Network Manager IP Edition
Version 3.9

Guide de reconnaissance

R2E2

Network Manager IP Edition
Version 3.9

Guide de reconnaissance

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 437.

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 de IBM Tivoli Network Manager IP Edition (numéro de produit 5724-S45) et à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

Table des matières

Tableaux

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 de reconnaissance* décrit les procédures d'administration et d'utilisation de Network Manager IP Edition pour effectuer des reconnaissances de réseau.

Public cible

Cette publication est conçue pour les utilisateurs et les administrateurs système et de réseau qui configurent IBM Tivoli Network Manager IP Edition.

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 xiv.

Contenu de la publication

La présente publication comporte les sections suivantes :

- Chapitre 1, «A propos de la reconnaissance», à la page 1

  Décrit la notion de reconnaissance ainsi que les paramètres servant à reconnaître un réseau.
- Chapitre 2, «Configuration de la reconnaissance de réseau», à la page 11

  Décrit les éléments prérequis pour pouvoir configurer et démarrer une reconnaissance.

  Il indique également les modalités d'exécution d'une reconnaissance via les éléments suivants :
  - Assistant reconnaissance permettant d'effectuer une reconnaissance initiale et de configurer les paramètres de reconnaissance de base.
  - Interface graphique Configuration de la reconnaissance permettant de configurer les paramètres de reconnaissance avancés.
  - Interface CLI et fichiers de configuration permettant de configurer le processus de reconnaissance.

  Ce chapitre contient également des informations sur la manière de configurer des paramètres de reconnaissance complexes en utilisant, par exemple, EMS, MPLS et NAT.
- Chapitre 3, «Surveillance de reconnaissances de réseau», à la page 173

  Décrit comment surveiller l'état et la progression de la reconnaissance de réseau à partir de l'interface graphique ou de la ligne de commande.
- Chapitre 4, «Classification des unités réseau», à la page 191

Décrit comment modifier la façon dont les périphériques réseau sont classés à l'issue de la reconnaissance.

- Chapitre 5, «Conservation de la topologie reconnue à jour», à la page 199

  Explique les procédures de planification d'une reconnaissance, de reconnaissance manuelle des périphériques et de suppression des périphériques.
- «Traitement des incidents liés à la reconnaissance à l'aide de rapports», à la page 207

  Indique comment traiter les problèmes liés au processus de reconnaissance et au réseau que vous souhaitez reconnaître.
- Annexe A, «Bases de données de reconnaissance», à la page 229

  Décrit les bases de données utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue la topologie réseau reconnue.
- Annexe B, «Processus de reconnaissance», à la page 339

  Décrit comment IBM Tivoli Network Manager IP Edition produit une topologie de réseau qui inclut les données de connectivité et de confinement.
- Annexe C, «Agents de reconnaissance», à la page 367

  Répertorie les agents de reconnaissance pouvant être exécutés dans le cadre de la reconnaissance. Elles contiennent également les agents à sélectionner, en fonction des caractéristiques de votre réseau.
- Annexe D, «Système auxiliaire», à la page 407

  Fournit des informations d'arrière-plan sur les auxiliaires, qui sont des applications spécialisées qui récupèrent des informations du réseau sur demande.
- «Principaux programmes stitcher de reconnaissance», à la page 409

  Décrit les programmes stitcher fournis avec IBM Tivoli Network Manager IP Edition.
- Annexe F, «Types d'interruption», à la page 429

  Décrit les différents types d'interruptions susceptibles d'être détectés par l'outil de recherche d'interruptions.

Publications

Cette section répertorie les publications de la bibliothèque Network Manager, ainsi que les documents annexes. 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 le noeud **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 permettent aux utilisateurs présentant un handicap physique, tel qu'une mobilité réduite ou une déficience visuelle, d'utiliser les 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 Tivoli

Pour en savoir plus sur la formation technique Tivoli, consultez le site Web IBM Tivoli suivant :

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

Informations de support

Si un problème survient lorsque vous utilisez votre logiciel IBM, vous souhaiterez sans doute le résoudre rapidement. IBM fournit les méthodes permettant d'obtenir l'assistance dont vous avez besoin :

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 de logiciel local gratuit qui vous aide à résoudre les questions et problèmes liés aux produits logiciels IBM. ISA permet d'accéder rapidement aux informations de support et aux outils de maintenabilité destinés à l'identification des problèmes. Pour installer le logiciel ISA, accédez à l'adresse 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
- Commandes d'interface (cases à cocher, boutons de commande, boutons d'option, sélecteurs rotatifs, zones, dossiers, icônes, zones de liste, éléments de zones de liste, listes multicolonne, containeurs, options de menu, noms de menu, onglets, feuilles de propriété), libellés (tels que **Conseil :** et **Considérations relatives au système d'exploitation :**)
- Mots clés et paramètres dans le texte

Italique

- Citations (par exemple, les titres de publications, disquettes et CD)
- Mots définis dans le texte (par exemple, une ligne spécialisée est appelée une ligne *point à point*)
- Mise en évidence des mots (exemple de mot en tant que mot : "Utilisez le mot *que* pour introduire une clause restrictive."; exemple de lettre en tant que lettre : "L'adresse LUN doit commencer par la lettre *L*.")
- Nouveaux termes dans un texte (sauf dans une liste de définitions) : une *vue* représente un cadre contenant des données dans un espace de travail
- Variables et valeurs à indiquer : ... 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 spécifiques au système d'exploitation

Cette publication utilise des variables d'environnement sans préfixe ni suffixe propre à la plateforme, à moins que la commande ne s'applique à une seule plateforme. Par exemple, le répertoire d'installation des composants centraux de Network Manager est représenté en tant que NCHOME.

Lorsque vous utilisez la ligne de commande Windows, vous devez utiliser le signe **%** avant et après les variables d'environnement, puis remplacer chaque barre oblique (*/*) par une barre oblique inverse (\) dans le chemin de répertoire. Par exemple, sous Windows, NCHOME est %NCHOME%.

Sous UNIX, placez un signe **$** avant les variables d'environnement. Par exemple, sous UNIX, NCHOME est $NCHOME.

Le nom des variables d'environnement n'est pas toujours le même sous Windows et UNIX. Par exemple, la variable %TEMP% sous Windows correspond à la variable $TMPDIR sous UNIX. Si vous faites appel à l'interpréteur de commandes sous Windows, vous pouvez utiliser les conventions UNIX.

Chapitre 1. A propos de la reconnaissance

Configurez la reconnaissance en définissant les paramètres qui régissent le mode d'exécution de la reconnaissance.

A propos des types de reconnaissance

Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Reconnaissance et nouvelle reconnaissance

Reconnaissance

Le terme reconnaissance est généralement utilisé pour désigner tout type de reconnaissance. Techniquement, seule la première reconnaissance exécuté après le démarrage du moteur de reconnaissance ncp_disco peut être désignée par le terme reconnaissance et chaque reconnaissance ultérieure doit être appelée nouvelle reconnaissance. Etant donné qu'il n'y a pas encore de données de reconnaissance en mémoire, les reconnaissances sont légèrement plus longues que les nouvelles reconnaissances.

Nouvelle reconnaissance

Après l'exécution d'une reconnaissance, toutes les reconnaissances ultérieures qui sont exécutées sont de nouvelles reconnaissances. Les nouvelles reconnaissances utilisent un flux de données différent de celui des reconnaissances, avec des programmes stitcher et des base de données différents. Si le moteur ncp_disco est redémarré, la reconnaissance suivante est une simple reconnaissance et les reconnaissances ultérieures sont de nouvelles reconnaissances. Excepté si vous exécutez des reconnaissances avancées ou modifiez le flux de données de reconnaissance, la différence entre une reconnaissance et une nouvelle reconnaissance n'est généralement pas importante et, pour simplifier la lecture, les instructions de cette documentation ne font pas de distinction entre une reconnaissance et une nouvelle reconnaissance, sauf si cela est nécessaire.

Reconnaissance complète ou partielle

Reconnaissance complète

Une reconnaissance complète est exécutée sur une grande portée et elle est 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.

Reconnaissance partielle

Une reconnaissance partielle est une nouvelle reconnaissance ultérieure d'une section du réseau reconnue 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 est basée sur les résultats de la dernière reconnaissance complète et peut uniquement être exécutée si le moteur de reconnaissance, le processus **ncp_disco**, n'a pas été arrêté depuis

la dernière reconnaissance complète. Une reconnaissance partielle est, par conséquent, un type de nouvelle reconnaissance.

Reconnaissance automatique et planifiée

Vous pouvez exécuter des reconnaissances à la demande, à l'aide de l'assistant, de l'interface graphique ou de la ligne de commande. Vous pouvez également configurer le démarrage automatique d'une reconnaissance.

Reconnaissance automatique
Après une reconnaissance, le processus de reconnaissance passe à l'état réactif, appelé mode de nouvelle reconnaissance, dans lequel une autre reconnaissance peut être déclenchée automatiquement à la réception d'une alerte envoyée par un périphérique réseau.

Reconnaissance planifiée
Vous pouvez planifier le démarrage d'une reconnaissance à l'heure de votre choix.

Concepts associés:

«Nouvelle reconnaissance complète ou partielle», à la page 362
En modifiant les programmes stitcher, vous pouvez configurer la manière dont DISCO traite les périphériques détecter en mode nouvelle reconnaissance.

Tâches associées:

«Planification de reconnaissances», à la page 199
Après l'exécution de la reconnaissance complète, vous pouvez planifier des reconnaissances supplémentaires en insérant l'heure, la date et le jour des reconnaissances à exécuter dans le fichier du programme stitcher `FullDiscovery.stch`.

«Démarrage d'une reconnaissance», à la page 52
Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

«Démarrage de reconnaissance partielle à partir de l'interface graphique», à la page 203
Le démarrage d'une reconnaissance partielle implique de définir un emplacement de départ et des portées.

«Configuration de la reconnaissance automatique», à la page 200
Network Manager fournit un mécanisme permettant de déclencher automatiquement une reconnaissance partielle en fonction de la réception d'une interruption. Cette opération est exécutée par le plug-in Disco sur la Passerelle d'événements. Les interruptions de périphérique peuvent indiquer un changement de périphérique réseau ou la présence d'un nouveau périphérique réseau. Pour plus d'informations sur le plug-in Disco, voir *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Portées

Définissez les zones du réseau (c'est-à-dire, les plages de sous-réseau) à inclure à la reconnaissance et celles à exclure. Les zones du réseau à inclure au processus de reconnaissance, ou à en exclure, sont collectivement connues sous le nom de portée de reconnaissance.

Il est important de limiter la portée de la reconnaissance, car la plage d'adresses IP reconnues par le processus de reconnaissance par défaut est potentiellement

illimitée. Sans portée définie, la reconnaissance tente de reconnaître tous les périphériques réseau. Une portée limite la reconnaissance aux éléments importants de votre réseau.

Important : Si votre réseau comprend des routes vers Internet, celles-ci sont reconnues. Puis, Network Manager utilise ces routes pour reconnaître des parties d'Internet.

Une portée peut contrôler la reconnaissance de périphériques sensibles que vous ne voulez pas interroger. Par exemple, lorsque l'interrogation d'un périphérique peut être à l'origine d'un problème de sécurité ou lorsque le processus d'interrogation surcharge le périphérique. Vous pouvez configurer la portée pour que des périphériques soient reconnus sans être instanciés en définition AOC. Ces périphériques ne sont pas représentés dans la topologie de réseau et les informations qui les concernent ne sont pas envoyées à la base de données MODEL. Vous pouvez également empêcher la reconnaissance des périphériques. La reconnaissance ne tente pas d'obtenir un accès SNMP à ces unités.

Une portée permet de limiter le volume des données que Network Manager tente de télécharger à partir des tables de routage des routeurs. Sans cette restriction, la reconnaissance d'un routeur qui connaît la table de routage pour tout Internet fait croître la durée de la reconnaissance de manière exponentielle.

Fix Pack 4 Si vous souhaitez utiliser la fonction de reconnaissance interdomaine pour regrouper plusieurs domaines dans une topologie unique, définissez leur portée de manière à réduire les liaisons entre eux. Par exemple, en divisant le réseau, évitez de disperser des connecteurs étroitement liés dans des domaines différents. Vérifiez que les périphériques sont sectorisés dans un seul domaine. En d'autres termes, les domaines ne doivent pas se chevaucher.

Restriction : Network Manager ne prend pas en charge le format IPv4 mappé en IPv6 et s'attend à ce que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappé IPv4 comme `::ffff:192.0.2.128`. A la place, entrez l'adresse `::ffff:c000:280` (format IPv6 standard, séparé par un deux points).

Types de configuration

Network Manager propose plusieurs types de configuration.

Vous pouvez autoriser les types de configuration ci-après :

- Vous pouvez inclure ou exclure des zones de votre réseau (soit des plages de sous-réseau, soit des périphériques spécifiques) dans la reconnaissance. Chaque zone configurée est appelée *zone*.

  Conseil : Si votre sous-réseau est peu peuplé, l'ajout de routeurs individuels permettra vraisemblablement une reconnaissance plus rapide que l'ajout du sous-réseau complet.
- Il est possible de spécifier des zones dans d'autres zones : dans une zone d'inclusion donnée, vous pouvez indiquer les périphériques ou sous-réseaux ne devant pas être détectés. Ces périphériques ne sont pas recherchés par l'outil de recherche PING ni interrogés par les agents de reconnaissance. Par exemple, vous pouvez définir une zone de portée d'inclusion constituée du sous-réseau 1.2.0.0/16 de classe B, au sein de laquelle vous pouvez spécifier une zone de

portée d'exclusion de sous-réseau 1.2.3.0/24 de classe C. Et enfin, au sein de la zone de portée d'exclusion, vous pouvez spécifier une zone de portée d'inclusion 1.2.3.128/26.

- Vous pouvez configurer un filtre qui détermine si un périphérique reconnu est interrogé pour obtenir des informations de connectivité.
- Vous pouvez configurer un filtre qui détermine si un périphérique d'une zone définie est à instancier. Si un périphérique est instancié, il est affiché sur la mappe réseau. Les périphériques qui ne sont pas instanciés ne sont pas envoyés à MODEL.
- Vous pouvez configurer la sectorisation multidiffusion. Vous pouvez ainsi configurer les sous-réseaux de multidiffusion devant être utilisés comme portées pour votre reconnaissance multidiffusion.

Définition de zones permettant de limiter la reconnaissance

Pour limiter la reconnaissance, vous devez définir des zones de reconnaissance. Vous pouvez les définir de différentes manières.

Choisissez l'une des méthodes suivantes afin de définir une zone de reconnaissance :

- Définissez des zones de reconnaissance à l'aide de l'interface graphique de configuration de la reconnaissance.
- Construisez des zones en ajoutant une insertion OQL à la table `scope.zones` à l'aide du fichier de configuration `DiscoScope.cfg`. Cette méthode s'adresse à des utilisateurs plus expérimentés.

Remarque : Si aucune information n'est indiquée dans la table `scope.zones` on considère que tous les éléments se situent dans la portée.

Pour chaque zone, vous devez indiquer les informations suivantes :

- Le type de protocole de réseau utilisé par la zone, même si actuellement seul le protocole IP est pris en charge. Vous pouvez définir autant de zones que nécessaire. Plusieurs zones peuvent également être définies au sein de la même insertion.
- L'action à prendre pour la zone, où les moyens `m_action=1` sont inclus dans la reconnaissance alors que les moyennes `m_action=2` ne le sont pas. Vous pouvez définir à la fois des zones d'inclusion et des zones d'exclusion. L'action à prendre dans la plus petite zone se substitue aux actions dans les zones plus larges.
- Une liste de liaisons de variables (`name=value`) qui définit la zone de reconnaissance actuelle.

Tâches associées:

«Définition de plusieurs zones d'inclusion», à la page 26
Vous pouvez définir plusieurs zones d'inclusion dans la table scope.zones.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Valeur de départ

Configurez les valeurs de départ pour spécifier les emplacements à partir desquels débuter la reconnaissance des périphériques. Les valeurs de départ de reconnaissance peuvent être des adresses IP ou des adresses de sous-réseau.

Vous pouvez indiquer des valeurs de départ de différentes manières :

- A l'aide de l'outil de recherche Ping : vous indiquez les adresses IP ou de sous-réseau à reconnaître en premier.
- A l'aide de l'outil de recherche File : vous indiquez un ou plusieurs fichier contenant chacun une liste d'adresses IP ou de sous-réseaux.

Conseil : Pour limiter la reconnaissance à une liste d'unités spécifiques, définissez l'emplacement de départ de la reconnaissance à l'aide d'une liste d'unités en utilisant l'outil de recherche de fichiers ou l'outil de recherche PING et désactivez le retour d'informations dans l'onglet **Avancé** de l'interface graphique de la configuration de la reconnaissance de réseau.

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

Accès à l'unité

Configurez l'accès aux périphériques en indiquant les noms de communauté SNMP et les paramètres Telnet de sorte que le système puisse accéder aux périphériques réseau.

Configurez l'accès aux périphériques comme suit :

- Indiquez les noms de communauté SNMP de sorte que Network Manager puisse accéder aux périphériques réseau utilisant le protocole SNMP et les interroger. Network Manager prend en charge les protocoles SNMP v1, v2 et v3,
- Indiquez les paramètres Telnet de sorte que le gestionnaire de réseau puisse accéder aux périphériques réseau utilisant le protocole Telnet et les interroger.

Agents

Les agents de reconnaissance vous permettent d'extraire des informations concernant les périphériques sur le réseau. Sélectionnez les agents adaptés à votre reconnaissance en fonction de votre type de réseau.

Les agents de reconnaissance extraient des détails sur les périphériques et recherchent leur connectivité. Ils peuvent également signaler l'existence de nouveaux périphériques en détectant de nouvelles connexions lors de la recherche de connectivité des périphériques. Les agents de reconnaissance peuvent être utilisés pour des tâches spécialisées. Par exemple, l'agent de reconnaissance du Cache ARP remplit la base de données du serveur auxiliaire à l'aide d'adresses IP en vue du mappage des adresses MAC.

Des agents par défaut sont fournis pour le type de reconnaissance que vous voulez effectuer, par exemple une reconnaissance de niveau 2 ou 3. Vous pouvez

sélectionner des ensembles d'agents différents pour des reconnaissances complètes et partielles. Les agents varient en fonction des variations des informations de connectivité des technologies matérielles sur le réseau.

Filtres

Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

Après avoir défini la portée de votre reconnaissance à l'aide de l'onglet **Portée**, il est possible de la limiter à l'aide de filtres. Par exemple, il se peut que vous vouliez maintenir les zones de portée que vous avez défini plus tôt, mais limiter la portée sur la base de l'emplacement (par exemple, uniquement le matériel de New York) ou du fournisseur de matériel (par exemple, les périphériques Cisco uniquement).

Vous pouvez filtrer les périphériques sur la base de plusieurs critères, y compris l'emplacement, la technologie et le fabricant.

Par défaut, les filtres de reconnaissance ne filtrent pas l'hôte de Network Manager car il sert généralement aussi de station d'interrogation pour l'analyse d'origine du problème. Afin que cette analyse fonctionne correctement, la station d'interrogation, et donc l'hôte de Network Manager, doivent faire partie de la topologie.

Pour obtenir plus d'informations sur l'analyse d'origine du problème, consultez les guides *IBM Tivoli Network Manager IP Edition - Guide d'administration* et *IBM Tivoli Network Manager IP Edition - Guide de traitement des incidents liés au réseau*.

Si vous avez besoin de filtrer l'hôte de Network Manager, vous devez modifier les programmes stitcher suivants et supprimer les sections de code, indiquées par des commentaires, qui empêchent l'hôte de Network Manager d'être filtré. Les programmes stitcher sont DetectionFilter.stch et InstantiationFilter.stch.

Filtre de pré-reconnaissance

Il se peut que vous vouliez appliquer ce filtre à des périphériques sensibles que vous ne voulez pas interroger. Un périphérique peut être considéré comme sensible car son interrogation peut comporter un risque de sécurité ou surcharger celui-ci.

Les filtres de pré-reconnaissance empêchent d'interroger les périphériques reconnus sur leurs informations de connectivité. Seuls les périphériques correspondant au filtre de pré-reconnaissance sont entièrement reconnus. Si aucun filtre de pré-reconnaissance n'est défini, tous les périphériques dans la portée sont reconnus.

Les filtres de pré-reconnaissance fournissent un mécanisme permettant d'établir la reconnaissance sur des plages d'ID complexes qui ne peuvent pas être facilement définies dans l'onglet **Portée**. Ils permettent de filtrer les périphériques en fonction de leur valeur sysObjectId. Les filtres par défaut permettent quant à eux de filtrer les noeuds d'extrémité, les imprimantes et les périphériques similaires. Bien qu'il soit possible de créer plusieurs filtres complexes afin d'optimiser cette fonction, n'oubliez pas de faire en sorte que leur maintenance reste facile. Le filtre agit sur les zones de la table OQL `details.returns` du service de reconnaissance (Disco) pour que vous puissiez utiliser les zones autres que les adresses IP, notamment m_ObjectId (similaire à sysObjectId). Un périphérique doit passer tous les filtres pour être reconnu.

Important : Définissez la logique du filtre de sorte que vous n'ayez pas besoin de modifier les filtres de pré-reconnaissance chaque fois que vous ajoutez de nouvelles portées.

Vous pouvez configurer la condition de filtrage afin de tester toutes les colonnes de la table Details.returns. Mais il se peut que vous deviez utiliser l'adresse IP (m_UniqueAddress) en tant que base pour le filtre pour limiter la détection d'un périphérique spécifique. Si le périphérique n'accorde pas l'accès SNMP à l'agent Details, ce dernier ne parviendra peut-être pas à extraire les variables MIB telles que l'ID Objet. Toutefois, le retour de l'adresse IP est garanti lorsque le périphérique est détecté.

Vous pouvez définir plusieurs filtres de pré-reconnaissance. Les filtres sont associés automatiquement à l'aide d'une expression booléenne ET. Tous les critères définis dans tous les filtres doivent être respectés.

Filtre de post-reconnaissance

Il se peut que vous vouliez appliquer ce filtre aux périphériques que vous voulez interroger, comme les postes de travail et les imprimantes. Un filtre de post-reconnaissance limite l'instanciation du périphérique. Si un filtre de post-reconnaissance est défini, seuls les périphériques qui transmettent le critère sont instanciés c'est-à-dire envoyés à MODEL. Si aucun filtre de post-reconnaissance n'est défini, tous les périphériques reconnus sont envoyés à MODEL.

Les données sur les périphériques non classés sont stockées dans la base de données topologiques NCIM. Néanmoins, le périphérique ne peut pas être visualisé dans Topoviz et ne peut pas être interrogé.

Vous pouvez définir plusieurs filtres de post-reconnaissance. Les filtres sont associés automatiquement à l'aide de l'expression booléenne ET, qui signifie que tous les critères définis dans tous les filtres doivent être respectés.

Le filtre de post-reconnaissance fait fonctionner la table scratchTopology.entityByName. Les zones disponibles dans ce filtre sont donc différentes de celles disponibles dans le filtre de pré-reconnaissance. Le filtre de post-reconnaissance fonctionne sur des zones topologiques plutôt que pour des informations de périphériques de base.

Concepts associés:

«Création de la topologie», à la page 355
La création de la topologie s'effectue en plusieurs étapes.

Tâches associées:

«Définition des filtres de reconnaissance», à la page 36
Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Référence associée:

«Principaux programmes stitcher de reconnaissance», à la page 409
Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

Annexe A, «Bases de données de reconnaissance», à la page 229
Il existe différentes bases de données spécialisées utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue la topologie réseau reconnue.

«Schéma de la base de données scratchTopology», à la page 321
La base de données scratchTopology est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Son nom de table de base de données complet est : scratchTopology.entityByName.

système de nom de domaine (DNS)

Configurez le DNS pour permettre à la reconnaissance d'accéder aux services DNS utilisés pour effectuer les recherches de nom de domaine.

Vous pouvez configurer trois types de systèmes de noms de domaine :

Serveur DNS
Serveur du réseau dédié à la réalisation de la résolution des noms de domaine.

