres échouent, indiquant l'échec d'un ou de plusieurs processus locaux, le domaine virtuel génère un événement de problème de vérification d'intégrité, et l'achemine vers l'autre domaine.
- Domaine distant : Si un domaine local détecte que son équivalent distant n'a pas généré d'événement de résolution de vérification d'intégrité dans l'intervalle configuré, le domaine local génère un événement de problème de vérification d'intégrité synthétique pour le domaine distant. Par exemple, si le domaine de secours ne reçoit pas d'événement de résolution de vérification d'intégrité du domaine principal, le domaine de secours génère un événement de problème de vérification d'intégrité pour le domaine principal.

Des événements de vérification d'intégrité sont également générés lorsque la connectivité avec la base de données NCIM est perdue.

Les événements de vérification d'intégrité comportent l'identificateur d'événement "ItnmHealthChk" dans la zone EventId de la table alerts.status.

Concepts associés:

«Reprise en ligne et reprise par restauration Network Manager», à la page 326
La reprise en ligne peut être lancée par le domaine principal ou par le domaine de secours et est déclenchée lorsqu'un problème de vérification d'intégrité est généré pour le domaine principal. La reprise par restauration est déclenchée par un événement de résolution de vérification d'intégrité ultérieur du domaine principal.

Tâches associées:

«Configuration des paramètres pour les vérifications d'intégrité», à la page 360
Si nécessaire, vous pouvez configurer des conditions préférées sous lesquelles les événements de vérification d'intégrité sont générés, en spécifiant des insertions OQL identiques dans le fichier de schéma du processus de domaine virtuel (`VirtualDomainSchema.cfg`) à la fois sur le serveur principal et sur le serveur de sauvegarde.

Référence associée:

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Flux de processus pour les événements de vérification d'intégrité :

Les événements de résolution de vérification d'intégrité sont générés par chaque serveur Network Manager pour indiquer un niveau d'intégrité élevé. Un événement de problème de vérification d'intégrité est l'un des déclencheurs de la reprise en ligne Network Manager.

La figure suivante montre la progression à travers le système d'un événement de vérification d'intégrité généré par le serveur Network Manager principal.

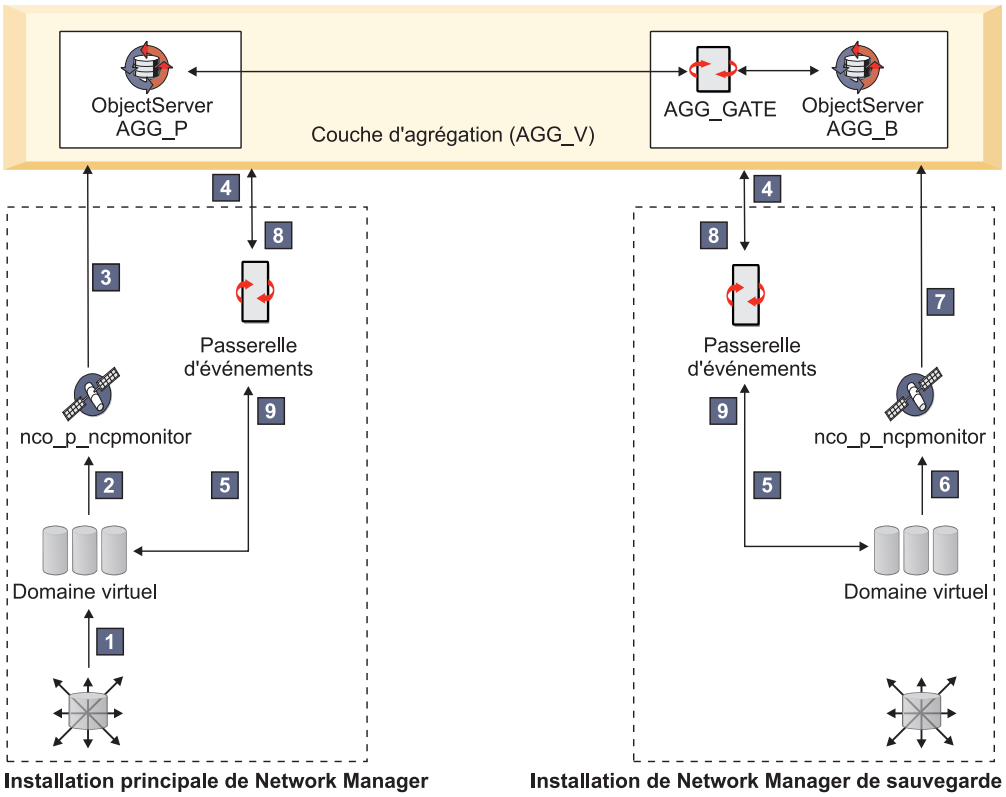

Figure 18. Flux de processus pour un événement de vérification d'intégrité

1 rapport d'état
Le processus **`ncp_ctrl`** signale l'état de ses services gérés.

2 Diagnostic d'intégrité

Le processus de domaine virtuel utilise ses filtres pour effectuer un diagnostic de vérification d'intégrité :

- Si le système est dans un état de bonne intégrité, le domaine virtuel génère un événement de résolution de vérification d'intégrité et l'envoie à la Sonde pour Tivoli Netcool/OMNIbus. Par défaut, les événements de vérification d'intégrité sont envoyés à la sonde toutes les 60 secondes.
- Si le système est dans un état de faible intégrité, le domaine virtuel génère un événement de problème de vérification d'intégrité et l'envoie à la Sonde pour Tivoli Netcool/OMNIbus.

3 Evénement de vérification d'intégrité envoyé au serveur ObjectServer

La Sonde pour Tivoli Netcool/OMNIbus fait suivre l'événement de vérification d'intégrité au serveur ObjectServer.

4 Evénement de vérification d'intégrité envoyé à la passerelle d'événements principale et de secours

Le serveur ObjectServer envoie l'événement de vérification d'intégrité à la passerelle d'événements des serveursprincipal et de secours.

5 Evénement de vérification d'intégrité renvoyé au domaine virtuel principal et de secours

La passerelle d'événements principale renvoie l'événement de vérification d'intégrité au domaine virtuel sur le serveur principal. La passerelle d'événements de secours renvoie l'événement de vérification d'intégrité au domaine virtuel sur le serveur de sauvegarde.

Pour un événement de résolution de vérification d'intégrité, le domaine virtuel contrôle l'horodatage de l'événement pour vérifier qu'il n'a pas plus de 5 minutes, puis met à jour la table state.domains pour indiquer que l'intégrité du serveur principal est bonne. (La passerelle d'événements écoute également les événements de vérification d'intégrité sur le serveur de sauvegarde. La table state.domains enregistre l'état en cours des serveurs principal et de secours.)

Pour un événement de problème de vérification d'intégrité, le domaine virtuel met à jour sa table state.domains pour indiquer que l'intégrité du serveur principal est faible. Le domaine virtuel fait passer le serveur de sauvegarde en mode actif, et le serveur principal passe en mode veille.

6 Echec de vérification d'intégrité généré pour le compte du domaine principal

Si le serveur de sauvegarde ne reçoit pas un événement de résolution de vérification d'intégrité provenant du serveur principal dans l'intervalle de temps configuré de 5 minutes, cela indique que le serveur principal ne fonctionne pas correctement ou qu'il existe un problème de communication avec le serveur ObjectServer. Le domaine virtuel de secours envoie un événement de problème de vérification d'intégrité à la Sonde pour Tivoli Netcool/OMNIbus pour le compte du serveur principal. Le domaine virtuel met à jour le tableau state.domains pour indiquer que le niveau d'intégrité du serveur principal est bas.

7 , 8 , et 9 Reprise en ligne déclenchée

La sonde envoie l'événement de problème de vérification d'intégrité au serveur ObjectServer, qui ensuite le fait suivre à la passerelle d'événements sur les serveurs Network Manager principal et de secours :

- La passerelle d'événements du serveur de sauvegarde envoie l'événement de problème de vérification d'intégrité au domaine virtuel, qui bascule ensuite le serveur de sauvegarde en mode actif.

- Si la passerelle d'événements principale est opérationnelle, elle transmet l'événement de problème de vérification d'intégrité au domaine virtuel principal. Si le domaine virtuel est opérationnel, il bascule le serveur principal en mode veille.

Lorsque le serveur de sauvegarde génère un événement de résolution de vérification d'intégrité, le flux de processus est identique à celui du serveur principal. Les événements de résolution de vérification d'intégrité régulièrement mis à jour relatifs aux serveurs principal et de sauvegarde sont conservés sur le serveur ObjectServer et peuvent être affichés à l'aide entre autre de la Liste d'événements actifs (AEL).

Si l'événement de problème de vérification d'intégrité est généré par le serveur de sauvegarde, pour indiquer que le serveur de sauvegarde est en état d'intégrité faible, les mêmes processus s'appliquent, excepté que le serveur principal n'est pas placé en veille et que le serveur de sauvegarde n'est pas basculé en mode actif. L'événement de problème vérification d'intégrité pour le serveur de sauvegarde est présent sur le serveur ObjectServer et peut être affiché entre autre via la Liste d'événements actifs .

Remarque : La Sonde pour Tivoli Netcool/OMNIbus et la passerelle d'événements des deux domaines doivent être configurées pour accéder au même serveur d'objets afin que les événements de vérification d'intégrité soient acheminés avec succès dans le système.

Reprise en ligne et reprise par restauration Network Manager

La reprise en ligne peut être lancée par le domaine principal ou par le domaine de secours et est déclenchée lorsqu'un problème de vérification d'intégrité est généré pour le domaine principal. La reprise par restauration est déclenchée par un événement de résolution de vérification d'intégrité ultérieur du domaine principal.

Un événement ItnmFailover est généré par **ncp_virtualdomain** lorsqu'un domaine Network Manager fait l'objet d'une reprise en ligne ou d'une reprise par restauration.

Reprise après incident

Lorsqu'une reprise en ligne se produit, le domaine Network Manager principal passe en mode veille (s'il est toujours en cours d'exécution) et le domaine de secours devient actif.

Les modifications suivantes se produisent lorsque le domaine de secours devient actif :

- La passerelle d'événements synchronise les événements avec le serveur ObjectServer.
- Le processus **ncp_poller** rétablit le sondage.
- La passerelle d'événements bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).
- Network Manager continue de surveiller le réseau et effectue une analyse RCA. Toutefois, la reconnaissance du réseau n'est pas effectuée et la topologie de réseau reste statique.

Lorsqu'un serveur Network Manager principal passe en mode veille, les modifications suivantes se produisent :

- La passerelle d'événements bascule du filtre d'événements entrants (StandbyEventFilter) au filtre de veille (EventFilter).
- Le processus **ncp_poller** interrompt toutes les interrogations.

Pour plus d'informations sur le filtre de veille et le filtre d'événements entrants, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Reprise après incident

Lorsqu'un serveur Network Manager principal en mode veille reprend un fonctionnement normal, il génère un événement de résolution de vérification d'intégrité.

L'événement de résolution de vérification d'intégrité passe à travers le système et le serveur Network Manager restauré devient actif à nouveau.

Lorsque le processus de domaine virtuel du serveur Network Manager de secours reçoit l'événement de résolution de vérification d'intégrité, le domaine virtuel repasse le serveur de sauvegarde en mode veille.

L'automatisation GenericClear du serveur ObjectServer est déclenchée par l'événement de résolution de vérification d'intégrité et efface l'événement de problème de vérification d'intégrité existant.

Concepts associés:

«Evénements de vérification d'intégrité et reprise en ligne», à la page 323
La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Reprise en ligne sur l'installation de sauvegarde sans réplication NCIM :

Cette configuration de reprise en ligne ne comprend pas de base de données topologiques NCIM sur l'installation de sauvegarde.

Lorsque vous installez le serveur de sauvegarde, le système crée automatiquement un domaine réseau nommé Backup au cours de l'installation. Il ne s'agit pas d'un domaine réel ; il n'est pas employé dans NCIM, et les utilisateurs ne peuvent pas exécuter d'action avec ce domaine. Assurez-vous qu'il n'existe pas un tel domaine de sauvegarde dans l'installation de sauvegarde. Le cas échéant, supprimez ce domaine à l'aide du script `domain_drop.pl`.

La figure suivante illustre un exemple d'architecture de reprise en ligne Network Manager, dans lequel la base de données topologiques NCIM n'est pas installée comme partie intégrante de l'installation Network Manager de sauvegarde.

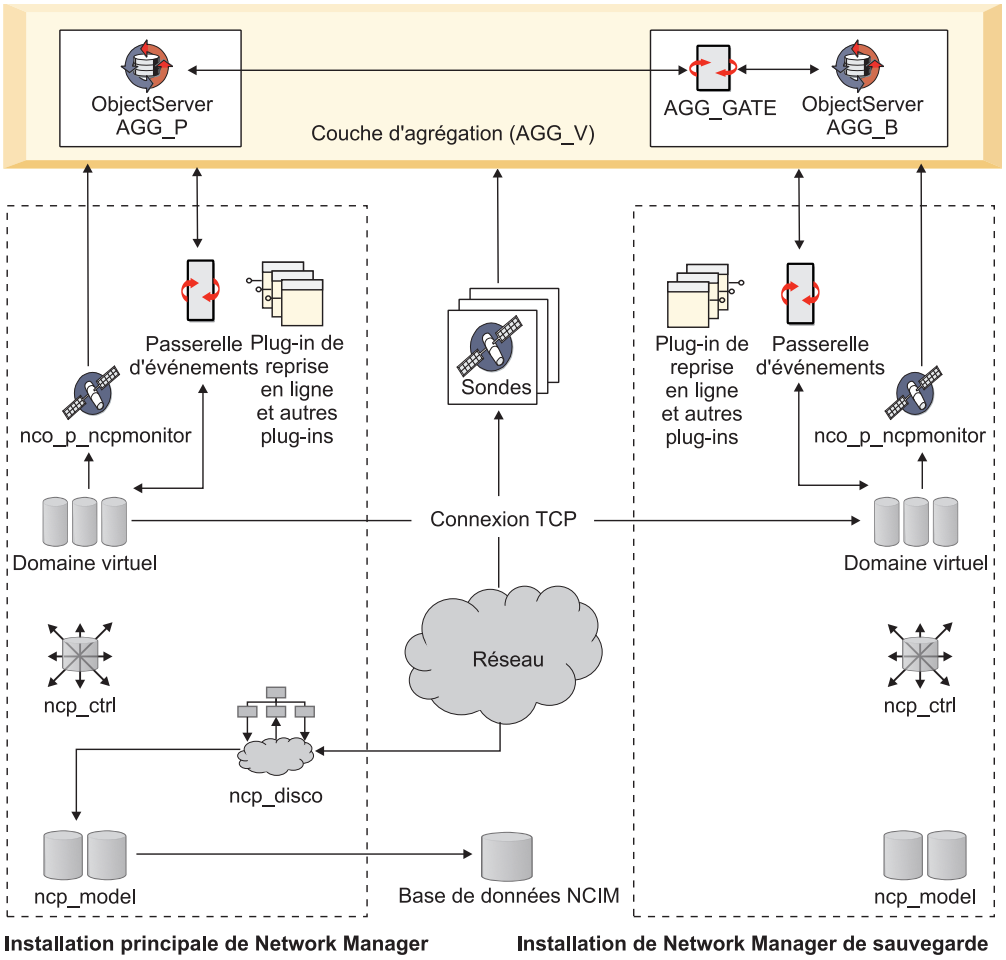

Figure 19. Exemple d'architecture de reprise en ligne

Reconnaissance

Bien que le moteur de reconnaissance (**ncp_disco**) et le serveur auxiliaire SNMP (**ncp_d_helpserv**) soient en cours d'exécution, le serveur Network Manager de secours n'est pas utilisé pour la reconnaissance réseau. Lorsque le domaine de secours est actif, la topologie ne change pas.

Applications Web

Les applications Web ne se connectent pas au domaine de secours, mais ces applications peuvent être configurées manuellement pour se connecter.

NCIM Lorsque la reprise en ligne est configurée sans réplication NCIM, le processus **ncp_model** de secours ne met pas à jour la base de données NCIM. Le processus **ncp_model** continue cependant à fournir des services de topologie à des processus tels que la passerelle d'événements. La base de données NCIM utilisée par les vues réseau et la vue panoramique conserve la dernière version de la topologie de réseau jusqu'à la restauration du serveur Network Manager principal et la reprise du système.

Remarque : Si vous implémentez la reprise en ligne sans réplication NCIM et que vous avez entré les noms de communauté SNMP à l'aide de l'interface graphique de la configuration de la reconnaissance, vous devez veillez à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques,

l'interrogateur de secours ne fonctionne pas correctement lors de la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez toutes les chaînes de communauté SNMP sur la ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Sondage
Lorsque le domaine de secours est en mode veille, le moteur d'interrogation s'exécute, mais les interrogations sont suspendues. Lorsque le domaine de secours devient actif, son processus **ncp_poller** démarre l'interrogation et utilise les détails de la cible SNMP et les règles d'interrogation provenant du domaine principal.

Domaine virtuel
Le composant du domaine virtuel ouvre une connexion socket sur le domaine virtuel du serveur Network Manager principal. Les données topologiques, ainsi que toutes les mises à jour ultérieures de topologie, sont copiées du processus **ncp_model** sur le serveur principal vers le processus **ncp_model** sur le serveur de sauvegarde.

Passerelle d'événements
Lorsque le domaine de secours est en mode veille, la passerelle d'événements n'effectue pas d'enrichissement des événements sur le serveur ObjectServer. Lorsque le domaine de secours devient actif, la passerelle d'événements bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Référence associée:

«Restrictions du processus de reprise en ligne de Network Manager», à la page 335
Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Reprise en ligne sur l'installation de sauvegarde avec réplication NCIM :

Cette configuration de reprise en ligne comprend une copie de la base de données topologiques NCIM sur l'installation de sauvegarde. Tous les processus de l'installation de sauvegarde pointent vers la base de données topologiques NCIM sur l'installation de sauvegarde.

La figure suivante illustre un exemple d'architecture de reprise en ligne Network Manager, dans lequel la base de données topologiques NCIM est installée comme partie intégrante de l'installation Network Manager de sauvegarde.

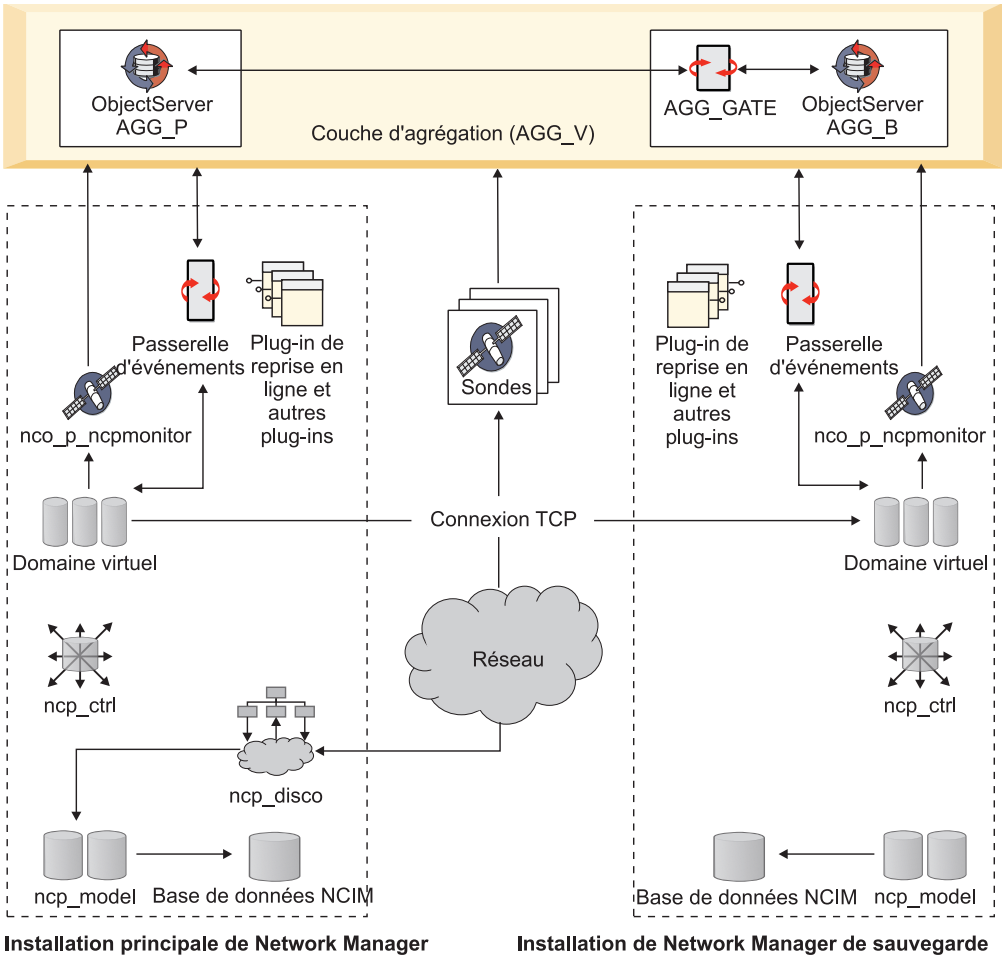

Figure 20. Exemple d'architecture de reprise en ligne

Reconnaissance

Bien que le moteur de reconnaissance (**ncp_disco**) et le serveur auxiliaire SNMP (**ncp_d_helpserv**) soient en cours d'exécution, le serveur Network Manager de secours n'est pas utilisé pour la reconnaissance réseau. Lorsque le domaine de secours est actif, la topologie ne change pas.

Applications Web

Les applications Web ne se connectent pas au domaine de secours, mais ces applications peuvent être configurées manuellement pour se connecter.