Fichier
Nom d'un fichier conservé sur l'hôte Network Manager, contenant les adresses IP et les noms d'hôte au format table de recherche.

Système
DNS local sur la machine gestionnaire de réseau.

Conversion d'adresse réseau

Configurer les données pour les passerelles NAT au sein de votre réseau.

Les passerelles NAT fournissent des mappages entre l'adresse IP privée dans votre réseau et les adresses IP publiques. Vous pouvez permettre au système de reconnaître les périphériques au sein d'espaces adresses privés en configurant les données pour les passerelles NAT.

Paramètres avancés

Configurez les paramètres de reconnaissance avancés pour augmenter la vitesse de la reconnaissance et l'équilibrer avec la charge sur le serveur. Généralement, des résultats de reconnaissance plus rapides utilisent une plus grande quantité de mémoire sur le serveur. Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants.

Remarque : Ne modifiez les paramètres avancés que si vous êtes un utilisateur avancé Network Manager.

Vous pouvez configurer les paramètres de reconnaissance avancés suivants :

Paramètres des outils de recherche :
Les outils de recherche sont des sous-systèmes de reconnaissance qui reconnaissent les périphériques sur le réseau. Vous pouvez configurer des paramètres tels que les délais d'attente, le nombre de nouvelles tentatives et le nombre d'unité d'exécution des outils de recherche.

Paramètres auxiliaires
Les auxiliaires sont des applications de reconnaissance utilisées par les agents pour extraire des informations des périphériques. Vous pouvez configurer des paramètres tels que les délais d'attente, le nombre de nouvelles tentatives et le nombre d'unité d'exécution des auxiliaires.

Autres paramètres
Vous pouvez configurer des paramètres de reconnaissance complexes, comme l'activation de la mise en cache des tables de reconnaissance, le modélisation du réseau local virtuel, le basculement de la reconnaissance, la vérification de l'outil de recherche de fichiers et les paramètres ayant un impact sur la vitesse de reconnaissance partielle.

La plupart des paramètres de reconnaissance avancés sont facultatifs.

Reconnaissance contextuelle

Si vous devez reconnaître des périphériques comme des périphériques SMS, MPLS Edge ou autres à l'aide de routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. Ce type de reconnaissance permet une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type particulier de périphériques est pris en charge par la reconnaissance.

Lors d'une reconnaissance contextuelle, des informations sur le périphériques sont transmises de la table `renvois` de l'agent Détails à la table `despatch`de l'agent Context adéquat.

Les agents Context utilisent des filtres dans les fichiers .agent des agents afin de déterminer les périphériques à traiter. Ceci s'applique pour tous les agents de reconnaissance. Si le périphérique ne correspond pas à un type pris en charge par les routeurs virtuels, c'est-à-dire qu'il ne requière pas de traitement contextuel, il est directement transmis à l'agent Associated Address.

Concepts associés:

«Reconnaissance des détails des périphériques (contextuels)», à la page 351
La reconnaissance des détails contextuels des périphériques s'effectue en plusieurs étapes.

Référence associée:

«Agents de reconnaissance contextuelle», à la page 396
Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

Auxiliaires

Les auxiliaires sont des applications spécialisées qui récupèrent des informations du réseau sur demande. La configuration par défaut de l'auxiliaire est suffisante pour la plupart des réseaux. Vous pouvez toutefois décider de modifier cette configuration pour différentes raisons.

La configuration du système auxiliaire peut accélérer la reconnaissance du réseau, mais n'est recommandée que pour les utilisateurs expérimentés.

Bien que les agents de reconnaissance récupèrent les informations de connectivité, ils n'interagissent pas directement avec le réseau. Ils extraient les informations de connectivité via le système auxiliaire, constitué d'un serveur auxiliaire et de différents auxiliaires.

Les motifs de configuration des auxiliaires sont :

- L'accélération du processus de reconnaissance via la réduction des délais d'attente et du nombre de nouvelles tentatives de l'auxiliaire.
- Si votre réseau est très fiable et que les périphériques qui le composent répondent rapidement, vous pouvez spécifier un délai d'attente court.
- Vous pouvez décider de modifier les délais d'attente par défaut pour les auxiliaires SNMP et Telnet si plusieurs périphériques ne répondent pas à SNMP et Telnet ou sont configurés pour ne pas répondre à des accès Telnet ou SNMP. Un délai d'attente par défaut long signifierait par conséquent que les auxiliaires attendent longtemps des réponses qu'ils ne recevront jamais.
- Pour réduire la quantité de trafic réseau engendrée par une reconnaissance, vous pouvez allonger le délai d'attente et désactiver le lancement de commandes PING sur la diffusion et la multidiffusion.

Reconnaissances spécialisées

Vous pouvez configurer le produit afin qu'il effectue des reconnaissances plus complexes, comme la reconnaissance MPLS (Multiprotocol Label Switching) ou NAT (Network Address Translation).

Parmi les reconnaissances spécialisées figurent :

Les reconnaissances EMS (Element Management System)
Collectent des données topologiques à partie des systèmes de gestion d'éléments et les intégrent à la topologie reconnue.

Les reconnaissances MPLS
Reconnaissent les réseaux privés virtuels de couche 3 et les réseaux privés virtuels de couche 2 étendus s'exécutant sur des réseaux principaux MPLS.

Les reconnaissances NAT
Reconnaissent les périphériques de passerelle NAT afin d'extraire les données sur les périphériques dans des espaces adresse privés.

Les reconnaissances de tiers :
Reconnaît les réseaux fournisseurs intervenants en tant qu'objet tiers sur plusieurs réseaux fonctionnant sur un réseau fournisseur. Exemples: réseaux VPN d'entreprise sur un réseau principal MPLS fournisseur.

Fix Pack 4 **Reconnaissances interdomaines**
Relient 2 ou plusieurs domaines reconnus. Les connexions entre les périphériques de différents domaines sont détectées et ajoutées à la topologie.

Chapitre 2. Configuration de la reconnaissance de réseau

Configurez la reconnaissance de votre réseau, y compris les types de périphériques à découvrir et les limites de cette reconnaissance.

Network Manager fournit des outils de reconnaissance de votre réseau qui utilisent une approche en phases.

- Utilisez l'assistant de configuration de la reconnaissance pour exécuter des reconnaissances initiales. L'assistant fournit une reconnaissance guidée et décide de la configuration en fonction des réponses que vous donnez tout au long de son exécution.
- Utilisez l'interface graphique de la configuration de la reconnaissance pour procéder aux reconnaissances suivantes. A l'aide de l'interface graphique, vous pouvez configurer des paramètres de reconnaissance détaillés, notamment la portée, les emplacements, les noms de communauté, la sélection d'agents.

Remarque : Vous pouvez également configurer une reconnaissance en utilisant les fichiers de configuration de reconnaissance et la ligne de commande. Toutefois, ne configurez la reconnaissance ainsi que si vous être un utilisateur Network Manager expérimenté et si vous comprenez les différents aspects de la reconnaissance, y compris les processus, les phases, les étapes, les auxiliaires, les agents, les programmes stitcher et les interruptions de reconnaissance.

Pour plus d'informations sur l'édition manuelle d'une topologie découverte après une reconnaissance, consultez *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*.

Planification de la reconnaissance

Avant de configurer et d'exécuter une reconnaissance, vérifiez plusieurs caractéristiques, paramètres et exigences du système.

Les notes suivantes vous aident à planifier la reconnaissance.

Sauvegarde des modifications dans l'interface graphique de la configuration de la reconnaissance de réseau

Pour sauvegarder les modifications de la configuration que vous avez apportées au cours d'une session, pensez à cliquer sur le bouton **Sauvegarder** avant de vous déconnecter, fermer la fenêtre de navigateur ou fermer l'onglet Configuration de la reconnaissance réseau. Il est recommandé de cliquer sur **Sauvegarder** lorsque vous vous déplacez d'onglet en onglet.

Système d'exploitation

Vérifiez que l'hôte sur lequel Network Manager est installé dispose de la totalité des derniers modules de correction.

Portée de la reconnaissance

Considérez les questions et les points suivants, relatifs à la portée de la reconnaissance :

- L'hôte Network Manager se trouve-t-il dans le réseau ?
- L'hôte est-il positionné de sorte à pouvoir interroger toutes les périphériques que vous souhaitez inclure dans votre reconnaissance ?

- Considérez tous les réseaux et sous-réseaux nécessaires et déterminez les masques de réseau associés.
- Y'a-t-il des parties du réseau que vous souhaitez exclure ?
- Rassemblez tous les noms de communauté SNMP relatifs aux unités à portée

Routage
Vérifiez que chaque réseau et sous-réseau à reconnaître peut être joint à l'aide du processus ICMP. Si nécessaire, ajoutez des routes à l'hôte Network Manager en utilisant la commande **route add**.

Listes de contrôle d'accès
Network Manager utilise plusieurs protocoles qui peuvent devoir traverser des pare-feu. Ces protocoles sont ICMP, SNMP, DNS, ARP, SSH et TELNET. Pour garantir que Network Manager peut accéder aux unités situées derrière ces pare-feu, demandez aux administrateurs des pare-feu concernés de les configurer.

Analyse origine du problème
Pour procéder à l'analyse origine du problème sur des unités d'une topologie, la reconnaissance doit identifier tous les périphériques sur lesquels vous pouvez souhaiter exécuter cette analyse. De plus, la reconnaissance doit identifier la station d'interrogation Network Manager. Pour plus d'informations sur l'analyse origine du problème, voir le *Guide de surveillance et RCA de Network Manager*.

Création et configuration de domaines réseau supplémentaires

Pour ajouter des domaines réseau supplémentaires, vous devez configurer le contrôle de processus pour les domaines et enregistrer ces derniers avec la base de données topologiques NCIM. Les configurations et les interrogations peuvent être copiées depuis les domaines existants. Configurez ou reconfigurez les vues de réseau pour afficher les périphériques dans les nouveaux domaines.

Avant de commencer :

- Définissez comment partitionner le réseau en domaines. Les partages naturels des domaines suivent souvent des lignes géographiques. Pour plus d'informations, voir «Instructions relatives au nombre de domaines réseau», à la page 15.
- Fix Pack 4 Si vous souhaitez utiliser la fonction de reconnaissance interdomaine pour regrouper les domaines dans une topologie unique, répartissez-les de manière à réduire les liaisons entre eux. Par exemple, en divisant le réseau, évitez de disperser des connecteurs étroitement liés dans des domaines différents. Vérifiez que les périphériques sont sectorisés dans un seul domaine. En d'autres termes, les domaines ne doivent pas se chevaucher.

1. Sauvegardez le fichier `$NCHOME\etc\precision\CtrlServices.cfg` pour le domaine qui a été créé au cours de l'installation du produit.
2. Faites une copie du fichier `CtrlServices.cfg` et renommez-le `CtrlServices.`*`DOMAINE`*`.cfg`, où *DOMAINE* est le domaine.

   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.
   Par exemple, `CtrlServices.MASTER.cfg`. Puis, effectuez les modifications requises dans le fichier `CtrlServices.`*`DOMAINE`*`.cfg`.

3. Pour configurer une reconnaissance pour le domaine :
   a. Sauvegardez et créez des versions spécifiques au domaine des fichiers de configuration de la reconnaissance. Par exemple, `DiscoPingFinderSeeds.MASTER.cfg`.
   b. Configurez les paramètres des fichiers spécifiques au domaine. Vous pouvez également configurer les paramètres de la reconnaissance après la création des domaines.
4. Sauvegardez et créez une version spécifique au domaine du fichier `$NCHOME/etc/precision/ConfigItnm.cfg`. Par exemple, `ConfigItnm.MASTER.cfg`. Ensuite, définissez les détails de la connexion pour le serveur d'objets dans ce fichier.
5. Pour enregistrer le nouveau domaine avec la base de données topologiques NCIM, sauvegardez et créez une version spécifique au domaine du fichier `$NCHOME/etc/precision/DbLogins.cfg`. Puis, éditez les informations de la connexion de base de données dans ce fichier.
6. Pour vous connecter à une autre source de données de l'Interface graphique Web Tivoli Netcool/OMNIbus :
   a. Sauvegardez et créez une copie spécifique au domaine du fichier `$NCHOME/etc/precisionModelNcimDb.cfg`. Par exemple, `ModelNcimDb.MASTER.cfg`.
   b. Dans le fichier spécifique au domaine, remplacez la propriété **m_WebTopDataSource** par le nom de la source de données.
7. Pour copier la configuration et les interrogations réseau d'un domaine existant, exécutez le script `domain_create.pl`. L'exemple suivant crée un domaine appelé MASTER avec le mot de passe PASSWORD.

   ```
   $NCHOME/precision/bin/ncp_perl
   $NCHOME/precision/scripts/perl/scripts/domain_create.pl -domain MASTER
    -password PASSWORD
   ```

   Le script `domain_create.pl` ne copie pas la topologie du domaine source, seulement la configuration et les interrogations.
8. Windows Pour exécuter des processus en tant que services, installez les services :
   a. Modifiez le fichier `InstallServices.cfg` afin qu'il inclue les services que vous voulez installer et les paramètres par défaut. Ce fichier utilise le même format que le fichier `CtrlServices.cfg`.
   b. Installez les services du nouveau domaine en exécutant la commande suivante :

      ```
      ncp_install_services -domain nom_domaine [-username nom_utilisateur]
      ```

      Utilisez l'option `-username` pour installer les services en tant qu'utilisateur spécifique du domaine. Si vous n'utilisez pas cette option, les services sont installés sous le compte LocalSystem.
   c. Cliquez sur **Démarrer** > **Panneau de commande** > **Outils d'administration** > **Services** pour vérifier que tous les services sont installés.
9. Démarrez Network Manager sur le domaine. Exemple :

   ```
   itnm_start ncp -domain MASTER
   ```
10. Créez de nouvelles vues de réseau qui capturent le nouveau domaine, ou modifiez vos vues de réseau existantes. Dans l'onglet **Filtre**, sélectionnez le nouveau domaine. Si vous ne définissez pas le nouveau domaine dans les vues de réseau, vous ne pouvez pas afficher ses périphériques. Pour plus

d'informations sur les vues de réseau, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*.

11. Répétez les étapes pour configurer tous les domaines.

Après la création des domaines :

- Démarrez le processus **ncp_ctrl** sur le domaine pour contrôler tous les processus qui s'y exécutent. Vous devez utiliser une instance de **ncp_ctrl** pour exécuter et gérer chaque domaine. Si le processus **ncp_ctrl** d'un domaine n'est pas en cours, ce dernier ne peut pas être configuré dans l'interface graphique.
- Modifiez les paramètres de la reconnaissance, si vous ne l'avez pas déjà fait à l'étape 3b, à la page 13.
- Exécutez les reconnaissances sur les domaines. Etant donné que les reconnaissances sont consommatrices de ressources, elles sont généralement exécutées sur un seul domaine à la fois. Pour exécuter des reconnaissances sur plusieurs domaines simultanément, vérifiez que vous disposez de suffisamment de ressources. Les vérifications habituelles sont les suivantes :
  - Vérifiez qu'un nombre suffisant de connexions de base de données sont configurées.
  - Assurez-vous que le trafic sur les périphériques réseau n'est pas trop chargé.
  - Assurez-vous que la mémoire disponible est suffisante sur l'hôte pour exécuter la reconnaissance, par exemple en vérifiant l'utilisation de la mémoire des processus Network Manager.

  Pour plus d'informations sur la reconnaissance de la configuration, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de reconnaissance* .
- Fix Pack 4 Pour visualiser les topologies reconnues pour chaque domaine dans un seul domaine regroupé, configurez la fonction de reconnaissance interdomaine.
- Configurez l'interrogation sur le domaine. Pour plus d'informations sur la configuration de l'interrogation réseau, voir le manuel *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Concepts associés:

«Portées», à la page 2
Définissez les zones du réseau (c'est-à-dire, les plages de sous-réseau) à inclure à la reconnaissance et celles à exclure. Les zones du réseau à inclure au processus de reconnaissance, ou à en exclure, sont collectivement connues sous le nom de portée de reconnaissance.

Tâches associées:

«Configuration des reconnaissances interdomaine», à la page 103
Pour visualiser les liens entre les périphériques dans différents domaines afin de les afficher dans les vues de réseau et de topologie, vous devez configurer et exécuter des reconnaissances interdomaine dans les différents domaines.

Référence associée:

«Fichiers de configuration de la reconnaissance», à la page 58
Dans les fichiers de configuration de la reconnaissance, définissez les paramètres de la reconnaissance en créant ou en éditant les instructions INSERT dans les bases de données des processus de reconnaissance.

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.

Reconnaissance du réseau à l'aide de l'assistant

L'assistant de configuration de reconnaissance a été conçu pour les utilisateurs ayant une expérience limitée dans la configuration des reconnaissances.

Important : Si vous souhaitez conserver les paramètres de configuration de reconnaissance que vous avez indiqués précédemment dans l'interface graphique, n'utilisez pas l'assistant. L'assistant de configuration de reconnaissance remplace tous les paramètres précédents.

Tâches associées:

«Surveillance de la reconnaissance de réseau à partir de l'interface graphique», à la page 173
Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

Lancement de l'assistant

Sélectionnez un domaine et lancez l'assistant pour commencer à configurer et exécuter une reconnaissance.

Pour lancer l'assistant, procédez comme suit :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance réseau**.
2. Dans l'angle supérieur gauche de l'onglet Configuration de la reconnaissance réseau, sélectionnez le domaine dans lequel vous souhaitez exécuter une reconnaissance, dans le menu **Domaine**.
3. Cliquez sur le bouton de l'assistant à droite du menu **Domaine**.

Choix d'une reconnaissance sectorisée ou non sectorisée

La fenêtre Portée de la reconnaissance propose l'option d'une reconnaissance sectorisée ou non sectorisée.

Pour sélectionner une reconnaissance sectorisée ou non sectorisée, procédez comme suit.

Restriction : Network Manager ne prend pas en charge le format IPv4 mappé en IPv6 et s'attend à ce que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappée IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

1. Sélectionnez **Sectorisée** ou **Non sectorisée**.

   Sectorisée
   Une reconnaissance sectorisée limite la reconnaissance à une certaine partie de votre réseau. Pour indiquer une reconnaissance sectorisée, indiquez à l'assistant la zone du réseau à laquelle la reconnaissance doit se limiter, puis attribuez des adresses IP ou des sous-réseaux en tant qu'emplacements de départ sur lesquels une commande PING doit être lancée pour le démarrage de la reconnaissance.

   Non sectorisée
   Une reconnaissance non sectorisée tente de reconnaître la totalité de votre réseau. Toutefois, vous devez également attribuer des adresses IP ou des sous-réseaux en tant qu'emplacements de départ sur lesquels une commande PING doit être lancée pour le démarrage de la reconnaissance.

   Avertissement : Si certaines routes de votre réseau se dirigent vers l'Internet, une reconnaissance non sectorisée détecte ces routes et commence à reconnaître des parties de l'Internet.

2. Si vous avez sélectionné **Sectorisée**, indiquez la zone du réseau à laquelle limiter la reconnaissance.

   Indiquez un ou plusieurs sous-réseaux à utiliser à la fois pour la sectorisation et les emplacements de départ en cliquant sur **Nouveau**, puis en entrant une adresse IP et un masque de réseau.

   Restriction : Pour des raisons de performance, les commandes PING seront uniquement lancées sur les adresses IPV4. Pour lancer des commandes PING sur des adresses IPV6, utilisez l'onglet Valeur de départ dans l'interface graphique de la configuration de la reconnaissance.

3. Si vous avez sélectionné l'option **Non sectorisée**, indiquez les emplacements de départ à utiliser pour votre reconnaissance non sectorisée.

   Cliquez sur **Nouveau...** et spécifiez une ou plusieurs adresses IP.

Configuration de l'accès SNMP à l'aide de l'assistant

Spécifiez les noms de communauté globaux, spécifiques de l'adresse ou spécifiques du réseau dans la fenêtre Noms de communauté SNMP.

Pour SNMP version 3, vous pouvez également spécifier des mots de passe pour les noms de communauté.

Lors de la reconnaissance de périphériques utilisant SNMPv3, le contexte de réseau local virtuel (VLAN) doit être ajouté aux commutateurs Cisco du groupe de vues de chaque réseau local virtuel.

Pour configurer l'accès SNMP, procédez comme suit.

1. Pour chaque nom de communauté SNMP et mot de passe associé à définir:
   a. Cliquez sur l'icône **Nouveau** située au-dessus du tableau **Noms de communauté SNMP** pour afficher la fenêtre Propriétés des mots de passe SNMP.
   b. Spécifiez des noms de communauté spécifiques aux adresses, au sous-réseaux ou globaux et, dans le cas de SNMPv3, indiquez les mots de passe de ces noms de communauté.

      Il se peut que vous deviez entrer un nom de communauté plusieurs fois. Par exemple, entrez une chaîne pour SNMPv1, une autre pour SNMPv2 et une autre pour SNMPv3.

      La spécification de noms de communauté classés en sous-réseaux permet une reconnaissance plus efficace et plus rapide.

      Restriction : Il est recommandé de ne pas utiliser le caractère @ dans les noms de communauté. L'utilisation de ce symbole dans un nom de communauté peut causer des problèmes de connexion aux périphériques au moment de la reconnaissance.
2. Utilisez les touches fléchées vers le haut et vers le bas pour agencer les noms de communauté selon l'ordre des utilisations les plus fréquemment attendues. Les noms de communauté les plus fréquemment utilisés doivent se situer au début.

Configuration de l'accès Telnet à l'aide de l'assistant

Dans la fenêtre Accès Telnet, définissez les paramètres d'accès Telnet.

Pour configurer l'accès à Telnet, procédez comme suit :

1. Après avoir indiqué les noms de communauté SNMP, cliquez sur l'icône **Nouveau** de la fenêtre Accès Telnet.
2. Pour chaque ensemble d'unités accessibles via Telnet pour lequel vous souhaitez définir des invites et des mots de passe, cliquez sur **Nouveau**.
3. Dans la fenêtre Mots de passe Telnet, vous pouvez indiquer un ensemble de périphériques accessibles via Telnet (tous les périphériques situés au sein d'un sous-réseau indiqué ou d'une adresse IP unique) avec des invites, des ID de connexion et des mots de passe de connexion pour cet ensemble de périphériques.

Spécification du type de reconnaissance

Dans la fenêtre Type de reconnaissance, spécifiez le type de reconnaissance : une reconnaissance Couche 3 ou Couche 2.

Une reconnaissance Couche 3 est plus rapide, mais ses résultats ne peuvent pas être utilisés pour l'analyse origine du problème. Une reconnaissance Couche 2 est plus détaillée et les résultats peuvent être utilisés pour une analyse d'origine du problème.

Pour spécifier le type de reconnaissance, procédez comme suit.

1. Dans la fenêtre Type de reconnaissance, spécifiez une reconnaissance Couche 2 ou Couche 3.
2. Si vous avez sélectionné **Couche 3**, la fenêtre Reconnaissance de noeud final s'affiche.

   Dans la fenêtre Reconnaissance de noeud final, vous pouvez éliminer par filtrage les périphériques de noeud final tels que les postes de travail et les imprimantes. Vous pouvez également éliminer par filtrage les périphériques sans accès SNMP.

   Conseil : L'élimination par filtrage de tous les noeuds finaux dans les réseaux qui en comportent un nombre important peut améliorer la performance et la vitesse de votre reconnaissance.
3. Si vous avez sélectionné **Couche 2 et Couche 3**, la fenêtre Modélisation de réseau local virtuel (VLAN) s'affiche.

   Dans la fenêtre Modélisation de réseau local virtuel (VLAN), vous configurez la reconnaissance pour modéliser le réseau local virtuel dans la topologie de résultat. Cela permet au réseaux locaux virtuels d'être pris en compte lors de l'exécution de l'analyse d'origine du problème. Les VLAN sont de concept Couche 2 et la modélisation VLAN est requise pour les reconnaissances Couche 2 uniquement. Spécifiez si vous voulez modéliser les VLAN. Lorsque vous avez spécifié une option, cliquez sur **Suivant** pour afficher la fenêtre Reconnaissance de noeud final.