NCIM Lorsque la reprise en ligne est configurée avec la réplication NCIM, le processus **ncp_model** met à jour la base de données NCIM. Le processus **ncp_model** conserve la valeur entityId pour chaque entité de NCIM lorsque la topologie est transférée vers la base de données NCIM de sauvegarde. Cela permet de s'assurer que les données de la base de données topologiques NCIM de sauvegarde sont l'exacte réplique des données de la base de données NCIM principale, et que la mise en corrélation des événements est cohérente lorsque l'installation de sauvegarde prend le relais. Les vues de topologie de réseau sont également répliquées sur la sauvegarde. La base de données NCIM conserve la dernière version de la topologie de réseau jusqu'à la restauration du serveur Network Manager principal et la reprise du système.

Remarque : Les vues topologiques peuvent être ajoutées, mises à jour ou supprimées uniquement sur le serveur principal. Les ajouts ou modifications sur les vues de réseau du serveur de sauvegarde alors qu'il est actif ne sont pas propagées vers le serveur principal.

Domaine virtuel

Le processus de domaine virtuel ouvre une connexion socket sur le domaine virtuel du serveur Network Manager principal. Les données de topologie, ainsi que toutes les mises à jour de topologie suivantes, sont copiées du processus **ncp_model** du serveur Network Manager principal vers le processus **ncp_model** du serveur Network Manager de sauvegarde.

Les données de configuration de l'interrogation sont également copiées du serveur principal vers le serveur de sauvegarde. Le processus de domaine virtuel du serveur principal vérifie régulièrement l'horodatage du fichier de configuration de l'interrogateur. Si le fichier semble avoir été mis à jour, le domaine virtuel le transfère au serveur de sauvegarde puis appelle le script `get_policies.pl` à l'aide du processus **ncp_ctrl** pour importer la configuration de l'interrogateur vers la base de données topologiques NCIM de sauvegarde.

Le composant du domaine virtuel vérifie régulièrement l'horodatage du fichier de configuration des vues de réseau. Si le fichier semble avoir été mis à jour, le domaine virtuel le transfère au serveur de sauvegarde puis appelle le script `networkViewUtil.pl` à l'aide du processus **ncp_ctrl** pour importer la configuration des vues de réseau vers la base de données topologiques NCIM de sauvegarde..

Sondage

Lorsque le domaine de secours est en mode veille, le moteur d'interrogation s'exécute, mais les interrogations sont suspendues. Comme les données de configuration SNMP (provenant du fichier `SnmpStackSecurityInfo.cfg`) et les données de configuration d'interrogation sont copiées du domaine principal vers le domaine de secours lorsque la connexion TCP est établie, et qu'elles sont mises à jour à des intervalles réguliers, les interrogations sont conservées à jour dans le domaine de secours.

Remarque :

- Seules les modifications apportées aux règles actives et les définitions associées sont répliquées sur le serveur de sauvegarde. Par exemple, si vous créez une règle d'interrogation mais ne l'activez pas, la règle n'est pas copiée sur le serveur de sauvegarde.
- Les règles d'interrogation doivent être ajoutées, mises à jour ou supprimées uniquement sur le serveur principal. Les ajouts ou les modifications apportées aux règles d'interrogation sur le serveur de sauvegarde alors qu'il est actif ne sont pas propagées vers le serveur principal.

Le processus **ncp_poller** lit la configuration SNMP directement à partir de son fichier de configuration, sans passer par l'auxiliaire SNMP de reconnaissance pour lire ce fichier.

Passerelle d'événements

Lorsque le domaine de secours est en mode veille, la passerelle d'événements n'effectue pas d'enrichissement des événements sur le serveur ObjectServer. Lorsque le domaine de secours devient actif, la

passerelle d'événements bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Référence associée:

«Restrictions du processus de reprise en ligne de Network Manager», à la page 335
Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Reprise en ligne sur l'installation de sauvegarde : Fix Pack 4

Tous les processus de l'installation de sauvegarde pointent vers la base de données topologiques NCIM sur l'installation principale ; cette dernière peut être une base de données autonome ou une base de données configurée pour la haute disponibilité.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

La fonction HADR DB2 dans le groupe de correctifs 4 de Network Manager 3.9 est disponible avec DB2 9.7 et DB2 10.1.

La figure ci-dessous présente un exemple d'architecture de reprise en ligne Network Manager, dans laquelle la base de données topologiques NCIM est configurée pour la haute disponibilité.

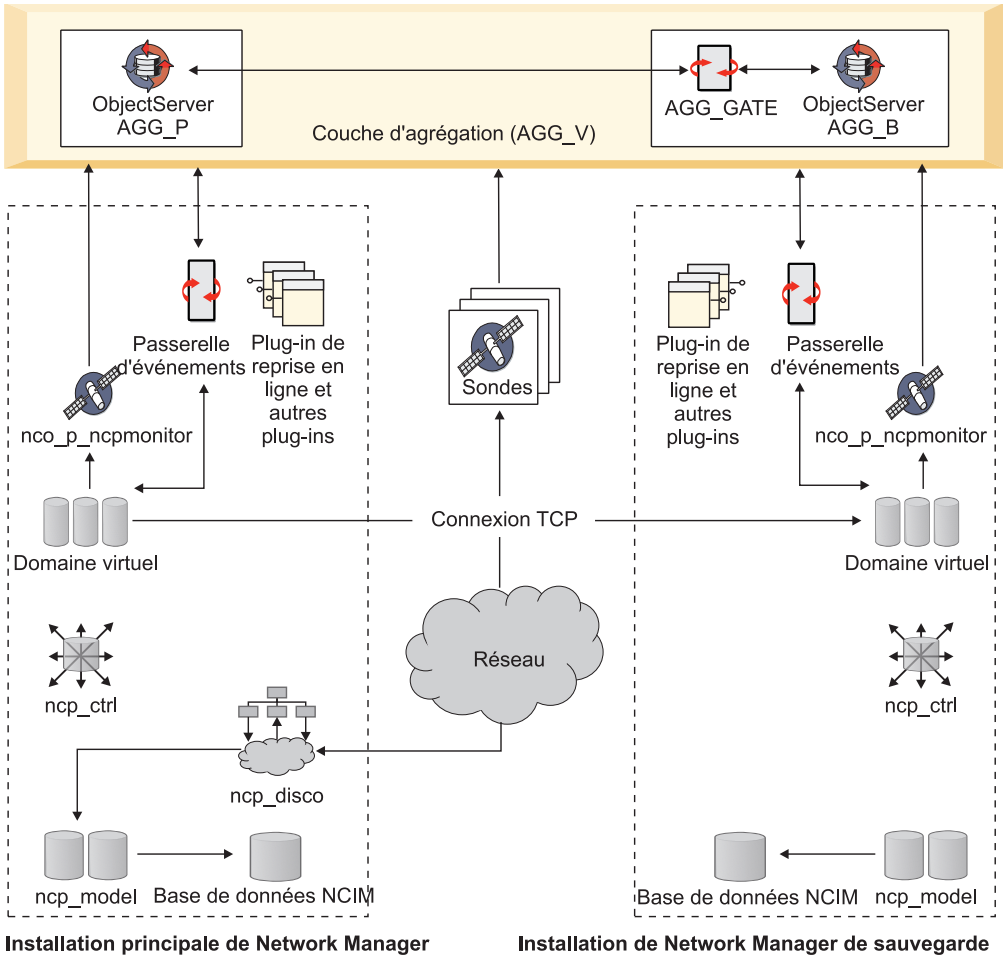

Figure 21. Exemple d'architecture de reprise en ligne avec haute disponibilité NCIM

La figure suivante diffère de la précédente en ce sens que la base de données topologiques NCIM n'est pas configurée pour la haute disponibilité.

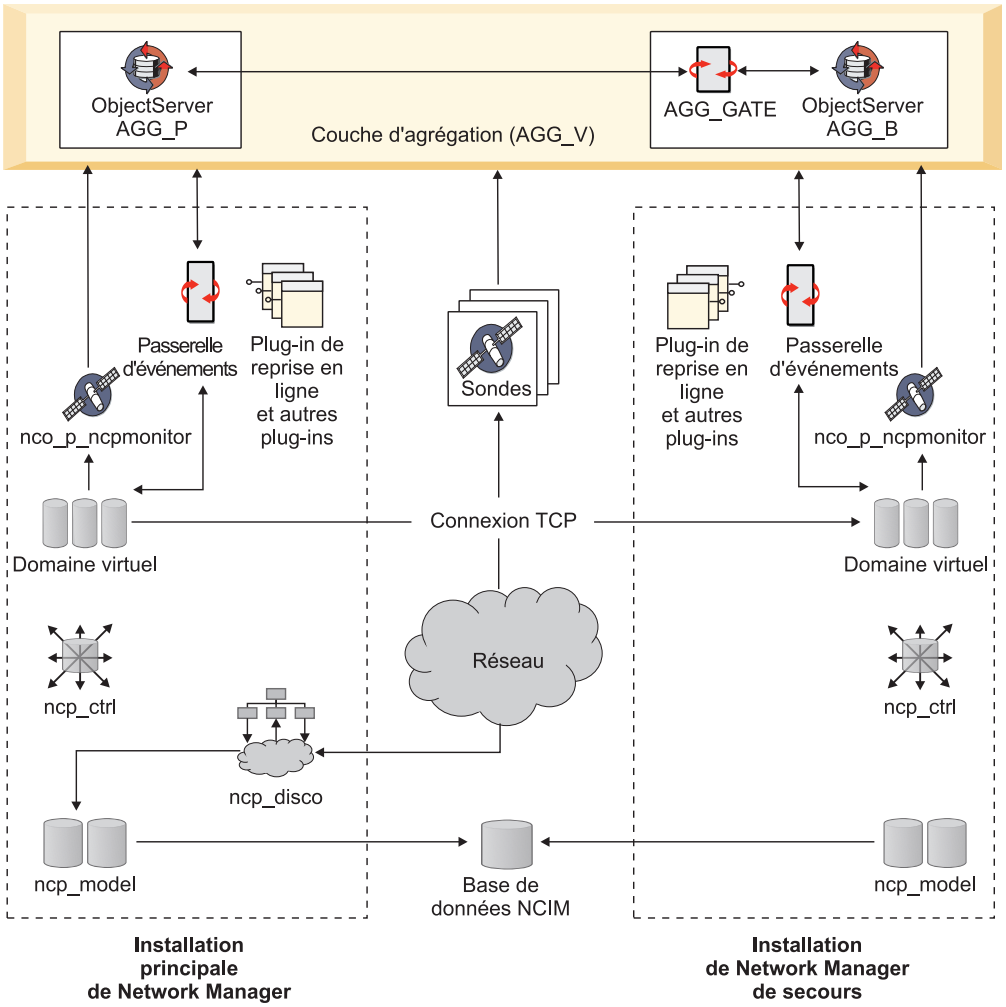

Figure 22. Exemple d'architecture de reprise en ligne sans haute disponibilité NCIM

Reconnaissance
Bien que le moteur de reconnaissance (**ncp_disco**) et le serveur auxiliaire SNMP (**ncp_d_helpserv**) soient en cours d'exécution, le serveur Network Manager de secours n'est pas utilisé pour la reconnaissance de réseau. Lorsque le domaine de secours est actif, la topologie ne change pas.

NCIM Le processus de secours **ncp_model** ne met pas à jour la base de données topologiques NCIM. Le processus **ncp_model** continue cependant à fournir des services de topologie à des processus tels que la passerelle d'événement. La base de données topologiques NCIM utilisée par les vues de réseau et la vue panoramique conserve la version la plus récente de la topologie de réseau jusqu'à la restauration du serveur Network Manager principal et la reprise en ligne du système.

Sondage
Lorsque le domaine de secours est en mode veille, le moteur d'interrogation s'exécute, mais les interrogations sont suspendues. Lorsque le domaine de secours devient actif, son processus **ncp_poller** démarre l'interrogation et utilise les détails de la cible SNMP et les règles d'interrogation provenant du domaine principal.

Le processus **ncp_poller** lit la configuration SNMP directement à partir de son fichier de configuration, sans passer par l'auxiliaire SNMP de reconnaissance pour lire ce fichier.

Domaine virtuel
Le composant de domaine virtuel de secours ouvre une connexion socket sur le domaine virtuel du serveur Network Manager principal. Les données topologiques, ainsi que toutes les mises à jour ultérieures de topologie, sont copiées du processus ncp_model sur le serveur principal vers le processus **ncp_model** sur le serveur de sauvegarde.

Passerelle d'événement
Lorsque le domaine de secours est en mode veille, la passerelle d'événement n'effectue pas d'enrichissement des événements sur le serveur ObjectServer. Lorsque le domaine de secours devient actif, la passerelle d'événement bascule du filtre de veille (StandbyEventFilter) au filtre d'événements entrants (EventFilter).

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Fix Pack 4 «A propos de la haute disponibilité de la base de données topologiques NCIM», à la page 309
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Référence associée:

«Restrictions du processus de reprise en ligne de Network Manager»
Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Restrictions du processus de reprise en ligne de Network Manager

Plusieurs restrictions s'appliquent au processus de reprise en ligne.

Le processus de reconnaissance (**ncp_disco**) effectue la reconnaissance de réseau seulement dans le domaine principal.

Le domaine de secours n'est pas utilisé pour la reconnaissance de réseau ; ainsi, lorsque le domaine de secours est actif, ne tentez pas de configurer la reconnaissance. De plus, lorsque le domaine de reconnaissance est actif, n'éditez pas la topologie de réseau reconnue pour ajouter ou supprimer manuellement des périphériques et des connexions.

Restriction : Network Manager ne prend pas en charge la fonction d'équilibrage de charge Tivoli Integrated Portal gérée par l'interface graphique Web Tivoli Netcool/OMNIbus.

Si vous exécutez plusieurs serveurs Tivoli Integrated Portal, ils s'exécutent chacun indépendamment. Si un des serveurs Tivoli Integrated Portal est défaillant, tous les serveurs restants continuent de fonctionner en tant qu'entités individuelles. Pour minimiser l'effet d'un serveur défaillant :

- Configurez chaque serveur Tivoli Integrated Portal avec sa propre URL unique pour l'authentification.
- Assurez-vous que chacun des serveurs est configuré avec le même ensemble d'utilisateurs, de rôles, de groupes, de profils de préférences et de ressources telles que les pages, vues, portlets et rapports.
- Configurez les serveurs en fonction des besoins de la haute disponibilité de la base de données. Par exemple, pour DB2, configurez les serveurs en fonction des exigences de la fonction à haut niveau de disponibilité après incident (HADR) DB2. Fix Pack 5 De même, si vous disposez d'une base de données Oracle, vous devez configurer les serveurs en fonction des exigences de la fonction RAC (Real Application Clusters).

Remarque : La reprise en ligne n'est pas prise en charge pour les agents de surveillance ITM dans l'architecture de reprise en ligne de Network Manager.

Tâches associées:

«Configuration de la reprise en ligne des processus centraux de Network Manager» , à la page 345
Vous pouvez configurer la reprise en ligne des processus centraux de Network Manager à l'aide du fichier `$NCHOME/etc/precision/ConfigItnm.cfg` pour activer la reprise en ligne.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Configuration de la reprise en ligne

Ces informations vous permettent de configurer la reprise en ligne dans vos installations Network Manager principales et de secours. Des instructions sont également disponibles pour la configuration facultative de la reprise en ligne de l'intégration de produits et de composants. Vous devez utiliser la documentation pour ces produits et références comme premier point de référence.

Avant de commencer à configurer la reprise en ligne, déterminez si vous souhaitez implémenter une solution de reprise en ligne complète pour tous les composants ou la repris en ligne pour Network Manager et un sous-ensemble de composants. Décidez également du nombre d'ordinateurs et des options de déploiement.

Pour la configuration de la reprise en ligne :

- Vous devez avoir installé et configuré IBM Tivoli Netcool/OMNIbus. Si vous envisagez d'exécuter un élément ObjectServer principal et de secours en mode de reprise en ligne, vous devez disposer de deux installations ObjectServer.

Conseil : Si vous utilisez IBM Tivoli Netcool/OMNIbus version 7.3 ou une version ultérieure, avec les fichiers de configuration de reprise en ligne fournis, assurez-vous de respecter les conventions d'attribution nom pour vos éléments ObjectServer et ObjectServer Gateway.

- Vous devez avoir installé une base de données topologiques. Pour la réplication NCIM, vous devez disposer de deux bases de données topologiques.
- Fix Pack 4 Pour la haute disponibilité de la base de données topologiques NCIM, vous avez besoin de deux bases de données topologiques. Fix Pack 4

  Remarque : Les utilisateurs peuvent inclure une configuration de basculement de base de données topologiques NCIM en utilisant la réplication NCIM (appelée également réplication de base de donnes de topologiques NCIM ou en utilisant la fonction haute disponibilité de base de données topologiques NCIM fournie par la base de données DB2. En particulier, DB2 fournit une fonction appelée HADR (High Availability Disaster Recovery) qui permet de configurer une configuration de basculement pour la base de données topologiques NCIM.

  La fonction HADR DB2 dans le groupe de correctifs 4 de Network Manager 3.9 est disponible avec DB2 9.7 et DB2 10.1.
- Vous devez avoir installé et configuré l'interface graphique Web et les applications Web Network Manager dans la structure de serveur Tivoli Integrated Portal.
- Vous devez avoir installé les processus centraux de Network Manager sur les serveurs principaux et de secours, sous deux domaines distincts.

Concepts associés:

«A propos des fichiers de configuration de reprise en ligne Tivoli Netcool/OMNIbus», à la page 314
Tivoli Netcool/OMNIbus version 7.3 ou ultérieure fournit un ensemble de fichiers de configuration que vous pouvez appliquer aux serveurs ObjectServer et aux passerelles ObjectServer afin d'implémenter une architecture composée de plusieurs couches.

Référence associée:

«Contraintes d'installation et de démarrage des composants», à la page 16
Certains composants doivent être installés et démarrés avant d'autres. Utilisez ces informations et les exemples d'installations pour comprendre l'ordre dans lequel vous devez installer et démarrer les composants.

Configuration de la reprise en ligne du serveur ObjectServer

La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

Dans une installation Tivoli Netcool/OMNIbus, chaque ordinateur sur lequel s'exécutent les composants Tivoli Netcool/OMNIbus doit être configuré avec les informations de communication de serveur qui permettent aux composants de l'architecture de s'exécuter et de communiquer entre eux. Configurez le fichier de données des connexions avec tous les détails de composant, de la manière suivante :

- UNIX Linux Mettez à jour les informations de communication pour tous les composants de serveur Tivoli Netcool/OMNIbus dans le déploiement en modifiant manuellement le fichier de données des connexions `$NCHOME/etc/omni.dat` qui est utilisé pour créer le fichier d'interface.

  Une bonne pratique suggérée consiste à ajouter tous les composants dans le déploiement tout entier à un fichier `omni.dat` unique, qui peut ensuite être

distribué au répertoire $NCHOME/etc sur tous les ordinateurs du déploiement. Vous pouvez ensuite générer les fichiers d'interfaces à partir de chaque ordinateur en exécutant la commande **$NCHOME/bin/nco_igen**. (Les fichiers d'interfaces sont nommés $NCHOME/etc/interfaces.*arch*, où *arch* est le nom du système d'exploitation.)

- Windows Configurez les informations de communication du serveur sur chaque ordinateur en utilisant l'éditeur de serveur qui est disponible en cliquant sur **Démarrer** > **Tous les programmes** > **NETCOOL Suite** > **Utilitaires système** > **Editeur des serveurs**. Les informations sont sauvegardées dans le fichier de données des connexions %NCHOME%\ini\sql.ini.

Exemple de configuration pour l'architecture de reprise en ligne de base (couche d'agrégation uniquement)

L'exemple de configuration suivant montre les détails des communications du serveur l'architecture de reprise en ligne de base dans le fichier $NCHOME/etc/omni.dat, où :

- AGG_P est le nom du serveur ObjectServer principal.
- AGG_B est le nom du serveur ObjectServer de secours.
- AGG_V est le nom de la paire de serveurs ObjectServer virtuels.
- AGG_GATE est le nom de la passerelle ObjectServer bidirectionnelle.
- NCO_PA représente le nom par défaut pour l'agent de processus. (Si vous avez configuré des agents de processus pour gérer les processus Tivoli Netcool/OMNIbus et pour exécuter des procédures externes, chaque agent de processus nommé de façon unique doit être ajouté avec le nom d'hôte et le numéro de port appropriés.)
- NCO_PROXY représente le nom par défaut pour le serveur proxy. (Si vous avez configuré un ou plusieurs serveurs proxy pour réduire le nombre de connexions de sonde directes aux serveurs ObjectServer, chaque serveur proxy nommé de façon unique doit être ajouté avec le nom d'hôte et le numéro de port appropriés.)

```
[AGG_P]
{
        Primary: primary_host.ibm.com 4100
}

[AGG_B]
{
        Primary: backup_host.ibm.com 4150
}

[AGG_V]
{
        Primary: primary_host.ibm.com 4100
        Backup: backup_host.ibm.com 4150
}

[AGG_GATE]
{
        Primary: backup_host.ibm.com 4105
}

[NCO_PA]
{
        Primary: primary_host.ibm.com 4200
}
```

```
[NCO_PROXY]
{
        Primary: primary_host.ibm.com 4400
}
```

Pour plus d'informations sur la configuration des informations de communication du serveur, les agents de processus et les serveurs proxy, consultez la documentation de Tivoli Netcool/OMNIbus à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Concepts associés:

«Architecture de reprise du serveur ObjectServer», à la page 312
Vous pouvez déployer Tivoli Netcool/OMNIbus par le biais d'une architecture à plusieurs niveaux évolutive afin que le système puisse continuer à fonctionner au maximum de sa capacité (et avec une perte d'événement minimale) en cas d'échec du serveur ObjectServer, de la passerelle ObjectServer ou du serveur proxy.

Configuration des serveurs ObjectServer et des passerelles pour la reprise en ligne :

Les procédures suivantes indiquent comment configurer la reprise en ligne du serveur ObjectServer dans Tivoli Netcool/OMNIbus.

«Tivoli Netcool/OMNIbus version 7.3 ou suivante» : Configuration de la reprise en ligne
«Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure», à la page 340 : Configuration de la reprise en ligne

Pour obtenir les informations les plus récentes et complètes sur la reprise en ligne du serveur ObjectServer, voir la documentation Tivoli Netcool/OMNIbus disponible à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html. La documentation Tivoli Netcool/OMNIbus doit être consultée en priorité et prime par rapport aux informations présentées dans la documentation Network Manager.

Tivoli Netcool/OMNIbus version 7.3 ou suivante :
Pour configurer la reprise en ligne :

1. Si nécessaire, créez l'ObjectServer AGG_P d'agrégation principal sur l'ordinateur désigné et appliquez la personnalisation SQL en exécutant la commande **nco_dbinit** avec le fichier d'importation `aggregation.sql` fourni :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_P -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

   Si l'ObjectServer est déjà installé et en cours d'exécution, appliquez à celui-ci le fichier d'importation `aggregation.sql` de la manière suivante :

   UNIX Linux
   ```
   $NCHOME/omnibus/bin/nco_sql -server AGG_P -user nom_utilisateur –password mot_de_passe < $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

   Windows
   ```
   "%NCHOME%\omnibus\bin\isql" -S AGG_P -U nom_utilisateur -P password -i "%NCHOME%\omnibus\extensions\multitier\objectserver\aggregation.sql"
   ```

2. Démarrez l'ObjectServer principal (si nécessaire) :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name AGG_P &
   ```

Si vous avez installé Tivoli Netcool/OMNIbus à l'aide du programme d'installation de Network Manager, vous pouvez aussi exécuter la commande **itnm_start** dans le répertoire $NCHOME/precision/bin :

UNIX Linux `itnm_start nco`

3. Créez (ou mettez à jour) l'ObjectServer AGG_B d'agrégation de sauvegarde sur un autre ordinateur et appliquez la personnalisation SQL, comme indiqué à l'étape 1, à la page 339. Lorsque vous appliquez la personnalisation SQL, la propriété **BackupObjectServer** est définie automatiquement sur TRUE et les automatisations requises par l'ObjectServer de sauvegarde sont activées.
4. Démarrez l'ObjectServer de sauvegarde (si nécessaire), comme indiqué à l'étape 2, à la page 339.
5. Sur l'ordinateur sur lequel l'ObjectServer de sauvegarde est installé, configurez la passerelle ObjectServer d'agrégation bidirectionnelle AGG_GATE :
   a. Copiez les fichiers de propriétés composés de plusieurs couches pour la passerelle à partir de l'emplacement $NCHOME/omnibus/extensions/multitier/gateway vers l'emplacement par défaut ($NCHOME/omnibus/etc) où sont contenus les fichiers de configuration et de propriétés :
      - AGG_GATE.map
      - AGG_GATE.props
      - AGG_GATE.tblrep.def
   b. Démarrez la passerelle AGG_GATE :

      ```
      $NCHOME/omnibus/bin/nco_g_objserv_bi -propsfile $NCHOME/omnibus/etc/
      AGG_GATE.props &
      ```

Tivoli Netcool/OMNIbus version 7.2.1 ou antérieure :
Pour configurer la reprise en ligne :

1. Si ce n'est déjà fait, créez l'ObjectServer principal sur l'ordinateur désigné en exécutant la commande **nco_dbinit** :

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server nom_serveur
   ```

   où *nom_serveur* est le nom désigné, par exemple NETCOOLPRI.
2. Démarrez l'ObjectServer principal (si nécessaire) :

   ```
   $NCHOME/omnibus/bin/nco_objserv -name nom_serveur &
   ```
3. Si ce n'est déjà fait, créez l'ObjectServer de sauvegarde sur un autre ordinateur, comme indiqué à l'étape 1.
4. Configurez l'ObjectServer de sauvegarde en modifiant son fichier de propriétés ($NCHOME/omnibus/etc/*nom_serveur*.props) et définissez la propriété **BackupObjectServer** sur True.
5. Démarrez l'ObjectServer de sauvegarde, comme indiqué à l'étape 2.
6. Sur l'ordinateur sur lequel l'ObjectServer de sauvegarde est installé, configurez la passerelle ObjectServer d'agrégation bidirectionnelle to_alert de sorte qu'elle échange des données d'alerte entre les ObjectServers principal et de sauvegarde :
   a. Créez le répertoire $NCHOME/omnibus/gates/*nom_passerelle* pour les fichiers de configuration de passerelle.
   b. Copiez tous les fichiers dans $NCHOME/omnibus/gates/objserv_bi vers le répertoire $NCHOME/omnibus/gates/*nom_passerelle*.
   c. Renommez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/objserv_bi.map en *nom_passerelle*.map.
   d. Renommez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/objserv_bi.props en *nom_passerelle*.props.

e. Modifiez les entrées suivantes dans le fichier *gateway_name*.props :

```
# Common Netcool/OMNIbus Properties.
MessageLog   : '$OMNIHOME/log/nom_passerelle.log'

# Common Gateway Properties.
Gate.MapFile   : '$OMNIHOME/gates/nom_passerelle/nom_passerelle.map'
Gate.StartupCmdFile  : '$OMNIHOME/gates/nom_passerelle/objserv_bi.startup.cmd'

# Bidirectional ObjectServer Gateway Properties.
Gate.ObjectServerA.Server  : 'primary_ObjectServer'
Gate.ObjectServerA.Username  : 'nom_utilisateur'
Gate.ObjectServerA.Password  : 'mot_de_passe'
Gate.ObjectServerA.TblReplicateDefFile:
   '$OMNIHOME/gates/nom_passerelle/objserv_bi.objectservera.tblrep.def'

Gate.ObjectServerB.Server  : 'backup_ObjectServer'
Gate.ObjectServerB.Username  : 'nom_utilisateur'
Gate.ObjectServerB.Password  : 'mot_de_passe'
Gate.ObjectServerB.TblReplicateDefFile:
   '$OMNIHOME/gates/nom_passerelle/objserv_bi.objectserverb.tblrep.def'
```

Remplacez *nom_passerelle* par le nom affecté à la passerelle, *primary_ObjectServer* et *backup_ObjectServer* par les noms ObjectServer, et indiquez le nom d'utilisateur et le mot de passe pour la connexion aux ObjectServers.

f. Copiez le fichier $NCHOME/omnibus/gates/*nom_passerelle*/*nom_passerelle*.props vers $NCHOME/omnibus/etc/*nom_passerelle*.props.

g. Démarrez la passerelle :

```
$NCHOME/omnibus/bin/nco_g_objserv_bi &
```

Connexion une paire de reprise en ligne ObjectServer

Chaque installation Network Manager qui se connecte à un serveur ObjectServer doit disposer d'une copie du fichier d'interfaces Tivoli Netcool/OMNIbus (sous UNIX ou sous Linux) ou du fichier de données de connexions (sous Windows).

En supposant que les informations de communication de serveur ont été configurées dans vos installations Tivoli Netcool/OMNIbus, le fichier $NCHOME/etc/interfaces.*arch* (où *arch* représente le nom du système d'exploitation) ou le fichier %NCHOME%\ini\sql.ini doit être disponible à l'emplacement d'installation NCHOME.

Pour garantir que les processus Network Manager peuvent se connecter à une paire de reprise en ligne ObjectServer, suivez une des procédures ci-après sur les serveurs Network Manager principaux et de secours :

- Si Network Manager et Tivoli Netcool/OMNIbus sont installés sur le même ordinateur mais à différents emplacements NCHOME, copiez le fichier $NCHOME/etc/interfaces.*arch* ou %NCHOME%\ini\sql.ini à partir de l'emplacement Tivoli Netcool/OMNIbus NCHOME dans l'emplacement d'installation NCHOME pour Network Manager. Si les deux produits sont installés au même emplacement NCHOME, aucune action n'est requise.
- Si Network Manager et Tivoli Netcool/OMNIbus sont installés sur différents ordinateurs, copiez le fichier $NCHOME/etc/interfaces.*arch* ou %NCHOME%\ini\sql.ini à partir de l'emplacement Tivoli Netcool/OMNIbus NCHOME dans l'emplacement d'installation NCHOME sur l'ordinateur où Network Manager est installé.

  Pour plus d'informations sur la configuration des informations de communication du serveur et la génération du fichier Tivoli Netcool/OMNIbus interfaces.*arch* ou du fichier sql.ini, voir la documentation de Tivoli

Netcool/OMNIbus à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Tâches associées:

«Configuration de la reprise en ligne du serveur ObjectServer», à la page 337
La manière dont vous configurez la reprise en ligne du serveur ObjectServer dépend de la version de Tivoli Netcool/OMNIbus.

«Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg», à la page 345
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

Configuration de la reprise en ligne de la source de données pour l'interface graphique Web Tivoli Netcool/OMNIbus

Si vous disposez d'une paire de reprise en ligne de serveurs ObjectServer à laquelle doit se connecter interface graphique Web, vous pouvez configurer la reprise en ligne de la source de données par le biais du fichier de configuration de la source de données `ncwDataSourceDefinitions.xml` dans l'installation interface graphique Web.

Ce fichier se trouve dans *rép_base_interface_web*`/etc/datasources`, où *rép_base_interface_web* est le répertoire d'installation de l'interface graphique Web V7.3.1 ; par exemple, `$NCHOME/omnibus_webgui`.

Pour configurer la reprise en ligne de la source de données :

1. Sur le serveur Tivoli Integrated Portal où l'interface graphique Web est installée, modifiez comme suit le fichier de configuration de la source de données :
   a. Utilisez l'attribut `name` de l'élément <ncwDataSourceEntry> pour spécifier un libellé pour la paire de reprise en ligne des serveurs ObjectServer ; par exemple, `VirtualObjectServerPair`.
   b. Définissez les détails de connexion pour les ObjectServers principal et de sauvegarde en utilisant l'élément <ncwDataSourceDefinition> et ses éléments enfant.

      Remarque : Les valeurs de l'attribut `name` des éléments <ncwDataSourceEntry> et <ncwDataSourceDefinition> doivent être identiques. Vous devez aussi définir les connexions ObjectServer en utilisant les noms d'hôte et les numéros de port plutôt que les noms de serveur ObjectServer qui sont configurés dans le fichier `omni.dat` ou `sql.ini`.

      Pour un exemple de la configuration requise, voir l'exemple de code dans «Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données», à la page 344.
   c. Redémarrez le serveur Tivoli Integrated Portal pour que les modifications soient prises en compte. Utilisez une des commandes ou méthodes suivantes :
      - UNIX Linux `itnm_start tip`
      - UNIX Linux `startServer.sh server1`
      - Windows `startServer.bat server1`

- Windows Dans le Panneau de configuration Windows, double-cliquez sur **Outils d'administration** puis sur **Services**. Dans la fenêtre Services, recherchez et démarrez le service **Tivoli Integrated Portal**.

Pour obtenir les informations les plus récentes et complètes sur la configuration de la reprise en ligne de la source de données dans l'interface graphique Web, voir la documentation Tivoli Netcool/OMNIbus interface graphique Web à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html. La documentation interface graphique Web doit être consultée en priorité et prime par rapport aux informations présentées dans la documentation Network Manager.

2. Vous devez également définir la valeur WebTopDataSource dans le fichier `ModelNcimDb.nom_domaine.cfg` sur la même valeur que celle affectée à <ncwDataSourceEntry> dans le fichier `ncwDataSourceDefinitions.xml`. En utilisant les paramètres dans «Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données», à la page 344, l'exemple suivant indique les modifications que vous devez apporter :
   a. Accédez au fichier `NCHOME/etc/precision/ModelNcimDb.nom_domaine.cfg` et ouvrez-le afin de le modifier.
   b. Recherchez l'insertion qui définit WebTopDataSource :

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
500,
0,
"OS"
);
```

   c. Modifiez la valeur WebTopDataSource dans la requête d'insertion suivante afin qu'elle corresponde à la source de données configurée dans <ncwDataSourceEntry> (dans ce cas, remplacez la valeur `OS` par `VirtualObjectServerPair`) :

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
```

```
500,
0,
"VirtualObjectServerPair"
);
```

Remarque : Le nom de la source de données interface graphique Web correspond à celui de la connexion et il est identique à celui défini dans l'interface graphique Web. Le nom peut ne pas toujours être identique à celui du serveur ObjectServer.

d. Effectuez cette modification à la fois sur les serveurs Network Manager centraux principal et de sauvegarde.

e. Redémarrez ncp_ctrl.

Exemple de configuration ncwDataSourceDefinitions.xml pour la reprise en ligne de la source de données

Dans l'exemple de code suivant, le texte en gras indique les valeurs qui sont applicables à la reprise en ligne de la source de données.

```
<ncwDefaultDataSourceList>
    <ncwDataSourceEntry name="VirtualObjectServerPair"/>
</ncwDefaultDataSourceList>

...

<ncwDataSourceDefinition type="singleServerOSDataSource" name="VirtualObjectServerPair" enabled="true">
    <ncwFailOverPairDefinition>
        <!--
         ! The primary ObjectServer to connect to.
         ! - host : The hostname or IP address of the server the ObjectServer is installed on.
         ! - port : The port number the ObjectServer is listening on.
         ! - ssl  : Enables SSL connection to the ObjectServer. [false|true]
         ! - minPoolSize : Specifies the minimum number of connections that will be added to the connection pool. Default value is 5.
         ! - maxPoolSize : Specifies the maximum number of connections that will be added to the connection pool. Default value is 10.
         !-->
        <ncwPrimaryServer>
            <ncwOSConnection host="nomhôte_AGG_P" port="port_AGG_P" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwPrimaryServer>
        <!--
         ! The optional failover ObjectServer to connect to.
         !-->
        <ncwBackUpServer>
            <ncwOSConnection host="nomhôte_AGG_B" port="port_AGG_B" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwBackUpServer>
</ncwFailOverPairDefinition>

</ncwDataSourceDefinition>
```

Configuration de l'authentification du serveur ObjectServer

Si vous utilisez un serveur ObjectServer comme registre d'utilisateurs central pour la gestion et l'authentification des utilisateurs, et que vous voulez que le serveur ObjectServer soit dans un référentiel fédéré, vous devez utiliser le script fourni avec Tivoli Integrated Portal pour configurer l'adaptateur VMM (Virtual Member Manager) pour le serveur ObjectServer. Configurez l'adaptateur pour les deux serveurs ObjectServer de la paire de reprise en ligne.

Sur chaque serveur Tivoli Integrated Portal où les applications Web Network Manager et l'interface graphique Web sont installés :

1. Accédez au répertoire *tip_home_dir*/bin.
2. Entrez la commande suivante sur la ligne de commande :

   confvmm4ncos *utilisateur mot_de_passe adresse port adresse2 port2*

   Où :

   - *utilisateur* est l'ID d'un utilisateur disposant de droits d'administration pour les serveurs ObjectServer.
   - *mot_de_passe* est le mot de passe pour l'ID utilisateur.
   - *adresse* est l'adresse IP du serveur ObjectServer principal.

- *port* est le numéro de port utilisé par le serveur ObjectServer principal.
- *adresse2* est l'adresse IP du serveur ObjectServer de sauvegarde.
- *port2* est le numéro de port utilisé par le serveur ObjectServer de sauvegarde.

3. Redémarrez le serveur Tivoli Integrated Portal à l'aide de l'une des commandes ou méthodes suivantes :
   - UNIX Linux `itnm_start tip`
   - UNIX Linux `startServer.sh server1`
   - Windows `startServer.bat server1`
   - Windows Dans le Panneau de configuration Windows, double-cliquez sur **Outils d'administration** puis sur **Services**. Dans la fenêtre Services, recherchez et démarrez le service **Tivoli Integrated Portal**.

Configuration de la reprise en ligne des processus centraux de Network Manager

Vous pouvez configurer la reprise en ligne des processus centraux de Network Manager à l'aide du fichier `$NCHOME/etc/precision/ConfigItnm.cfg` pour activer la reprise en ligne.

Vous devez aussi utiliser le fichier `$NCHOME/etc/precision/ServiceData.cfg` pour configurer une connexion de socket TCP entre les domaines Network Manager principal et de secours.

Concepts associés:

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315

La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg :

Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

Le contenu du fichier `ConfigItnm.DOMAINE.cfg` doit être identique sur les serveurs de domaine principal et de secours.

Pour configurer la reprise en ligne à l'aide du fichier `ConfigItnm.DOMAINE.cfg` :

1. Sur le serveur Network Manager principal, éditez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAINE_PRINCIPAL.cfg` comme suit :
   a. Activez la reprise en ligne et, option, la réplication NCIM, et spécifiez les noms de domaine virtuel, de sauvegarde et principal pour les processus Network Manager. Vous pouvez insérer les valeurs requises dans la table `itnmDomain.failover` en modifiant la section suivante dans le fichier :

```
insert into itnmDomain.failover
(
    FailoverEnabled,
    IsReplicatingNcim,
    PrimaryDomainName,
```

```
    BackupDomainName,
    VirtualDomainName
)
values
(
    0,
    0,
    "NCOMS_P",
    "NCOMS_B",
    "NCOMS_V"
);
```

Renseignez la section `values` comme suit, dans l'ordre indiqué :

Colonne	Valeur requise
`FailoverEnabled`	Spécifiez `1` pour activer la reprise en ligne pour les domaines principal et de secours. La valeur par défaut `0` signifie que la reprise en ligne est désactivée.
`IsReplicatingNcim`	Spécifiez `1` pour forcer Network Manager à répliquer la base de données topologiques NCIM dans le domaine principal vers une base de données NCIM indépendante dans le domaine de secours. La valeur par défaut `0` signifie que les deux domaines partagent la même base de données NCIM et que Network Manager ne répliquera pas la base de données topologiques NCIM.
`PrimaryDomainName`	Remplacez `NCOMS_P` par le nom réel du domaine principal Network Manager dans la paire de reprise en ligne.
`BackupDomainName`	Remplacez `NCOMS_B` par le nom réel du domaine principal de sauvegarde Network Manager dans la paire de reprise en ligne.
`VirtualDomainName`	Remplacez `NCOMS_V` par un nom désigné pour le domaine virtuel Network Manager dans la paire de reprise en ligne.

b. Spécifiez le nom d'ObjectServer auquel la Sonde pour Tivoli Netcool/OMNIbus et la passerelle d'événements se connecteront. Insérez la valeur requise dans la table `itnmDomain.objectServer` en modifiant la section suivante dans le fichier :