Optimisation de la reconnaissance

Dans la fenêtre Optimisation de la reconnaissance, optimisez la reconnaissance de la connectivité, de la richesse des informations et de la vitesse.

Pour optimiser la reconnaissance, procédez comme suit.

1. Fournissez des montants variables des informations de connectivité en sélectionnant l'une des options suivantes.

   Connectivité la plus précise possible et richesse des informations
   Cette option fournit des informations de connectivité détaillées entre les commutateurs, les noeuds finaux et les routeurs ainsi que des informations détaillées sur chaque unité reconnue. Cependant, la reconnaissance peut nécessiter un délai important pour s'effectuer.

   Connectivité la plus précise possible mais préférence pour la rapidité de la reconnaissance plutôt que pour la richesse des informations
   Cette option fournit des informations de connectivité complètes. Cependant, la reconnaissance fournit moins d'informations détaillées sur chaque unité reconnue dans le but d'accélérer la reconnaissance.

Informations riches sur les périphériques mais préférence pour la rapidité de la reconnaissance, plutôt que pour la précision de la connectivité

Cette option fournit des informations détaillées sur chaque unité reconnue. Cependant, la reconnaissance fournit moins d'informations de connectivité détaillées dans le but d'accélérer la reconnaissance. Par exemple, la reconnaissance peut fournir des informations sur la manière dont les commutateurs sont connectés entre eux, mais ne fournit peut-être pas d'informations sur la connectivité entre les commutateurs et les noeuds finaux ou entre les commutateurs et les routeurs.

Remarque : Cette option est plus appropriée si vous souhaitez collecter des données d'inventaire au lieu d'effectuer l'analyse de l'origine du problème (RCA). La RCA dépend de l'exactitude des données de connectivité.

Durée de reconnaissance la plus rapide

Cette option se concentre sur la rapidité de la reconnaissance. Cependant, les informations de connectivité fournies sont limitées ainsi que les informations détaillées sur chaque unité.

2. Si vous sélectionnez l'une des deux premières options, cela signifie que l'exactitude de la connectivité est importante. La fenêtre Fiabilité du réseau s'affiche.
3. Si vous sélectionnez l'une des deux dernières options, cela signifie que vous souhaitez transiger sur les informations relatives à l'exactitude de la connectivité pour assurer une reconnaissance plus rapide. Dans ce cas, l'assistant demande quelle proportion de votre réseau est composé d'unités Cisco. Si une grande partie de votre réseau est composée d'unités Cisco, l'assistant peut éteindre les agents reconnaissant la connectivité pour les périphériques non Cisco, accélérant ainsi la reconnaissance de manière significative. La fenêtre Matériel Cisco s'affiche.
   a. Spécifiez quelle proportion de votre réseau est composée de matériel Cisco en sélectionnant l'une des options suivantes :

      Tout Cette option fait exécuter le Cisco Discovery Protocol (CDP) par l'assistant.

      Une grande partie du réseau, Une partie du réseau, Je ne sais pas

      Cette option fait exécuter le CDP par l'assistant. Cependant, si vous avez choisi une reconnaissance Couche 2 et Couche 3 ou si vous avez indiqué vouloir exclure les noeuds finaux de la reconnaissance, cette option appelle le protocole Spanning Tree (STP) ainsi que le CDP.

      Aucun

      Cette option indique que ni le protocole CDP, ni le protocole STP n'est utilisé.

   b. Lorsque vous avez sélectionné une de ces options, cliquez sur **Suivant**.
   c. Si la réponse à la question relative au matériel Cisco était **Tout le réseau** ou **Aucune**, la fenêtre Fiabilité du réseau s'affiche.
   d. Si la réponse était **Une grande partie du réseau**, **Une partie du réseau** ou **Je ne sais pas**, la fenêtre Protocole Spanning Tree s'affiche, dans laquelle vous spécifiez si le protocole Spanning Tree est activé sur tous les commutateurs du réseau.

Indication de la fiabilité de votre réseau

Dans la fenêtre Fiabilité du réseau, sélectionnez une description de la fiabilité de votre réseau en répondant aux commandes PING et aux demandes SNMP. La description ordonne à l'assistant d'établir la durée des délais d'attente.

Pour décrire la fiabilité de votre réseau, lorsque vous répondez à la commande PING et aux demandes SNMP, choisissez une option correspondant à la fiabilité de votre réseau.

Très fiable
Cette description indique que le réseau doit être fiable pour les réponses aux requêtes ping et SNMP. Sélectionnez cette option pour autoriser l'assistant à appliquer des délais d'attente très courts, sans nouvelles tentatives. Cette option est appropriée à un réseau très fiable et produit des reconnaissances rapides. Si vous avez demandé la durée de reconnaissance la plus rapide dans la fenêtre d'optimisation de reconnaissance, les délais d'attente sont encore plus courts.

Assez fiable
Cette description indique que le réseau doit être fiable pour la plupart des réponses aux requêtes ping et SNMP. Sélectionnez cette option pour autoriser l'assistant à appliquer des délais d'attente légèrement plus longs, avec une seule nouvelle tentative pour les requêtes SNMP et ping.

Peu fiable
Cette description indique que le réseau ne doit pas nécessairement être fiable pour les réponses aux requêtes ping et SNMP. Sélectionnez cette option pour autoriser l'assistant à appliquer des délais d'attente plus longs et deux nouvelles tentatives pour les requêtes SNMP et les requêtes ping. Les délais d'attente plus longs sont adaptés aux réseaux moins fiables.

Révision de la configuration

Dans la fenêtre Récapitulatif de configuration, passez vos paramètres en revue. Vous pouvez également sauvegarder vos paramètres et, de manière facultative, démarrer la reconnaissance avec les paramètres que vous avez configuré.

Pour revoir vos paramètres de configuration, procédez comme suit :

1. Révisez les paramètres sur la fenêtre Récapitulatif de configuration.
   Cliquez sur n'importe quel lien pour retourner à la fenêtre concernée et modifier les paramètres nécessaires.
2. Lorsque vous êtes satisfait des paramètres de la reconnaissance, sélectionnez l'une des options suivantes.
   - Sélectionnez **Démarrer la reconnaissance** pour utiliser les paramètres de configuration de reconnaissance que vous avez spécifiés, puis cliquez sur **Terminer** pour démarrer la reconnaissance.
   - Si vous ne sélectionnez pas **Démarrer la reconnaissance**, les paramètres de reconnaissance sont sauvegardés lorsque vous cliquez sur **Terminer**.

Tâches associées:

«Surveillance de la reconnaissance de réseau à partir de l'interface graphique», à la page 173
Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

Reconnaissance du réseau à l'aide de l'interface graphique

Pour réaliser une reconnaissance personnalisée, renseignez les onglets de la page Configuration de la reconnaissance réseau. Ces onglets permettent de configurer davantage de paramètres complexes de reconnaissance que l'Assistant de configuration de la reconnaissance.

A faire : Pour sauvegarder les modifications de la configuration que vous avez apportées au cours d'une session, cliquez sur le bouton **Sauvegarder** avant de vous déconnecter, fermez la fenêtre de navigateur ou fermez l'onglet Configuration de la reconnaissance. Il est recommandé de cliquer sur **Sauvegarder** lorsque vous vous déplacez d'onglet en onglet.

Les paramètres que vous pouvez définir sur les onglets de la page Configuration de la reconnaissance réseau sont décrits dans la rubrique suivante.

La plupart des paramètres que vous pouvez définir à la page Configuration de la reconnaissance réseau sont facultatifs.

Pour exécuter la reconnaissance, vous devez indiquer au minimum les paramètres suivants :

- Unité de départ
- Noms de communauté SNMP corrects pour le réseau à reconnaître.

Si un onglet contient des données, celles-ci proviennent de configurations antérieures. Les données sont conservées dans le fichier de configuration de reconnaissance approprié.

Définir la portée de la reconnaissance

Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Vous pouvez définir autant de zones que nécessaire. Vous pouvez ajouter de nouvelles zones, modifier ou supprimer des zones existantes. Il est possible de spécifier des zones dans d'autres zones : dans une zone d'inclusion donnée, vous pouvez indiquer les périphériques ou sous-réseaux ne devant pas être détectés. Ces périphériques ne sont pas recherchés par l'outil de recherche PING ni interrogés par les agents de reconnaissance. Par exemple, vous pouvez définir une zone de portée d'inclusion constituée du sous-réseau 1.2.0.0/16 de classe B, au sein de laquelle vous pouvez spécifier une zone de portée d'exclusion de sous-réseau 1.2.3.0/24 de classe C. Et enfin, au sein de la zone de portée d'exclusion, vous pouvez spécifier une zone de portée d'inclusion 1.2.3.128/26.

Pour définir la portée de la reconnaissance :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **Portée**.
3. Pour ajouter une nouvelle zone de portée, cliquez sur **Nouveau**  . La page Propriétés de portée s'affiche.
4. Remplissez les zones comme suit, puis cliquez sur **OK**.

   Portée :

   Sélectionnez l'une des options suivantes :

Sous-réseau

Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

Vous pouvez indiquer une adresse de sous-réseau ou une adresse IP individuelle par le biais de ces zones.

- Par exemple, pour spécifier un sous-réseau de classe C IPv4 10.30.2.0, entrez `10.30.2.0/24`, où `10.30.2.0` correspond au préfixe de sous-réseau et `24` au masque de sous-réseau.
- Pour spécifier un périphérique individuel, entrez une adresse IP IPv4 et un masque de sous-réseau de valeur `32`. Par exemple, entrez `10.30.1.20/32`.
- Si vous utilisez IPv6, utilisez un masque de sous-réseau égal ou supérieur à 112 afin d'éviter des temps de reconnaissance excessifs.

Caractère générique

Utilisez l'astérisque (*) comme caractère générique.

Par exemple, pour spécifier une portée correspondant à toutes les adresses IP commençant par le préfixe de sous-réseau 10.30.200., entrez `10.30.200.*`.

Restriction : Network Manager ne prend pas en charge le format IPv6 mappé IPv4 et exige que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappé IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

Protocole

Sélectionnez le protocole Internet requis : IPv4 ou IPv6.

Action

Définissez l'intervalle de sous-réseau en tant que zone d'inclusion ou d'exclusion. Si l'intervalle de sous-réseau est une zone d'inclusion sur laquelle vous prévoyez de lancer une commande PING lors de la reconnaissance, cliquez sur **Ajout à la liste des emplacements de départ de commande PING**. Lorsque vous cliquez sur cette option, les périphériques faisant partie de la zone de portée sont ajoutés automatiquement en tant que périphériques de départ de la reconnaissance.

Restriction : L'option `Ajout à la liste des emplacements de départ de commande PING` n'est pas disponible pour les zones de portée IPv6. Cela empêche le balayage des sous-réseaux IPv6 par des commandes ping, ce qui concernerait potentiellement des milliards de périphériques. Une telle opération peut se solder par une reconnaissance inachevée.

5. Pour modifier une zone de portée existante, cliquez sur la ligne souhaitée. Dans la page Propriétés de portée, modifiez les propriétés tel que décrit à l'étape 4, à la page 23.
6. Pour supprimer une zone de portée existante, cochez la case **Sélectionner** en regard de la ou des lignes requises, puis cliquez sur **Supprimer** .

7. Cliquez sur **Sauvegarder**  .

Si vous effectuez un mappage d'adresse NAT, vous devez configurer les passerelles NAT, puis retourner à l'onglet **Portée** pour définir le mappage d'adresse.

Concepts associés:

«Définition de zones permettant de limiter la reconnaissance», à la page 4
Pour limiter la reconnaissance, vous devez définir des zones de reconnaissance. Vous pouvez les définir de différentes manières.

«Filtres», à la page 6
Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

«Portées», à la page 2
Définissez les zones du réseau (c'est-à-dire, les plages de sous-réseau) à inclure à la reconnaissance et celles à exclure. Les zones du réseau à inclure au processus de reconnaissance, ou à en exclure, sont collectivement connues sous le nom de portée de reconnaissance.

«Types de configuration», à la page 3
Network Manager propose plusieurs types de configuration.

Tâches associées:

«Traitement des incidents liés aux périphériques manquants», à la page 212
Si un périphérique qui doit figurer dans la topologie de réseau est absent, procédez comme suit pour traiter le problème.

«Configuration d'une reconnaissance multidiffusion», à la page 42
Configurez une reconnaissance multidiffusion en activant les agents obligatoires et en sectorisant la reconnaissance.

Référence associée:

«Principaux programmes stitcher de reconnaissance», à la page 409
Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

Annexe A, «Bases de données de reconnaissance», à la page 229
Il existe différentes bases de données spécialisées utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue la topologie réseau reconnue.

«Schéma de la base de données scratchTopology», à la page 321
La base de données scratchTopology est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Son nom de table de base de données complet est : scratchTopology.entityByName.

«Fichier de configuration DiscoScope.cfg», à la page 76
Le fichier de configuration DiscoScope.cfg permet de configurer la portée d'une reconnaissance.

«Référence pour la configuration de reconnaissance NAT», à la page 158
Utilisez ces instructions pas à pas pour configurer une reconnaissance NAT.

Définition de plusieurs zones d'inclusion

Vous pouvez définir plusieurs zones d'inclusion dans la table scope.zones.

Dans l'exemple suivant, trois zones d'inclusion distinctes sont définies au sein d'une unique insertion.

```
insert into scope.zones
(
    m_Protocol,
    m_Action,
    m_Zones
)
values
(
        1,
        1,
        [
              {
                                    m_Subnet="172.16.1.0",
                                    m_NetMask=24
              },
              {
                        m_Subnet="172.16.2.*"
              },
              {
                                    m_Subnet="172.16.3.0",
                                    m_NetMask=255.255.255.0
              }
        ]
);
```

L'exemple ci-dessus définit trois zones d'inclusion IP différentes, chacune utilisant une syntaxe distincte pour définir le masque de sous-réseau. Network Manager reconnaît :

- Toute unité du sous-réseau 172.16.1.0 (avec un masque de sous-réseau de 24, c'est-à-dire 24 bits activés et 8 bits désactivés, ce qui implique un masque de réseau de 255.255.255.0).
- Toute unité dont l'adresse IP commence par "172.16.2", c'est-à-dire toute unité du sous-réseau 172.16.2.0 disposant du masque 255.255.255.0.
- Toute unité du sous-réseau 172.16.3.0 disposant du masque 255.255.255.0.

Concepts associés:

«Définition de zones permettant de limiter la reconnaissance», à la page 4
Pour limiter la reconnaissance, vous devez définir des zones de reconnaissance. Vous pouvez les définir de différentes manières.

Emplacement de la reconnaissance

Pour définir l'emplacement de la reconnaissance, fournissez les points de départ à partir desquels rechercher des périphériques.

Pour exécuter la reconnaissance, vous devez indiquer au minimum les paramètres suivants :

- Unité de départ
- Noms de communauté SNMP corrects pour le réseau à reconnaître.

Utilisez les méthodes suivantes pour définir l'emplacement de la reconnaissance :

Outil de recherche Ping
: Définissez l'emplacement de l'outil de recherche Ping à l'aide d'un périphérique ou d'une adresse de sous-réseau à laquelle l'outil de recherche

peut commencer à chercher des périphériques. Vous pouvez indiquer des emplacements de départ pour l'outil de recherche Ping et enregistrer ces emplacements. Vous pouvez choisir d'activer ou non l'outil de recherche Ping pour la reconnaissance.

Outil de recherche File
Définissez l'emplacement de l'outil de recherche de fichiers en utilisant un fichier texte sur les hôtes Network Manager pour lesquels vous disposez d'un accès en lecture. Ce fichier doit être un fichier texte structuré contenant les emplacements sous la forme d'adresses IP et de noms d'unité dans des colonnes. En règle générale, vous utilisez un fichier qui existe déjà sur l'hôte Network Manager. Cependant, si vous souhaitez créer un fichier pour contenir les emplacements, vous devez écrire les droits d'accès pour le répertoire dans lequel vous souhaitez stocker le fichier.

Il existe également un mécanisme permettant de déclencher une reconnaissance partielle en fonction de la réception d'une interruption. Cette opération est exécutée par le plug-in Disco sur la Passerelle d'événements. Pour plus d'informations sur le plug-in Disco, voir *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Lors de l'exécution d'une reconnaissance IPv6, vérifiez que les conditions suivantes sont respectées :

- Assurez-vous qu'il existe au moins un périphérique de départ IPv6 dans chaque portée IPv6.
- Si vous spécifiez un sous-réseau IPv6 comme valeur de départ, vérifiez que le sous-réseau est petit en indiquant une valeur haute pour le masque de réseau.

Par défaut, les outils de recherche Ping et File sont désactivés.

Pour définir l'emplacement de la reconnaissance :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **Valeur de départ**.
3. Facultatif : Pour désactiver l'outil de recherche Ping ou File décochez les cases **Utiliser l'outil de recherche Ping lors de la reconnaissance** ou **Utiliser l'outil de recherche de fichiers lors de la reconnaissance** .
4. Ajouter ou modifier un emplacement ping :
   - Pour ajouter un nouvel emplacement ping, cliquez sur **Nouveau**  .
   - Pour modifier un emplacement ping existant, cliquez sur l'entrée souhaitée dans la liste.

   La page Propriétés d'emplacement ping s'affiche.
5. Remplissez les zones comme suit, puis cliquez sur **OK**.

   Emplacement de départ :
   Sélectionnez l'une des options suivantes :

   IP Entrez une adresse IP.

   Sous-réseau
   Indiquez un sous-réseau et entrez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

Restriction : Network Manager ne prend pas en charge le format IPv6 mappé IPv4 et exige que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappé IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

Délai d'attente
Définissez, en millisecondes, le temps d'attente d'une réponse après le lancement d'une commande PING sur une adresse, avant dépassement du délai.

Nouvelles tentatives
Indiquez le nombre de fois qu'une recherche PING peut être relancée sur un périphérique.

6. Pour supprimer un emplacement ping existant, cochez la case **Sélectionner** en regard de la ligne requise, puis cliquez sur **Supprimer** .
7. Ajouter ou modifier un emplacement file :
   - Pour ajouter un nouvel emplacement file à l'outil de recherche de fichiers, cliquez sur **Nouveau** .
   - Pour modifier un emplacement file existant, cliquez sur l'entrée souhaitée dans la liste.

   La page Propriétés d'emplacement file s'affiche.
8. Remplissez les zones comme suit, puis cliquez sur **OK**.

   Nom du fichier
   Indiquez le chemin du fichier sur le poste de travail hôte qui contient les données de départ de reconnaissance.

   Délimiteur
   Définit le délimiteur de colonne. Utilisez une expression régulière si nécessaire. Par exemple, si les colonnes Nom et IP sont séparées par une ou plusieurs tabulations, insérez `[ espace_tab ]+`, où *espace_tab* représente le caractère de tabulation réel. Pour insérer ce caractère de tabulation, créez une tabulation dans un éditeur de texte, copiez la tabulation et collez-la dans la zone.

   Colonne Nom
   Entrez le numéro de la colonne contenant les noms des périphériques de départ de reconnaissance.

   Colonne IP
   Entrez le numéro de la colonne qui contient les adresses IP des périphériques de départ de reconnaissance.
9. Pour supprimer un emplacement file existant, cochez la case **Sélectionner** en regard de la ligne requise, puis cliquez sur **Supprimer** .
10. Cliquez sur **Sauvegarder** .

Vous pouvez également définir un emplacement pour une reconnaissance à l'aide de l'*outil de recherche Collector*. L'outil de recherche Collector récupère les données topologiques auprès d'un EMS. Les données topologiques sont collectées par les collecteurs EMS, qui sont des modules logiciel qui récupèrent les données topologiques contenues dans une base de données EMS, les convertissement au

format XML et les transfèrent vers Network Manager IP Edition pour les assembler dans la topologie. Vous devez définir l'emplacement de l'outil de recherche Collector pour activer Network Manager IP Edition afin de trouver des collecteurs EMS.

Référence associée:

«Fichier de configuration DiscoPingFinderSeeds.cfg», à la page 72
Le fichier de configuration DiscoPingFinderSeeds.cfg permet de définir l'emplacement de l'outil de recherche Ping et de restreindre la détection des unités.

«Fichier de configuration DiscoCollectorFinderSeeds.cfg», à la page 67
Le fichier de configuration `DiscoCollectorFinderSeeds.cfg` définit la façon dont les données topologiques sont acquises depuis les collecteurs Element Management System (EMS) lors de la reconnaissance.

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

Tailles des masques de sous-réseau IPv6

Des milliards de périphériques sont susceptibles d'être la cible d'une commande PING au sein d'un seul sous-réseau IPv6. Pour garantir que la reconnaissance aboutisse, vous devez spécifier un masque de sous-réseau suffisamment large si vous indiquez un sous-réseau IPv6 comme emplacement de départ de la commande PING.

Le tableau suivant fournit des exemples de tailles de masques de sous-réseau IPv6 configurées dans des emplacements de départ de commandes PING ainsi que l'estimation correspondante du temps requis pour lancer des commandes PING sur les périphériques du sous-réseau. Les estimations de durées sont basées sur un espacement des commandes PING de 100 ms. Ce tableau montre qu'il est préférable de limiter la taille des masques de sous-réseau IPv6 dans vos emplacements de départ de sous-réseau.

Tableau 1. Délais de réponse à des commandes PING pour les masques de sous-réseau IPv6

Taille du masque de sous-réseau IPv6	Nombre d'adresses IPv6 dans le sous-réseau	Durée de lancement d'une commande PING pour le sous-réseau
120	256	26 secondes
112	65536	1 heure 48 minutes
100	268 millions	Environ 8 ans 1/2

L'estimation de la durée indiquée dans le tableau fait référence à la durée nécessaire pour lancer des commandes PING sur tous les emplacements de départ d'un emplacement de départ de sous-réseau spécifié pour l'outil de recherche Ping. La reconnaissance durerait plus longtemps, car des commandes PING doivent être lancées sur beaucoup plus de périphériques au sein de la portée de la reconnaissance.

Configuration de l'accès aux unités

Indiquez les noms de communauté SNMP et les informations d'accès Telnet pour permettre aux auxiliaires et à l'interrogation Network Manager d'accéder aux unités sur votre réseau.

Notez les informations suivantes sur l'auxiliaire SNMP et l'auxiliaire Telnet :

Auxiliaire SNMP
Vous devez indiquer les noms de communauté SNMP pour l'auxiliaire SNMP et les opérations d'interrogation afin d'accéder aux unités de votre réseau. Il se peut que vous deviez entrer un nom de communauté plusieurs fois. Par exemple, une fois pour SNMPv1, une fois pour NMPv2, et une fois pour SNMPv3.

Auxiliaire Telnet
Entrez les invites appropriées des unités, l'ID de connexion et le mot de passe pour l'auxiliaire Telnet et les agents de reconnaissance utilisant Telnet. Vous pouvez configurer des propriétés d'accès via Telnet privilégiées. Le mode d'accès privilégié permet l'exécution de certaines commandes, ce qui peut modifier la configuration du périphérique. Par défaut, lorsque la reconnaissance accède au périphérique à l'aide de Telnet, l'accès est accordé en mode utilisateur. Ce mode autorise uniquement l'exécution de commandes de base, telles les commandes affichant l'état du système. Ce mode d'accès par défaut est une fonction de sécurité destinée à empêcher la reconnaissance d'apporter toute modification à la configuration d'un périphérique sans un changement explicite vers le mode privilégié.

Les noms de communauté et les données d'accès Telnet peuvent être *globaux*, ce qui signifie que la reconnaissance essaye d'utiliser le nom de communauté pour chaque périphérique rencontré, ou bien limités à des sous-réseaux spécifiques (c'est-à-dire utilisés uniquement sur des périphériques faisant partie d'un sous-réseau spécifique) ou même limités à des périphériques spécifiques. La spécification de noms de communauté et de données d'accès Telnet par sous-réseau permet une reconnaissance plus efficace et plus rapide. En général, plus les données d'identification sont spécifiques, plus vite celles-ci seront découvertes lors de la reconnaissance.

Remarque : La vitesse de la reconnaissance liée aux paramètres de nom de communauté dans l'interface graphique affecte uniquement les reconnaissances initiales. Une fois que Network Manager a identifié les noms de communauté corrects, il stocke ces informations dans la base de données relationnelle NCMONITOR. Les reconnaissances effectuées ultérieurement recherchent les noms de communauté SNMP et autres informations d'accès aux périphériques SNMP associés dans cette base de données.