```
insert into itnmDomain.objectServer
(
    ServerName
)
values
(
    "NCOMS"
);
```

Renseignez la section `values` de la manière suivante :

Colonne	Valeur requise
ServerName	Si vous utilisez Tivoli Netcool/OMNIbus version 7.3 ou suivante, et que vous avez configuré la reprise en ligne du serveur d'objets ObjectServer en utilisant les fichiers de configuration comportant plusieurs couches fournis et les conventions de dénomination pour la configuration composée de plusieurs couches, spécifiez AGG_V comme nom de la paire d'agrégation virtuelle. La valeur initiale indiquée est soit le nom du serveur d'objets ObjectServer installé par le programme d'installation Network Manager, soit NCOMS si aucun serveur ObjectServer n'a été installé. Pour des versions antérieures de Tivoli Netcool/OMNIbus, spécifiez le nom de remplacement défini pour la paire virtuelle ObjectServer. Si la reprise en ligne d'ObjectServer n'est pas configurée, spécifiez le nom de l'ObjectServer unique utilisé.

Remarque : Aucune configuration de reprise en ligne supplémentaire n'est requise dans le fichier des propriétés d'analyse. Les paramètres de propriétés d'analyse par défaut fournissent la prise en charge appropriée pour la reprise en ligne lors de l'exécution de l'analyse.

2. Enregistrez le fichier.
3. Copiez le contenu entier du fichier $NCHOME/etc/precision/ConfigItnm.*PRIMARY_DOMAIN*.cfg du serveur principal vers le fichier $NCHOME/etc/precision/ConfigItnm.*BACKUP_DOMAIN*.cfg du serveur de sauvegarde.

Tâches associées:

«Configuration de la reprise en ligne à l'aide du fichier CtrlServices.cfg»
Le fichier $NCHOME/etc/precision/CtrlServices.cfg pour le contrôleur de processus maître, **ncp_ctrl**, offre une méthode alternative pour la configuration de la reprise en ligne des composants centraux de Network Manager. Ce fichier requiert la spécification d'options de ligne de commande individuelles pour les processus **ncp_virtualdomain**, **ncp_model**, **ncp_g_event** et **ncp_poller** dans les serveurs de domaine principal et de secours.

Configuration de la reprise en ligne à l'aide du fichier CtrlServices.cfg :

Le fichier $NCHOME/etc/precision/CtrlServices.cfg pour le contrôleur de processus maître, **ncp_ctrl**, offre une méthode alternative pour la configuration de la reprise en ligne des composants centraux de Network Manager. Ce fichier requiert la spécification d'options de ligne de commande individuelles pour les processus **ncp_virtualdomain**, **ncp_model**, **ncp_g_event** et **ncp_poller** dans les serveurs de domaine principal et de secours.

Remarque : L'utilisation d'options de ligne de commande pour la reprise en ligne, telles que -virtualDomain et -backupDomain dans le fichier CtrlServices.cfg est conservée principalement pour des raisons de compatibilité avec les versions antérieures de Network Manager. La méthode préférée pour la configuration de la reprise en ligne est d'utiliser le fichier$NCHOME/etc/precision/ConfigItnm.*DOMAINE*.cfg.

Si vous avez besoin d'informations sur la configuration de la reprise en ligne à l'aide du fichier CtrlServices.cfg, consultez la documentation de Network

Manager version 3.8 à l'adresse http://www-01.ibm.com/support/knowledgecenter/SSSHRK_3.8.0/com.ibm.networkmanagerip.doc_3.8/itnm/ip/wip/install/task/nmip_ins_conffailoverprocessctrl.html.

Tâches associées:

«Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg», à la page 345
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

«Passage à la configuration de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM», à la page 350
Vous pouvez modifier une architecture de reprise en ligne existante afin d'inclure la haute disponibilité de la base de données topologiques NCIM.

Configuration de la connexion de socket TCP entre les domaines :

Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Pour configurer la connexion TCP :

1. Sur le serveur principal Network Manager, démarrez manuellement le processus **ncp_virtualdomain** à partir du répertoire `$NCHOME/precision/bin` :

   ```
   ncp_virtualdomain -domain PRIMARYDOMAIN_NAME
   ```

   Lorsque le processus **ncp_virtualdomain** démarre pour la première fois, il écrit une ligne dans le fichier `$NCHOME/etc/precision/ServiceData.cfg` qui contient les informations de connexion TCP et multidiffusion pour les processus Network Manager. Cette ligne fait référence à `ncp_virtualdomain` et inclut le port sur lequel le composant Virtual Domain du serveur principal accepte les connexions TCP depuis le serveur de sauvegarde. Par exemple :

   ```
   SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55 PORT: 1234
    SERVERNAME: myhostname DYNAMIC: NO
   ```

   Conseil : Le paramètre `DYNAMIC:NO` force le processus **ncp_virtualdomain** à utiliser le même port et la même adresse lors de son prochain démarrage.
2. Enregistrez le fichier.
3. Arrêtez le processus **ncp_virtualdomain**.
4. Copiez la ligne `SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ...` dans le fichier `$NCHOME/etc/precision/ServiceData.cfg` du serveur principal dans le fichier `$NCHOME/etc/precision/ServiceData.cfg` sur le serveur de sauvegarde. Vérifiez qu'une seule ligne `SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ...` est présente dans le fichier.

   Important : La ligne `SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ...` doit être identique dans le fichier `$NCHOME/etc/precision/ServiceData.cfg` dans les deux domaines.

   Pour plus d'informations sur la communication inter-processus et le fichier `ServiceData.cfg`, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées:

«Définition d'un port fixe pour la connexion de socket TCP»
Pour éviter des problèmes de pare-feu ou des conflits de port, vous pouvez définir un port fixe pour la connexion de socket TCP qui permet au processus Virtual Domain sur le serveur de sauvegarde d'établir une connexion au processus sur le serveur principal.

Définition d'un port fixe pour la connexion de socket TCP :

Pour éviter des problèmes de pare-feu ou des conflits de port, vous pouvez définir un port fixe pour la connexion de socket TCP qui permet au processus Virtual Domain sur le serveur de sauvegarde d'établir une connexion au processus sur le serveur principal.

Lors du démarrage initial, le processus **ncp_virtualdomain** sur le serveur principal ajoute une ligne au fichier NCHOME/etc/precision/ServiceData.cfg avec des informations sur ses détails de connexion, incluant le numéro de port. Pour définir un port fixe, vous devez remplacer le numéro de port initial par votre valeur requise.

Pour configurer un port fixe pour la reprise en ligne :

1. Modifiez le fichier $NCHOME/etc/precision/ServiceData.cfg sur le serveur principal, en procédant comme suit :
   a. Recherchez la ligne qui référence ncp_virtualdomain. Par exemple :

      ```
      SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55
       PORT: 1234 SERVERNAME: myhostname DYNAMIC: NO
      ```

      Dans cet exemple, le processus **ncp_virtualdomain** accepte les connexions du serveur de sauvegarde sur le port 1234.
   b. Modifiez le paramètre PORT en le définissant à la valeur requise.
   c. Notez le numéro de port puis enregistrez et fermez le fichier ServiceData.cfg.
2. Sur le serveur de sauvegarde, modifiez le fichier $NCHOME/etc/precision/ServiceData.cfg en mettant à jour le numéro de port spécifié sur la ligne qui référence ncp_virtualdomain.

   Important : Cette ligne du fichier $NCHOME/etc/precision/ServiceData.cfg doit être identique dans les deux domaines.

   Pour plus d'informations sur le fichier ServiceData.cfg, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées:

«Configuration de la connexion de socket TCP entre les domaines», à la page 348
Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Passage à la configuration de reprise en ligne avec haute disponibilité de la base de données topologiques NCIM :

Vous pouvez modifier une architecture de reprise en ligne existante afin d'inclure la haute disponibilité de la base de données topologiques NCIM.

Remarque : Dans les éditions Network Manager précédentes, les utilisateurs pouvaient inclure une configuration de reprise en ligne de la base de données topologiques NCIM en utilisant la réplication NCIM (aussi appelée réplication de la base de données topologiques NCIM). La fonction de réplication NCIM a été remplacée par la fonction de haute disponibilité fournie par la base de données prise en charge:

- Si vous disposez d'une base de données DB2, vous pouvez utiliser la fonction de reprise à haut niveau de disponibilité après incident (HADR) afin de configurer la reprise en ligne pour NCIM.
- Fix Pack 5 Si vous disposez d'une base de données Oracle, vous pouvez utiliser la fonction RAC (Real Application Clusters) afin de configurer la reprise en ligne pour NCIM.

Pour configurer la haute disponibilité de la base de données topologiques NCIM :

1. Configurez la haute disponibilité de la base de données topologiques NCIM en utilisant la fonction de haute disponibilité fournie par la base de données prise en charge.

   DB2 Si vous disposez d'une base de données DB2, suivez les procédures décrites dans la documentation DB2 afin de définir la configuration de reprise en ligne pour la base de données topologiques NCIM avec la fonction de reprise à haut niveau de disponibilité après incident (HADR). Voir la rubrique Informations connexes ultérieurement pour connaître les liens vers votre centre de documentation DB2.

   Oracle Fix Pack 5 Si vous disposez d'une base de données Oracle, suivez les procédures décrites dans la documentation Oracle pour configurer l'environnement RAC (Real Application Clusters) à haute disponibilité. A l'aide d'Oracle RAC, vous pouvez créer une configuration de haute disponibilité pour votre base de données topologiques NCIM. Pour plus d'informations sur l'installation et la configuration d'Oracle RAC, voir Informations connexes plus loin pour un lien vers la documentation Oracle.
2. Configurez Network Manager pour qu'il fonctionne avec la base de données prise en charge, comme décrit dans «Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC», à la page 351.

Concepts associés:

Fix Pack 4 «A propos de la haute disponibilité de la base de données topologiques NCIM», à la page 309
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

Tâches associées:

«Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg», à la page 345
Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

«Configuration de la reprise en ligne à l'aide du fichier CtrlServices.cfg», à la page 347
Le fichier `$NCHOME/etc/precision/CtrlServices.cfg` pour le contrôleur de processus maître, **ncp_ctrl**, offre une méthode alternative pour la configuration de la reprise en ligne des composants centraux de Network Manager. Ce fichier requiert la spécification d'options de ligne de commande individuelles pour les processus **ncp_virtualdomain**, **ncp_model**, **ncp_g_event** et **ncp_poller** dans les serveurs de domaine principal et de secours.

Fix Pack 4 «Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC»
Vous pouvez configurer les processus principaux de Network Manager en vue de l'utilisation du catalogue DB2 et de l'interface graphique Network Manager pour qu'ils fonctionnent dans l'environnement de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Fix Pack 5 De la même manière, vous pouvez également configurer les processus principaux de Network Manager et l'interface graphique de Network Manager pour qu'ils fonctionnent dans l'environnement RAC (Real Application Clusters) d'Oracle.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Configuration de Network Manager pour qu'il fonctionne avec DB2 HADR ou Oracle RAC

Vous pouvez configurer les processus principaux de Network Manager en vue de l'utilisation du catalogue DB2 et de l'interface graphique Network Manager pour qu'ils fonctionnent dans l'environnement de reprise à haut niveau de disponibilité après incident (HADR) de DB2. Fix Pack 5 De la même manière, vous pouvez également configurer les processus principaux de Network Manager et l'interface graphique de Network Manager pour qu'ils fonctionnent dans l'environnement RAC (Real Application Clusters) d'Oracle.

DB2 Pour les instructions relatives aux pratiques recommandées pour l'implémentation d'une solution haute disponibilité en utilisant HADR DB2, voir *IBM DB2 High Availability for Tivoli Netcool products - Best Practices* sur https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices.

Remarque : Si vous implémentez la reprise en ligne, vous devez veiller à ce que l'installation principale et celle de secours utilisent des clés de chiffrement identiques. Si les clés de chiffrement ne sont pas identiques, l'interrogateur de secours ne fonctionne pas correctement pendant la reprise en ligne. Pour garantir que l'installation principale et celle de secours utilisent des clés de chiffrement identiques, copiez le fichier suivant depuis le serveur principal vers le même emplacement sur le serveur de secours : `$NCHOME/etc/security/keys/conf.key`. Si vous entrez tous les noms de communauté SNMP en ligne de commande sans les chiffrer, vous n'avez pas besoin d'effectuer cette tâche. Pour plus d'informations sur la modification de la clé de chiffrement, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Concepts associés:

Fix Pack 4 «A propos de la haute disponibilité de la base de données topologiques NCIM», à la page 309
Network Manager vous permet de configurer la base de données topologiques NCIM (Network Connectivity and Inventory Model) en vue de la haute disponibilité, minimisant ainsi l'impact d'une défaillance d'un ordinateur ou du réseau. Les sections suivantes donnent un aperçu de la haute disponibilité de base de données topologiques NCIM et expliquent comment la configurer.

«Architecture de reprise en ligne Network Manager (processus centraux)», à la page 315
La reprise en ligne de Network Manager peut être implémentée en définissant des installations Network Manager principale et de secours s'exécutant sur des serveurs différents. Les deux installations peuvent être connectées à un seul serveur d'objets Tivoli Netcool/OMNIbus ou à une paire virtuelle de serveurs d'objets.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Forcer Network Manager à utiliser le catalogue DB2 ou un service Oracle RAC :
Fix Pack 5

Utilisez ces informations pour forcer les processus principaux de Network Manager à utiliser le catalogue DB2 ou à se connecter à un nom de service Oracle RAC, en fonction de votre type de base de données.

DB2 Pour les bases de données DB2, les processus de base Network Manager doivent utiliser le catalogue DB2 afin d'obtenir des informations sur le serveur DB2 alternatif. Pour forcer les processus de base Network Manager à utiliser le catalogue DB2, éditez les deux fichiers de configuration `DbLogins.`*Domaine*`.cfg` et `MibDbLogin.cfg` et exécutez la commande DB2 **`UPDATE ALTERNATE SERVER FOR DATABASE`**.

Oracle Fix Pack 5 Pour les bases de données Oracle, les processus principaux de Network Manager doivent se connecter au nom de service utilisé par Oracle RAC.

Oracle Pour configurer les processus de base de Network Manager de sorte qu'ils utilisent un nom de service au lieu d'un SID, éditez les deux fichiers de configuration `DbLogins.`*Domaine*`.cfg` et `MibDbLogin.cfg`.

Les deux fichiers de configuration, `DbLogins.`*Domaine*`.cfg` et `MibDbLogin.cfg`, que vous devez éditer font partie de l'installation de base de Network Manager. Par conséquent, ces fichiers de configuration se trouvent sur le serveur sur lequel Network Manager est installé. Si la reprise en ligne de Network Manager est configurée, vous pouvez éditer ces fichiers de configuration sur les serveurs Network Manager principal et de secours.

1. Sur le serveur principal de Network Manager, ouvrez le fichier `$NCHOME/etc/precision/DbLogins.`*Domaine*`.cfg` et apportez les modifications suivantes en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	1. Recherchez l'attribut `m_PortNum`. 2. Ne modifiez pas la valeur de l'attribut `m_PortNum` de `"DNCIM",`. Attribuez la valeur 0 (zéro) à tous les autres attributs `m_PortNum`. 3. Associez l'attribut `m_DbName` à l'alias catalogué localement pour le serveur DB2 NCIM principal. 4. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

Option	Description
Oracle **Pour les bases de données Oracle**	1. Recherchez l'attribut `m_OracleService` et ajoutez-le après `m_PortNum` s'il n'existe pas déjà. 2. Ne modifiez pas la valeur de l'attribut `m_OracleService` de `"DNCIM",`. Définissez la valeur de tous les autres attributs `m_OracleService` sur 1. 3. Vérifiez que `m_DbName` est défini sur la valeur `SERVICE_NAME` d'Oracle, comme spécifié dans `$ORACLE_HOME/network/admin/tnsnames.ora` 4. Vérifiez que le nom d'hôte SCAN d'Oracle RAC est spécifié pour `m_Hostname`. 5. Vous pouvez, si vous le souhaitez, définir votre propre chaîne de connexion Oracle RAC personnalisée à l'aide de l'attribut `m_ConnectionString`, comme indiqué ici. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins. 6. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

2. Sur le serveur principal de Network Manager, ouvrez le fichier `$NCHOME/etc/precision/MibDbLogin.cfg` et apportez les modifications suivantes en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	1. Recherchez l'attribut `m_PortNum`. 2. Attribuez la valeur 0 (zéro) à l'attribut `m_PortNum`. 3. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

Option	Description
Oracle **Pour les bases de données Oracle**	1. Recherchez l'attribut `m_OracleService` et ajoutez-le après `m_PortNum` s'il n'existe pas déjà. 2. Affectez à l'attribut `m_OracleService` la valeur 1. 3. Vérifiez que `m_DbName` est défini sur la valeur `SERVICE_NAME` d'Oracle, comme spécifié dans `$ORACLE_HOME/network/admin/tnsnames.ora` 4. Vérifiez que le nom d'hôte SCAN d'Oracle RAC est spécifié pour `m_Hostname`. 5. Vous pouvez, si vous le souhaitez, définir votre propre chaîne de connexion Oracle personnalisée à l'aide de l'attribut `m_ConnectionString`, comme indiqué ici. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins. 6. Enregistrez puis quittez le fichier de configuration. Effectuez les mêmes opérations sur le serveur de secours de Network Manager, si nécessaire.

3. Oracle Fix Pack 5 Pour les bases de données Oracle, vous devez également apporter la modification suivante :
   a. Editez le fichier `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`.
   b. Ajoutez le paramètre suivant au fichier :

      ```
      tnm.database.jdbc.url=jdbc.oracle:thin@NOM_SERVEUR:NUMERO_PORT:NOM_BASE_DE_DONNEES
      ```

      Où :
      - *NOM_SERVEUR* correspond au nom du serveur sur lequel le service Oracle RAC est installé.
      - *NUMERO_PORT* est le numéro de port appropriés sur ce serveur.
      - *NOM_BASE_DE_DONNEES* est le nom de la base de données, tel que défini dans tnm.database.dbname, dans le fichier tnm.properties.

   c. Enregistrez le fichier tnm.properties.
4. DB2 Pour les bases de données DB2, vous devez aussi exécuter la commande **UPDATE ALTERNATE SERVER FOR DATABASE** depuis les serveurs principal et de secours sur lesquels DB2 est installé. Pour plus de détails sur cette commande, y compris les droits requis pour l'exécuter, voir les informations connexes ci-dessous pour connaître les liens vers le centre de documentation DB2.

   Exécutez la commande **UPDATE ALTERNATE SERVER FOR DATABASE** sur le serveur DB2 principal pour mettre à jour l'autre serveur DB2 comme suit :

   ```
   db2 update alternate server for database alias-base-de-données
   using hostname nom-hôte port numéro-port
   ```

   où :

- *alias-base-de-données* — Spécifie l'alias de la base de données dans laquelle le serveur alternatif doit être mis à jour.
- *nom-hôte* — Spécifie un nom d'hôte qualifié complet ou l'adresse IP du noeud sur lequel se trouve le serveur alternatif pour la base de données.
- *numéro-port* — Spécifie le numéro de port du serveur alternatif de l'instance du gestionnaire de bases de données.

Effectuez les mêmes opérations sur le serveur DB2 de secours.

L'exemple suivant montre comment exécuter la commande **UPDATE ALTERNATE SERVER FOR DATABASE** sur le serveur DB2 principal :

```
db2 update alternate server for database TAURUS using hostname co110002
port 50000
```

L'exemple suivant montre comment exécuter la commande **UPDATE ALTERNATE SERVER FOR DATABASE** sur le serveur DB2 de secours :

```
db2 update alternate server for database TAURUS using hostname co110004
port 50000
```

Tâches associées:

«Définition d'une adresse URL de connexion personnalisée pour identifier les serveurs DB2 ou Oracle RAC», à la page 357
Utilisez ces informations pour définir une adresse URL de connexion personnalisée permettant d'identifier les serveurs DB2, ou d'identifier le service Oracle 11 RAC. Cette connexion permettra à l'interface graphique de Network Manager de fonctionner dans l'environnement DB2 HADR ou Oracle RAC, selon votre type de base de données.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Chaîne de connexion Oracle personnalisée :

Vous pouvez définir une chaîne de connexion Oracle personnalisée. Cette chaîne de connexion peut être utilisée pour se connecter à un cluster Oracle RAC, ou à d'autres fins.

Pour définir une chaîne de connexion ORACLE personnalisée, modifiez le fichier de configuration `$NCHOME/etc/precision/DbLogins.Domain.cfg` et configurez l'insertion dans le fichier pour inclure une zone `m_ConnectionString` de sorte que l'insertion ressemble à ceci :

```
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_Schema,
    m_Hostname,
    m_Username,
```

```
    m_Password,
    m_PortNum,
    m_ConnectionString,
    m_EncryptedPwd
)
values
(
    "NCIM",
    "oracle",
    "ORATEST",
    "ncim",
    "server1.location1.acme.com",
    "ncim",
    "ncim",
    1521,
    "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=server1.location1.acme.com3)
(PORT=1521))(CONNECT_DATA=(SID=ORATEST)))",
    0
);
```

En utilisant l'attribut `m_ConnectionString` de la sorte, vous remplacez les valeurs de `m_DbName`, `m_Hostname` et `m_PortNum`. Vous devez toujours fournir ces valeurs, elles seront remplacées par la valeur spécifiée dans l'attribut `m_ConnectionString` lors de la connexion à la base de données.

Définition d'une adresse URL de connexion personnalisée pour identifier les serveurs DB2 ou Oracle RAC :

Utilisez ces informations pour définir une adresse URL de connexion personnalisée permettant d'identifier les serveurs DB2, ou d'identifier le service Oracle 11 RAC. Cette connexion permettra à l'interface graphique de Network Manager de fonctionner dans l'environnement DB2 HADR ou Oracle RAC, selon votre type de base de données.

Pour définir une adresse URL de connexion personnalisée afin d'identifier les serveurs DB2 principal et de secours ou pour identifier les services Oracle RAC, éditez trois fichiers de propriétés et spécifiez la connexion d'URL aux serveurs. Spécifiez la même connexion d'URL dans chaque fichier de propriétés.

Les deux fichiers de propriétés suivants sont applicables à l'interface graphique de Network Manager :

- `$NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties`
- `$NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties`

Le fichier de propriétés suivant fait partie de l'installation de base de Network Manager : `$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties`

Pour définir une URL de connexion personnalisée, procédez comme suit :

1. Ouvrez les fichiers `$NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties` et `$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties` pour les éditer et apportez-y les modifications suivantes, en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	Spécifiez la connexion d'URL aux serveurs DB2 principal et de secours, à l'aide de la syntaxe suivante : `tnm.database.jdbc.url=jdbc:db2://`*`serveur_db2_principal`*`:`*`numéro_port_db2_principal`*`/`*`nom_bdd`*`:clientRerouteAlternateServerName=`*`serveur_db2_secours`*`;clientRerouteAlternatePortNumber=`*`port_db2_secours`*`;` où : • *serveur_db2_principal* : spécifie le nom du serveur principal sur lequel s'exécute la base de données DB2. • *numéro_port_db2_principal* : spécifie le numéro de port du serveur principal sur lequel s'exécute la base de données DB2. • *nom_bdd* : spécifie le nom de la base de données DB2. • *serveur_db2_secours* : spécifie le nom du serveur de secours sur lequel s'exécute la base de données DB2. • *port_db2_secours* : spécifie le numéro de port du serveur de secours sur lequel s'exécute la base de données DB2.
Oracle **Pour les bases de données Oracle**	Spécifiez la connexion d'URL aux serveurs Oracle RAC, à l'aide de la syntaxe suivante : `tnm.database.jdbc.url=jdbc:oracle:thin:@`*`nom_hôte_SCAN_Oracle_RAC`*` :`*`numéro_port_Oracle_RAC`*`/`*`nom_service_Oracle_RAC`* où : • *nom_service_Oracle_RAC* — Spécifie l'adresse SCAN (Single Client Access Name) d'Oracle sur laquelle la base de données Oracle RAC est exécutée. • *numéro_port_Oracle_RAC* — Spécifie le numéro de port sur lequel la base de données Oracle RAC est exécutée. • *nom_service_Oracle_RAC* — Spécifie le nom de service avec lequel la base de données Oracle RAC est exécutée.

2. Ouvrez le fichier `$NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties` pour l'éditer et apportez les modifications suivantes en fonction de votre type de base de données :

Option	Description
DB2 **Pour les bases de données DB2**	Spécifiez la connexion d'URL aux serveurs DB2 principal et de secours, à l'aide de la syntaxe suivante : `ncpolldata.database.jdbc.url=jdbc:db2://`*`serveur_db2_principal`*`:`*`numéro_port_db2_principal`*`/`*`nom_bdd`*`:clientRerouteAlternateServerName=`*`serveur_db2_secours`*`;clientRerouteAlternatePortNumber=`*`port_db2_secours`*`;` où : • *serveur_db2_principal* : spécifie le nom du serveur principal sur lequel s'exécute la base de données DB2. • *numéro_port_db2_principal* : spécifie le numéro de port du serveur principal sur lequel s'exécute la base de données DB2. • *nom_bdd* : spécifie le nom de la base de données DB2. • *serveur_db2_secours* : spécifie le nom du serveur de secours sur lequel s'exécute la base de données DB2. • *port_db2_secours* : spécifie le numéro de port du serveur de secours sur lequel s'exécute la base de données DB2.
Oracle **Pour les bases de données Oracle**	Spécifiez la connexion d'URL aux serveurs Oracle RAC, à l'aide de la syntaxe suivante : `ncpolldata.database.jdbc.url=jdbc:oracle:thin:@`*`nom_hôte_SCAN_Oracle_RAC`*` :`*`numéro_port_Oracle_RAC`*`/`*`nom_service_Oracle_RAC`* où : • *nom_service_Oracle_RAC* — Spécifie l'adresse SCAN (Single Client Access Name) d'Oracle sur laquelle la base de données Oracle RAC est exécutée. • *numéro_port_Oracle_RAC* — Spécifie le numéro de port sur lequel la base de données Oracle RAC est exécutée. • *nom_service_Oracle_RAC* — Spécifie le nom de service avec lequel la base de données Oracle RAC est exécutée.

Tâches associées:

«Forcer Network Manager à utiliser le catalogue DB2 ou un service Oracle RAC», à la page 352
Utilisez ces informations pour forcer les processus principaux de Network Manager à utiliser le catalogue DB2 ou à se connecter à un nom de service Oracle RAC, en fonction de votre type de base de données.

Information associée:

Centre de documentation IBM DB2 version 10.5
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) de DB2 10.1, reportez-vous au centre de documentation

d'IBM DB2 version 10.1. Recherchez par exemple "high availability".

Centre de documentation IBM DB2 version 9.7
Pour plus d'informations sur la fonction de reprise à haut niveau de disponibilité après incident (HADR) d'IBM DB2 version 9.7, reportez-vous au centre de documentation d'IBM DB2 version 9.7. Recherchez par exemple "high availability".

Documentation en ligne de la base de données Oracle

Configuration des paramètres pour les vérifications d'intégrité

Si nécessaire, vous pouvez configurer des conditions préférées sous lesquelles les événements de vérification d'intégrité sont générés, en spécifiant des insertions OQL identiques dans le fichier de schéma du processus de domaine virtuel (`VirtualDomainSchema.cfg`) à la fois sur le serveur principal et sur le serveur de sauvegarde.

Le composant de domaine virtuel utilise deux tables (config et state) de la base de données **`ncp_virtualdomain`** pour la prise en charge de la reprise en ligne de Network Manager. Les filtres et les enregistrements de vérification d'intégrité sont stockés dans ces tables, qui peuvent être mises à jour via le fichier `VirtualDomainSchema.cfg`. Pour plus d'informations sur les tables de base de données config et state, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données de gestion*.

Pour modifier les valeurs par défaut pour les paramètres de vérification d'intégrité :

1. Sur le serveur Network Manager principal, modifiez le fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg` en spécifiant les insertions OQM suivantes :
   - Mettez à jour les valeurs des colonnes dans la table config.defaults pour spécifier des périodes de temps différentes pour les vérifications d'intégrité de reprise en ligne.

     Par exemple, vous pouvez utiliser la colonne m_HealthCheckPeriod pour modifier l'intervalle de temps entre chaque vérification d'intégrité. Vous pouvez aussi utiliser la colonne m_FailoverTime pour modifier l'intervalle de temps après lequel la reprise en ligne est déclenchée par le domaine de secours, lorsque le domaine principal est considéré comme étant de faible intégrité. Les valeurs par défaut sont les suivantes :

     ```
     insert into config.defaults
     (
         m_HealthCheckPeriod,
         m_FailoverTime,
         m_AutoTopologyDownload
     )
     values
     ( 60, 300, 1 );
     ```

   - Si nécessaire, mettez à jour la table state.filters pour définir des filtres individuels pour chaque interrogateur configuré dans le fichier `$NCHOME/etc/precision/CtrlServices.cfg`. Par exemple, pour un interrogateur configuré supplémentaire, PingPoller :

     ```
     insert into state.filters
     (
         m_ServiceName,
         m_Filter,
         m_Description
     )
     values
     ```