Pour exécuter la reconnaissance, vous devez indiquer au minimum les paramètres suivants :

- Unité de départ
- Noms de communauté SNMP corrects pour le réseau à reconnaître.

Vous pouvez également 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. Pour plus d'informations, voir *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Lors de la reconnaissance de périphériques utilisant SNMPv3, le contexte de réseau local virtuel (VLAN) doit être ajouté aux commutateurs Cisco du groupe de vues de chaque réseau local virtuel.

Pour configurer l'accès aux unités :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **Mots de passe**.
3. Pour ajouter un nouveau nom de communauté SNMP, cliquez sur **Nouveau**  . La page Propriétés des mots de passe SNMP s'affiche.
4. Renseignez les zones comme suit, puis cliquez sur **OK** :

   Nom de communauté
   Entrez un nom. Lorsque vous sauvegardez le nom de communauté, celui-ci est chiffré, mais la valeur affichée dans l'interface graphique n'est jamais chiffrée. Pour une reconnaissance rapide, classez les chaînes SNMP par fréquence, en commençant par la chaîne la plus courante.

   Restriction : Il est recommandé de ne pas utiliser le caractère @ dans les noms de communauté. L'utilisation de ce symbole dans un nom de communauté peut causer des problèmes de connexion aux périphériques au moment de la reconnaissance.

   Appliquer à
   La reconnaissance se termine plus rapidement si vous spécifiez la portée correcte des noms de communauté. Sélectionnez une des options suivantes :

   Toutes les unités
   Sélectionnez cette option si le nom de communauté est global.

   Adresse IP
   Sélectionnez cette option si le nom de communauté est spécifique à une adresse IP et entrez l'adresse IP.

   Sous-réseau
   Sélectionnez cette option si le nom de communauté est spécifique à un sous-réseau. Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

   Version SNMP
   Indiquez la version du protocole SNMP de cette communauté SNMP. Si vous indiquez `SNMP V3`, renseignez les zones supplémentaires suivantes :

   Nom de sécurité
   Entrez un nom.

   Niveau
   Indiquez le niveau d'authentification et de confidentialité requis.

   NoAuthNoPriv,
   Sélectionnez cette option pour les communautés SNMP qui ne possèdent pas de clé d'authentification ou de clé privée. Dans ce cas, il n'est pas nécessaire d'indiquer de mot de passe.

AuthNoPriv
Sélectionnez cette option pour les communautés SNMP qui possèdent une clé d'authentification mais pas de clé privée. Indiquez ensuite un mot de passe dans la zone **Mot de passe d'authentification**.

AuthPriv
Sélectionnez cette option pour les communautés SNMP qui possèdent à la fois une clé d'authentification et une clé privée. Indiquez ensuite les mots de passe dans les zones **Mot de passe d'authentification** et **Mot de passe privé**.

Type d'auto.
Indiquez le type de chiffrement pour le mot de passe d'authentification.

Restriction : L'option de chiffrement MD5 n'est pas disponible si vous exécutez une installation FIPS 140–2 de Network Manager.

Type Priv
Indiquez le type de chiffrement pour le mot de passe de confidentialité.

Restriction : L'option de chiffrement DES n'est pas disponible si vous exécutez une installation FIPS 140–2 de Network Manager.

Port SNMP
Indiquez le port requis.

Délai d'attente
Définissez, en millisecondes, le temps d'attente d'une réponse avant dépassement du délai.

Nouvelles tentatives
Indiquez le nombre de fois que l'auxiliaire SNMP et les opérations d'interrogation tentent d'accéder à un périphérique.

5. Cliquez sur **Déplacer vers le haut**  et **Déplacer vers le bas**  pour agencer les noms de communauté SNMP. Placez les noms le plus fréquemment utilisés au début de la liste.
6. Cliquez sur **Sauvegarder**.
7. Pour ajouter des informations d'accès Telnet, cliquez sur **Nouveau**. 
La page Propriétés des mots de passe SNMP s'affiche.
8. Renseignez les zones comme suit :

Appliquer à
Sélectionnez l'une des options suivantes :

Toutes les unités
Sélectionnez cette option si les données s'appliquent globalement.

Adresse IP
Sélectionnez cette option si la chaîne de caractères est spécifique à un périphérique et entrez l'adresse IP du périphérique.

Sous-réseau
Sélectionnez cette option si la chaîne de caractères est spécifique à un sous-réseau. Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

Invite de nom d'utilisateur
Entrez le message d'invite que vous voulez afficher lors de la connexion. Si vous ne connaissez pas le format exact de l'invite, utilisez une expression régulière.

Nom d'utilisateur
Entrez le nom d'utilisateur.

Invite de mot de passe
Entrez le message d'invite que vous voulez afficher lorsque le mot de passe est requis au moment de la connexion. Si vous ne connaissez pas le format exact de l'invite, utilisez une expression régulière.

Mot de passe
Entrez le mot de passe.

Invite de console
Entrez le message d'invite qui s'affichera lors de la connexion. Si vous ne connaissez pas le format exact de l'invite, utilisez une expression régulière.

Port d'accès
Indiquez le port sur lequel l'auxiliaire Telnet et les agents de reconnaissance tentent d'accéder aux périphériques.

Délai d'attente
Définissez, en millisecondes, le temps d'attente d'une réponse avant dépassement du délai.

Utiliser SSH
Sélectionnez cette option pour configurer l'auxiliaire Telnet afin d'utiliser le programme Secure Shell (SSH).

9. Facultatif : Pour configurer les propriétés du mode d'accès privilégié via Telnet :
   a. Cliquez sur **Avancé**. La page Propriétés du mode d'accès privilégié via Telnet s'affiche.
   b. Renseignez les zones comme suit, puis cliquez sur **OK** :

      Commande
      Tapez la commande nécessaire pour passer au mode d'accès Telnet privilégié. Cette commande est généralement `enable`.

      Invite de mot de passe
      Entrez le message d'invite que vous voulez afficher lorsque le mot de passe est requis au moment de la connexion. Si vous ne connaissez pas le format exact de l'invite, utilisez une expression régulière.

      Mot de passe
      Entrez le mot de passe requis pour le mode privilégié.

      Invite de console
      Entrez le message d'invite qui s'affichera lors de la connexion. Si vous ne connaissez pas le format exact de l'invite, utilisez une expression régulière.

Commandes nécessitant le mode :

Spécifie les commandes que vous voulez rendre accessible depuis un mode privilégié. Pour ajouter de nouvelles commandes, cliquez sur **Nouveau...** et entrez la commande dans la zone **Commande privée**. Les commandes suivantes sont nécessaires pour utiliser le mode `activer` :

- **`afficher exécuter`**
- **`afficher table-adresse-mac`**
- **`afficher conversion d'adresses réseau`**

10. Cliquez sur **OK**. Cliquez sur **Sauvegarder**  .

Lorsque vous sauvegardez les paramètres de mot de passe Telnet, les mots de passe suivants sont automatiquement chiffrés :

- Mot de passe Telnet
- Mot de passe du mode privilégié Telnet (si indiqué)

Lorsque vous sauvegardez les paramètres de mot de passe, les mots de passe suivants sont automatiquement chiffrés :

- Nom de communauté SNMP
- Mot de passe d'authentification SNMP
- Mot de passe privé SNMP

Si nécessaire, modifiez les paramètres de chiffrement SNMP et Telnet. Par exemple, vous pouvez modifier le fichier de clés de chiffrement ou désactiver le chiffrement.

Tâches associées:

«Activation de l'agent StandardMPLSTE», à la page 151
Pour reconnaître des tunnels MPLS TE, vous devez activer l'agent StandardMPLSTE et ajouter les noms de communauté SNMP appropriés.

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

«Connectivité de la couche réseau de couche 3», à la page 381
Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

Activation des agents

Vous devez activer les agents appropriés pour la reconnaissance que vous souhaitez réaliser. Vous pouvez indiquer des agents pour une reconnaissance complète ou une reconnaissance partielle.

Vous pouvez augmenter la vitesse d'une reconnaissance partielle en sélectionnant uniquement les agents essentiels à la reconnaissance des nouveaux périphériques ou des périphériques modifiés. Il est possible d'exécuter une reconnaissance partielle si vous savez que de nouveaux périphériques ont été ajoutés au réseau ou que des ingénieurs ont travaillé sur un périphérique et ont ajouté ou supprimé des composants sur ce périphérique.

Remarque : Plus le nombre d'agents exécutés est élevé, plus la quantité de données extraites du réseau est importante et plus la reconnaissance est lente.

Pour activer les agents :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. En fonction de vos exigences, cliquez sur l'un des onglets suivants :

Onglet	Description
Agents de reconnaissance complète	Sélectionnez des agents de cet onglet pour exécuter une reconnaissance complète.
Agents de reconnaissance partielle	Sélectionnez des agents de cet onglet pour exécuter une reconnaissance partielle. **Remarque :** Le bouton **Réinitialiser** de la fenêtre Agents de reconnaissance partielle définit les agents partiels afin qu'ils correspondent aux paramètres définis dans la fenêtre Agents de reconnaissance complète.

   La Liste des agents apparaît, affichant tous les agents de reconnaissance disponibles pour l'option de reconnaissance sélectionnée.
3. Cochez les cases situées en regard des agents requis. Pour obtenir la description d'un agent, sélectionnez son nom.

   Pour sélectionner tous les agents requis pour une reconnaissance de niveau 3, cochez la case **Couche 3**. Pour sélectionner tous les agents requis pour une reconnaissance de niveau 2 et 3, cochez la case **Reconnaissance complète de niveau 2 et de niveau 3**.
4. Cliquez sur **Sauvegarder**  . Si vous avez sélectionné une combinaison d'agents non valide ou une combinaison pouvant aboutir à une reconnaissance inefficace, un avertissement s'affiche.
5. Le cas échéant, suivez les étapes affichées dans l'avertissement :
   - Si vous avez sélectionné un agent devant être exécuté avec un ou plusieurs autres agents, l'avertissement indique que les agents supplémentaires seront sélectionnés. Cliquez sur **OK** pour sélectionner les agents ou sur **Annuler**.
   - Si vous avez sélectionné un agent ne pouvant être exécuté avec un ou plusieurs autres agents, l'avertissement indique que les agents redondants seront automatiquement désélectionnés. Cliquez sur **OK** pour désélectionner l'agent recommandé ou sur **Annuler**.

Tâches associées:

«Activation des agents de reconnaissance des collecteurs», à la page 138
Par défaut, les agents de reconnaissance des collecteurs ne sont pas activés. Vous devez les activer si vous exécutez une reconnaissance qui inclut une reconnaissance basée sur les collecteurs.

«Configuration d'agents MPLS», à la page 143
Lors de la configuration d'une reconnaissance MPLS, vous devez activer un ou plusieurs agents MPLS. Vous pouvez également résoudre la difficulté posée par les adresses IP en double dans différents VPN en configurant l'agent AsAgent.

Référence associée:

Annexe C, «Agents de reconnaissance», à la page 367
Ces informations permettent à la sélection d'agents de reconnaissance d'être exécutée comme appartenant à votre reconnaissance.

Définition des filtres de reconnaissance

Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

Un filtre est constitué d'une ou plusieurs conditions. Les conditions de filtre sont définies en OQL (Object Query Language). Vous pouvez ajouter les types de filtres suivants :

Filtres de pré-reconnaissance
Les filtres de pré-reconnaissance empêchent d'interroger les périphériques reconnus sur leurs informations de connectivité.

Filtres de post-reconnaissance
Les filtres de post-reconnaissance empêchent les périphériques reconnus d'être transmis à MODEL.

Remarque : Pour vous assurer que des alertes ne soient pas émises pour des interfaces exclues par le filtre de post-reconnaissance, vous devez définir la variable `RaiseAlertsForUnknownInterfaces`. Pour ce faire, procédez comme suit :

1. Modifiez le fichier de configuration `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Ajoutez la ligne suivante au fichier :
   ```
   update config.properties set RaiseAlertsForUnknownInterfaces = 1;
   ```

Les étapes d'ajout, d'édition et de suppression des filtres sont identiques pour les deux types.

Pour définir les filtres de reconnaissance :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **Filtres**.
3. Pour utiliser un filtre dans la reconnaissance, sélectionnez un filtre dans la liste **Filtres disponibles** et cliquez sur **Ajouter**. Le filtre est ajouté dans la zone **Filtre de pré-reconnaissance sélectionné** ou **Filtre de post-reconnaissance sélectionné**, selon le type de filtre.
4. Pour supprimer un filtre, sélectionnez un filtre de la liste **Filtres disponibles** et cliquez sur **Supprimer**.

5. Pour ajouter un nouveau filtre ou éditer un filtre existant, cliquez sur **Bibliothèque de filtres**. La page Bibliothèque de filtres s'affiche.
6. Ajouter ou éditer le filtre comme suit :

Action	Instructions
Ajouter un nouveau filtre	Cliquez sur **Ajouter** et saisissez le nom requis dans la zone **Nom**.
Editer un filtre existant	Sélectionnez le filtre requis dans la liste.

7. Dans l'**Onglet général**, créez les conditions de filtre comme suit :
   a. Sélectionnez la zone requise et la valeur de comparaison.
   b. Saisissez la valeur de comparaison avec la zone sélectionnée. Voir «Modèle de filtre» pour exemple.
   c. Cliquez sur **Ajouter une ligne**  ou sur **Supprimer cette ligne**  pour ajouter ou supprimer des lignes.
   d. Sélectionnez **Tous** pour combiner plusieurs conditions dans une relation AND ou **N'importe lequel** pour combiner les conditions dans une relation OR.
   e. Cliquez sur **Sauvegarder**.
8. Facultatif : Dans l'onglet **Avancé**, saisissez les clauses WHERE SQL requises. Pour des conditions multiples, utilisez une relation AND ou OR selon les besoins. Cliquez sur **Sauvegarder**.

   Remarque : Le filtre est en fait basé sur le formatage OQL standard, bien que l'interface graphique se rapporte à la clause SQL.
9. Cliquez sur **Fermer** pour fermer la Bibliothèque de filtres, puis cliquez sur **Sauvegarder** pour sauvegarder vos paramètres de filtre.

Modèle de filtre

L'exemple suivant montre une condition de filtre pour un filtre de pré-reconnaissance :

```
m_ObjectId not like 1\.3\.6\.1\.4\.1\.2\.3\.1\.
```

Pour plus d'informations sur la syntaxe OQL, consultez *IBM Tivoli Network Manager IP Edition Language Reference*.

Concepts associés:

«Filtres», à la page 6
Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

Tâches associées:

«Traitement des incidents liés aux périphériques manquants», à la page 212
Si un périphérique qui doit figurer dans la topologie de réseau est absent, procédez comme suit pour traiter le problème.

Référence associée:

«Principaux programmes stitcher de reconnaissance», à la page 409
Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

Annexe A, «Bases de données de reconnaissance», à la page 229
Il existe différentes bases de données spécialisées utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue

la topologie réseau reconnue.

«Schéma de la base de données scratchTopology», à la page 321
La base de données scratchTopology est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Son nom de table de base de données complet est : scratchTopology.entityByName.

Valeurs de filtre disponibles

Ces informations de référence permettent de vous familiariser avec les valeurs acceptables lorsque vous définissez les filtres de reconnaissance sur la page Configuration de la reconnaissance réseau.

Valeurs de filtre de pré-reconnaissance

Lors de l'établissement d'un filtre de pré-reconnaissance, vous pouvez filtrer en fonction de n'importe quelle zone de la table Details.returns. Ces zones se présentent de la manière suivante :

m_Name

m_UniqueAddress

m_Protocol

m_ObjectId

m_Description

m_HaveAccess

m_UpdAgent

m_AddressSpace

De plus, à l'aide de l'onglet **Avancé**, vous pouvez établir des lignes de filtre à l'aide de n'importe quelle zone située au sein de la zone m_ExtraInfo.

Valeurs de filtre de post-reconnaissance

Lors de l'établissement d'un filtre de post-reconnaissance, vous pouvez filtrer en fonction de n'importe quelle zone de la table scratchTopology.entityByName. Ces zones se présentent de la manière suivante :

EntityName
Nom unique d'une entité réseau.

Address
Liste contenant une adresse pour l'objet pour les couches 1 à 7 du modèle OSI.

Description
Description sysDescr ou autre.

EntityType
Type de l'entité.

EntityOID
Classe du périphérique.

Status
Statut de l'entité.

IsActive
Indique si l'entité est active.

Contains
Entités ou autres conteneurs inclus dans cette entité.

UpwardConnections
Entités dont cette entité fait physiquement partie.

RelatedTo
Périphériques auxquels est connectée une entité.

ExtraInfo
Information supplémentaire.

De plus, à l'aide de l'onglet **Avancé**, vous pouvez établir des lignes de filtre à l'aide de n'importe quelle zone située au sein de la zone ExtraInfo.

Configuration du système de nom de domaine

Vous pouvez indiquer les méthodes utilisées par les auxiliaires DNS pour réaliser des recherches de noms de domaine.

Les auxiliaires sont des applications spécialisées qui récupèrent des informations de et concernant les périphériques réseau pour les agents de reconnaissance.

Chacune des méthodes que vous indiquez utilise l'une des trois méthodes de domaine suivantes :

Serveur DNS
Serveur du réseau dédié à la réalisation de la résolution des noms de domaine.

Fichier
Nom d'un fichier conservé sur l'hôte Network Manager, contenant les adresses IP et les noms d'hôte au format table de recherche.

Système
Système DNS local de la machine hôte Network Manager.

Conseil : Vous pouvez définir autant de méthodes que nécessaire. Vous pouvez modifier l'ordre dans lequel ces méthodes sont récupérées par l'auxiliaire DNS de sorte que la méthode pour laquelle les accès sont les plus fréquents soit récupérée en premier. Cela permet une utilisation plus efficace des ressources lors de la reconnaissance.

Pour configurer les services de nom de domaine :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur l'onglet **DNS**.
3. Ajoutez un nouvel auxiliaire DNS ou éditez un auxiliaire existant comme suit :
   - Pour ajouter un nouvel auxiliaire DNS, cliquez sur **Nouveau**  .
   - Pour éditer un auxiliaire existant, cliquez sur son nom.

   La page Propriétés des services DNS s'affiche.
4. Renseignez les zones comme suit, puis cliquez sur **OK**.

   Nom du service
   Entrez le nom de la méthode.

   Type Sélectionnez l'une des options suivantes :

Serveur DNS

Entrez l'adresse IP du serveur DNS requis. Dans la zone **Délai d'attente**, indiquez le nombre de secondes d'attente de réponse du serveur DNS avant dépassement du délai.

Fichier

Entrez le nom du fichier qui contient les informations de recherche de domaine. Indiquez l'ordre dans lequel ces informations apparaissent dans la table de recherche en sélectionnant un des boutons radios suivants :

- **Nom, puis IP**
- **IP, puis nom**

Système

Sélectionnez cette option pour utiliser le système DNS local sur le serveur Network Manager.

Suffixe de domaine

Spécifiez le suffixe à ajouter à chaque nom d'unité après que le nom ait été trouvé. Le suffixe de domaine spécifié n'est jouté que si le nom du périphérique n'en comporte pas déjà un.

Remarque : Si vous vous attendez à ce que la reconnaissance renvoie une partie ou la totalité des noms de périphériques avec les suffixes de domaine déjà présents, vous pouvez spécifier une liste des suffixes de domaine prévus. La valeur spécifiée dans la zone **Suffixe de domaine** n'est pas ajoutée aux noms d'unités renvoyés par la reconnaissance et comportant les suffixes prévus. Pour spécifier une liste de suffixes de domaine anticipés, vous devez configurer le fichier de configuration DiscoDNSHelperSchema.cfg depuis la ligne de commande.

5. Répétez les étapes 3, à la page 39 à 4, à la page 39 pour ajouter ou éditer les méthodes requises.
6. Dans la colonne **Déplacer**, cliquez sur **Déplacer vers le haut**  et **Déplacer vers le bas**  pour agencer les méthodes selon l'ordre des utilisations les plus fréquemment attendues, avec les méthodes les plus fréquemment utilisées en haut.
7. Cliquez sur **Sauvegarder**  .

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

«Fichier de configuration DiscoDNSHelperSchema.cfg», à la page 67
Le fichier de configuration DiscoDNSHelperSchema.cfg définit l'accès au système d'adressage par domaines, qui permet à la reconnaissance de rechercher des noms de domaine, en configurant l'auxiliaire DNS.

Configuration de la conversion NAT

Pour configurer une conversion NAT afin de reconnaître des environnements NAT, mappez l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associé.

Après l'activation de la conversion NAT, vous devez mapper les zones de portée de la reconnaissance aux espaces adresse NAT via l'onglet **Portée**.

Pour configurer des passerelles NAT :

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **NAT**.
3. Ajoutez une nouvelle passerelle NAT ou éditez une passerelle existante :
   - Pour ajouter une nouvelle passerelle NAT, cliquez sur **Nouveau**  .
   - Pour éditer une passerelle NAT existante, cliquez sur l'adresse IP dans la ligne requise.

   La page Passerelle de conversion d'adresses réseau s'affiche.
4. Renseignez les zones comme suit, puis cliquez sur **OK** :

   Adresse IP
   Entrez l'adresse IP publique du périphérique de passerelle de conversion d'adresses réseau.

   Espace adresse
   Entrez l'identificateur d'espace adresse à utiliser pour le domaine NAT associé.
5. Cliquez sur **Sauvegarder**  .
6. Pour activer la conversion NAT pour la reconnaissance, sélectionnez **Activer la prise en charge de la conversion d'adresses réseau (NAT)**. Cliquez sur **Sauvegarder**, puis mappez les zones de portée de la reconnaissance aux espaces adresse NAT :
   a. Cliquez sur **Portée**.
   b. Cliquez sur une zone de portée afin de l'éditer. La page Propriétés de la portée s'affiche.
   c. Dans la zone **Espace adresse**, entrez l'espace adresse NAT et cliquez sur **OK**. La zone **Espace adresse** apparaît uniquement dans les Propriétés de la portée après que l'option **Activer la prise en charge de la conversion d'adresses réseau (NAT)** ait été sélectionnée.
   d. Répétez les deux étapes précédentes pour toutes les zones de portée requises.
   e. Cliquez sur **Sauvegarder**  .

   La vue NAT Address Spaces Dynamic Distinct est créé automatiquement si **Activer la prise en charge de la conversion d'adresses réseau (NAT)** est activé. Une fois la reconnaissance terminée, utilisez Vues de réseau pour visualiser la vue réseau espaces adresse NAT.

Tâches associées:

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la

reconnaissance, ainsi que les zones que vous souhaitez exclure.

«Configuration des reconnaissances NAT», à la page 155
Configurez une reconnaissance NAT afin de reconnaître des environnements NAT en mappant l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associée.

Référence associée:

«Référence pour la configuration de reconnaissance NAT», à la page 158
Utilisez ces instructions pas à pas pour configurer une reconnaissance NAT.

Configuration d'une reconnaissance multidiffusion

Configurez une reconnaissance multidiffusion en activant les agents obligatoires et en sectorisant la reconnaissance.

Concepts associés:

«Types de configuration», à la page 3
Network Manager propose plusieurs types de configuration.

Tâches associées:

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Référence associée:

«Table scope.multicastSource», à la page 256
La table scope.multicastSource définit les routes IPM à reconnaître. Cette table est particulièrement utile si vous disposez de plusieurs sources de route IPM car cela vous permet de définir la portée de la reconnaissance multidiffusion en fonction de la source de la route IPM afin qu'elle porte sur les sources pertinentes.

«Table scope.multicastGroup», à la page 255
La table scope.multicastGroup définit quels groupes de multidiffusion reconnaître et quels détails extraire de ces groupes.

Activation des agents de multidiffusion

Pour découvrir des groupes de multidiffusion, vous devez activer les agents appropriés et ajouter les noms de communauté SNMP correspondants.

Pour activer les agents, procédez comme suit.

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur l'onglet **Agents de reconnaissance complète**. La Liste des agents apparaît, affichant tous les agents de reconnaissance disponibles pour l'option de reconnaissance sélectionnée.
3. Cliquez sur **Reconnaissance de couche 2 et 3 complète** > **Multidiffusion**.
4. Cochez la case en regard des agents que vous souhaitez activer.
   a. Activez l'agent StandardPIM pour découvrir les groupes de multidiffusion indépendants des protocoles et conformes à la MIB RFC2934 PIM.
   b. Activez l'agent StandardIPMRoute pour découvrir les réseaux de multidiffusion IP conformes à la MIB RFC2932 IPMRoute.
   c. Activez l'agent StandardIGMP pour reconnaître les groupes de multidiffusion exécutant le protocole IGMP (Internet Group Membership Protocol).
5. Cliquez sur **Sauvegarder**  .

6. Facultatif : Si vous souhaitez reconnaître des groupes de multidiffusion, activez également les agents appropriés pour les reconnaissances partielles.
7. Vérifiez que les noms de communauté SNMP sont correctement configurés pour accéder aux périphériques dans les groupes de multidiffusion.

Référence associée:

«Agents de multidiffusion», à la page 389
Les agents de multidiffusion extraient des données d'unités participant aux groupes et routes de multidiffusion.

Configuration d'une reconnaissance multidiffusion

Configurez les groupes et les sources de multidiffusion à découvrir à l'aide de l'onglet **Multidiffusion**.

Pour configurer une reconnaissance multidiffusion, procédez comme suit.

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur **Multidiffusion**.
3. Dans la section **Groupes de multidiffusion**, créez un groupe de multidiffusion ou éditez un groupe existant :
   - Pour créer un groupe à découvrir, cliquez sur **Nouveau**  .
   - Pour éditer un groupe existant, cliquez sur le nom du groupe.

   La page Propriétés du groupe de multidiffusion apparaît.
4. Définissez les propriétés de la portée à l'aide des zones suivantes :

   Nom du groupe
   Indiquez un nom pour ce groupe de multidiffusion.

   Mode PIM
   Indiquez si vous souhaitez inclure ou exclure les données PIM (Protocol Independent Multicast) dans la reconnaissance. Par défaut, les données PIM sont incluses.

   Mode de route IPM
   Indiquez si vous souhaitez inclure ou exclure les données de groupe IPM (Internet Protocol Multicast) dans la reconnaissance. Par défaut, les données de groupe IPM sont incluses.

   Mode IGMP
   Indiquez si vous souhaitez inclure ou exclure les données IGMP (Internet Group Management Protocol) dans la reconnaissance. Par défaut, les données IGMP sont incluses.

   Protocole
   Seul IPv4 est pris en charge.

   Indiquez les sous-réseaux de groupe à ajouter aux groupes de multidiffusion
   Utilisez les zones et boutons suivants pour ajouter et supprimer des sous-réseaux de groupe :

   Sous-réseau
   Entrez un sous-réseau et masque de réseau pour un sous-réseau de groupe à ajouter aux groupes de multidiffusion.

   Ajouter
   Cliquez sur **Ajouter** pour ajouter ce groupe.

Supprimer
Sélectionnez un sous-réseau de groupe dans la liste adjacente et cliquez sur **Delete** pour supprimer le groupe sélectionné.

Remarque : Les adresses de multidiffusion réservées sont exclues de la portée par défaut.

5. Cliquez sur **OK**.
6. Pour supprimer un ou plusieurs groupes, sélectionnez les groupes que vous souhaitez supprimer et cliquez sur le bouton **Supprimer**  . Pour sélectionner ou désélectionner tous les groupes, cliquez sur le bouton **Sélectionner tout**  or **Désélectionner tout**  .
7. Dans la section **Sources de multidiffusion**, créez une source de multidiffusion ou éditez une source existante.
   - Pour créer une source à découvrir, cliquez sur **Nouveau**  .
   - Pour éditer une source existante, cliquez sur le nom de la source.

   La page Propriétés de la source de multidiffusion apparaît.
8. Définissez les propriétés de la source à l'aide des zones suivantes :

Mode de route IPM
Indiquez si vous souhaitez inclure ou exclure le groupe :
- **Inconnu - utiliser la valeur par défaut**
- **Inclure une source**
- **Exclure une source**

Protocole
Seul IPv4 est pris en charge.

Indiquez les sous-réseaux de groupe à ajouter aux sources de multidiffusion
Utilisez les zones et boutons suivants pour ajouter et supprimer des sous-réseaux de groupe :

Sous-réseau
Entrez un sous-réseau et masque de réseau pour un sous-réseau de groupe à ajouter aux sources de multidiffusion.

Ajouter
Cliquez sur **Ajouter** pour ajouter ce groupe.

Supprimer
Sélectionnez un sous-réseau de groupe dans la liste adjacente et cliquez sur **Delete** pour supprimer le groupe sélectionné.

Indiquez les sous-réseaux de source à ajouter aux sources de multidiffusion
Utilisez les zones et boutons suivants pour ajouter et supprimer des sous-réseaux de groupe :

Sous-réseau
Entrez un sous-réseau et masque de réseau pour un sous-réseau de sources à ajouter aux sources de multidiffusion.

Ajouter
Cliquez sur **Ajouter** pour ajouter ce groupe.

Supprimer
Sélectionnez un sous-réseau de source dans la liste adjacente et cliquez sur **Supprimer** pour supprimer la source sélectionnée.

9. Cliquez sur **OK**.
10. Pour supprimer un ou plusieurs groupes, sélectionnez les groupes que vous souhaitez supprimer et cliquez sur le bouton Supprimer  . Pour sélectionner ou désélectionner tous les groupes, cliquez sur le bouton Sélectionner tout  or Désélectionner tout  .
11. Cliquez sur **Sauvegarder**  .

Paramètres de reconnaissance avancés

Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

Définissez les paramètres avancés à partir de l'onglet **Avancé** de la page Configuration de la reconnaissance réseau. Après les avoir définis, cliquez sur **Sauvegarder**  .

Avertissement : Ne modifiez les paramètres avancés que si vous êtes un utilisateur Network Manager expérimenté. Si vous modifiez les paramètres avancés et que la reconnaissance ne fonctionne pas comme prévu, cliquez sur le bouton **Réinitialiser** pour restaurer les paramètres par défaut.

«Configuration avancée de l'outil de recherche»
«Configuration avancée de l'outil de recherche Ping», à la page 46
«Configuration avancée de la reconnaissance», à la page 48
«Configuration avancée de l'auxiliaire Telnet», à la page 46
«Configuration avancée de l'auxiliaire SNMP», à la page 47
«Configuration avancée de l'auxiliaire DNS», à la page 48
«Configuration avancée de la reconnaissance», à la page 48

Configuration avancée de l'outil de recherche

Pour configurer les paramètres avancés de l'outil de recherche File, utilisez la zone ci-après :

Outils de recherche File simultanés
Indiquez le nombre d'unités d'exécution à utiliser par l'outil de recherche File. Chaque unité d'exécution peut traiter un fichier de départ différent simultanément. Si vous disposez de nombreux fichiers de départ et de ressources de secours sur le serveur de reconnaissance, un nombre plus important d'unités de secours peut permettre une reconnaissance plus rapide. Si vous disposez d'un seul fichier de départ, l'augmentation du nombre d'unités d'exécution n'a pas d'impact.

Configuration avancée de l'outil de recherche Ping

Pour configurer les paramètres avancés de l'outil de recherche Ping, utilisez les zones ci-après :

Outils de recherche Ping simultanés
Indiquez le nombre d'unités d'exécution à utiliser par l'outil de recherche Ping. Chaque unité d'exécution traite une insertion pingFinder.pingRules à la fois. L'augmentation du nombre d'unités d'exécution n'accélère pas un balayage unique de commande ping de grande portée, mais peut accélérer le retour d'informations de nombreuses adresses. Cependant, vous devez équilibrer la vitesse par rapport aux ressources de votre hôte et à la capacité du récepteur ping de traiter en temps voulu les réponses à la commande ping. Si le nombre d'unités d'exécution est trop élevé, le récepteur ping ne pourra pas suivre et il en résultera des échecs dus à des erreurs de commande ping et une perte de la reconnaissance de périphérique.

Des études ont montré que le nombre par défaut de 10 unités d'exécution est optimal dans la plupart des cas. Vous pouvez augmenter graduellement le nombre d'unités d'exécution, surveiller le nombre d'échecs de la commande ping et noter les économies de temps réalisées. En fonction des ressources disponibles, à un certain point, les avantages commencent à décroître au fur et à mesure que la charge des ressources augmente.

Délai d'attente par défaut
Indiquez, en millisecondes, le temps d'attente d'une réponse après le lancement d'une commande ping sur une adresse. Si vous savez que le temps d'attente du réseau est faible, un temps d'attente réduit peut permettre une reconnaissance plus rapide. Une valeur trop faible pour votre réseau peut empêcher la reconnaissance de certains périphériques.

Nombre de tentatives par défaut
Indiquez le nombre de fois qu'une recherche ping peut être relancée sur une unité suite à une commande ping initiale ayant échoué.

Durée entre les commandes ping
Spécifiez l'intervalle en millisecondes entre chaque tentative de commande PING effectuée sur les périphériques contenus dans une liste ou un sous-réseau. Si le trafic réseau résultant de la reconnaissance ne vous pose pas de problème, vous pouvez diminuer cette valeur.

Autoriser la commande ping sur la diffusion
Pour activer la commande ping sur une adresse de diffusion, cochez cette case.

Autoriser la commande ping sur la multidiffusion
Pour activer la commande ping sur une adresse de multidiffusion, cochez cette case.

Configuration avancée de l'auxiliaire Telnet

Pour définir des paramètres avancés pour l'auxiliaire Telnet, utilisez les zones suivantes :

Auxiliaires Telnet simultanés
Indiquez le nombre d'unités d'exécution à utiliser par l'auxiliaire Telnet. Si le réseau comprend de nombreux périphériques auxquels vous voulez accéder à l'aide de Telnet ou SSH, augmentez cette valeur pour obtenir une reconnaissance plus rapide. Des exemples courants de ces périphériques

sont les commutateurs Catalyst, l es périphériques MPLS et les passerelles NAT. Si vous modifiez cette valeur, vérifiez que votre système est configuré pour autoriser au moins ce nombre de sessions Telnet simultanées.

Délai d'attente par défaut
Indiquez, en millisecondes, le temps d'attente maximal pour accéder à un périphérique.

Nombre de tentatives
Indiquez le nombre de tentatives de reconnexion au périphérique suite à une tentative de connexion initiale ayant échoué.

Conseil : Vous pouvez également configurer d'autres paramètres avancés dans le fichier `DiscoTelnetHelperSchema.cfg`.

Configuration avancée de l'auxiliaire SNMP

Pour définir des paramètres avancés pour l'auxiliaire SNMP, utilisez les zones suivantes :

Auxiliaires SNMP simultanés
Indiquez le nombre d'unités d'exécution à utiliser par l'auxiliaire. Si vous disposez de nombreux périphériques avec accès SNMP et ressources de secours sur le serveur de reconnaissance, un nombre plus important d'unités de secours peut permettre une reconnaissance plus rapide. Si vous modifiez cette valeur, vérifiez que votre système est configuré pour autoriser au moins ce nombre de sessions SNMP simultanées. Cette valeur doit être supérieure au nombre d'unités d'exécution utilisées par l'agent de reconnaissance Details.

Délai d'attente
Indiquez, en millisecondes, le temps d'attente maximale pour accéder à un périphérique.

Nombre de tentatives
Indiquez le nombre de tentatives de récupération d'une ou plusieurs variables SNMP d'un périphérique suite à une tentative initiale ayant échoué.

Ralentissement GetNext
Indiquez le retard, en millisecondes, entre les requêtes GetNext SNMP. Le paramètre **`m_GetNextSlowDown`** s'applique lorsque le nombre de requêtes GETNEXT séparées émises pour récupérer une variable SNMP non scalaire dépasse la valeur du paramètre **`m_GetNextBoundary`**.

Limite GetNext
Indiquez le nombre minimal de requêtes GETNEXT à émettre lorsqu'une variable SNMP non scalaire est récupérée depuis le périphérique. Le paramètre **`m_GetNextBoundary`** s'applique avant que le retard spécifié par le paramètre **`m_GetNextSlowDown`** soit introduit.

L'auxiliaire SNMP est utilisé pour envoyer des demandes SNMP à des périphériques réseau. Pour plus d'informations sur la configuration de l'Auxiliaire SNMP, voir *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Configuration avancée de l'auxiliaire DNS

Pour définir des paramètres avancés pour l'auxiliaire DNS, utilisez les zones suivantes :

Auxiliaires DNS simultanés
Indiquez le nombre d'unités d'exécution à utiliser par l'auxiliaire. Si vous modifiez cette valeur, vérifiez que votre système est configuré pour autoriser au moins ce nombre de sessions DNS simultanées.

Délai d'attente par défaut
Indiquez, en millisecondes, le temps d'attente maximal d'une réponse depuis un périphérique.

Configuration avancée de la reconnaissance

Pour indiquez une commande de retour d'informations avancée, et plus de paramètres de reconnaissance avancés, utilisez les zones suivantes :

Activer le contrôle des retours d'informations
Indiquez si la commande de retours d'informations doit être activée. Les retours d'informations correspondent aux données renvoyées par les agents et utilisées par la reconnaissance pour rechercher d'autres unités. Parmi les exemples de données de retour d'informations, on trouve les adresses IP des voisins distants et les adresses du sous-réseau dans lequel un voisin local existe.

Pas de retour d'informations
Les retours d'informations sont désactivés pour toutes les reconnaissances et les nouvelles reconnaissances. Seuls les périphériques spécifiés dans les outils de recherche sont reconnus. Cette option garantit une réalisation des reconnaissances et des nouvelles reconnaissances la plus rapide possible. Toutefois, la topologie de réseau obtenue est incomplète si vous n'indiquez pas tous les périphériques que vous souhaitez découvrir en tant qu'emplacement de départ.

Conseil : Désactivez le retour d'informations si vous souhaitez découvrir uniquement une liste de certains périphériques. Indiquez les périphériques que vous souhaitez reconnaître en tant qu'emplacements de départ.

Retour d'informations
Les retours d'informations sont activés pour les reconnaissances complètes, les nouvelles reconnaissances complètes et les reconnaissances partielles. Cette option fournit une topologie complète dans toutes les situations, mais est celle qui prend le plus de temps.

Retour d'informations uniquement pour les reconnaissances complètes
Ce paramètre est activé par défaut. Les retours d'informations sont activés pour les reconnaissances complètes et les nouvelles reconnaissances complètes mais ils sont désactivés pour les reconnaissances partielles.

Activer la vérification de la commande ping
Indiquez si la reconnaissance doit vérifier les interfaces sur lesquelles exécuter la commande ping. Si une commande ping ne peut être lancée sur un périphérique, ce dernier n'est pas interrogé quant aux alertes.

Ne pas vérifier si une commande ping peut être lancée
Il n'est pas vérifié si une commande ping peut être lancée sur les interfaces reconnues. Les interfaces sont interrogées peu importe si une commande ping peut être lancée lors de la reconnaissance.

Vérifier si une commande ping peut être lancée
Après la reconnaissance, il est vérifié si une commande ping peut être lancée sur chaque interface reconnue. La vérification est exécutée sur la table details.returns. Il est possible d'exécuter une commande PING sur les interfaces ayant une entrée dans cette table, mais pas d'exécuter une commande PING sur celles n'ayant pas d'entrée dans cette table. Les interfaces sur lesquelles exécuter la commande ping sont marquées pour être interrogées.

Détecter le meilleur paramètre
Ce paramètre est activé par défaut. Si la commande de retour d'informations a été activée, après la reconnaissance, il est vérifié si une commande ping peut être lancée sur chaque interface reconnue. La vérification est exécutée sur la table details.returns. Il est possible d'exécuter une commande ping sur les interfaces ayant une entrée dans cette table, mais pas d'exécuter une commande ping sur celles n'ayant pas d'entrée dans cette table. Les interfaces sur lesquelles exécuter la commande ping sont marquées pour être interrogées.

Restriction : Cette option ne fonctionne que si vous sélectionnez l'une des options ci-dessous dans la liste **Activer le contrôle des retours d'information** : `Retour d'informations` ou `Retour d'informations uniquement pour les reconnaissances complètes`.

Activer 'Autoriser virtuel'
Indiquez comment la reconnaissance doit traiter les adresses IP virtuelles : [1].

Ne pas autoriser virtuel
Aucune reconnaissance d'adresses IP virtuelles.

Autoriser virtuel
Reconnaissance d'adresse IP virtuelles. Ce paramètre est activé par défaut.

Autoriser si dans scope.special
Reconnaissance d'adresses IP virtuelles uniquement si l'adresse est définie dans la table scope.special. Cette table définit les adresses IP de gestion.

Activer la modélisation des réseaux locaux virtuels
Activez ce paramètre pour modéliser les réseaux locaux virtuels dans cette reconnaissance. Si vous activez la modélisation des réseaux locaux virtuels,

1. Les unités sont généralement reconnues à l'aide des adresses IP récupérées par l'agent AssocAddress. Si un périphérique est reconnu à l'aide d'une adresse IP non récupérée par l'agent AssocAddress, cela signifie probablement qu'il s'agit d'une adresse IP non standard. Ce type d'adresse IP est appelé *adresse IP virtuelle*. Parmi les exemples d'adresses IP virtuelles, on trouve les adresses HSRP et VRRP qui sont partagées par plusieurs périphériques pour une tolérance aux pannes. D'autres exemples incluent certaines interfaces de gestion pouvant se situer sur un seul périphérique mais n'apparaissant pas dans la table IP pour des raisons de sécurité ou autres. Les adresses IP virtuelles incluent des adresses de gestion. Une adresse de gestion est une adresse IP dont l'unique rôle est de gérer le périphérique. Les adresses de gestion sont souvent situées sur un réseau distinct isolé du trafic client. Ces adresses sont définies dans la table scope.special.

vous pouvez partitionner les topologies en fonction de l'appartenance à un réseau local virtuel. La désactivation de la modélisation VLAN réduit la durée de reconnaissance.

Activer la désignation SysName
Activez ce paramètre pour désigner les dispositifs à l'aide de la valeur de la variable SNMP sysName en tant que source principale des informations de désignation. La variable sysName doit être définie et doit être unique dans le réseau. L'activation de ce paramètre n'a pas d'impact sur la durée de reconnaissance, car la variable sysName est extraite par l'agent Details par défaut.

Activer la mise en cache des tables de reconnaissance
Activez ce paramètre pour mettre en cache des données lors du processus de reconnaissance afin d'activer la reconnaissance de données si le moteur de reconnaissance, **ncp_disco**, échoue. Une reconnaissance exécutée dans ce mode est plus lente qu'une reconnaissance standard, en raison du temps supplémentaire requis pour le stockage de données sur le disque tout au long du processus de reconnaissance.

Activer la vérification de l'outil de recherche de fichiers
Activez ce paramètre pour utiliser l'outil de recherche Ping afin de vérifier l'existence des unités indiquées dans les fichiers utilisés par l'outil de recherche de fichiers. Si vous activez ce paramètre, vérifiez que l'outil de recherche Ping est activé. Activez ce paramètre si vous n'êtes pas sûr que les périphériques sont encore connectés au réseau. Par exemple, vous pouvez activer ce paramètre si votre réseau a une évolution rapide.

Activer la régénération des couches suite à une nouvelle reconnaissance
Activez ce paramètre pour régénérer les couches de la topologie suite à une nouvelle reconnaissance partielle. Si cette option est sélectionnée, la topologie est plus précise car elle affiche toutes les données de connectivité. Toutefois, il faut plus de temps pour ajouter des périphériques à la topologie.

Conseil : Etant donné que cette option allonge les temps de reconnaissance, désélectionnez-la s'il est important que les reconnaissances partielles s'exécutent le plus rapidement possible.

Activer la reconnaissance VPN MPLS basée sur RT
Ce paramètre concerne les reconnaissances MPLS. Activez ce paramètre pour afficher les dispositifs périphériques fournisseurs uniquement (reconnaissance MPLS basée sur RT).

Activer la reconnaissance d'unités associées
Par défaut, les voisins distants d'un périphérique ne sont pas reconnus, même si la reconnaissance de ce périphérique indique que les voisins distants ont changé. Les voisins distants peuvent être reconnus de nouveau lors de la nouvelle reconnaissance suivante. Activez ce paramètre si vous souhaitez modifier ce comportement par défaut et reconnaître de nouveau tout voisin distant modifié lors de la nouvelle reconnaissance de cette unité.

Conseil : Si vous souhaitez qu'une nouvelle reconnaissance partielle se produise le plus rapidement possible, désactivez cette option.

Activez la désignation d'interface ifName/ifDescr
Modifie la convention de dénomination par défaut pour l'interface reconnue. Si vous sélectionnez cette option, indiquez également la

convention de dénomination dans le programme stitcher `BuildInterfaceName.stch`. Si cette option est activée, les données des zones ifName et ifDescr de la table d'interface SNMP permettent de nommer les interfaces. Par exemple, `Fa0/0, Gi 1.0.2:0, Gigabit Ethernet 4/1`.

Conseil : Si cette option est activée, certains périphériques peuvent signaler des noms d'interface et des descriptions trop longs pour être affichés dans la topologie. Si des périphériques signalent des noms et des descriptions d'interface longs ou incorrects, désélectionnez cette option.

Activer l'inférence des PE à l'aide des données BGP sur les CE
Reconnaît les réseaux fournisseurs intervenants en tant qu'objet «tiers» sur plusieurs réseaux fonctionnant sur un réseau fournisseur. Par exemple, il s'agit de réseaux VPN d'entreprise sur un réseau principal MPLS fournisseur. Sélectionnez cette option si vous souhaitez relier tous vos réseaux dans une seule topologie et réaliser une analyse des causes sur vos réseaux.

Fix Pack 4 Si vous souhaitez utiliser la fonction de reconnaissance interdomaine, désactivez cette option. Si cette option est sélectionnée, des erreurs sont générées lors de la reconnaissance interdomaine.

Cette option déduit l'existence de périphériques PE (provider-edge) inaccessibles à l'aide de données BGP sur les périphériques CE (customer-edge) qui pointent sur les périphériques PE. Afin de reconnaître ces données BGP, les agents de reconnaissance BGP doivent être activés. Pour spécifier les périphériques PE déduits qui sont valides, remplissez la table scope.inferMPLSPEs en utilisant des entrées de portée de format standard, comme dans la table scope.zones. Une fois remplie, la table scope.inferMPLSPEs définit les adresses IP affichées sur les périphériques CE considérés comme des périphériques PE valides.

Activer l'inférence des routeurs CE MPLS sur /30 sous-réseaux
Génère les événements affectés par un service sur les réseaux VPN clients. Sélectionnez cette option si vous êtes un fournisseur de services sans accès aux routeurs CE clients.

Concepts associés:

«A propos des événements affectés par le service», à la page 142
Une alerte d'événement affecté par le service (SAE) avertit les opérateurs qu'un service client critique a été affecté par un ou plusieurs événements de réseau.

«Option permettant de reformer les couches topologiques», à la page 364
Vous pouvez indiquer si vous voulez reformer les couches topologiques à la suite d'une nouvelle reconnaissance partielle. A l'aide de cette option, vous pouvez augmenter la vitesse de la nouvelle reconnaissance partielle.

Tâches associées:

«Configuration de la méthode de reconnaissance MPLS», à la page 146
Vous pouvez configurer une reconnaissance MPLS de deux manières : reconnaissance basée cible de routage (RT) ou reconnaissance basée LSP (Label Switched Path).

«Induction de l'existence de routeurs CE», à la page 148
Vous pouvez induire l'existence des routeurs CE de vos clients en créant des spécifications dans les options de configuration de la reconnaissance avancée de l'interface graphique de la configuration de la reconnaissance.

Référence associée:

«Principaux programmes stitcher de reconnaissance», à la page 409
Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

«Base de données de reprise après incident», à la page 330
La reprise après incident avec la base de données de reprise ne doit pas être confondue avec la reprise d'agent et d'outil de recherche, configurée directement à partir de la table disco.config. Si elle est sélectionnée, la reprise d'agent et d'outil de recherche fonctionne que la reprise avec la base de données de reprise soit implémentée ou pas.