```
(
    "PingPoller",
    "m_ChangeTime > eval(time,'$TIME - 300') and m_CtrlState <> 7",
    "The Poller has been running within the last 300 seconds"
);
```

2. Sauvegardez et fermez le fichier.
3. Apportez des modifications identiques au fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg` sur le serveur de sauvegarde.

Concepts associés:

«Evénements de vérification d'intégrité et reprise en ligne», à la page 323
La reprise en ligne est pilotée par les vérifications d'intégrité qui sont configurées pour s'exécuter périodiquement pour évaluer l'intégrité des domaines Network Manager principal et de secours.

Configuration de dépendances de processus pour la reprise en ligne

Lors de l'exécution de Network Manager en mode de reprise en ligne, vous devez démarrer les processus Network Manager à l'aide du processus **ncp_ctrl**. L'ordre dans lequel les processus démarrent est important et il est défini par les dépendances des processus qui sont configurées dans le fichier `$NCHOME/etc/precision/CtrlServices.cfg`.

Le composant de domaine virtuel (**ncp_virtualdomain**), qui gère la reprise en ligne, dépend de tous les processus qu'il surveille car il ne peut pas correctement déterminer leur état tant que les processus sont en cours d'exécution. Dans le fichier `CtrlServices.cfg` du domaine principal et dans celui du domaine de secours, l'entrée pour le processus **ncp_virtualdomain** a la configuration par défaut suivante :