«Table disco.config», à la page 230
La table config configure le fonctionnement général du processus de reconnaissance.

«Table inferMPLSPEs», à la page 253
Utilisez la table inferMPLSPE lorsque vous déduisez des périphériques PE (provider-edge) inaccessibles à l'aide de données BGP sur les périphériques CE (customer-edge). Cette table vous permet, le cas échéant, de spécifier les zones à traiter pour déterminer quels sont les périphériques PE déduits qui sont valides.

Démarrage d'une reconnaissance

Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

Avant de lancer la reconnaissance, modifiez tous les paramètres de configuration de reconnaissance requis.

Vous pouvez démarrer les types de reconnaissance suivants :

Reconnaissance
Exécutez une reconnaissance complète pour découvrir votre réseau pour la première fois ou pour régénérer la topologie de réseau si vous savez que le réseau a changé.

Reconnaissance partielle
Exécutez une reconnaissance partielle si vous savez que les modifications apportées à votre réseau se limitent à quelques périphériques. Vous devez configurer la sectorisation et les emplacements de départ de chaque reconnaissance partielle. Si la relation de ces périphériques qui se trouvent dans la portée des des périphériques voisins a changé, les périphériques voisins peuvent également être reconnus. Si la reconnaissance partielle doit reconnaître une grande quantité de périphériques en fonction des informations de connectivité, une reconnaissance complète est démarrée.

Remarque : Si vous arrêtez une reconnaissance, vous devez alors effectuer une reconnaissance complète pour pouvoir exécuter une reconnaissance partielle.

Pour démarrer une reconnaissance, procédez comme suit.

1. Cliquez sur **Reconnaissance** > **Etat de la reconnaissance réseau**.
2. Sélectionnez le domaine dans lequel vous souhaitez exécuter une reconnaissance, dans le menu **Domaine**. Vous pouvez commencer à saisir le nom du domaine et les domaines concordants apparaissent sous la zone **Domaine**.
3. Démarrez une reconnaissance complète ou partielle :
   - Pour démarrer une reconnaissance complète, cliquez sur **Démarrer la reconnaissance**  uniquement. La reconnaissance commence.

Important : Dans Network Manager V3.9, il n'est plus nécessaire de cliquer sur **Arrêter la reconnaissance**, puis sur **Démarrer la reconnaissance** pour sélectionner les modifications de la configuration de reconnaissance. Network Manager sélectionne les modifications de configuration de reconnaissance lorsque vous cliquez sur **Démarrer la reconnaissance**  .

- Pour démarrer une reconnaissance partielle, cliquez sur la flèche vers le bas en regard du bouton **Démarrer la reconnaissance**  et sélectionnez **Démarrer la reconnaissance partielle** dans le menu (si une reconnaissance complète n'a pas été exécutée depuis le dernier démarrage du moteur de reconnaissance **`ncp_disco`**, l'option permettant de démarrer une reconnaissance partielle est grisée). La fenêtre Reconnaissance partielle s'affiche. Indiquez les adresses IP et les sous-réseaux contenant les périphériques devant être reconnus :

a. Sous **Reconnaissance partielle**, sélectionnez les noeuds et sous-réseaux requis.
b. Pour ajouter un nouveau sous-réseau ou noeud, cliquez sur **Nouveau.**
c. Renseignez les zones comme suit, puis cliquez sur **OK** :

Nouvelle reconnaissance
Sélectionnez l'une des options suivantes :

Adresse IP
Entrez l'adresse IP requise.

Sous-réseau
Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

d. Pour ajouter de nouvelles zones de portée, cliquez sur **Portée**.
e. Pour ajouter une nouvelle zone de portée de reconnaissance, cliquez sur **Nouveau**  . Pour éditer une zone de portée existante, cliquez sur l'entrée requise dans la liste.
f. Renseignez les zones comme suit, puis cliquez sur **OK** :

Portée :
Sélectionnez l'une des options suivantes :

Sous-réseau
Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

Vous pouvez indiquer une adresse de sous-réseau ou une adresse IP individuelle par le biais de ces zones.

- Par exemple, pour spécifier un sous-réseau de classe C IPv4 10.30.2.0, entrez `10.30.2.0/24`, où `10.30.2.0` correspond au préfixe de sous-réseau et `24` au masque de sous-réseau.
- Pour spécifier un périphérique individuel, entrez une adresse IP IPv4 et un masque de sous-réseau de valeur `32`. Par exemple, entrez `10.30.1.20/32`.

- Si vous utilisez IPv6, utilisez un masque de sous-réseau égal ou supérieur à 112 afin d'éviter des temps de reconnaissance excessifs.

Caractère générique
Utilisez l'astérisque (*) comme caractère générique.

Par exemple, pour spécifier une portée correspondant à toutes les adresses IP commençant par le préfixe de sous-réseau 10.30.200., entrez `10.30.200.*`.

Restriction : Network Manager ne prend pas en charge le format IPv6 mappé IPv4 et exige que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappé IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

Protocole
Sélectionnez le protocole Internet requis : IPv4 ou IPv6.

Action
Définissez l'intervalle de sous-réseau en tant que zone d'inclusion ou d'exclusion. Si l'intervalle de sous-réseau est une zone d'inclusion sur laquelle vous prévoyez de lancer une commande PING lors de la reconnaissance, cliquez sur **Ajout à la liste des emplacements de départ de commande PING**. Lorsque vous cliquez sur cette option, les périphériques faisant partie de la zone de portée sont ajoutés automatiquement en tant que périphériques de départ de la reconnaissance.

Restriction : L'option `Ajout à la liste des emplacements de départ de commande PING` n'est pas disponible pour les zones de portée IPv6. Cela empêche le balayage des sous-réseaux IPv6 par des commandes ping, ce qui concernerait potentiellement des milliards de périphériques. Une telle opération peut se solder par une reconnaissance inachevée.

g. Cliquez sur **OK**, puis sur **Accéder**. Lorsqu'une reconnaissance complète ou partielle s'exécute, le bouton **Démarrer la reconnaissance** est désactivé  .

4. Pour arrêter une reconnaissance, cliquez sur **Arrêter la reconnaissance**  . L'arrêt de la reconnaissance nécessite un bref laps de temps pendant lequel les boutons **Démarrer la reconnaissance** et **Arrêter la reconnaissance** sont désactivés. Si vous arrêtez une reconnaissance, vous ne pouvez pas ensuite effectuer de reconnaissance partielle tant que vous n'avez pas exécuté une reconnaissance complète.

Remarque : Lorsque vous arrêtez une reconnaissance, le cache de la reconnaissance est perdu. C'est la raison pour laquelle vous devez attendre la fin de la reconnaissance complète suivante avant de lancer une reconnaissance partielle. Il est possible de configurer le moteur de reconnaissance de sorte qu'il sauvegarde le cache de reconnaissance au cours de l'exécution de la reconnaissance, ce qui vous permet de procéder à une reconnaissance partielle juste après l'arrêt manuel d'une reconnaissance. Vous pouvez configurer le

moteur de reconnaissance de sorte qu'il sauvegarde le cache de reconnaissance en cliquant sur **Activation du cache des tables de reconnaissance** dans l'onglet **Avancé**.

Vous pouvez surveiller la progression de la reconnaissance pendant son exécution.

Une fois la reconnaissance terminée, le bouton **Démarrer la reconnaissance** est activé et vous pouvez exécuter une autre reconnaissance complète ou partielle à tout moment. Si le plug-in Disco Passerelle d'événements est activé, une nouvelle reconnaissance peut être déclenchée automatiquement lorsqu'un événement de réinitialisation (ID événement `NmosSnmpReboot` déclenché par la règle d'interrogation rebootDetection) est reçu.

Concepts associés:

«A propos des types de reconnaissance», à la page 1
Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Tâches associées:

«Surveillance de la reconnaissance de réseau à partir de l'interface graphique», à la page 173
Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

«Démarrage de reconnaissance partielle à partir de l'interface graphique», à la page 203
Le démarrage d'une reconnaissance partielle implique de définir un emplacement de départ et des portées.

«Traitement des incidents liés à une reconnaissance en veille», à la page 213
Si vous démarrez la reconnaissance et qu'après quelques minutes aucun périphérique n'a été découvert, exécutez les étapes de traitement des incidents suivantes.

Schémas et tables pour les paramètres de reconnaissance de l'interface graphique

Ces informations de référence indiquent dans quels schémas et tables les paramètres entrés dans les onglets de la page Configuration de la reconnaissance réseau sont sauvegardés.

Le tableau suivant indique les tables dans lesquelles les paramètres entrés dans chaque onglet de la page Configuration de la reconnaissance réseau sont sauvegardés. Dans ces tables, *NOM_DOMAINE* représente le nom des domaines réseau de votre déploiement, par exemple NCOMS.

Tableau 2. Schémas et tables sur lesquels les paramètres de reconnaissance sont mappés

Onglet Configuration de la reconnaissance réseau	**Description**	**Nom du schéma ou de la table**
Portée	Zones du réseau (c'est-à-dire intervalles de sous-réseau) que vous voulez inclure dans la reconnaissance et celles que vous voulez exclure.	`DiscoScope.`*`NOM_DOMAINE`*`.cfg`
Valeur de départ	L'emplacement à partir duquel commence la reconnaissance des périphériques. Il peut s'agir d'une ou plusieurs adresses IP ou adresses de sous-réseaux. Pour définir cet emplacement, les *outils de recherche* suivants sont utilisés : Ping et File.	Outil de recherche : `DiscoPingFinderSeeds.`*`DOMAIN_NAME`*`.cfg` Outil de recherche File : `DiscoFileFinderParseRules.`*`NOM_DOMAINE`*`.cfg`
Agents de reconnaissance complète et **Agents de nouvelle reconnaissance partielle**	Les agents de reconnaissance à utiliser pour examiner la connectivité des périphériques. Des agents par défaut sont fournis pour le type de reconnaissance que vous voulez effectuer, par exemple une reconnaissance de niveau 2 ou 3. Vous pouvez sélectionner un ensemble d'agents différent pour des reconnaissances complètes et partielles. Les agents varient en fonction des variations des informations de connectivité des technologies matérielles sur le réseau.	`DiscoAgents.`*`NOM_DOMAINE`*`.cfg`
Accès à l'unité	Noms de communauté SNMP et paramètres Telnet utilisés par Network Manager pour interroger les périphériques qui utilisent SNMP et Telnet.	Noms de communauté SNMP : `SnmpStackSecurityInfo.cfg` Accès Telnet : `TelnetStackPasswords.cfg`
Filtres	Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres de pré-reconnaissance empêchent d'interroger les périphériques reconnus sur leurs informations de connectivité. Les filtres de post-reconnaissance empêchent les périphériques reconnus d'être transmis à MODEL.	`DiscoSchema.`*`NOM_DOMAINE`*`.cfg`
DNS	Accédez aux services de nom de domaine utilisés pour effectuer des recherches de noms de domaines.	`DiscoDNSHelperSchema.cfg`
Conversion d'adresses réseau (NAT)	Données fournissant des mappages de reconnaissance entre les données d'espace adresse et les adresses IP réelles des périphériques pour faciliter les reconnaissances ultérieures.	`DiscoSchema.`*`NOM_DOMAINE`*`.cfg`
Multidiffusion	Groupes et sources de multidiffusion utilisés par le moteur de reconnaissance pour configurer les portées de multidiffusion.	`DiscoScope.`*`NOM_DOMAINE`*`.cfg`

Tableau 2. Schémas et tables sur lesquels les paramètres de reconnaissance sont mappés (suite)

Onglet Configuration de la reconnaissance réseau	Description	Nom du schéma ou de la table
Avancé	Les paramètres avancés contrôlent les fonctions de la reconnaissance tels que les processus simultanés et les délais d'attente. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en équilibrant la vitesse avec la charge du serveur. Généralement, des résultats de reconnaissance plus rapides utilisent une plus grande quantité de mémoire sur le serveur.	`DiscoSchema.`*`NOM_DOMAINE`*`.cfg`

Reconnaissance du réseau à l'aide de l'interface de ligne de commande

Les utilisateurs expérimentés peuvent configurer et suivre une reconnaissance à l'aide de fichiers de configuration et de requêtes de base de données.

1. Créez les paramètres de la reconnaissance en modifiant les fichiers de configuration. Dans ces fichiers, créez ou éditez des insertions dans les bases de données du processus de reconnaissance. Vous pouvez par exemple définir les agents et les programmes stitcher utilisés dans la reconnaissance.
2. Indiquez des informations supplémentaires que les agents de reconnaissance doivent extraire à partir des périphériques réseau.
3. Configurez la gestion des interruptions afin que les alertes SNMP soient transmises à des paires hôte/socket. Cette tâche est requise si avez installé plusieurs produits de gestion de réseau sur un seul hôte, ou si vous devez déboguer des alertes.

Démarrez ou planifiez la reconnaissance si nécessaire. Si le processus **ncp_disco** est déjà en cours d'exécution, il analyse périodiquement les répertoires contenant les fichiers de configuration et charge les définitions d'agent de reconnaissance ou les programmes stitcher nouveaux ou modifiés.

Tâches associées:

«Surveillance de la reconnaissance à partir de la ligne de commande», à la page 179

Lorsque le processus **ncp_disco** svous pouvez surveiller l'avancement de la reconnaissance en utilisant le fournisseur de services OQL, le processus **ncp_oql**, pour interroger les bases de données de reconnaissance et déterminer ce qui se passe à tout instant.

Fichiers de configuration de la reconnaissance

Dans les fichiers de configuration de la reconnaissance, définissez les paramètres de la reconnaissance en créant ou en éditant les instructions INSERT dans les bases de données des processus de reconnaissance.

Tous les schémas des bases de données de reconnaissance sont dans le fichier de configuration `DiscoSchema.cfg`. Ce fichier ne contient pas d'instruction INSERT. N'éditez pas ce fichier.

Le tableau suivant répertorie les fichiers de configuration qui peuvent être édités pour configurer une reconnaissance. Le paramétrage que vous pouvez effectuer dans certains fichiers est équivalent aux paramètres de l'interface de configuration de la reconnaissance. Le tableau indique dans quel onglet de l'interface graphique les paramètres peuvent être définis. D'autres paramétrages ne peuvent être effectués que dans les fichiers de configuration.

Tableau 3. Fichiers de configuration de la reconnaissances éditables par l'utilisateur

Tâche de configuration de la reconnaissance	**Fichier de configuration**	**Onglet Interface graphique**
Définir la portée de la reconnaissance		
Définition des zones d'inclusion et d'exclusion	DiscoScope.cfg	**Portée**
Ignorer la portée de la reconnaissance	DiscoScope.cfg	**Portée**
Emplacement de la reconnaissance		
Valeur de départ	DiscoPingFinderSeeds.cfg	**Valeur de départ**
Exécution de plusieurs instances d'un outil de recherche		
Configuration du lancement de commandes PING sur des adresses de diffusion et de multidiffusion	DiscoPingFinderSeeds.cfg	**Avancé**
Utilisation de l'outil de recherche File	DiscoFileFinderParseRules.cfg	**Valeur de départ**
Activation de la vérification de périphérique de l'outil de recherche File	DiscoConfig.cfg	**Avancé**
Activation de la vérification de la commande PING	DiscoConfig.cfg	
Utilisation et configuration de l'outil de recherche Collector	DiscoCollectorFinderSeeds.cfg	
SNMP		
Configuration des noms de communauté et mots de passe SNMP	SnmpStackSecurityInfo.cfg	**Mots de passe**

Tableau 3. Fichiers de configuration de la reconnaissances éditables par l'utilisateur (suite)

Tâche de configuration de la reconnaissance	**Fichier de configuration**	**Onglet Interface graphique**
Configuration de l'auxiliaire SNMP	DiscoSnmpHelperSchema.cfg	**Avancé**
Substitution des paramètres de l'auxiliaire SNMP pour des périphériques et sous-réseaux spécifiques		
Telnet		
Configuration de l'accès Telnet à des périphériques réseau	TelnetStackPasswords.cfg	**Mots de passe**
Configuration de l'auxiliaire Telnet	DiscoTelnetHelperSchema.cfg	**Avancé**
Configuration d'une reconnaissance contextuelle	DiscoConfig.cfg	
Agents		
Activation et désactivation d'agents de reconnaissance	DiscoAgents.cfg	**Agents de reconnaissance complète Agents de nouvelle reconnaissance partielle**
Périphériques de filtrage envoyés aux agents	Fichiers de définition des agents de reconnaissance	**Filtres**
Filtrage des données de topologie renvoyées par un agent	Fichiers de définition des agents de reconnaissance	
Filtrage des données de topologie renvoyées par tous les agents	DiscoAgentReturns.filter	
Modification du nombre d'unités d'exécution utilisées par un agent	DiscoAgents.cfg	
Activation de l'opération à unités d'exécutions multiples pour des agents Perl	Fichiers de définition des agents de reconnaissance	
Activation et désactivation de la correspondance partielle	Fichier de définition de l'agent IpForwardingTable.agnt (pour des unités modernes utilisant RFC2096) Fichier de définition de l'agent IpRoutingTable.agnt (pour des unités anciennes utilisant RFC1213).	
Restriction de la reconnaissance		
Restriction de la détection de périphériques	DiscoScope.cfg DiscoPingFinderSeeds.cfg	**Portée Valeur de départ**

Tableau 3. Fichiers de configuration de la reconnaissances éditables par l'utilisateur (suite)

Tâche de configuration de la reconnaissance	**Fichier de configuration**	**Onglet Interface graphique**
Restriction de l'interrogation de périphériques	DiscoScope.cfg	
Restriction de l'instanciation de périphériques		
Configuration des services d'auxiliaire DNS	DiscoDNSHelperSchema.cfg	**DNS**
Configuration d'une reconnaissance de conversion NAT	agent NATTextFileAgent agent NATGateway	**Conversion d'adresses réseau (NAT)**
Spécification de la configuration avancée		
Configuration avancée de l'outil de recherche File Configuration avancée de l'outil de recherche PING Configuration avancée de l'auxiliaire DNS Configuration avancée de l'auxiliaire SNMP Configuration avancée de l'auxiliaire Telnet	DiscoFileFinderParseRules.cfg DiscoPingFinderSeeds.cfg DiscoDNSHelperSchema.cfg DiscoSnmpHelperSchema.cfg DiscoTelnetHelperSchema.cfg **Remarque :** En tant qu'utilisateur expérimenté, vous pouvez spécifier des paramètres de configuration avancés dans les fichiers de configuration disponibles dans l'onglet Avancé de l'interface graphique.	**Avancé**

Fichiers de définition des agents de reconnaissance

Les fichiers de définition des agents de reconnaissance définissent le fonctionnement des agents de reconnaissance.

Filtrages d'unités à l'aide de fichiers de définition

Remarque : Network Manager tue tous les agents de reconnaissance à la fin de l'étape 3 de la collecte de données. Cette action garantit que la reconnaissance suivante redémarre les agents et les force à relire leurs fichiers de configuration au début d'une reconnaissance, en détectant les modifications apportées aux fichiers de configuration.

Vous pouvez appliquer un filtre à un agent de reconnaissance en modifiant le filtre des unités prises en charge dans la section DiscoAgentSupportedDevices( ); du fichier de définition de l'agent ($NCHOME/precision/disco/agents/*.agnt). Tous les agents de reconnaissance disposent d'un fichier de définition dans ce répertoire, qu'ils soient textuels ou précompilés.

Le filtre des unités prises en charge est un filtre destiné aux attributs de la table agentTemplate.despatch.

La section DiscoAgentSupportedDevices( ); accepte des tests de comparaison OQL complets utilisant des opérateurs comme `like`, `<` , `>` , `=` , and `<>`. Des informations

détaillées concernant les tests de comparaison dans OQL sont disponibles dans *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*.

Conseil : La modification des fichiers de définition des agents peut introduire des erreurs d'analyse. Pour vérifier que votre agent ne contient pas d'erreurs d'analyse, exécutez-le en mode débogage et examinez la sortie de débogage.

Exemple : reconnaissance d'unités qui utilisent CDP

L'agent de reconnaissance CDP, défini dans le fichier de l'agent $NCHOME/precision/disco/agents/CDP.agnt, doit être activé avant que la reconnaissance ne puisse détecter les périphériques qui utilisent CDP. Activez l'agent CDP en définissant la valeur de la colonne m_Valid sur 1, comme indiqué dans l'insertion suivante.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
values
(
                'CDP', 1, 7, 0, 3
);
```

Exemple : filtrage d'unités envoyées pour l'agent CDP

L'exemple suivant présente la section DiscoAgentSupportedDevices(); du fichier de définition d'agent `CDP.agnt`. Seules les entités réseau qui correspondent à l'ID objet indiqué sont traitées par l'agent CDP (i.e. les périphériques qui utilisent le protocole de reconnaissance Cisco Discovery). L'agent CDP ne traite pas les périphériques dont l'ID objet est 1.3.6.1.4.1.9.1.226.

```
DiscoAgentSupportedDevices
(
            " (
                        ( m_ObjectId like '1\.3\.6\.1\.4\.1\.9\..*' )
                        AND
                                                                ( m_ObjectId <> '1.3.6.1.4.1.9.1.226' )
            ) "
);
```

Exemple : utilisation de caractères génériques dans les filtres d'unités

L'exemple suivant présente l'utilisation de caractères génériques dans la colonne de l'adresse IP. L'agent n'accepte que les périphériques dont l'adresse IP commence par 10.10.2.

```
DiscoAgentSupportedDevices
(
                                    " ( m_UniqueAddress like '10\.10\.2\..*' ) "
);
```

Exemple : utilisation de plusieurs conditions de filtres d'unités

L'exemple suivant présente la combinaison de plusieurs conditions de filtre. L'agent accepte uniquement les périphériques dont l'ID objet est ID 1.3.6.1.4.1.9.5.7, dont l'adresse IP commence par 10.10. et qui ne portent pas le nom clandestine.

```
DiscoAgentSupportedDevices
(
            "(
                                                    ( m_ObjectId = '1.3.6.1.4.1.9.5.7' )
                    AND
                    ( m_UniqueAddress like '^10\.10\..*' )
                    AND
                                                    ( m_Name not like '.*[cC]landestin[eE].*' )
            )"
);
```

Activation de l'opération à unités d'exécutions multiples pour les agents de reconnaissance Perl

Le nombre d'unités d'exécution utilisées par les agents de reconnaissance est défini dans le fichier de configuration `DiscoAgents.cfg`. L'opération à unités d'exécutions multiples doit être activée sur les agents Perl pour que le paramétrage du fichier de configuration `DiscoAgents.cfg` ait un effet.

Pour activer l'opération à unités d'exécutions multiples sur un agent de reconnaissance Perl, ajoutez la ligne suivante à son fichier de définition :

```
DiscoAgentDefaultThreads( 10 );
```

L'insertion ci-dessus spécifie que l'agent utilise 10 unités d'exécution par défaut. Si vous définissez un nombre différent d'unités d'exécution dans le fichier de configuration `DiscoAgents.cfg`, cette valeur remplace la valeur dans le fichier de définition de l'agent.

Restriction : Nombre de modules complémentaires CPAN fréquemment utilisés avec Perl ne sont pas compatibles avec des unités d'exécution multiples. Les agents de reconnaissance Perl qui utilisent ces modules devront peut-être être limités à une unité d'exécution unique.

Filtrage des données topologiques retournées par un agent de reconnaissance

Pour filtrer des données topologiques retournées par un agent unique, définissez un filtre dans le fichier d'agent (.agnt) adéquat.

Exemple : exclusion des interfaces câble-modem de l'abonné

Le fichier d'agent CMTS.agnt extrait les données des modems câbles connectés à une unité de services de terminaison de modem câble. Cet exemple décrit un filtre ajouté au fichier CMTS.agnt qui filtre les interfaces des modems câbles d'inscription des données topologiques retournées pour les périphériques CMTS. Le filtre exemple se présente comme suit :

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
                        m_LocalNbr->m_IfType = 229
            )"
      }
};
```

Exemple : définition de plusieurs filtres topologiques

L'exemple suivant présente comment définir plusieurs filtres de données topologiques dans un agent. Le premier filtre indique qu'à chaque fois qu'un enregistrement est retourné et que la valeur ifIndex de l'interface est 4, les zones the m_Name, m_HaveAccess, m_LocalNbr->m_SubnetMask, and m_RemoteNbr->m_RemoteNbrPhysAddr doivent être supprimées de l'enregistrement. Le deuxième filtre supprime les enregistrements retournés lorsque la valeur ifIndex de l'interface est 5.

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
                        m_LocalNbr->m_IfIndex = 4
            )"
            DiscoDeleteFields {
```

```
                "m_Name",
                "m_HaveAccess",
                                "m_LocalNbr->m_SubnetMask",
                                "m_RemoteNbr->m_RemoteNbrPhysAddr",
        }
    }
    DiscoReturnsFilter
    {
        "(
                    m_LocalNbr->m_IfIndex = 5
        )"
    }
};
```

Exemple : désactivation de la correspondance partielle

L'exemple suivant peur être ajouté au fichier de définition IpForwardingTable.agnt pour garantir que si un routeur dont la valeur m_ObjectId est '1.3.6.1.4.1.9.1.48' est reconnu (c'est-à-dire un routeur Cisco 7505), la correspondance partielle n'est tentée que si le routeur exécute IOS version 12.2 ou supérieure.

```
DiscoRouterPartialMatchRestrictions
(
                                    "(m_ObjectId='1.3.6.1.4.1.9.1.48', m_OSVersion>='12.2',
                                    m_MibVar='sysDescr')"
);
```

Exemple : désactivation de la correspondance partielle à l'aide de caractères génériques

L'exemple suivant garantit que la correspondance partielle n'est pas utilisée sur les routeurs Cisco 2600, les routeurs Cisco 7505 qui exécutent une version d'IOS antérieure à la version 12.2 et les routeurs Redstone.

```
DiscoRouterPartialMatchRestrictions
(
                                    "(m_ObjectId='1.3.6.1.4.1.9.1.209'),
                                    (m_ObjectId='1.3.6.1.4.1.9.1.48', m_OSVersion>='12.2',
                                      m_MibVar='sysDescr'),
            (m_ObjectId like '1\.3\.6\.1\.4\.1\.2773\..*')"
);
```

Référence associée:

«Table disco.agents», à la page 243
La table Agents indique les agents de reconnaissance utilisés par DISCO. Chaque agent à exécuter doit avoir une insertion dans la table disco.agents du fichier de configuration DiscoAgents.cfg qui l'active (définissez m_Valid=1). Si m_Valid=0, l'agent n'est pas exécuté.

«Base de données agentTemplate», à la page 334
Les bases de données de chaque agent de reconnaissance sont basées sur un modèle appelé base de données agentTemplate.

Fichier de configuration Agents.cfg

Le fichier de configuration DiscoAgents.cfg définit les agents exécutés pendant une reconnaissance.

Table de base de données utilisée

Le fichier de configuration DiscoAgents.cfg peut être utilisé pour configurer des insertions dans la table disco.agents de la base de données.

Exemple : activation de l'agent de reconnaisance IpRoutingTable

L'exemple suivant active l'agent de reconnaissance IpRoutingTable.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
```

```
    )
values
(
                'IpRoutingTable', 1, 0, 0, 2
    );
```

Exemple : activation des agents Details et Associated Address

Les insertions OQL exemples suivantes activent les agents Details et Associated Address.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
                'Details', 1, 0, 0, 1
    );

insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
                'AssocAddress', 1, 0, 0, 2
    );
```

Exemple : activation de l'agent ARP Cache

L'agent ARP Cache participe à la résolution d'adresses MAC vers des adresses IP lors de la reconnaissance. Vous devez activer cet agent pour une reconnaissance Couche 2. L'exemple suivant indique comment s'assurer que l'agent ARP Cache s'exécute lors d'une reconnaissance.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
values
(
                'ArpCache', 1, 0, 0, 2
);
```

Exemple: désactivation des agents StandardSwitch et SuperStack3ComSwitch

L'exemple suivant désactive les agents de reconnaissance StandardSwitch et SuperStack3ComSwitch.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
values
(
                'StandardSwitch', 0, 1, 1, 3
    );

insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
    )
```

```
values
(
                'SuperStack3ComSwitch', 0, 1, 1, 3
    );
```

Exemple : modification du nombre d'unités d'exécution utilisées par l'agent de reconnaissance IpRoutingTable

L'exemple suivant définit à 50 le nombre d'unités d'exécution utilisées par l'agent de reconnaissance IpRoutingTable. L'augmentation du nombre d'unités d'exécution utilisées par un agent permet à ce dernier de traiter davantage d'unités simultanément et peut accélérer la reconnaissance. Toutefois, l'augmentation du nombre d'unités d'exécution utilisées par un agent exploite également davantage de mémoire.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass,
m_IsIndirect, m_Precedence, m_NumThreads
    )
values
(
                'IpRoutingTable', 1, 0, 0, 2, 50
    );
```

Exemple : modification du nombre d'unités d'exécution utilisées par l'agent de reconnaissance Perl NMAPScan

L'exemple suivant définit à 50 le nombre d'unités d'exécution utilisées par l'agent de reconnaissance Perl NMAPScan. Pour définir le nombre d'unités d'exécution utilisées par un agent de reconnaissance Perl, vous devez d'abord activer plusieurs unités d'exécution pour cet agent dans le fichier de définition de l'agent de reconnaissance.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass,
m_IsIndirect, m_Precedence, m_NumThreads
    )
values
(
                'NMAPScan', 1, 0, 0, 2, 50
    );
```

Référence associée:

«Table disco.agents», à la page 243
La table Agents indique les agents de reconnaissance utilisés par DISCO. Chaque agent à exécuter doit avoir une insertion dans la table disco.agents du fichier de configuration DiscoAgents.cfg qui l'active (définissez m_Valid=1). Si m_Valid=0, l'agent n'est pas exécuté.

Fichier de configuration DiscoAgentReturns.filter

Le fichier de configuration DiscoAgentReturns.filter vous permet d'appliquer un filtre de données topologiques aux données renvoyées par tous les agents de reconnaissance.

Filtrage des données topologiques renvoyées par tous les agents

Le fichier de configuration $NCHOME/precision/disco/agents/DiscoAgentReturns.filter filtre les mêmes données topologiques de toutes les tables returns des agents. La syntaxe utilisée dans ce fichier est identique à celle utilisée dans les filtres de topologie des fichiers de définition des agents de reconnaissance.

Exemple : exclusion des interfaces câble-modem de l'abonné

L'exemple suivant exclut les interfaces câble modem de l'abonné des données topologiques :

```
DiscoAgentReturnsFilterList
{
      DiscoReturnsFilter
      {
            "(
                        m_LocalNbr->m_IfType = 229
            )"
      }
};
```

Concepts associés:

«Agents», à la page 367
Les agents de reconnaissance extraient des informations sur les périphériques du réseau. Ils signalent également l'existence de nouveaux périphériques lors de la recherche de connectivité des périphériques. Ils sont utilisés pour des tâches spécialisées. Par exemple, l'agent de reconnaissance du Cache ARP remplit la base de données du serveur auxiliaire à l'aide d'adresses IP en vue du mappage des adresses MAC.

Fichier de configuration DiscoARPHelperSchema.cfg

Le fichier de configuration DiscoARPHelperSchema.cfg accomplit la résolution de l'adresse IP en adresse MAC.

Base de données utilisée

Le fichier de configuration DiscoARPHelperSchema.cfg définit des insertions dans la table de base de données ARPHelper.configuration.

Exemple: configuration de l'auxiliaire ARP

L'exemple suivant d'insertion configure l'auxiliaire ARP de sorte qu'il n'utilise qu'une seule unité d'exécution.

```
insert into ARPHelper.configuration
(
        m_NumThreads
)
values
(
        1
);
```

Référence associée:

«Base de données de l'auxiliaire ARP», à la page 304
La base de données de l'auxiliaire ARP est définie par le fichier de configuration DiscoARPHelperSchema.cfg. Le nom qualifié complet de sa table est ARPHelper.configuration.

Fichier de configuration DiscoCollectorFinderSeeds.cfg

Le fichier de configuration `DiscoCollectorFinderSeeds.cfg` définit la façon dont les données topologiques sont acquises depuis les collecteurs Element Management System (EMS) lors de la reconnaissance.

Base de données utilisée

Le fichier de configuration `DiscoCollectorFinderSeeds.cfg` définit des insertions dans la base de données collectorFinder.

Notez qu'un autre fichier est associé à la base de données collectorFinder, le fichier DiscoCollectorFinderSchema.cfg, mais vous ne devriez pas avoir à le modifier.

Exemple : configuration d'un collecteur unique

L'exemple suivant définit l'emplacement d'un collecteur s'exécutant sur le serveur local. Cet exemple n'indique pas de valeurs pour les autres zones, telles quem_DataSourceId et m_NumRetries. Elles prennent automatiquement les valeurs par défaut de la table de configuration.

```
insert into collectorFinder.collectorRules
                ( m_Port)
values
                ( 8082 );
```

Référence associée:

«Base de données collectorFinder», à la page 278
La base de données collectorFinder définit le fonctionnement des outils de recherche Collector.

Fichier de configuration DiscoDNSHelperSchema.cfg

Le fichier de configuration DiscoDNSHelperSchema.cfg définit l'accès au système d'adressage par domaines, qui permet à la reconnaissance de rechercher des noms de domaine, en configurant l'auxiliaire DNS.

Tables de base de données utilisées

Le fichier de configuration DiscoDNSHelperSchema.cfg peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- DNSHelper.configuration
- DNShelper.methods

Exemple : configuration de l'auxiliaire DNS

L'exemple d'insertion suivant configure l'auxiliaire DNS en utilisant les informations des tables de base de données DNSHelper.configuration et DNShelper.methods. L'exemple présente des insertions dans la table de base de données DNShelper.methods correspondant aux types de méthode suivants :

- 0 - Système
- 1 - DNS utilisant `m_NameDomain` pour spécifier un suffixe de domaine à ajouter à tous les noms d'unités reconnues.

- 1 - DNS utilisant m_NameDomainList pour spécifier une liste de suffixes de domaines prévus.
- 2 - Fichier

```
insert into DNSHelper.configuration
(
     m_NumThreads, m_MethodList, m_TimeOut
)
values
(
     1, ['HostsFile'] , 5
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType
)
values
(
     "HostService", 0
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_NameServerAddr, m_TimeOut, m_NameDomain
)
values
(
     "abcIPv6DNS", 1, "2222:15f8:106:203:250:4ff:fee8:6d75", 3,
"tivlab.raleigh.ibm.com"
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_TimeOut, m_NameServerAddr, m_NameDomainList
)
values
(
     "defIPv6DNS", 1, 3, "2222:15f8:106:203:250:4ff:fee8:6d75",
     ['uk.eu.org',
     'fra.eu.org',
     'de.eu.org',
     'it.eu.org',
     'sp.eu.org']
);

insert into DNSHelper.methods
(
     m_MethodName, m_MethodType, m_FileName, m_FileOrder
)
values
(
     'HostsFile', 2, 'etc/hosts', 1
);
```

Référence associée:

«Base de données de l'auxiliaire DNS», à la page 305
La base de données de l'auxiliaire DNS est définie par le fichier de configuration DiscoDNSHelperSchema.cfg; Ses noms de table de base de données complets sont : DNSHelper.configuration; DNShelper.methods.

Fichier de configuration DiscoFileFinderParseRules.cfg

Le fichier DiscoFileFinderParseRules.cfg file peut être utilisé pour indiquer les fichiers à analyser pour une liste d'adresses IP d'unités du réseau.

Tables de base de données utilisées

Ce fichier de configuration peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- fileFinder.parseRules
- fileFinder.configuration

Notez qu'un autre fichier de configuration est associé à la base de données fileFinder, le fichier DiscoFileFinderSchema.cfg, mais vous ne devriez pas avoir à le modifier.

Exemple : configuration de l'outil de recherche de fichiers de sorte qu'il utilise 5 unités d'exécution

L'exemple suivant d'insertion configure l'outil de recherche de fichiers pour utiliser cinq unités d'exécution.

```
insert into fileFinder.configuration
      ( m_NumThreads )
values
      ( 5 );
```

Exemple: configuration de l'outil de recherche de fichiers pour analyser /var/tmp/logged_hosts

L'exemple de configuration suivant demande à l'outil de recherche de fichiers d'analyser un fichier texte exemple, logged_hosts, sauvegardé dans le répertoire /var/tmp directory. Le contenu du fichier exemple est présenté ci-dessous.

```
vi /var/tmp/logged_hosts

172.16.1.21   dharma              04:02:08
172.16.1.201  phoenix             19:07:08
172.16.1.25   lnd-sun-tivoli   15:10:00
172.16.2.33   ranger              19:07:07
~
"/var/tmp/logged_hosts" [Read only] 4 lines, 190 characters
```

Les trois colonnes de ce fichier exemple contiennent respectivement une adresse IP, le nom du périphérique et une valeur de temps. Les colonnes sont séparées par des espaces, qui peuvent être constitués de plusieurs tabulations, d'espaces ou d'une combinaison des deux. Vous pouvez utiliser l'outil de recherche de fichiers pour analyser ce fichier texte exemple en utilisant une insertion similaire à celle de l'exemple.

```
insert into fileFinder.parseRules
(
                        m_FileName, m_Delimiter, m_ColDefs
)
values
(
        "/var/tmp/logged_hosts",
                "[     ]+",
        [
            {
                                m_VarName="m_UniqueAddress",
                m_ColNum=1
```

```
            },
            {
                                m_VarName="m_Name",
                m_ColNum=2
            }
        ]
);
```

L'insertion ci-dessus indique que :

- Le chemin complet et le nom du fichier sont /var/tmp/logged_hosts.
- Le délimiteur du fichier source est un espace. Le délimiteur de colonne est indiqué dans l'insertion à l'aide d'une expression régulière simple, [*tab space*]+ . Vous devez appuyer sur les touches **tabulation** et **espace** plutôt que d'entrer \t pour représenter le caractère de tabulation.
- La première colonne contient des adresses IP et doit être mappée à la colonne m_UniqueAddress de la table finders.returns.
- La deuxième colonne contient des adresses IP et doit être mappée à la colonne m_Name de la table finders.returns.

Etant donné que la troisième colonne du fichier texte exemple n'est pas pertinente, elle n'a pas été mappée à une colonne de finders.returns et est ignorée par l'outil de recherche de fichiers lors de la reconnaissance.

Exemple : configuration de l'outil de recherche de fichiers pour analyser le fichier /etc/hosts

L'insertion suivante demande à l'outil de recherche de fichiers de :

- Analyser /etc/hosts.
- Traiter les espaces en tant que séparateurs de données.
- Utiliser les définitions de colonnes suivantes :
  - m_UniqueAddress pour la première colonne
  - m_Name for the second column

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/etc/hosts",
                        "[     ]",
            [
                {
                                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                },
                {
                                    m_VarName="m_Name",
                    m_ColNum=2
                }
            ]
);
```

Exemple : configuration de l'outil de recherche de fichiers pour analyser /etc/defaultrouter

L'insertion suivante demande à l'outil de recherche de fichiers de :

- Analyser /etc/defaultrouter.
- Traiter une ou plusieurs occurrences d'espaces en tant que séparateurs de données.
- Utiliser m_UniqueAddress en tant que définition de colonne.

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/etc/defaultrouter",
                        "[     ]+",
            [
                {
                                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                }
            ]
);
```

Référence associée:

«Base de données fileFinder», à la page 282
La base de données fileFinder définit le fonctionnement de l'outil de recherche File.

Fichier de configuration DiscoHelperServerSchema.cfg

Le fichier de configuration `DiscoHelperServerSchema.cfg` définit le contenu des diverses bases de données auxiliaires.

Tables de base de données utilisées

Ce fichier de configuration peut être utilisé pour configurer des insertions dans les tables de base de données suivantes.

Tables de base de données de l'auxiliaire ARP :

- ARPHelper.ARPHelperTable
- ARPHelper.ARPHelperConfig

Tables de base de données de l'auxiliaire DNS :

- DNSHelper.DNSHelperTable
- DNSHelper.DNSHelperConfig

Tables de base de données de l'auxiliaire Ping :

- PingHelper.PingHelperTable
- PingHelper.PingHelperConfig

Tables de base de données de l'auxiliaire SNMP :

- SnmpHelper.SnmpHelperTable
- SnmpHelper.SnmpHelperConfig

Tables de base de données de l'auxiliaire Telnet :

- TelnetHelper.TelnetHelperTable

- TelnetHelper.TelnetHelperConfig

Tables de base de données de l'auxiliaire XMLRPC :

- XmlRpcHelper.XmlRpcHelperTable
- XmlRpcHelper.XmlRpcHelperConfig

Référence associée:

«Bases de données du serveur auxiliaire», à la page 287
Lorsque le serveur auxiliaire démarre, il crée une base de données pour chaque auxiliaire qui doit être exécuté.

Fichier de configuration DiscoPingFinderSeeds.cfg

Le fichier de configuration DiscoPingFinderSeeds.cfg permet de définir l'emplacement de l'outil de recherche Ping et de restreindre la détection des unités.

Tables de base de données utilisées

Le fichier de configuration DiscoPingFinderSeeds.cfg peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- pingFinder.pingRules
- pingFinder.scope

Notez qu'un autre fichier de configuration est associé à la base de données pingFinder, le fichier DiscoPingFinderSchema.cfg, mais vous ne devriez pas avoir à le modifier.

Remarque : Si vous définissez l'emplacement d'une reconnaissance IPv6, sachez que des milliards de périphériques sont susceptibles d'être la cible d'une commande PING au sein d'un seul sous-réseau IPv6. Pour garantir que la reconnaissance aboutisse, vous devez spécifier un masque de sous-réseau suffisamment large si vous indiquez un sous-réseau IPv6 comme emplacement de départ de la commande PING.

Exemple : définition de l'emplacement de l'outil de recherche Ping avec une seule adresse d'unité.

L'exemple d'insertion suivant définit un emplacement unique dont l'adresse IP est 10.10.2.224. Cet exemple n'indique pas de valeurs pour m_NumRetries et m_TimeOut, car ces paramètres prennent automatiquement les valeurs par défaut de la table de configuration.

Restriction : Network Manager ne prend pas en charge le format IPv4 mappé en IPv6 et s'attend à ce que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappée IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

```
insert into pingFinder.pingRules
               ( m_Address, m_RequestType )
values
               ( "10.10.2.224", 1 );
```

Exemple : définition de l'emplacement de l'outil de recherche Ping ayant une adresse de sous-réseau de classe B.

L'insertion exemple suivante définit un sous-réseau de classe B comme emplacement.

```
insert into pingFinder.pingRules
                ( m_Address, m_RequestType, m_NetMask )
values
                ( "10.10.0.0", 2, "255.255.0.0" );
```

Exemple : définition de l'emplacement de l'outil de recherche Ping ayant des adresses de sous-réseau de classe C.

L'exemple d'insertion suivant définit deux sous-réseaux de classe C comme emplacement.

```
insert into pingFinder.pingRules
                ( m_Address, m_RequestType, m_NetMask )
values
                ( "10.10.2.0", 2, "255.255.255.0" );

insert into pingFinder.pingRules
                ( m_Address, m_RequestType, m_NetMask )
values
                ( "10.10.47.0", 2, "255.255.255.0" );
```

Exemple : restriction de la détection d'unités

L'exemple d'insertion suivant configure l'outil de recherche Ping de sorte qu'il utilise la table scope.zones et la portée de reconnaissance.

```
insert into pingFinder.scope
                ( m_UseScope, m_UsePingEntries )
values
                ( 1, 1 );
```

Important : Il est déconseillé d'utiliser d'autres combinaisons des filtres m_UseScope et m_UsePingEntries. Indiquer les valeurs (0,0) entraîne une reconnaissance sans limite. Indiquer les valeurs (0,1) entraîne l'envoi de commandes PING sur des unités que vous ne souhaitez pas reconnaître.

Référence associée:

«Base de données pingFinder», à la page 283
La base de données pingFinder définit le fonctionnement de l'outil de recherche Ping.

«Tailles des masques de sous-réseau IPv6», à la page 29
Des milliards de périphériques sont susceptibles d'être la cible d'une commande PING au sein d'un seul sous-réseau IPv6. Pour garantir que la reconnaissance aboutisse, vous devez spécifier un masque de sous-réseau suffisamment large si vous indiquez un sous-réseau IPv6 comme emplacement de départ de la commande PING.

Fichier de configuration DiscoPingHelperSchema.cfg

Le fichier de configuration DiscoPingHelperSchema.cfg définit la manière dont les commandes PING doivent être lancées sur les périphériques.

Table de base de données utilisée

Le fichier de configuration DiscoPingHelperSchema.cfg peut être utilisé pour configurer des insertions dans la table de base de données pingHelper.configuration.

Dans cet exemple de configuration du fichier DiscoPingHelperSchema.cfg, les paramètres spécifient :

- D'utiliser 20 unités d'exécution d'exécution de processus.
- D'attendre une réponse d'un périphérique pendant 250 ms maximum.
- D'effectuer cinq nouvelles tentatives maximum sur les périphériques qui ne répondent pas.
- D'attendre 50 ms entre les lancements de commandes PING sur les périphériques d'un sous-réseau.
- De ne pas utiliser le lancement de commandes PING sur la diffusion ou la multidiffusion.

```
insert into pingHelper.configuration
(
        m_NumThreads,
        m_TimeOut,
        m_NumRetries,
        m_InterPingTime,
        m_Broadcast,
        m_Multicast
)
values
(
                20, 250, 5, 50, 0, 0
);
```

Référence associée:

«Connectivité de la couche réseau de couche 3», à la page 381
Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

«Base de données de l'auxiliaire Ping», à la page 306
La base de données de l'auxiliaire Ping est définie par le fichier de configuration DiscoPingHelperSchema.cfg;. Son nom de table de base de donnée complet est pingHelper.configuration.

Fichier de configuration DiscoConfig.cfg

Le fichier de configuration DiscoConfig.cfg permet à l'outil de recherche Ping de vérifier automatiquement les unités découvertes par l'outil de recherche de fichiers et de permettre une reconnaissance contextuelle.

Table de base de données utilisée

Le fichier de configuration DiscoConfig.cfg peut être utilisé pour configurer des insertions dans les tables suivantes :

- disco.config
- disco.managedProcesses

- disco.NATStatus
- disco.ipCustomTags
- disco.filterCustomTags
- translations.NATAddressSpaceIds
- translations.collectorInfo
- failover.restartPhaseAction
- failover.config
- failover.doNotCache

Les exemples suivants illustrent les insertions dans la table de base de données disco.config.

Exemple : envoi de commandes PING sur les périphériques de l'outil de recherche de fichiers

L'exemple de commande suivant configure la reconnaissance de sorte que les périphériques reconnus par l'outil de recherche de fichiers soient automatiquement vérifiés par l'outil de recherche Ping.