```
dependsOn=[ "ncp_poller(default)", "ncp_g_event" ];
```

Aucune autre configuration n'est nécessaire pour définir les dépendances de processus pour la reprise en ligne, à condition que cette valeur par défaut soit conservée.

Pour plus d'informations sur la gestion des dépendances de processus, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Traitement des incidents de reprise en ligne

Examinez ces informations pour vous aider à résoudre des problèmes que vous pourriez rencontrer avec la reprise en ligne.

Vérification de la configuration de la reprise en ligne des serveurs ObjectServer de Tivoli Netcool/OMNIbus

Si la reprise en ligne des serveurs ObjectServer est configurée, il peut être utile de vérifier sa configuration.

1. Après avoir démarré les deux serveurs ObjectServer, vérifiez que les événements transmis au serveur ObjectServer principal sont affichés dans la liste d'événements actifs.
2. Arrêtez le serveur ObjectServer principal et recherchez s'il y a des messages de reprise en ligne dans le fichier journal du serveur ObjectServer (`$NCHOME/omnibus/log/`*`NOM_PRINCIPAL`*`.log`).
3. Consultez la liste d'événements actifs pour vérifier que les événements transmis au serveur ObjectServer principal sont affichés.

4. Restaurez le serveur ObjectServer principal à un état d'exécution et vérifiez que la reprise par restauration s'est produite en consultant son fichier journal.

Pour des informations sur l'utilisation des commandes Tivoli Netcool/OMNIbus pour démarrer et arrêter le serveur ObjectServer, consultez la documentation de Tivoli Netcool/OMNIbus disponible à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm. Pour des informations sur le démarrage et l'arrêt du serveur ObjectServer à l'aide de commandes Network Manager, consultez le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Suivi de la reprise en ligne des processus centraux de Network Manager

Vous pouvez effectuer plusieurs actions et contrôles pour vérifier si la reprise en ligne des processus centraux de Network Manager fonctionne comme prévu.

Suivi de la reprise en ligne au démarrage

Pour s'assurer que le domaine principal démarre son exécution en tant que domaine actif, démarrez le domaine principal et son processus de domaine virtuel avant de démarrer le domaine de secours. Si le domaine de secours est démarré avant que le processus de domaine virtuel principal ait démarré, le domaine de secours peut devenir actif, commencer à interroger le réseau et générer des événements de problème de vérification d'intégrité à propos du domaine principal. Ce problème se résout cependant de lui-même après le démarrage du domaine virtuel principal et la transmission entre les domaines des événements de vérification d'intégrité.

Au démarrage, la topologie et les règles sont copiées du domaine principal vers le domaine de secours. Le domaine de secours ne peut cependant pas devenir actif (lors d'une reprise en ligne) tant qu'il n'a pas initialisé sa topologie. Pour vérifier que la topologie a été initialisée :

- Recherchez un fichier cache de topologie d'une taille différente de zéro (`Store.Cache.kernel.activeModel.domain`) dans le répertoire `$NCHOME/var/precision` du domaine de secours.
- Si la réplication NCIM est configurée, vérifiez que des entités existent dans le domaine de secours. Il doit y avoir le même nombre d'entités dans les tables ncim.entityData principale et de secours.

  Conseil : Un certain temps peut être nécessaire pour que la topologie et les règles soient copiées du domaine principal vers le domaine de secours, en particulier pour les topologies de grande taille. Prévoyez donc un intervalle de temps raisonnable avant de vérifier le fichier cache et les entités de la topologie dans le domaine de secours.

Génération d'événements pour le démarrage : Surveillez la liste d'événements actifs pour les événements Network Manager ItnmServiceState et ItnmFailoverConnectionevents pour vérifier que les processus de domaine virtuel sont en cours d'exécution et que la connexion de socket TCP a été établie :

- Après le démarrage de chaque processus **`ncp_virtualdomain`** local, le processus **`ncp_ctrl`** génère un événement de résolution ItnmServiceState.
- Lorsqu'une connexion TCP est établie entre les processus de domaine virtuel, un événement de résolution ItnmFailoverConnection est généré.

Suivi de la reprise en ligne lorsque le système est dans un état stabilisé

Un comportement de reprise en ligne normal et en *état stabilisé* peut être obtenu seulement après le démarrage et la connexion des processus de domaine virtuel dans les domaines principal et de secours. Le comportement en état stabilisé peut être défini comme suit :

- Le domaine principal est actif et fonctionne comme s'il était le seul domaine. Le processus de reconnaissance reconnaît le réseau, qui est surveillé par l'interrogateur, et les événements sont enrichis par la passerelle d'événements.
- Le domaine de secours est en mode veille. La reconnaissance n'est pas initiée, et l'interrogateur fait le suivi des règles configurées dans le domaine principal, mais n'interroge pas les périphériques. De son côté, la passerelle d'événements ne met pas à jour les événements dans le serveur ObjectServer.

Vous pouvez exécuter des requêtes OQL sur chaque domaine pour vérifier l'état des processus :

- Vous pouvez vérifier l'état de processus Network Manager individuels en interrogeant la base de données du processus **ncp_ctrl**. Tous les processus qui s'exécutent sans problème doivent avoir la valeur `serviceState = 4` dans la table de base de données services.inTray pour indiquer que le service est «actif et en cours d'exécution».
- Les processus **ncp_poller** et **ncp_g_event** ont chacun une table de base de données config.failover associée, qui identifie leur état de reprise en ligne actuel. Lorsqu'ils s'exécutent correctement dans un état stabilisé, ces processus ont le paramètre `FailedOver = 0` dans la table OQL config.failover dans les deux domaines. (Le processus de domaine virtuel met à jour périodiquement la zone FailedOver.)

  Conseil : Le schéma de la base de données de configuration est définie dans les fichiers suivants : `$NCHOME/etc/precision/NcPollerSchema.cfg` et `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

  Pour plus d'informations sur l'exécution de requêtes OQL, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Génération d'événements dans un état stabilisé : Chaque domaine génère des événements sur son état, sur la base des filtres du fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg`. Ces événements sont générés selon un intervalle configuré dans la zone m_HealthCheckInterval. Surveillez les événements Network Manager ItnmHealthChk et ItnmDatabaseConnection dans la liste d'événements actifs pour vérifier si les domaines principal et de secours sont dans un bon état d'intégrité :

- Chaque domaine génère des événements de résolution ItnmHealthChk lorsque son état d'intégrité est bon.
- Le domaine principal génère un événement de problème ItnmDatabaseConnection si la connexion à la base de données NCIM principale est perdue. Si la connexion n'est pas rétablie dans l'intervalle de temps défini pour l'entrée state.filters NCIM dans le fichier `VirtualDomainSchema.cfg`, le domaine principal génère un événement de problème ItnmHealthChk à propos du domaine principal.

- Si le domaine de secours ne reçoit pas un événement de résolution ItnmHealthChk du domaine principal dans l'intervalle de temps m_FailoverTime configuré, le domaine de secours génère un événement de problème ItnmHealthChk synthétique pour le compte du domaine principal.

  Si le domaine principal ou le domaine de secours génère un événement de problème ItnmHealthChk pour le domaine principal, la reprise en ligne est déclenchée et le domaine de secours devient actif. Si le domaine principal est toujours en cours d'exécution, il passe en mode veille.

  Conseil : Pour les événements de vérification d'intégrité, la zone Node identifie le domaine pour lequel l'événement de vérification d'intégrité est généré.

Suivi de la reprise en ligne et de la reprise par restauration

Lorsqu'une reprise en ligne se produit, le domaine de secours devient actif, l'interrogateur de secours surveille le réseau et la passerelle d'événements met à jour les événements du serveur ObjectServer. Vous pouvez exécuter des requêtes OQL pour vérifier l'état des processus **ncp_poller** et **ncp_g_event**. Ces processus ont chacun une table de base de données config.failover associée, qui identifie leur état de reprise en ligne actuel. Lorsque le domaine de secours est actif, ces processus ont le paramètre `FailedOver = 1` dans la table config.failover pour indiquer qu'ils sont dans un état de reprise en ligne. (Si le domaine principal est toujours en cours d'exécution, la valeur `FailedOver = 1` est également affectée aux processus associés.)

Lorsqu'une reprise par restauration se produit, le domaine de secours passe en veille et le domaine principal redevient actif. Ceci est analogue à ce qui se produit au démarrage.

Génération d'événements lors de la reprise en ligne et de la reprise par restauration : Surveillez les événements Network Manager ItnmHealthChk et ItnmFailover dans la liste d'événements actifs pour vérifier le comportement de la reprise en ligne et de la reprise par restauration :

- Un événement de problème ItnmHealthChk à propos du domaine principal indique qu'une reprise en ligne a été déclenchée. Un événement ultérieur de résolution ItnmHealthChk à propos du domaine principal indique qu'une reprise par restauration a été déclenchée.
- Des événements ItnmFailover sont générés pour indiquer quand un domaine Network Manager fait l'objet d'une reprise en ligne ou d'une reprise par restauration. La description de l'événement indique si le domaine est le domaine principal ou le domaine de secours, et s'il est devenu actif ou est passé en mode veille.

Référence associée:

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Recherche des causes d'une reprise en ligne

La reprise en ligne pouvant être initiée par le domaine principal ou par le domaine de secours, il est important d'identifier le domaine qui a initié la reprise en ligne.

Effectuez l'un ou l'autre des actions suivantes :

- Examinez le fichier journal du domaine virtuel (`$NCHOME/log/precision/ncp_virtualdomain.DOMAINE.log`) et le fichier journal de la passerelle d'événements (`$NCHOME/log/precision/ncp_g_event.DOMAINE.log`).
- Examinez les événements ItnmHealthChk et ItnmFailover dans la liste d'événements actifs. (Ceci est l'approche la plus simple.)

Si le domaine principal a initié la reprise en ligne, ceci indique une défaillance de l'un des processus du domaine principal. Vous pouvez vérifier l'état des processus en interrogeant la base de données du processus **ncp_ctrl**. La zone `serviceState` de la table de base de données services.inTray montre l'état opérationnel en cours pour chacun des processus. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Si le domaine de secours a initié la reprise en ligne, ceci indique un échec de routage des événements de vérification d'intégrité à travers le système pour une des raisons suivantes :

- Le domaine principal n'a pas généré d'événement de vérification d'intégrité (par exemple parce que le serveur principal était hors fonction).
- Les processus de la Sonde pour Tivoli Netcool/OMNIbus ou de la passerelle d'événements des deux domaines ne sont pas configurés pour accéder au même serveur ObjectServer.
- Le plug-in de reprise en ligne de la passerelle d'événements n'est pas activé.
- Le fichier de règles de la Sonde pour Tivoli Netcool/OMNIbus a été modifié de sorte que l'événement de vérification d'intégrité ne contient pas les informations requises.
- La passerelle d'événements de sauvegarde ne laisse pas passer les événements de vérification d'intégrité à travers le filtre nco2ncp.

  Pour plus d'informations sur l'activation du plug-in de reprise en ligne et sur les filtres d'événements, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Vérifiez aussi que le domaine virtuel est configuré (dans le fichier `$NCHOME/etc/precision/CtrlServices.cfg`) pour avoir une dépendance de tous les processus dont la liste figure dans le fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg`.

Tâches associées:

«Configuration de la reprise en ligne à l'aide du fichier ConfigItnm.cfg», à la page 345

Lorsque vous utilisez le fichier `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` pour configurer la reprise en ligne, les processus Network Manager lisent le fichier lors du démarrage pour déterminer s'ils s'exécutent dans le domaine principal ou de sauvegarde. De même, le processus **ncp_model** détermine si la réplication NCIM est utilisée et s'exécute comme il convient en fonction de cette configuration.

Référence associée:

«Evénements d'état Network Manager», à la page 183
Network Manager peut générer des événements présentant l'état des différents processus Network Manager. Ces événements sont également appelés événements d'état Network Manager et ont comme valeur `ITNM Status` pour la zone alerts.status AlertGroup.

Examen des problèmes de connexion TCP

Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées du domaine principal vers le domaine de secours.

Si la connexion TCP est perdue :

- Vérifiez que le domaine virtuel est configuré (dans `$NCHOME/etc/precision/CtrlServices.cfg`) pour avoir une dépendance de tous les processus dont la liste figure dans le fichier `$NCHOME/etc/precision/VirtualDomainSchema.cfg`.
- Vérifiez que le processus **ncp_config** est en cours d'exécution. Vous pouvez vérifier l'état de **ncp_config** en interrogeant la base de données du processus **ncp_ctrl**. S'il s'exécute sans problème, **ncp_config** doit avoir la valeur `serviceState = 4` dans la table services.inTray. Pour plus d'informations sur la façon d'identifier les processus qui sont en cours d'exécution, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Si la connexion TCP n'est pas établie :

- Vérifiez que les fichiers `$NCHOME/etc/precision/ServiceData.cfg` des deux domaines ont la même entrée pour le processus de domaine virtuel.
- Vérifiez que les pare-feu de frontière entre les domaines autorisent la connexion TCP sur le port de serveur défini.
- Vérifiez que le port défini est disponible pour être utilisé sur le domaine principal.

Tâches associées:

«Configuration de dépendances de processus pour la reprise en ligne», à la page 361
Lors de l'exécution de Network Manager en mode de reprise en ligne, vous devez démarrer les processus Network Manager à l'aide du processus **ncp_ctrl**. L'ordre dans lequel les processus démarrent est important et il est défini par les dépendances des processus qui sont configurées dans le fichier `$NCHOME/etc/precision/CtrlServices.cfg`.

«Configuration de la connexion de socket TCP entre les domaines», à la page 348
Une connexion de socket TCP est requise entre les processus de domaine virtuel dans les domaines principal et de sauvegarde afin que les données de topologie et les mises à jour de la topologie puissent être copiées dans le domaine de secours.

Séquence pour le redémarrage des processus serveur dans une configuration de reprise en ligne

Utilisez ces informations comme un guide pour le redémarrage des processus serveur si votre environnement de reprise en ligne Network Manager requiert un réamorçage de tous les serveurs.

Démarrez les processus dans l'ordre suivant :

1. Démarrez le serveur ObjectServer principal. Selon votre installation et votre configuration, vous pouvez utiliser un des méthodes suivantes :
   - Le contrôle de processus Tivoli Netcool/OMNIbus sous UNIX, Linux et Windows

- Les services sous Windows
- La commande **nco_objserv** de Tivoli Netcool/OMNIbus
- La commande **itnm_start** de Network Manager

Pour des informations sur l'utilisation des commandes Tivoli Netcool/OMNIbus pour démarrer le serveur ObjectServer, consultez la documentation de Tivoli Netcool/OMNIbus disponible à l'adresse http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm. Pour des informations sur le démarrage du serveur ObjectServer à l'aide de commandes Network Manager, consultez le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

2. Démarrez le serveur ObjectServer de sauvegarde.
3. Démarrez la base de données topologiques si elle n'est pas déjà en cours d'exécution.
4. Démarrez le serveur Network Manager principal où les processus centraux sont installés à l'aide de la commande **itnm_start** ou bien en démarrant le contrôleur de processus maître, **ncp_ctrl**.

   Vérifiez aussi que le processus de domaine virtuel du domaine principal a démarré en exécutant la commande **itnm_status** dans le répertoire `$NCHOME/precision/bin`.

   Pour des informations sur le démarrage du serveur et des processus Network Manager, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide d'administration*.
5. Démarrez le serveur Network Manager de sauvegarde où les processus centraux sont installés.

Conseil : Le serveur Tivoli Integrated Portal où les applications Web Network Manager et l'interface graphique Web Tivoli Netcool/OMNIbus sont installés démarre automatiquement lorsque l'ordinateur est démarré.

Changement de l'adresse IP et du nom d'hôte de l'installation Network Manager IP Edition

Si vous changez l'adresse IP et le nom d'hôte du serveur sur lequel l'un des composants de Network Manager IP Edition ou des produits intégrés est installé, vous devez configurer Network Manager IP Edition ainsi que les produits et composants associés.

Changement de l'adresse IP et du nom d'hôte pour Network Manager IP Edition

Si vous voulez changer l'adresse IP et le nom d'hôte du serveur sur lequel les composants centraux de Network Manager IP Edition sont installés, vous devez effectuer certaines tâches de configuration.

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Network Manager IP Edition.

1. Placez-vous dans le répertoire suivant : NCHOME/etc/.
2. Editez le fichier de configuration `itnm.cfg`.
3. Changez le paramètre suivant : `ncp`. Mettez-le à jour avec le nouveau nom d'hôte du serveur Network Manager IP Edition, par exemple `ncp=myhost`
4. Sauvegardez le fichier `itnm.cfg`.

5. Sauvegardez le fichier `itnm.cfg`.
6. Placez-vous dans le répertoire suivant : `NCHOME/etc/precision/`.
7. Editez le fichier `ServiceData.cfg`.
8. Changez la ligne suivante :

   ```
   SERVICE: ncp_config DOMAIN: NCOMS ADDRESS: adresse_IP_serveur_Network_Manager
   PORT: numéro_port SERVERNAME: nom_hôte_serveur_Network_Manager DYNAMIC: NO
   ```

   Où :

   - *adresse_IP_serveur_Network_Manager* est la nouvelle adresse IP du serveur Network Manager IP Edition.
   - *nom_hôte_serveur_Network_Manager* est le nouveau nom d'hôte du serveur Network Manager IP Edition.
9. Sauvegardez le fichier `ServiceData.cfg`.

Changement de l'adresse IP et du nom d'hôte sur le serveur Tivoli Netcool/OMNIbus

Si vous voulez changer l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez effectuer certaines tâches de configuration.

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Tivoli Netcool/OMNIbus :

1. Placez-vous dans le répertoire suivant : `NCHOME/etc/`.
2. Editez le fichier `omni.dat`.
3. Recherchez les lignes contenant le serveur Tivoli Netcool/OMNIbus. Ces lignes sont similaires aux suivantes :

   ```
   [NCOMS]
   {
           Primary: nom_hôte_serveur_OMNIbus 4100
   }
   [NCO_PA]
   {
           Primary: nom_hôte_serveur_OMNIbus 4200
   }
   ```

   Où :

   - *nom_hôte_serveur_OMNIbus* est le nom d'hôte du serveur Tivoli Netcool/OMNIbus.

   Changez le nom d'hôte du serveur Tivoli Netcool/OMNIbus sur chacune de ces lignes.
4. Exécutez l'utilitaire `NCHOME/bin/nco_igen` pour appliquer les modifications.
5. Répétez les étapes précédentes sur chaque hôte se connectant au serveur Tivoli Netcool/OMNIbus ; par exemple, effectuez ces modifications pour les sondes, les passerelles et les serveurs d'objets connectés.

Mise à jour de Network Manager IP Edition avec une nouvelle adresse IP et un nouveau nom d'hôte Tivoli Netcool/OMNIbus

Si vous mettez à jour l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez configurer Network Manager IP Edition de sorte qu'il utilise la nouvelle adresse IP et le nouveau nom d'hôte.

Effectuez les opérations suivantes pour mettre à jour Network Manager IP Edition et qu'il prenne connaissance des modifications apportées au nom d'hôte du serveur Tivoli Netcool/OMNIbus :

1. Mettez à jour les composants de base de Network Manager IP Edition en éditant le fichier de configuration `NCHOME/etc/precision/itnm.cfg`.
2. Changez le paramètre suivant : `nco`. Mettez-le à jour avec le nouveau nom d'hôte du serveur Tivoli Netcool/OMNIbus, par exemple `nco=omnihost`.
3. Sauvegardez le fichier `itnm.cfg`.
4. Mettez à jour les composants de l'interface graphique de Network Manager IP Edition en éditant le fichier `rép_base_webgui/etc/datasources`, où `rép_base_webgui` est le répertoire d'installation de l'interface graphique Web, par exemple `$NCHOME/omnibus_webgui`.
5. Mettez à jour les applications Web de Network Manager IP Edition afin de les configurer de sorte qu'elles utilisent le nom d'hôte modifié du serveur Tivoli Netcool/OMNIbus :
   a. Modifiez le fichier suivant :

      ```
      NCHOME/omnibus_webgui/etc/datasources/ncwDataSourceDefinitions.xml
      ```

   b. Changez les valeurs d'hôte et de port dans les sections suivantes pour qu'elles correspondent à la configuration mise à jour :
      - `<ncwPrimaryServer>`
      - `<ncwBackUpServer>`

      Remarque : Ne changez cette section que si un serveur d'objets Tivoli Netcool/OMNIbus de secours est configuré.
   c. Sauvegardez le fichier `ncwDataSourceDefinitions.xml` modifié.
   d. Redémarrez le serveur Tivoli Integrated Portal pour appliquer les modifications.

Mise à jour de Tivoli Integrated Portal avec une nouvelle adresse IP et un nouveau nom d'hôte Tivoli Netcool/OMNIbus

Si le serveur Tivoli Integrated Portal a été initialement configuré en vue de l'utilisation du serveur d'objets Tivoli Netcool/OMNIbus comme référentiel utilisateur principal et que vous mettez à jour l'adresse IP et le nom d'hôte du serveur Tivoli Netcool/OMNIbus, vous devez configurer Tivoli Integrated Portal de sorte qu'il utilise la nouvelle adresse IP et le nouveau nom d'hôte.

Effectuez les opérations suivantes pour configurer Tivoli Integrated Portal en vue de l'utilisation du nouveau nom d'hôte du serveur Tivoli Netcool/OMNIbus :

1. Modifiez le fichier suivant :

   ```
   TIPHOME/profiles/TIPProfile/config/cells/TIPCell/wim/config/
   wimconfig.xml
   ```

2. Changez les propriétés `host1` et `port1` pour qu'elles correspondent à votre configuration mise à jour dans le fichier suivant :

   ```
   config:repositories adapterClassName=
   "com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter"
   ```

3. Sauvegardez le fichier `wimconfig.xml` modifié.
4. Redémarrez le serveur Tivoli Integrated Portal pour appliquer les modifications.

Changement de l'adresse IP et du nom d'hôte sur le serveur Tivoli Integrated Portal

Si vous voulez changer l'adresse IP et le nom d'hôte de Tivoli Integrated Portal, vous devez configurer Tivoli Integrated Portal.

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Tivoli Integrated Portal :

1. Placez-vous dans le répertoire suivant : `TIPHOME/profiles/TIPProfile/bin/`.
2. Utilisez la commande `wsadmin` pour changer l'adresse IP et le nom d'hôte du serveur Tivoli Integrated Portal :

   ```
   wsadmin.sh -user tipadmin -password mot de passe
   -c "\$AdminTask changeHostName -hostName new_hostname -nodeName new_node"
   -c "\$AdminConfig save"
   ```

   La sortie est similaire à l'exemple suivant :

   ```
   WASX7209I: Connected to process "server1" on node TIPNode
    using SOAP connector;The type of process is: UnManagedProcess
   WASX7029I: For help, enter: "$Help help"
   wsadmin>
   ```

   Notez la valeur du nom de noeud Tivoli Integrated Portal. Dans l'exemple précédent, il s'agit de `TIPNode`.
3. Depuis l'invite de commande `wsadmin>`, exécutez la commande suivante :

   ```
   $AdminTask changeHostName { -nodeName TIP_node_name
   -hostName TIP_server_hostname};
   ```

   Où :

   - *TIP_node_name* est le nom de noeud Tivoli Integrated Portal.`TIPNode` dans l'exemple précédent dans cette procédure.
   - *TIP_server_hostname* est le nouveau nom d'hôte du serveur Tivoli Integrated Portal.

     Exemple :

     ```
     wsadmin>$AdminTask changeHostName { -nodeName TIPNode
     -hostName myhost };
     ```
4. Depuis l'invite de commande `wsadmin>`, exécutez les commandes suivantes pour enregistrer le fichier, puis quitter.

   ```
   wsadmin>$AdminConfig save
   wsadmin>exit
   ```
5. Redémarrez le serveur Tivoli Integrated Portal.

Mise à jour de Network Manager pour un nom d'hôte modifié du serveur Tivoli Integrated Portal

Si vous changez le nom d'hôte du serveur Tivoli Integrated Portal, vous devez configurer Network Manager IP Edition en vue de l'utilisation du nouveau nom d'hôte.

Pour configurer Network Manager IP Edition en vue de l'utilisation du nouveau nom d'hôte, procédez comme suit :

1. Mettez à jour les composants centraux de Network Manager IP Edition en éditant le fichier de configuration : `NCHOME/etc/itnm.cfg`.
2. Changez le paramètre suivant :

   ```
   tip
   ```

   Mettez-le à jour avec le nouveau nom d'hôte du serveur Tivoli Integrated Portal, par exemple

   ```
   tip=tiphost
   ```
3. Sauvegardez le fichier `itnm.cfg`.

Changement de l'adresse IP et du nom d'hôte sur le serveur du moteur de déploiement

Si vous avez changé l'adresse IP et le nom d'hôte sur les serveurs où sont installés les composants de Network Manager IP Edition, vous devez définir l'adresse IP et le nom d'hôte du moteur de déploiement IBM.

Pour changer l'adresse IP et le nom d'hôte d'IBM Autonomic Deployment Engine (DE), procédez comme suit :

1. Placez-vous dans le répertoire `$DE_HOME/bin/`, où `DE_HOME` est :
   - `/usr/ibm/common/acsi/` dans le cas d'une installation root,
   - `$HOME/.acsi_$LOGNAME/` dans le cas d'une installation non root.
2. Utilisez la commande `de_chghostname` pour changer le nom d'hôte du serveur du moteur de déploiement :

   ```
   ./de_chghostname.sh -name nom_hôte_serveur_moteur_déploiement
   ```

   Où *nom_hôte_serveur_moteur_déploiement* est le nouveau nom d'hôte du serveur du moteur de déploiement.

Changement de l'adresse IP de Tivoli Common Reporting

Si vous voulez changer l'adresse IP et le nom d'hôte du serveur Tivoli Common Reporting, vous devez effectuer certaines tâches de configuration.

Effectuez les opérations suivantes pour changer l'adresse IP et le nom d'hôte sur le serveur Tivoli Common Reporting :

1. Sur le serveur sur lequel Tivoli Common Reporting est installé, exportez la configuration Tivoli Common Reporting avec la commande suivante :

   ```
   $TCR_HOME/cognos/bin/tcr_cogconfig -e cogstartup.xml.exported
   ```
2. Mettez à jour le fichier `cogstartup.xml.exported` en remplaçant toutes les instances de l'ancien nom d'hôte par le nouveau nom d'hôte.
3. Remplacez le fichier `$TCR_HOME/cognos/configuration/cogstartup.xml` original par le fichier `cogstartup.xml.exported`.

4. Mettez à jour le fichier $TCR_HOME/cognos/configuration/cogconfig.prefs en remplaçant toutes les instances de l'ancien nom d'hôte par le nouveau nom d'hôte.
5. Mettez à jour la chaîne de connexion en vous plaçant d'abord dans le répertoire /opt/IBM/tivoli/tipv2Components/TCRComponent/bin/, puis en émettant la commande suivante :

   ```
   ./trcmd.sh -user utilisateur -password mot_de_passe -datasource
   -add servletInventory -connectionName servletInventory
   -dbType type_base_de_données -connectionString chaîne_connexion -force
   ```

   Où :

   - *utilisateur* est le nom d'utilisateur de la base de données.
   - *mot_de_passe* est le mot de passe de l'utilisateur de la base de données.
   - *type_base_de_données* est le type de base de données.
   - *chaîne_connexion* est la chaîne de connexion à utiliser, comprenant le nouveau nom d'hôte.

   Exemple :

   ```
   ./trcmd.sh -user tipadmin -password passw0rd -datasource
   -add servletInventory -connectionName servletInventory -dbType XML
   -connectionString "http://abc.xyz.com:16310/tarf/servlet/inventory#'?search=%2f
   %2f%2a'
   + '&CAMpassport=' + CAMPassport() #" -force
   ```

6. Redémarrez le serveur Tivoli Integrated Portal et le serveur Tivoli Common Reporting.

Configuration de Network Manager IP Edition pour une adresse IP modifiée du serveur NCIM DB2

Si vous changez l'adresse IP ou le nom d'hôte du serveur qui héberge la base de données topologiques NCIM, vous devez configurer Network Manager IP Edition pour utiliser la nouvelle adresse.

1. Sur le serveur sur lequel Network Manager IP Edition est installé, éditez le fichier suivant :

   ```
   NCHOME/etc/precision/DbLogins.DOMAIN.cfg
   ```

2. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.
3. Modifiez le fichier suivant :

   ```
   NCHOME/etc/precision/MibDbLogin.cfg
   ```

4. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.
5. Sur le serveur sur lequel les applications Web de Network Manager IP Edition sont installées, éditez le fichier suivant :

   ```
   NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties
   ```

6. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.
7. Modifiez le fichier suivant :

   ```
   NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties
   ```

8. Changez les paramètres de nom d'hôte dans ce fichier et sauvegardez le fichier.

Configuration des variables d'environnement

Avant de démarrer un composant ou de travailler avec un fichier de configuration, définissez les variables d'environnement de Network Manager en effectuant le sourçage du script de ces variables.

Le script d'environnement définit les variables d'environnement requises suivantes. Le cas échéant, les autres variables d'environnement sont définies automatiquement par les composants Network Manager.

NCHOME
L'emplacement d'origine Netcool qui correspond par défaut au répertoire `netcool` situé sous le répertoire d'installation :

- UNIX `/opt/IBM/tivoli/netcool`
- Windows `C:\IBM\tivoli\netcool`

ITNMHOME et PRECISION_HOME
L'emplacement d'origine Network Manager qui correspond par défaut au répertoire `NCHOME/precision` situé sous le répertoire d'installation :

- UNIX `/opt/IBM/tivoli/netcool/precision`
- Windows `C:\IBM\tivoli\netcool\precision`

Remarque : Le script définit également PRECISION_HOME. Par défaut, PRECISION_HOME est défini au même emplacement que ITNMHOME, mais il est utilisé par d'autres éléments du produit.

TIPHOME
L'emplacement d'origine Tivoli Integrated Portal qui correspond par défaut au répertoire `tip` situé sous le répertoire d'installation :

- UNIX `/opt/IBM/tivoli/tipv2`
- Windows `C:\IBM\tivoli\tipv2`

Pour définir les variables d'environnement, sourcez le script adapté à votre système d'exploitation.

- UNIX Exécutez le script *répertoire_installation*`/netcool/env.sh`. Sur les shells Bash et Korn, sourcez le script env.sh à l'aide d'une commande similaire à la commande suivante :
  `./opt/IBM/tivoli/netcool/env.sh`
- Windows Exécutez le fichier de commandes *Installation directory*`\netcool\env.bat`.

Après avoir défini les variables d'environnement, démarrez Network Manager et assurez-vous qu'il fonctionne correctement.

Structure de répertoire par défaut

Utilisez ces informations pour comprendre la structure de répertoire de Network Manager.

Structure de répertoire de niveau supérieur

Au sein du répertoire dans lequel Network Manager est installé, les sous-répertoires suivants sont créés : `netcool`, `tipv2` et `tipv2Components`.

- Le répertoire `netcool` contient les fichiers de configuration de Network Manager.
- Le répertoire `tipv2` contient les personnalisations de WebSphere Application Server et de Tivoli Integrated Portal. Le répertoire `tipv2` est le répertoire par défaut suggéré par le programme d'installation de Tivoli Integrated Portal et peut être défini indépendamment du répertoire d'installation de Network Manager. Si vous installez Network Manager dans une installation existante de Tivoli Integrated Portal, les fichiers Tivoli Integrated Portal sont installés dans le répertoire Tivoli Integrated Portal existant.
- Le répertoire `tipv2Components` contient les fichiers du serveur Enterprise Storage Server (ESS), des extensions BIRT (Business Intelligence and Reporting Tools) et de Tivoli Common Reporting.

Pour des informations sur les répertoires d'installation pour Tivoli Netcool/OMNIbus et l'interface graphique Web Tivoli Netcool/OMNIbus, voir le manuel *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.

Répertoires utilisés par le programme d'installation

Le programme d'installation installe les fichiers dans NCHOME, TIPHOME et d'autres répertoires, en fonction du système d'exploitation installé et de l'utilisateur procédant à l'installation. Le tableau suivant répertorie les répertoires supplémentaires utilisés par le programme d'installation.

Tableau 28. Répertoires utilisés par le programme d'installation

Installation	Répertoires utilisés pour les fichiers d'installation
UNIX Systèmes d'exploitation UNIX, utilisateur root	`/usr/ibm/common/acsi`
	`/var/ibm/common/acsi`
UNIX Systèmes d'exploitation UNIX, utilisateur non-root	`~/.acsi_$HOSTNAME`
	`~/tivoli`
	`~/.cit` (i.e. le répertoire de base de l'utilisateur)
Windows Windows 64 bit	`C:\Program Files (x86)\IBM\Common\acsi`
Windows Windows 32 bit	`C:\Program Files\IBM\Common\acsi`

Contenu du répertoire netcool

Le tableau suivant décrit le contenu du répertoire netcool. Tous les chemins indiqués sont relatifs à `NCHOME`. Dans ce tableau, *arch* indique un répertoire du système d'exploitation. Le nom de ce répertoire varie en fonction du système d'exploitation sur lequel le logiciel est installé :

- Solaris – `solaris2`
- Linux – `linux2x86`
- AIX – `aix5`
- Windows – `win32`
- zLinux - `linux2s390`

Si vous avez installé d'autres produits IBM Tivoli, comme IBM Tivoli Business Service Manager, sur le même serveur que Network Manager, des dossiers et des fichiers supplémentaires peuvent être présents. Voir la documentation pour tout autre produit que vous avez installé pour plus d'informations sur leurs répertoires et fichiers.

Tableau 29. Répertoires de `NCHOME`

Répertoire	**Description**
`bin`	Contient des scripts encapsuleurs qui définissent l'environnement et exécutent les fichiers binaires pour le produit ou les composants fournis avec Network Manager.
`etc`	Contient des fichiers de configuration pour les produits ou les composants fournis avec Network Manager.
`etc/precision`	Fichiers de configuration de l'ensemble des composants de Network Manager.
`ini`	Seulement sur les systèmes d'exploitation Windows. Contient des fichiers spécifiques à IBM Tivoli Netcool/OMNIbus.
`installation`	Contient des fichiers utilisés par le processus d'installation. Vous ne devriez pas avoir à modifier le contenu de ce répertoire.
`licence`	Contient le texte de l'accord de licence du produit en différentes langues.
`environnement local`	Seulement sur les systèmes d'exploitation Windows. Contient des fichiers de recherche pour l'internationalisation des différents composants.
`journal`	Contient des fichiers journaux.
`log/install`	Contient des fichiers journaux pour l'installation.
`log/precision`	Contient des fichiers journaux créés par les processus Network Manager.
`omnibus`	S'il existe, contient des fichiers IBM Tivoli Netcool/OMNIbus.
`omnibus_webgui`	S'il existe, contient des fichiers de l'interface graphique Web Tivoli Netcool/OMNIbus.
`PD/precision`	Content des scripts FFDC.
`platform/`*`arch`*	Contient le kit Java Development Kit (JDK) et l'environnement d'exécution Java (JRE) utilisés par Tivoli Integrated Portal.
`precision`	Contient des fichiers pour Network Manager. Voir plus loin dans cette rubrique.
`probes`	Contient des fichiers pour l'analyse pour IBM Tivoli Netcool/OMNIbus et le processus nco_p_ncpmonitor.
`_uninst`	Contient les fichiers pour la désinstallation.
`var`	Contient des données d'application permanentes.
`var/install`	Contient des fichiers base de données pour le processus d'installation.

Tableau 29. Répertoires de NCHOME (suite)

Répertoire	Description
var/precision	Utilisé par le processus ncp_store pour conserver des informations placées dans la mémoire cache pouvant être utilisées pour restaurer les bases de données si un processus se termine inopinément.

Contenu du répertoire precision

Le tableau suivant décrit le contenu du répertoire NCHOME/precision. Tous les chemins indiqués sont relatifs à NCHOME/precision.

Dans ce tableau, *arch* indique un répertoire du système d'exploitation. Le nom de ce répertoire varie en fonction du système d'exploitation sur lequel le logiciel est installé :

- Solaris – solaris2
- Linux – linux2x86
- AIX – aix5
- Windows – win32
- zLinux - linux2s390

Remarque : NCHOME/precision correspond au chemin d'accès défini par défaut pour PRECISION_HOME et ITNMHOME.

Tableau 30. Répertoires de NCHOME/precision

Répertoire	Description
adapters/ncp_dla	Contient des fichiers pour l'adaptateur de bibliothèque utilisé pour l'intégration avec des produits tels que IBM Tivoli Application Dependency Discovery Manager.
adapters/itnm_systemsDirectorLiC	Contient des fichiers pour l'intégration avec IBM Systems Director.
aoc	Contient les fichiers de classe d'objet active (AOC) utilisés par le système de distribution et de gestion de classe dynamique, CLASS.
bin	Contient des scripts encapsuleurs pour tous les fichiers exécutables. Les fichiers exécutables sont conservés à l'emplacement suivant : platform/*arch*/bin
collectors/perlCollectors	Contient des fichiers pour les intégrations EMS.
contrib	Contient des utilitaires non pris en charge de gestion de Network Manager. Egalement utilisé par la solution Netcool for Asset Management afin de contenir des exemples de rapports SQL*Plus.
cshrc	Seulement sur les systèmes d'exploitation UNIX. Utilisé pour configurer l'environnement de l'interpréteur de commandes C.
disco	Contient des fichiers utilisés par DISCO. Contient les fichiers de définition des agents, les agents de reconnaissance, les outils de recherche, les fichiers des auxiliaires et les programmes stitcher.
eventGateway	Contient les programmes stitcher pour la passerelle d'événements et RCA.

Tableau 30. Répertoires de NCHOME/precision (suite)

Répertoire	Description
integration	Contient les fichiers pour l'intégration de l'interface graphique de composant.
installation	Contient des fichiers utilisés par le processus d'installation.
java_api	Contient l'interface de programme d'application JAVA permettant de développer des applications Java qui s'intègrent aux composants de Network Manager.
environnement local	Seulement sur les systèmes d'exploitation Windows. Contient des fichiers de recherche pour l'internationalisation des différents composants.
mibs	Contient des fichiers MIB (Management Information Base).
PD	Tout fichier principal généré par Network Manager est écrit dans un sous-répertoire du répertoire PD. Les fichiers principaux peuvent faciliter le diagnostic de la cause d'un incident.
perl	Contient les fichiers perl utilisés dans Network Manager.
platform/*arch*	Contient les sous-répertoires spécifiques au système d'exploitation sur lequel vous avez installé Network Manager.
platform/*arch*/bin	Contient des fichiers exécutables pour les composants de Network Manager. Les fichiers sont ajoutés à votre environnement PATH. Les scripts encapsuleurs correspondant à ces fichiers exécutables se trouvent dans le répertoire NCHOME/precision/bin.
platform/*arch*/jre	Contient l'environnement d'exécution JAVA utilisé par Network Manager.
platform/*arch*/lib	Contient les bibliothèques d'objets utilisées par tous les composants de Network Manager.
platform/java/lib	Installation de l'interface graphique de la configuration de surveillance. Installation de l'outil de configuration des utilisateurs.
products	Contient les fichiers d'interface graphique pour les produits intégrés.
profil	Seulement sur les systèmes d'exploitation UNIX. Utilisé pour configurer l'environnement de l'interpréteur de commandes bash.
profils	Contient les fichiers liés à l'interface graphique. **Remarque :** Tous les fichiers spécifiques à Network Manager qui se trouvaient précédemment dans le répertoire TIPHOME/profiles se trouvent maintenant dans le répertoire ITNMHOME/profiles.
scripts	Contient des scripts fournis avec les produits Network Manager. Il est conseillé de conserver les scripts définis par l'utilisateur dans ce répertoire afin d'en faciliter la gestion.
système	Contient les fichiers pour le fonctionnement du produit.
systemApps	Contient les fichiers pour les applications Web.

Référence associée:

«Exigences relatives au répertoire d'installation», à la page 53
Le répertoire dans lequel vous installez Network Manager doit répondre à certaines exigences.

Configuration de périphériques Juniper PE

L'une des interrogations de périphérique activées par défaut est l'interrogation PING distant Juniper. Pour garantir l'extraction de données par cette interrogation, vous devez configurer chaque périphérique Juniper PE pour fournir l'accès à certaines tables au sein du périphérique.

Les opérations d'interrogation PING distant sur les périphériques Juniper requièrent l'accès aux tables `pingCtlTable` et `jnxPingCtlTable` au sein des périphériques Juniper PE. Pour cela, utilisez le modèle de contrôle d'accès basé sur la vue SNMP (VACM) pour la vue `PrecisionIP`.

Assurez-vous de configurer chaque périphérique Juniper PE pour garantir l'accès à ces tables pour la vue `PrecisionIP` avant d'activer la stratégie d'interrogation PING distant Juniper.

L'exemple suivant montre comment configurer un périphérique Juniper PE pour fournir l'accès pour la vue `PrecisionIP` dans les tables requises pour l'interrogation PING distant.

Configuration de l'accès à l'aide du VACM

Procédez comme suit pour garantir l'accès aux tables `pingCtlTable` et `jnxPingCtlTable` pour la vue `PrecisionIP` sur un périphérique Juniper PE :

1. Exécutez la commande `telnet` pour vous connecter au périphérique PE.
2. Saisissez `configure` pour lancer la ligne de commande d'édition.
3. Saisissez `edit snmp`, puis appuyez sur **Entrée**.
4. Saisissez `edit view PrecisionIP`, puis appuyez sur **Entrée**.
5. Saisissez `set oid 1.3.6.1.2.1.80 include`, puis appuyez sur **Entrée**.
6. Saisissez `set oid 1.3.6.1.4.1.2636.3.7` include, puis appuyez sur **Entrée**.
7. Saisissez `up`, puis appuyez sur **Entrée**.
8. Saisissez `edit community watermelon`, puis appuyez sur **Entrée**, où `watermelon` est le nouveau nom de communauté d'écriture.
9. Saisissez `set view PrecisionIP`, puis appuyez sur **Entrée**.
10. Saisissez `set authorization read-write`, puis appuyez sur **Entrée**.
11. Saisissez `commit`, puis appuyez sur **Entrée**.
12. Saisissez `exit`, puis appuyez sur **Entrée**. De nouvelles entrées sont créées pour la vue `PrecisionIP` dans la table MIB `vacmViewTreeFamilyTable` sur le périphérique PE.

    Pour consulter le récapitulatif de la section insérée, saisissez `show configuration snmp`, puis appuyez sur **Entrée**. L'écran suivant s'affiche :

    ```
    vue PrecisionIP {
    oid 1.3.6.1.2.1.80 include;
    oid 1.3.6.1.4.1.2636.3.7 include;
    }
    community watermelon {
    vue PrecisionIP;
    authorization read-write;
    }
    ```

    Ces paramètres fournissent l'accès aux tables requises pour les opérations d'interrogation PING distant avec le nom de communauté `watermelon`.

Mise à niveau des bibliothèques des clients Oracle

Network Manager utilise les bibliothèques des clients Oracle 10 et Oracle 11. Si vous avez installé Network Manager avec les bibliothèques du client Oracle 10, vous pouvez faire une mise à niveau vers les bibliothèques du client Oracle 11.

Pour faire une mise à niveau des bibliothèques du client Oracle 10 vers le client Oracle 11 :

1. Modifiez le fichier `DbLogins.cfg`, puis modifiez le paramètre `m_Server` en lui attribuant une valeur `Oracle11`. Le fichier `DbLogins.cfg` se trouve à l'emplacement suivant :
   - UNIX UNIX:`$NCHOME/etc/precision/DbLogins.cfg`
   - Windows Windows:`%NCHOME%\etc\precision\DbLogins.cfg`
2. Sous AIX, effectuez uniquement la procédure suivante :
   a. Modifiez le script encapsuleur `$NCHOME/precision/bin/ncp_common`.
   b. Recherchez le bout de code suivant dans ce fichier :

```
si [ "ncp_perl" = "$BINARYNAME" ]; alors
        #
        # ncp_perl peut utiliser uniquement le client Oracle 10
        # sur lequel il a été compilé
        #
        DIRLIST=${PRECISION_HOME}/platform/$1/lib:${ORACLE10_CLIENT}:
${NCHOME}/platform/$1/lib
    autre
        #
        # Pour utiliser les bibliothèques du client Oracle 11,
        # modifiez la ligne ci-dessous
pour utiliser ORACLE11_CLIENT :
        #
        DIRLIST=${PRECISION_HOME}/platform/$1/lib:${ORACLE10_CLIENT}:
${NCHOME}/platform/$1/lib
    fi
```

3. Dans la deuxième ligne commençant par `DIRLIST=`, modifiez la variable `ORACLE10_CLIENT` (mise en gras) en `ORACLE11_CLIENT`.

Configuration de l'espace disque d'Informix sous Windows

Si vous utilisez Network Manager avec Informix sur des systèmes d'exploitation Windows, configurez la gestion de l'espace disque pour Informix après avoir effectué une installation correcte.

Après avoir effectué une installation correcte de Network Manager sur des systèmes d'exploitation Windows, procédez selon ces étapes pour configurer les éléments suivants si vous utilisez Informix :

- Définissez Informix pour qu'il vérifie la quantité d'espace disque libre disponible pour la base de données toutes les 5 minutes et pour qu'il crée de l'espace supplémentaire si l'occupation est supérieure à 90%.
- Définissez le planificateur Informix pour qu'il effectue des statistiques de mise à jour une fois par jour.

1. Fermez la session Windows et réouvrez une session en tant qu'utilisateur Informix.
2. Accédez à **Démarrer** > **Tous les programmes** > **IBM Informix Dynamic Server** > **ITNM**.
3. Entrez la commande suivante : `SET NCHOME=`*`emplacement d'installation de Network Manager`*

4. Entrez la commande suivante : `%ITNMHOME%\install\scripts\ids_post_install_sysadmin.bat`

Soutien des unités d'archivage dans une installation FIPS 140-2

Si vous avez installé une installation FIPS 140-2, vous pouvez tout de même installer des algorithmes non conformes à FIPS 140–2, comme les normes DES et MD5, pour pouvoir accéder à l'équipement d'archivage sur votre réseau.

1. Accédez au répertoire où vous avez extrait le module d'installation Network Manager.
2. Passez au sous-répertoire du package d'installation décompressé : `COI/PackageSteps/Non-FIPS_back_end/FILES`
3. Selon votre système d'exploitation, vérifiez que le fichier suivant est présent :
   - UNIX `Non-FIPS_back_end-arch-v.r.f.m.tar.gz`
   - Windows `Non-FIPS_back_end-arch-v.r.f.m.zip`

   où :
   - *v.r.f.m* est le numéro de version.
   - *arch* est le nom de l'architecture du système d'exploitation sur laquelle le produit est installé, par exemple `solaris2`.
4. Selon votre système d'exploitation, effectuez les étapes suivantes :
   - UNIX Sur des systèmes UNIX, exécutez la commande suivante : `tar -xzvf Non-FIPS_back_end-arch-v.r.f.m.tar.gz -C $NCHOME *libNCP*`
   - Windows Sur des systèmes Windows, décompressez le fichier zip et utilisez l'Explorateur Windows pour copier les bibliothèques de DLL `libNcp*` du dossier `COI\PackageSteps\Non-FIPS_back_end\FILES\precision\platform\win32\bin` vers le dossier `%NCHOME%\precision\platform\win32\bin`

   Le résultat est que vous devez avoir deux bibliothèques partagées à l'emplacement correct, par exemple :
   - UNIX Sur des systèmes UNIX :
     - `$NCHOME/precision/platform/solaris2/lib/libNcpSnmpPrivDES.so`
     - `$NCHOME/precision/platform/solaris2/lib/libNcpSnmpAuthMD5.so`
   - Windows Sur des systèmes Windows :
     - `%NCHOME%\precision\platform\win32\bin\libNcpSnmpPrivDES.so`
     - `%NCHOME%\precision\platform\win32\bin\libNcpSnmpAuthMD5.so`

   Ces bibliothèques permettent au moteur d'interrogation Network Manager, ncp_poller, d'utiliser les algorithmes de chiffrement DES et MD5.
5. Modifiez le fichier de configuration `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`
6. Modifiez la propriété suivante en "false" : `tnm.fips.mode=false` La configuration des algorithmes de chiffrement DES et MD5 pour SNMPv3 peut être effectuée à l'aide de l'interface graphique de configuration de la reconnaissance.

Tâches associées:

«Décompression du fichier d'installation», à la page 61
Si vous avez téléchargé le fichier d'installation, vous devez décompresser le module d'installation avant d'installer le produit.

Configuration de l'authentification du fournisseur de services OQL

Les requêtes sur les bases de données du composant Network Manager peuvent être exécutées à partir de la ligne de commande à l'aide du processus du fournisseur de services OQL, ncp_oql. Vous pouvez configurer ncp_oql pour une authentification sur la base de données NCIM ou sur Tivoli Netcool/OMNIbus ObjectServer. Sinon, vous pouvez configurer ncp_oql pour autoriser l'exécution de requêtes sans authentification.

Le moteur d'authentification du fournisseur de services OQL, ncp_auth, n'est plus utilisé dans la version 3.9. Par défaut, il n'y a pas d'authentification pour les requêtes ncp_oql provenant de la ligne de commande. Vous pouvez configurer le fournisseur de services OQL pour s'authentifier sur la base de données NCIM ou sur ObjectServer, en procédant comme suit :

- *Authentification sur la base de données NCIM* : force le fournisseur de services OQL à s'authentifier à l'aide du nom d'utilisateur et du mot de passe de la base de données NCIM, comme indiqué lors de l'installation et comme configuré dans le fichier de configuration DbLogins.cfg.
- *Authentification sur ObjectServer* : force le fournisseur de services OQL à s'authentifier à l'aide du nom de compte administrateur et du mot de passe de Tivoli Netcool/OMNIbus, comme indiqué lors de l'installation.

L'authentification du fournisseur de services OQL est contrôlée par la valeur de `m_OQLAuthenticationMode` dans la table config.settings. La zone accepte les valeurs suivantes :

- 0 : Aucune authentification. Le nom d'utilisateur et le mot de passe ne sont pas requis. S'ils sont spécifiés sur la ligne de commande, ils sont ignorés.
- 1 : Authentification sur la base de données NCIM.
- 2 : Authentification sur Tivoli Netcool/OMNIbus ObjectServer.

Pour configurer l'authentification du fournisseur de services OQL :

1. Modifiez le fichier de configuration **`ncp_config`**, `$NCHOME/etc/precision/ConfigSchema.cfg`.
2. Configurez l'une des insertions suivantes dans la table config.settings :
   - Configurez l'authentification sur la base de données NCIM.

     ```
     insert into config.settings
     (
             m_OQLAuthenticationMode,
     )
     values
     (
             1,
     );
     ```

   - Configurez l'authentification sur ObjectServer.

     ```
     insert into config.settings
     (
             m_OQLAuthenticationMode,
     )
     values
     (
             2,
     );
     ```

Configuration de l'auxiliaire SNMP

L'auxiliaire SNMP est utilisé par les fonctions de reconnaissance et d'interrogation pour envoyer des demandes SNMP à des périphériques réseau. Vous pouvez configurer la façon dont l'auxiliaire SNMP émet les demandes SNMP ainsi que la façon dont il traite les résultats des demandes SNMP.

Pour des informations sur les endroits où est utilisé l'auxiliaire SNMP dans les fonctions de reconnaissance et d'interrogation, voir les guides suivants :

- Pour la reconnaissance, voir *IBM Tivoli Network Manager IP Edition - Guide de reconnaissance* .
- Pour l'interrogation, voir *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Configuration de la régulation de l'auxiliaire SNMP

Vous pouvez activer la régulation dans l'auxiliaire SNMP. L'activation de la régulation augmente le délai entre les demandes SNMP de Network Manager envoyées à un périphérique réseau. Ainsi, la charge sur le périphérique réseau est moindre. Par défaut, la régulation est désactivée dans l'auxiliaire SNMP.

A propos de la régulation de l'auxiliaire SNMP

La régulation de l'auxiliaire SNMP établit un délai entre les demandes SNMP envoyées par l'auxiliaire SNMP avec une formule utilisant les paramètres GeneralSlowdown, GetNextBoundary et GetNextSlowdown.

Voici comment l'auxiliaire SNMP envoie des demandes sans régulation (par défaut) et avec régulation :

- Si la régulation est désactivée, les opérations GetNext SNMP fonctionnent comme suit : l'auxiliaire SNMP envoie la première demande Get SNMP et une fois que Network Manager obtient une réponse, l'auxiliaire SNMP envoie immédiatement la demande GetNext.
- Lorsque la régulation est activée, un délai est appliqué entre les demandes GetNext. Il s'agit généralement d'un délai défini court ou long. Le système effectue le suivi des demandes GetNext envoyées à un périphérique réseau et une fois que le nombre dépasse une certaine valeur, le délai plus long est appliqué ; sinon, le délai plus court est appliqué. Le système utilise les paramètres `GeneralSlowdown`, `GetNextBoundary` et `GetNextSlowdown` définis dans la table de base de données snmpStack.accessParameters afin de déterminer le délai à appliquer. Pour plus d'informations sur la table de base de données snmpStack.accessParameters, voir *IBM Tivoli Network Manager IP Edition - Guide de reconnaissance* .

Activation de la régulation de l'auxiliaire SNMP

Vous pouvez activer la régulation de l'auxiliaire SNMP.

Pour activer la régulation de l'auxiliaire SNMP, procédez comme suit :

1. Modifiez le fichier de configuration `NCHOME/etc/precision/NcPollerSchema.cfg`.

   Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire `NCHOME/etc/precision/NcPollerSchema.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* correspond au nom du domaine.
2. Ajoutez la ligne suivante à la fin du fichier :

   ```
   update config.properties set EnableThrottling = 1;
   ```

3. Sauvegardez le fichier NCHOME/etc/precision/NcPollerSchema.cfg.
4. Activez les modifications en exécutant l'une des actions suivantes ou les deux :
   - Démarrez ou planifiez un nouvelle reconnaissance complète. Désormais, la reconnaissance utilisera la régulation.
   - Redémarrez le moteur d'interrogation, ncp_poller, avec l'option de ligne de commande -readsnmpconfig spécifiée.

Configuration de la prise en charge de GetBulk pour SNMP v2 et v3

Vous pouvez configurer l'auxiliaire SNMP pour utiliser l'opération GetBulk lorsque SNMP v2 ou v3 est utilisé. L'utilisation de l'opération GetBulk améliore la vitesse de la reconnaissance et l'efficacité de l'interrogation. Par défaut, l'auxiliaire SNMP n'utilise pas GetBulk.

A propos de GetBulk

Les commandes SNMP v2 et SNMP v3 GetBulk permettent de transférer des données de manière plus efficace. L'activation de l'auxiliaire SNMP pour l'utilisation de GetBulk réduit le temps nécessaire aux phases de collecte de données de reconnaissance. L'utilisation de GetBulk augmente également l'efficacité de l'interrogation.

La configuration de l'auxiliaire SNMP pour l'utilisation de GetBulk réduit l'empreinte des ressources de Network Manager des manières suivantes :

- Elle réduit l'impact sur la gestion du réseau car le nombre de paquets SNMP échangés est moins important.
- Elle réduit l'impact sur les unités gérées car le nombre de paquets SNMP traités est moins important.
- Elle réduit le temps UC requis par les processus Network Manager, comme le moteur de reconnaissance, ncp_disco, et le moteur d'interrogation, ncp_poller, en raison des frais généraux réduits.

L'utilisation de GetBulk réduit le temps nécessaire aux phases de collecte de données de reconnaissance ; un pourcentage élevé du temps requis pour la collecte de données étant un temps d'attente consacré au passage des paquets à travers le réseau. Cela réduit considérablement le temps nécessaire à la collecte de données pour les tables de grandes tailles, telles que les tables d'interface et de routage.

Configuration de Network Manager pour utiliser GetBulk

Vous pouvez configurer l'auxiliaire SNMP pour utiliser GetBulk. Vous pouvez également exclure des unités spécifiques de la prise en charge GetBulk.

Si vous configurez l'auxiliaire SNMP pour utiliser GetBulk, cette configuration s'applique à tous les interrogateurs du domaine en cours. L'auxiliaire SNMP utilise également GetBulk pour toutes les unités du domaine accessibles à l'aide de SNMP v2 ou de SNMP v3, sauf si vous excluez des unités spécifiques comme indiqué dans les étapes suivantes.

Remarque : Lorsque GetBulk est activé, une requête GetBulk est toujours envoyée à la place d'une requête GetNext pour chaque unité compatible avec GetBulk.

Pour configurer l'auxiliaire SNMP pour utiliser GetBulk, procédez comme suit.

1. Modifiez le fichier de configuration NCHOME/etc/precision/NcPollerSchema.cfg.

Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire NCHOME/etc/precision/ NcPollerSchema.*NOM_DOMAINE*.cfg, où *NOM_DOMAINE* correspond au nom du domaine.

2. Recherchez l'insertion dans la base de données config.properties et définissez la valeur de la propriété UseGetBulk à 1.
3. Sauvegardez le fichier NCHOME/etc/precision/NcPollerSchema.cfg.
4. Facultatif : Si vous disposez d'unités réseau ne prenant pas en charge GetBulk, vous pouvez alors exclure ces unités une par une en procédant comme suit :
   a. Modifiez le fichier de configuration suivant : NCHOME/etc/precision/ SnmpStackSecurityInfo.cfg.

      Remarque : Vous pouvez rendre le fichier SnmpStackSecurityInfo.cfg spécifique au domaine en le copiant dans NCHOME/etc/precision/ SnmpStackSecurityInfo.*NOM_DOMAINE*.cfg, où *NOM_DOMAINE* est le nom du domaine.
   b. Pour chaque périphérique que vous voulez exclure de la prise en charge GetBulk, ajoutez une insertion dans le fichier de configuration SnmpStackSecurityInfo.cfg, similaire à l'exemple suivant. L'insertion de l'exemple suivant exclut l'unité 10.0.13.74 de la prise en charge GetBulk.

      ```
      insert into snmpStack.accessParameters
          ( m_NetAddress, m_UseGetBulk )
      values
          ( '10.0.13.74', 0 );
      ```
   c. Une fois l'insertion ajoutée pour chaque unité à exclure, enregistrez le fichier NCHOME/etc/precision/ SnmpStackSecurityInfo.cfg.
5. Activez les modifications en exécutant l'une des actions suivantes ou les deux :
   - Démarrez ou planifiez un nouvelle reconnaissance complète. La reconnaissance utilise maintenant GetBulk.
   - Redémarrez le moteur d'interrogation, ncp_poller, avec l'option de ligne de commande -readsnmpconfig spécifiée.

Configuration du nombre maximal de répétitions pour les requêtes GetBulk

La commande GetBulk est utilisée pour récupérer toutes les lignes d'une table à partir d'une ressource du réseau, par exemple pour récupérer toutes les lignes d'une table de routage à partir d'un routeur. Le paramètre max-repetitions indique le nombre de lignes de la table à récupérer en une seule opération GetBulk. Vous pouvez ajuster les paramètres de configuration GetBulk afin de réduire le nombre de paquets échangés dans le cadre de l'opération GetBulk.

L'auxiliaire SNMP détermine la valeur du nombre maximal de répétitions pour les requêtes GetBulk (paramètre max-repetitions) en se basant sur le calcul suivant :

max-repetitions = DefaultGetBulkMaxReps / #varbinds

Où :

- La propriété *DefaultGetBulkMaxReps* est définie dans le fichier $NCHOME/etc/precision/NcPollerSchema.cfg. La valeur par défaut est 20. Cette propriété définit le nombre affecté à la zone max-repetitions dans les requêtes GetBulk émises par les processus Network Manager. La valeur 20 est utilisée lorsque la requête GetBulk contient une valeur varbind unique. Si plusieurs

valeurs varbind sont incluses, la valeur est ajustée en conséquence (divisée par le nombre de varbinds), de sorte que les réponses contiennent toujours un nombre similaire de varbinds.

- *#varbinds* correspond au nombre de liaisons de variable demandées. Dans l'auxiliaire SNMP, cette valeur correspond généralement à 1. Toutefois, celle-ci peut varier en fonction de l'emplacement où celui-ci est déployé et des facteurs suivants :
  - Dans le moteur de reconnaissance, ncp_disco, la valeur *#varbinds* peut varier en fonction du code dans l'agent de reconnaissance.
  - Dans le moteur d'interrogation, ncp_poller, la valeur *#varbinds* peut varier en fonction des objets MIB inclus dans la définition d'interrogation.

1. Modifiez le fichier de configuration suivant : `$NCHOME/etc/precision/NcPollerSchema.cfg`.

   Remarque : Vous pouvez rendre le domaine du fichier NcPollerSchema.cfg spécifique en le copiant dans le répertoire `$NCHOME/etc/precision/NcPollerSchema.`*`NOM_DOMAINE`*`.cfg`, où *NOM_DOMAINE* correspond au nom du domaine.
2. Recherchez la ligne qui définit la valeur de la propriété *DefaultGetBulkMaxReps*.
3. Changez la valeur affectée à la propriété *DefaultGetBulkMaxReps*.
4. Sauvegardez le fichier `$NCHOME/etc/precision/NcPollerSchema.cfg`.
5. Redémarrez le moteur d'interrogation, ncp_poller, pour activer les changements de configuration.

Configuration d'une connexion unique entre le module Représentations Graphiques et Tivoli Monitoring

Les instructions ci-dessous expliquent comment configurer IBM Tivoli Monitoring et le module Représentations Graphiques pour la connexion unique (SSO) en utilisant `ITMWebService`. En bas de cette rubrique figurent également des instructions sur la façon de configurer Tivoli Integrated Portal pour communiquer avec un service Web Tivoli Monitoring distant, qui fonctionne seulement dans un environnnement de connexion unique.

- Installez Tivoli Monitoring 6.2.2. Vous devez configurer le serveur Tivoli Enterprise Portal de Tivoli Monitoring pour utiliser LDAP et la connexion unique pendant l'étape de configuration. Reportez-vous à la documentation Tivoli Monitoring, mais, essentiellement, vous devez exécuter ce qui suit :
  - Pendant la configuration du serveur Tivoli Enterprise Portal, cochez les cases LDAP et SSO (connexion unique). Entrez les informations pour la connexion à LDAP.
  - Lorsque la configuration de la connexion unique est affichée, entrez `TIPRealm` pour le nom de "realm" (portée) et votre domaine réseau pour le nom de domaine (par exemple, `raleigh.ibm.com`).
  - Exportez les clés LTPA sur le disque. Pour plus d'informations, voir : http://www-01.ibm.com/support/knowledgecenter/SS7JFU_7.0.0/com.ibm.websphere.express.doc/info/exp/ae/tsec_altpaexp.html?cp=SS7JFU_7.0.0%2F1-3-0-0-2-1.
  - Prenez note du mot de passe.
  - Copiez le fichier `\ibm\itm\cnps\sqllib\kfwtipewas.properties` dans le répertoire `\ibm\itm\cnps` et exécutez `reconfigure` pour serveur Tivoli Enterprise Portal. Lorsque `reconfigure` est terminé, la fonction de service web est activée.

- Installez et configurez Tivoli Integrated Portal pour y inclure le composant de représentation graphique.

Pour configurer la connexion unique pour le composant de représentation graphique et Tivoli Monitoring :

1. Configurez la sécurité LDAP (Lightweight Directory Access Protocol) (LDAP) dans Tivoli Integrated Portal :
   a. Ajoutez et configurez un référentiel LDAP.
   b. Configurez Tivoli Integrated Portal pour vous permettre de gérer les utilisateurs LDAP dans le portail.
2. Configurez Tivoli Integrated Portal pour la connexion unique. Vérifiez que Tivoli Monitoring et le serveur d'applications intégré pour Tivoli Integrated Portal utilisent les mêmes clés LTPA (importez les clés LTPA exportées de Tivoli Monitoring), les noms de domaine (Realm), et échangez les certificats SSL. Pour plus d'informations, voir : http://www-01.ibm.com/support/knowledgecenter/SS7JFU_7.0.0/com.ibm.websphere.express.doc/info/exp/ae/tsec_altpaimp.html?cp=SS7JFU_7.0.0%2F1-3-0-0-2-2
3. Sur Tivoli Integrated Portal Server, accédez au répertoire *rép_base_tip*/profiles/TIPProfile/bin et exécutez la commande suivante pour configurer Tivoli Integrated Portal pour qu'il utilise une connexion unique pour la communication avec Tivoli Monitoring :

   Windows `tipcli.bat ITMLogin -hostname <nom_hôte_TEPS> -port 1920`

   Linux UNIX `tipcli.sh ITMLogin -hostname <nom_hôte_TEPS> -port 1920`
4. Arrêtez et redémarrez Tivoli Integrated Portal Server :
   a. Dans le répertoire *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'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 *rép_base_tip*/profiles/TIPProfile/bin, en fonction de votre système d'exploitation, entrez l'une des commandes suivantes :
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`
5. Créez les utilisateurs dans Tivoli Integrated Portal et affectez-leur un rôle doté des privilèges de consultation pour les graphiques de Tivoli Monitoring, tel que `chartAdministrator`.
6. Associez les utilisateurs que vous avez créés à un utilisateur Tivoli Enterprise Portal.
   a. Connectez vous à Tivoli Enterprise Portal et associez le même utilisateur de LDAP avec un utilisateur Tivoli Enterprise Portal.
   b. Dans Tivoli Enterprise Portal, sélectionnez **Edit --> Manage Users (Editer - Gérer les utilisateurs)**.
   c. Cliquez sur le bouton pour créer un nouvel utilisateur et entrez l'identifiant d'utilisateur et le nom d'utilisateur. Pour être cohérent, vous pouvez utiliser le même ID d'utilisateur que dans Tivoli Integrated Portal.

d. Entrez le nom distinctif. Vous pouvez l'obtenir à partir de Tivoli Integrated Portal sur le panneau Manage Users (Gérer les utilisateurs). Vous pouvez également le trouver en utilisant le bouton **Rechercher** dans Tivoli Enterprise Portal. Si vous ne le localisez pas avec le bouton **Rechercher**, copiez-le et collez-le à partir du panneau Manage Users (Gérer les utilisateurs) de Tivoli Integrated Portal. Il devrait se présenter comme ceci : `uid=IDutilisateur,o=IBM,c=US`

e. Attribuez à l'utilisateur le droit `Workspace Administration Mode` (Mode Administration Espace de travail).

Remarque : Lorsque vous vous connectez à Tivoli Integrated Portal, vous ne pouvez pas utiliser `sysadmin` qui est l'utilisateur Tivoli Monitoring par défaut ou `tipadmin` qui est l'utilisateur Tivoli Integrated Portal par défaut parce qu'aucun de ces utilisateurs n'est enregistré sous LDAP.

7. Lorsque vous avez terminé, exécutez ces étapes pour tester la configuration :
   a. Connectez vous à Tivoli Integrated Portal sous l'identité de l'un des utilisateurs avec accès graphique que vous avez créés.
   b. Créez une nouvelle page en utilisant **Paramètres** > **Gestion de page** > **Nouvelle Page**.
   c. Sélectionnez le portlet de représentations graphiques et cliquez sur **OK**.
   d. Donnez un nom à la page et enregistrez-la.
   e. Allez au portlet de représentations graphiques et sélectionnez **Graphiques Tivoli**.
   f. Dans la barre d'outils du tableau, cliquez sur **Nouveau** pour créer une nouvelle connexion et fournir les informations nécessaires pour la connexion au service web distant Tivoli Monitoring et cliquez sur **OK**. Par exemple :
      - Nom : `ITM`
      - Protocole : `http`. Cette valeur pourra ensuite être changée en `https` si nécessaire mais pour le test `http` est suffisant.
      - Nom d'hôte : *`nom_serveur_TEPS`*`.raleigh.ibm.com`. Il s'agit du nom d'hôte du serveur Tivoli Enterprise Portal, par exemple `tiv-isc09.ibm.com`.
      - Port : `15200`. Si vous utilisez `https`, le port par défaut est `15201`.
      - Nom du service : `TIPWebServiceHttpRouter`.
   g. Sélectionnez l'un de ces groupes. Il va remplir le tableau avec les graphiques et les tableaux de cet espace de travail Tivoli Monitoring.
   h. Sélectionnez un graphique et cliquez sur **Terminer**.

      Le graphique est importé, ce qui peut prendre un certain temps. Lorsque le traitement est terminé, le graphique est restitué sur le portlet. Si vous ne le voyez pas, examinez tout message d'erreur et vérifiez que vous avez exécuté ces étapes correctement.

Tâches associées:

«Configuration de la connexion unique (SSO)», à la page 228
Suivez les instructions ci-après pour la prise en charge de la connexion unique et pour la configuration d'un référentiel fédéré.

«Ajout d'un référentiel LDAP externe», à la page 221
Après l'installation, vous pouvez ajouter un serveur IBM Tivoli Directory Server ou un serveur Microsoft Active Directory Server comme référentiel LDAP pour Network Manager.

«Configuration d'un référentiel LDAP externe», à la page 223
Vous pouvez configurer le Tivoli Integrated Portal Server pour communiquer avec un référentiel LDAP externe.

«Gestion des utilisateurs LDAP sur la console», à la page 224
Pour créer ou gérer sur la portail des utilisateurs qui sont définis dans votre référentiel LDAP, dans la console d'administration WebSphere Application Server, spécifiez les types d'entités pris en charge.

IBM Support Assistant (ISA)

IBM Support Assistant est un outil vous permettant de rechercher des informations de support et de formation sur les produits.

Si vous avez besoin d'ouvrir un PMR (Problem Management Record), IBM Support Assistant peut vous faire gagner du temps en récupérant automatiquement les informations de support. IBM Support Assistant fournit les services suivants :

- Accès amélioré aux informations de support IBM, aux forums IBM et aux autres ressources via une interface de recherche fédérée (une seule recherche sur plusieurs ressources)
- Accès simple aux supports de formation IBM et aux calendriers de formation sur les produits.
- Accès simple aux pages d'accueil des produits, aux pages de support produit et aux forums sur les produits IBM via des liens appropriés.
- Temps de résolution des PMR amélioré via la collecte d'informations systèmes clés et l'envoi des données à IBM via la création électronique d'un PMR.

Un plugin Network Manager est disponible pour IBM Support Assistant. Ce plugin est nécessaire pour qu'IBM Support Assistant puisse diagnostiquer les problèmes de Network Manager.

Pour plus d'informations sur IBM Support Assistant, reportez-vous au site Web IBM suivant : http://www.ibm.com/software/support/isa

Installation du collecteur IBM Support Assistant Lite

Le collecteur IBM Support Assistant (ISA) Lite pour Network Manager fournit une collecte des données automatisée sur des systèmes où Network Manager est installé. Il peut collecter les informations sur les journaux, les fichiers de règles, les données de configuration, etc.

Pour installer le collecteur ISA Lite, procédez selon les étapes suivantes :

1. Installez Network Manager.
2. Ouvrez la note technique http://www-01.ibm.com/support/docview.wss?uid=swg27015867.
3. Suivez les étapes de la note technique pour configurer et utiliser le collecteur ISA Lite pour Network Manager.

Annexe. Glossaire de Network Manager

Ces informations permettent de comprendre la terminologie du produit Network Manager.

La liste suivante fournit des explications sur la terminologie Network Manager.

affichage de la santé du réseau
Vue d'interface graphique composite comportant un portlet Vues de réseau au-dessus et un portlet **Liste des événements actifs** en dessous. Utilisez la vue de la santé du réseau pour afficher des événements d'un périphérique réseau.

agent Voir agent de reconnaissance.

agent de reconnaissance
Partie de code qui s'exécute lors d'une reconnaissance et extrait des informations détaillées à partir de périphériques reconnus.

analyse de Tivoli Netcool/OMNIbus (nco_p_ncpmonitor)
Acquiert et traite les événements générés par les processus et les interrogations Network Manager, et transmet ces événements au serveur ObjectServer.

analyse origine du problème (RCA)
Processus de détermination de la cause première d'une ou de plusieurs alertes de périphérique.

base de données NCIM
Base de données relationnelle qui stocke des données de topologie ainsi que des données administratives, telles que des données associées aux règles et définitions d'interrogation, et des données de performance des périphériques.

base de données OQL
Les processus Network Manager stockent les informations de configuration, de gestion et de fonctionnement dans des bases de données OQL.

classe d'objet actif (AOC)
Elément de la topologie hiérarchique prédéfinie des périphériques réseau utilisé par le gestionnaire de la classe d'objet active, `ncp_class`, pour classer les périphériques réseau découverts suite à une reconnaissance.

courtier de messages
Composant qui gère la communication entre les processus Network Manager. Le courtier utilisé par Network Manager s'appelle Really Small Message Broker. Pour garantir le bon fonctionnement de Network Manager, Really Small Message Broker doit fonctionner en continu.

définition d'interrogation
Définit comment interroger une interface ou un périphérique réseau et filtrer de manière plus détaillée les interfaces ou les périphériques cible.

domaine
Voir domaine réseau.

domaine réseau
Collection d'entités réseau à reconnaître et gérer. Une seule installation Network Manager peut gérer plusieurs domaines réseau.

données de performances
Données de performances pouvant être regroupées dans des rapports. Les rapports de performance vous permettent d'afficher l'historique des données de performances collectées par le système de surveillance à des fins de diagnostic.

emplacement de départ de reconnaissance
Un ou plusieurs périphériques à partir desquels démarrer la reconnaissance.

enrichissement d'événement
Processus d'ajout d'informations de topologie à l'événement.

entité Concept de base de données topologiques. Tous les périphériques et les composants de périphérique reconnus par Network Manager sont des entités. De plus, les collectes de périphériques, tels des réseaux VPN et des réseaux locaux virtuels, ainsi que les éléments de topologie qui forment une connexion complexe, sont des entités.

fichiers AOC
Fichiers utilisés par le gestionnaire de la classe d'objet active, `ncp_class`, pour classer les périphériques réseau suite à une reconnaissance. Cette classification est définie dans les fichiers AOC à l'aide d'un ensemble de filtres sur l'ID objet et d'autres paramètres relatifs aux MIB de périphérique.

fichiers de configuration
Chaque processus Network Manager a un ou plusieurs fichiers de configuration permettant de contrôler le comportement de processus en définissant des valeurs dans les bases de données de processus. Les fichiers de configuration peuvent également être spécifiques à un domaine.

gestionnaire de topologie (ncp_model)
Stocke les données de topologie suite à une reconnaissance et les envoie vers la base de données topologiques NCIM où elles peuvent être interrogées via SQL.

graphique MIB SNMP
Interface permettant d'afficher un graphique en temps réel des variables MIB pour un périphérique, puis de l'utiliser pour l'analyse et la résolution des problèmes liés au réseau.

hiérarchie de classe
Topologie hiérarchique prédéfinie des périphériques réseau utilisée par le gestionnaire de la classe d'objet active, `ncp_class`, pour classer les périphériques réseau découverts suite à une reconnaissance.

interface graphique Configuration de la reconnaissance
Interface graphique permettant de configurer les paramètres de reconnaissance.

interface graphique de l'interrogation réseau
Interface graphique de l'administrateur. Active la définition des règles d'interrogation et des définitions d'interrogation.

interface graphique Etat de la reconnaissance
Interface graphique permettant de lancer et de surveiller une reconnaissance en cours d'exécution.

langage OQL
Version du langage SQL (Structured Query Language) conçue pour Network Manager. Les processus Network Manager créent leurs bases de données et interagissent via le langage OQL.

moteur de reconnaissance (ncp_disco)
Processus Network Manager qui effectue la reconnaissance de réseau.

moteur d'interrogation (ncp_poller)
Processus Network Manager qui interroge les interfaces et les périphériques cible. Le moteur d'interrogation collecte également des données de performances à partir des périphériques interrogés.

navigateur de structure
Interface graphique permettant d'analyser la santé des composants de périphérique pour isoler les incidents au sein d'un périphérique réseau.

navigateur MIB SNM
Interface graphique qui permet de récupérer des informations sur la variable MIB provenant des périphériques réseau, afin de prendre en charge le diagnostic des problèmes liés au réseau.

ncp_disco
Voir moteur de reconnaissance.

ncp_g_event
Voir passerelle d'événements.

ncp_model
Voir gestionnaire de topologie.

ncp_poller
Voir moteur d'interrogation.

outils Web
Outils d'extraction de données spécialisés permettant de récupérer des données à partir des périphériques réseau et pouvant être lancés à partir de l'interface graphique de visualisation de réseau Vues de réseau ou Vue tronçon de réseau, ou via une URL dans un site Web.

passerelle d'événements (ncp_g_event)
Processus Network Manager qui effectue l'enrichissement d'événement.

phase de reconnaissance
Une reconnaissance de réseau est divisée en quatre phases : interrogation de périphériques, résolution d'adresses, téléchargement de connexions et corrélation de connectivité.

Plug-in de reprise en ligne
Reçoit des événements de vérification d'intégrité Network Manager de la passerelle d'événements et les transfère au processus de domaine virtuel qui décide en fonction de l'événement, si une reprise en ligne doit être lancée.

plug-in RCA
En fonction des données de l'événement et de la topologie reconnue, ce plug-in tente d'identifier des événements causés par ou entraînant d'autres événements à l'aide des règles codées dans des programmes stitcher RCA.

portée de la reconnaissance
Limites d'une reconnaissance, exprimées à l'aide d'un ou de plusieurs sous-réseaux ou masques réseau.

programmes stitcher de passerelle d'événements
Programme stitcher qui effectue une recherche de topologie lors du processus d'enrichissement d'événement.

programme stitcher
Code utilisé dans les processus suivants : reconnaissance, enrichissement d'événements et analyse de la cause première. Voir aussi programme stitcher de reconnaissance, programme stitcher de passerelle d'événements et programme stitcher RCA.

programme stitcher de reconnaissance
Partie de code qui s'exécute lors du processus de reconnaissance. Il existe plusieurs programmes stitcher de reconnaissance, qui peuvent être regroupés en deux grandes catégories : les programmes stitcher de collecte de données qui transfèrent des données entre les bases de données lors des phases de collecte de données d'une reconnaissance, et les programmes stitcher de traitement des données qui génèrent la topologie réseau lors de la phase de traitement des données.

programme stitcher RCA
Programmes stitcher qui traitent un événement déclencheur lorsqu'il est transféré via le plug-in RCA.

reconnaissance complète
Reconnaissance s'exécutant sur une grande portée destinée à découvrir tous les périphériques réseau que vous souhaitez gérer. Les reconnaissances complètes sont généralement appelées reconnaissances, excepté si elles sont opposées à des reconnaissances partielles. Voir aussi reconnaissance partielle.

reconnaissance partielle
Nouvelle reconnaissance ultérieure d'une section du réseau reconnu précédemment. La section du réseau est généralement définie à l'aide d'une portée de reconnaissance constituée d'une plage d'adresses, d'un périphérique unique ou d'un groupe de périphériques. Une reconnaissance partielle repose sur les résultats de la dernière reconnaissance complète et peut uniquement être exécutée si le moteur de reconnaissance, `ncp_disco`, n'a pas été arrêté depuis la dernière reconnaissance complète. Voir aussi reconnaissance complète.

règle d'interrogation
Définit les périphériques à interroger. Définit également d'autres attributs d'une interrogation, tels la fréquence d'interrogation.

reprise en ligne
Dans votre environnement Network Manager, une architecture de reprise en ligne peut être utilisée pour configurer votre système pour une haute disponibilité, en minimisant l'impact d'un incident matériel ou réseau.

vue de recherche d'erreur
Vue d'interface graphique composite comprenant un portlet **Liste des événements actifs** au-dessus et un portlet Vue tronçon de réseau en dessous. Utilisez la vue permettant de rechercher les problèmes afin de surveiller les événements de réseau.

vues de chemin
Interface graphique de visualisation du réseau qui affiche des périphériques et des liens qui constituent un chemin réseau entre deux

périphériques sélectionnés. Créez des vues de chemin ou modifiez des vues de chemin existantes afin d'aider les opérateurs de réseau à visualiser les chemins réseau.

vues de réseau
Interface graphique de visualisation du réseau qui affiche des vues de réseau reconnu organisées de manière hiérarchique. Les Vues de réseau permettent de visualiser les résultats d'une reconnaissance ou d'identifier et résoudre des incidents liés au réseau.

Vue tronçon de réseau
Interface graphique de visualisation du réseau. La Vue tronçon de réseau permet de rechercher un périphérique spécifique sur le réseau et d'afficher un périphérique réseau spécifié. Vous pouvez également utiliser la Vue tronçon de réseau comme point de départ pour le traitement des incidents liés au réseau. Anciennement appelée Vue Tronçon.

Remarques

Ces informations s'appliquent au document PDF d'IBM Tivoli Network Manager IP Edition 3.9.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services 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, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service 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 donne 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

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues 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 autre 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 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
Australie
IBM Corporation
896471/H128B
76 Upper Ground
Londres
SE1 9PZ
Royaume-Uni
IBM Corporation
JBF1/SOM1 294
Route 100
Somers, NY, 10589-0100
Etats-Unis

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.

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 programme 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.

Marques

Les termes figurant dans le tableau 31 sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

Tableau 31. Marques d'IBM

AIX	iSeries	RDN
ClearQuest	Lotus	SecureWay
Cognos	Netcool	solidDB
Current	NetView	System z
DB2	Remarques	Tivoli
developerWorks	OMEGAMON	WebSphere
Serveur de stockage Enterprise	PowerVM	z/OS
IBM	PR/SM	z/VM
Informix	pSeries	zSeries

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 dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group 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.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Cette offre logicielle n'utilise pas de cookies ni aucune autre technologie afin de collecter des informations personnelles.

Pour plus d'informations sur l'utilisation de diverses technologies à ces fins, notamment les cookies, consultez les règles de confidentialité d'IBM à l'adresse http://www.ibm.com/privacy.

Index

Nombres

A

B

C

D

E

F

G

H

I

J

K

L

M

N

U

V

W

Z