```
update disco.config set m_CheckFileFinderReturns = 1;
```

Exemple : activation de la reconnaissance contextuelle

Avertissement : L'activation d'une reconnaissance contextuelle active automatiquement tous les agents Contexte. La désactivation d'une reconnaissance contextuelle désactive automatiquement tous les agents Contexte. N'activez ni ne désactivez manuellement les agents Contexte, que ce soit via les fichiers de configuration ou l'interface graphique de configuration de la reconnaissance.

Pour activer une reconnaissance contextuelle, ajoutez l'insertion suivante au fichier `DiscoConfig.cfg` :

```
insert into disco.config
(
      m_UseContext
)
values
(
      1
)
```

L'insertion de la valeur `0` désactive la reconnaissance contextuelle.

Enrichissement de la topologie à l'aide de balises personnalisées

Vous pouvez utiliser les tables disco.ipCustomTags et disco.filterCustomTags afin d'enrichir la topologie reconnue en associant une ou plusieurs balises de paires nom-valeur aux entités identifiées.

Concepts associés:

«Reconnaissance des détails des périphériques (contextuels)», à la page 351
La reconnaissance des détails contextuels des périphériques s'effectue en plusieurs étapes.

Tâches associées:

«Ajout de balises aux entités à l'aide de tables de balises personnalisées», à la page 218
Vous pouvez ajouter des balises de paire nom-valeur à des entités par la création d'insertions contenant les données de paires nom-valeur dans la table disco.ipCustomTags ou dans la table disco.filterCustomTags.

Référence associée:

«Agents de reconnaissance contextuelle», à la page 396
Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

«Table disco.config», à la page 230
La table config configure le fonctionnement général du processus de reconnaissance.

Fichier de configuration DiscoScope.cfg

Le fichier de configuration DiscoScope.cfg permet de configurer la portée d'une reconnaissance.

Tables de base de données utilisées

Ce fichier de configuration peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- scope.zones
- scope.detectionFilter
- scope.instantiateFilter
- scope.special

Exemple : définition d'une zone d'inclusion

L'exemple d'insertion suivant définit le sous-réseau 10.10.2.* en tant que zone d'inclusion.

Restriction : Network Manager ne prend pas en charge le format IPv4 mappé en IPv6 et s'attend à ce que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge l'adresse IPv6 mappée d'IPv4 suivante : ::ffff:192.0.2.128. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : ::ffff:c000:280.

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
        [
            {
                                m_Subnet="10.10.2.*"
            }
        ]
);
```

Exemple : définition de plusieurs zones d'inclusion

L'exemple suivant définit trois zones d'inclusion IP différentes, chacune utilisant une syntaxe distincte pour définir le masque de sous-réseau. Les périphériques suivants sont reconnus :

- Tout périphérique du sous-réseau 172.16.1.0 (disposant du masque de sous-réseau 24, c'est-à-dire 24 bits activés et 8 bits désactivés, ce qui implique un masque de réseau de 255.255.255.0).
- Tout périphérique du sous-réseau 172.16.2.0 disposant du masque 255.255.255.0.
- Tout périphérique du sous-réseau 172.16.3.0 disposant du masque 255.255.255.0.

```
insert into scope.zones
(
    m_Protocol,
    m_Action,
    m_Zones
)
values
(
        1,
        1,
        [
              {
                    m_Subnet="172.16.1.0",
                    m_NetMask=24
              },
              {
                        m_Subnet="172.16.2.*"
              },
              {
                                    m_Subnet="172.16.3.0",
                                    m_NetMask=255.255.255.0
              }
        ]
);
```

Exemple : définition d'une zone d'exclusion

L'exemple d'insertion suivant définit une zone d'exclusion unique pour le protocole IP, et associe la zone à un sous-réseau.

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        2,
        [
            {
                m_Subnet="172.16.1.0",
                m_NetMask=24
        ]
);
```

Exemple : définition d'une zone d'inclusion dans un domaine NAT

L'exemple suivant définit une zone d'inclusion zone. La zone d'inclusion comprend toute unité dont l'adresse IP commence par 172.16.2 et qui appartient également à l'espace d'adresse NAT NATDomain1. Le protocole est défini sur 1, c'est-à-dire sur IP.

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.2.*",
            }
        ],
        "NATDomain1"
);
```

Exemple : restriction de l'interrogation d'unités en fonction de l'adresse IP

L'exemple suivant indique comment empêcher toute interrogation supplémentaire d'unités qui correspondent à une adresse donnée. Seuls les périphériques dont l'adresse IP n'est pas 10.10.63.234 sont interrogés plus en détail.

Il ne doit y avoir qu'une seule insertion par protocole dans la table scope.detectionFilter. Plusieurs conditions doivent être définies dans une seule insertion.

Dans la table scope.detectionFilter, indiquez :

- Le type de protocole de réseau. Seul le protocole IP est actuellement pris en charge.
- Les conditions de filtre. Seuls les périphériques qui passent ce filtre, c'est-à-dire qui répondent aux critères de ce filtre, sont interrogés en détail. Si aucun filtre n'est indiqué, touts les périphériques passent par le filtre de détection.

```
insert into scope.detectionFilter
(
        m_Protocol, m_Filter
)
values
(
        1,
        "( ( m_UniqueAddress <> '10.10.63.234' ) )"
);
```

Un programme stitcher compare chaque unité découverte à la condition de filtre de la table scope.detectionFilter table. Le résultat de ce test détermine si le périphérique est reconnu ou non.

Etant donné que le flux de processus de la reconnaissance est entièrement configurable, vous pouvez indiquer au programme stitcher d'agir à n'importe quel moment du processus de reconnaissance. Par défaut, le programme stitcher accomplit le test conditionnel sur les détails du périphérique retournés par l'agent Détails. Votre filtre doit donc être basé sur les colonnes de la table Details.returns.

Bien que vous puissiez configurer la condition de filtre de sorte qu'elle teste n'importe quelle colonne de la table Details.returns, vous pouvez devoir utiliser l'adresse IP comme base du filtre afin de restreindre la détection d'un périphérique particulier. Si le périphérique n'accorde pas d'accès SNMP à l'agent Détails, ce dernier peut ne pas récupérer les variables MIB telles que l'ID objet. Toutefois, l'adresse IP est retournée dans tous les cas lorsque le périphérique est détecté.

Les exemples suivants indiquent une configuration alternative du filtre de détection.

Exemple : restriction de l'interrogation en fonction de l'ID objet

L'exemple suivant indique comment empêcher toute interrogation supplémentaire de périphériques qui correspondent à un ID objet donné. La clause OQL `not like` indique que seuls les périphériques qui passent le filtre (c'est-à-dire les périphériques pour lesquels l'OID n'est *pas* 1.3.6.1.4.1.*) sont interrogés plus en détail.

Il est nécessaire d'utiliser la barre oblique inversée pour échapper le `.`, qui serait sinon traité comme caractère générique. Une explication complète de la syntaxe d'OQL est disponible dans *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*.

```
insert into scope.detectionFilter
(
        m_Protocol,
        m_Filter
)
values
(
        1,
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

Exemple : combinaison de plusieurs restrictions de filtre

Vous pouvez combiner plusieurs filtres de condition dans une seule insertion OQL. L'exemple suivant garantit que seuls les périphériques ne disposant pas ni de l'OID ni de l'adresse IP indiqués sont détectés :

```
insert into scope.detectionFilter
(
        m_Protocol,
        m_Filter
)
values
(
        1,
        "(
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
                AND
                ( m_UniqueAddress <> '10.10.63.234' )
        )"
);
```

Restriction de l'instanciation : limitation lors de l'exclusion d'interfaces par filtrage

Prenez en compte la limitation suivante lorsque vous désirez restreindre l'instanciation d'interfaces.

Restriction : Pour vous assurer que des alertes ne soient pas émises pour des *interfaces* exclues par le filtre d'instanciation, vous devez définir la variable `RaiseAlertsForUnknownInterfaces`. Pour ce faire, procédez comme suit :

1. Modifiez le fichier de configuration `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Ajoutez la ligne suivante au fichier :

```
update config.properties set RaiseAlertsForUnknownInterfaces = 1;
```

Exemple : restriction de l'instanciation en fonction de l'adresse IP

Pour restreindre les périphériques instanciés, ajoutez une insertion OQL dans la table scope.instantiateFilter. Il ne doit y avoir qu'une seule insertion par protocole dans la table scope.instantiateFilter. La table instantiateFilter requiert les informations suivantes :

- Le type de protocole de réseau. Seul le protocole IP est actuellement pris en charge.
- Le test conditionnel. Seuls les périphériques qui passent le filtre sont transmis à MODEL. Si aucun filtre n'est défini, tous les périphériques reconnus sont transmiss à MODEL.

Le filtre d'instanciation fonctionne de la même façon que le filtre de détection, car un programme stitcher est appelé pour comparer les périphériques reconnus à l'aide du test défini dans la table scope.instantiateFilter. Par défaut, le test a lieu après la génération de la topologie de départ, mais avant l'envoi des enregistrements à MODEL. Le test conditionnel doit donc être basé sur les colonnes de la table scratchTopology.entityByName.

Avertissement : Vérifiez qu'il n'y a qu'une seule insertion par protocole dans la table scope.instantiateFilter. Il est nécessaire de combiner plusieurs filtres dans une seule insertion de la même manière que pour la table detectionFilter.

L'exemple suivant indique comment restreindre l'instanciation de périphériques en fonction de l'adresse IP en filtrant la colonne m_Addresses de la table scratchTopology.entityByName.

La colonne m_Addresses est une liste d'adresses de niveau 1-7 du modèle OSI pour le périphérique. Le filtre exemple suivant teste la valeur de m_Addresses(2), c'est-à-dire la troisième entrée de la liste d'adresses (la numérotation de la liste démarre à 0). La troisième entrée de la liste d'adresses est l'adresse de niveau 3, c'est-à-dire l'adresse IP du périphérique.

L'insertion suivante garantit que seuls les périphériques qui passent le filtre sont instanciés, c'est-à-dire seuls les périphériques dont l'adresse IP n'est ni 172.16.1.231, ni 172.16.5.47 et ne commence pas par 192.168.123.

Vous pouvez également restreindre l'instanciation en fonction d'autres adresses du périphérique stockées dans la colonne scratchTopology.entityByName.m_Addresses. Par exemple, m_Addresses(1) contient l'adresse de niveau 2 du périphérique, c'est-à-dire l'adresse MAC.

```
insert into scope.instantiateFilter
(
        m_Protocol,
        m_Filter
)
values
(
```

```
        1,
        "(
                                ( Address(2) <> "172.16.1.231" )
                AND
                                ( Address(2) <> "172.16.5.47")
                AND
                                ( Address(2) not like "192\.168\.123\..*" )
        )"
);
```

Exemple : restriction de l'instanciation en fonction de l'ID objet

L'exemple suivant indique comment empêcher l'instanciation d'unités qui correspondent à un ID objet donné. La clause OQL `not like` indique que seuls les périphériques qui passent le filtre (c'est-à-dire les périphériques pour lesquels l'OID n'est *pas* 1.3.6.1.4.1.*) sont instanciés.

```
insert into scope.instantiateFilter
(
        m_Protocol,
        m_Filter
)
values
(
                1,          // The backslash is used here to escape the .
                "(          // which would otherwise be treated
                                // as a wildcard.
                ( EntityOID not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

Exemple : restriction de l'instanciation complexe

Vous pouvez configurer une instanciation complexe en combinant des conditions dans l'insertion.

L'exemple suivant présente une insertion plus complexe, qui combine un certain nombre de conditions liées à différentes colonnes de la table scratchTopology.entityByName.

```
insert into scope.instantiateFilter
(
        m_Protocol,
        m_Filter
)
values
(
        1,
        "(
                                ( Address(2) = '10.82.219.1' )
                OR
                                ( Address(2) = '10.82.213.5' )
                OR
                                ( Address(2) = '10.82.213.6' )
        )
        OR
        (
                                ( EntityName LIKE 'Tivoli' )
                AND
                                ( EntityType < 3 )
        )
        OR
        (
                                ( EntityType >= 3 )
```

```
                AND
                                ( EntityType <> 7 )
        )"
);
```

L'insertion ci-dessus garantit que seuls les périphériques suivants sont transmis à MODEL pour être instanciés :

- Tout périphérique dont l'adresse IP est 10.82.219.1, 10.82.213.5 ou 10.82.213.6
- Tout périphérique qui n'est pas un serveur Web dont le nom contient la chaîne `tivoli` (en majuscules ou minuscules) et pour lequel `EntityType < 3`, c'est-à-dire, une interface ou un châssis
- Tout périphérique dont `EntityType` est égal à 3, 4, 5, 6 ou 8, c'est-à-dire une interface logique, un objet VLAN (Virtual Local Area Network), une carte, une alimentation ou un module

Référence associée:

«Base de donnée de portée de la reconnaissance», à la page 251
La base de donnée de portée limite l'étendue ou la portée de la reconnaissance. La base de donnée de portée vous permet de configurer une gamme de protocoles et d'attributs qui définissent les zones à inclure ou à exclure du processus de reconnaissance.

Périphériques possédant des interfaces hors portée :

Un réseau peut contenir des périphériques se trouvant dans la portée de reconnaissance mais contenant des interfaces hors portée. Puisque le périphérique se trouve dans la portée de reconnaissance, le comportement par défaut des agents de reconnaissance de couche 3 est de télécharger la table d'interface du périphérique et de reconnaître toutes les interfaces d'un périphérique, même si celles-ci sont elles mêmes hors portée.

Si cette situation s'applique à votre réseau et si vous voulez modifier la façon dont le processus de reconnaissance traite les périphériques se trouvant en partie dans la portée de reconnaissance, plusieurs possibilités s'offrent à vous pour modifier le processus de reconnaissance et de surveillance pour exclure ces interfaces de la reconnaissance.

Un ajustement possible de la configuration consiste à modifier l'insertion dans la table scope.instantiateFilter de sorte que les interfaces hors portée ne soient pas instanciées. Cette solution signifie que les interfaces hors portée sont toujours reconnues, mais qu'elles ne sont pas transmises à MODEL pour être instanciées en classe d'objet active. Par conséquent, les interfaces hors portée ne sont pas représentées dans la topologie ou surveillées.

Exemple : contrôle des adresses IP par la table scope.special pour la surveillance des périphériques : Fix Pack 4

Placez des entrées dans la table scope.special des périphériques réseau accessible via plusieurs adresses IP. Les entrées dans la table scope.special contrôlent les adresses IP qu'utilise Network Manager IP Edition pour surveiller les services des règles d'interrogation ICMP (ping) et SNMP.

L'exemple suivant présente une instruction INSERT pour la table scope.special. Il définit l'adresse IP 192.168.1.3 comme interface de gestion potentielle pour les châssis et les interfaces. il fournit des informations client supplémentaires qui sont

ajoutées à la section ExtraInfo de l'entité dans le modèle de table de base de données master.entityByName si l'adresse IP est reconnue.

```
insert into scope.special
(
        m_Zones,
        m_Identifier,
        m_Priority,
        m_NonPingable,
        m_AdminInterface,
        m_ExtraInfo,
        m_Protocol,
        m_IsManagement,
        m_OutOfBand,
        m_IsValidVirtual
)
values
(
        [
                {
                        m_Subnet="192.168.1.3",
                        m_NetMask=32
                }
        ],
        "CustomerFacing",
        99,
        0,
        1,
        {
                m_CustomerName = 'MyCompany',
                m_CustomerType = 'Internal'
        },
        1,
        0,
        1,
        0
);
```

Si le périphérique dispose des deux adresses IP 172.20.1.1 et 192.168.1.3, la configuration implique que l'adresse 172.20.1.1 n'est pas choisie comme adresse IP de gestion du périphérique. L'adresse IP 192.168.1.3 est utilisée. L'exemple suivant montre l'entrée de topologie finale dans master.entityByName dans cette instance. Les données dans ExtraInfo préfixé avec m_ScopeSpecial proviennent de l'entrée scope.zones qui correspond à l'adresse IP 192.168.1.3.

```
{
        EntityName='192.168.1.3';
        Address=['','','192.168.1.3'];
        EntityType=1;
        EntityOID='1.3.6.1.4.1.8072.3.2.10';
        IsActive=1;
        Status=1;
        ExtraInfo={
                m_SysName='SYS1';
                m_DNSName='DNS1';
                m_time=1362486845;
                m_DisplayLabel='DNS1';
                m_AssocAddress=[{m_IfIndex = 1, m_IpAddress = '172.20.1.1',
 m_Protocol = 1, m_IfOperStatus = 1 },{m_IfIndex = 2,
m_IpAddress = '192.168.1.3', m_Protocol = 1,
m_IfOperStatus = 1 }];
                m_ScopeSpecialIsManagement=1;
                m_ScopeSpecialPriority=99;
                m_ScopeSpecialIdentifier='CustomerFacing';
                m_ScopeSpecialExtraInfo={
                          m_CustomerName = 'MyCompany',
                    m_CustomerType = 'Internal'
```

```
                    };
                m_DefinedMgmtIP=1;
                m_IsOutOfBand=1;
                m_BaseName='192.168.1.3';
                m_AddressSpace=NULL;
                m_AccessProtocol=1;
                m_AccessAddress='192.168.1.3';
                };
        LingerTime=3;
        ActionType=0;
        CreateTime=1362486848;
        ChangeTime=1362486848;
        ClassName='NetworkDevice';
        ClassId=5;
        ObjectId=2272;
}
```

Fichier de configuration DiscoSnmpHelperSchema.cfg

Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Table de base de données utilisée

Le fichier de configuration DiscoSnmpHelperSchema.cfg peut être utilisé pour configurer des insertions dans la table de base de données snmpHelper.

Vous pouvez également 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. Pour plus d'informations, voir *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Exemple : configuration de délais d'attente et d'unités d'exécution

L'exemple de configuration suivant entraîne le comportement suivant de l'auxiliaire SNMP :

- 120 unités d'exécution de programme sont démarrées pour traiter les requêtes entrantes de données SNMP du serveur auxiliaire. L'auxiliaire SNMP traite un maximum de 120 requêtes comme celles-ci simultanément.
- un périphérique dispose de trois secondes pour répondre à une requête SNMP émise par l'auxiliaire SNMP avant que cette dernière n'expire. Si le périphérique n'a pas répondu à l'issue de cette période, l'auxiliaire émet une nouvelle et dernière fois la requête.

```
insert into snmpHelper.configuration
(
        m_NumThreads,
        m_TimeOut,
        m_NumRetries,
)
values
(
        120, 3000, 1
);
```

Référence associée:

«Reconnaissance de la connectivité pour les commutateurs Ethernet», à la page 376
Les agents de reconnaissance qui reconnaissent les informations de connectivité entre les commutateurs Ethernet disposent de trois étapes opérationnelles principales : accéder au commutateur et télécharger les interfaces de commutateurs ; reconnaître les informations VLAN du commutateur ; télécharger la table de base

de données de réacheminement du commutateur.

«Reconnaissance de connectivité pour les périphériques ATM», à la page 386
Le mode de transfert asynchrone (ATM) est un protocole de commutation alternatif pour les données dont le format est mixte (comme les données pures, les voix et les vidéos). Plusieurs types d'agents de reconnaissance peuvent être utilisés pour reconnaître les périphériques ATM sur un réseau.

«Reconnaissance des passerelles NAT», à la page 390
Il existe plusieurs agents qui téléchargent les informations de conversion d'adresse réseau (NAT) à partir de passerelles NAT connues.

«Reconnaissance des informations de confinement», à la page 391
Un principe important utilisé par le modèle de réseau est le confinement. Un conteneur stocke d'autres objets. Vous pouvez placer n'importe quel objet dans un conteneur, voire mélanger plusieurs objets dans le même conteneur.

«Agents de reconnaissance utilisant d'autres protocoles», à la page 393
Network Manager propose des agents reconnaissant des périphériques qui utilisent d'autres protocoles que ceux décrits précédemment

«Agents de reconnaissance spécifiques à une tâche», à la page 397
Il existe un groupe d'agents spécifiques à une tâche.

«Base de données de l'auxiliaire SNMP», à la page 307
La base de données de l'auxiliaire SNMP est définie par le fichier de configuration DiscoSnmpHelperSchema.cfg. Son nom de table de base de données complet est snmpHelper.configuration.

Fichier de configuration DiscoTelnetHelperSchema.cfg

Le fichier de configuration DiscoTelnetHelperSchema.cfg définit le fonctionnement de l'auxiliaire Telnet, qui retourne les résultats d'une opération Telnet dans un périphérique indiqué.

Tables de base de données utilisées

Le fichier de configuration DiscoTelnetHelperSchema.cfg peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- telnetHelper.configuration
- telnetHelper.deviceConfig

Vous pouvez configurer l'auxiliaire Telnet afin d'utiliser le programme Secure Shell (SSH). SSH permet l'authentification et fournit des comunications plus sécurisées sur le réseau.

Exemple : configuration de l'auxiliaire Telnet

L'exemple d'insertion suivant peut être ajouté au fichier de configuration DiscoTelnetHelperSchema.cfg pour configurer le fonctionnement de l'auxiliaire Telnet. L'insertion configure l'auxiliaire Telnet afin qu'il :

- Utiliser 20 unités d'exécution de processus
- Attendre une réponse des unités pendant au maximum 5000 ms
- Essayer la requête trois fois maximum

```
insert into telnetHelper.configuration
(
          m_NumThreads,
          m_TimeOut,
          m_Retries
)
values
```

```
(
        20,
        5000,
        3
);
```

Configuration des paramètres spécifiques des unités

L'auxiliaire Telnet accepte également des insertions multiples dans la table telnetHelper.deviceConfig du fichier de configuration DiscoTelnetHelperSchema.cfg qui définissent l'interaction des opérations Telnet.

Les exemples suivants indiquent comment configurer des paramètres Telnet spécifiques aux unités. Vous pouvez configurer des paramètres d'unités en fonction de la variable MIB sysObjectID, de l'adresse IP ou du sous-réseau. La méthode la plus efficace de définition de ces options est de se baser sur la variable MIB sysObjectID. Cette variable identifie le fournisseur du périphérique. Les options de configuration spécifiques à un périphérique varient généralement en fonction du fournisseur de ladite unité. Vous pouvez configurer des valeurs pour toutes les périphériques Cisco par exemple, quel que soit l'emplacement de ces unités sur le réseau.

Exemple : configuration de paramètres pour des unités d'un fournisseur spécifique

La configuration classique suivante indique comment configurer des paramètres pour tous les périphériques d'un fournisseur spécifique. L'insertion spécifie :

- 1.3.6.1.4.1.9.1. comme étant la variable MIB sysObjectID à laquelle cette entrée de configuration doit correspondre. Tous les périphériques dont l'ID objet est de la forme 1.3.6.1.4.1.9.1.* correspondent. Cela concerne, à quelques exceptions près, des périphériques Cisco.
- terminal length est la commande qui définit la longueur de page de sortie pour les périphériques Cisco.

  Remarque : Cette commande varie en fonction des périphériques des différents types de fournisseurs.
- Pas de pagination
- Demander depuis l'unité distante
- Réponse à envoyer à l'unité distante pour qu'elle poursuive la sortie paginée.

```
insert into telnetHelper.deviceConfig
(
        m_SysObjectId,
        m_PageLengthCmd,
        m_PageLength,
        m_ContinueMsg,
        m_ContinueCmd
)
values
(
        "1.3.6.1.4.1.9.1.", "terminal length", 0, ".*[Mm]ore.*", " "
);
```

Le fichier de configuration DiscoTelnetHelperSchema.cfg contient des insertions avec des paramètres de configurations spécifiques à des unités par défaut pour les types de fournisseurs suivants :

- Unités Cisco IOS
- Unités Cisco Cat OS

- Unités Juniper JUNOS
- Unités Juniper ERX
- Unités Huawei
- Unités Dasan

Exemple : configuration des paramètres de réponse d'unités en fonction de l'adresse IP

Si la sortie de la commande telnet est supérieure à une page, le périphérique envoie un message lui demandant s'il convient d'afficher la page suivante. Configurez les messages devant être reçus et les réponses devant être données par l'auxiliaire Telnet, dans le fichier de configuration DiscoTelnetHelperSchema.cfg.

Les commandes commençant par m_Continue (tel que m_ContinueMsg) et m_PageLength (tel que m_PageLengthCmd) sont incompatibles : vous devez utiliser l'une ou l'autre. Si ces paramètres ne sont pas configurés correctement pour vos unités, les données peuvent être perdues.

L'exemple suivant montre comment configurer des paramètres pour des unités, en fonction de leur adresse IP. L'insertion spécifie :

- 192.168.112.0 comme adresse IP
- L'invite de l'unité distante est une expression régulière contenant `"wish to continue"`
- La réponse à envoyer à l'unité distante pour qu'elle poursuive la sortie paginée est "y".

```
insert into telnetHelper.deviceConfig
(
          m_IpOrSubNet,
          m_NetMaskBits,
          m_Protocol,
          m_ContinueMsg,
          m_ContinueCmd
)
values
(
          192.168.112.0,
          24,
          1,
          ".*wish to continue.*",
          "y"
);
```

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

«Reconnaissance de la connectivité pour les commutateurs Ethernet», à la page 376
Les agents de reconnaissance qui reconnaissent les informations de connectivité entre les commutateurs Ethernet disposent de trois étapes opérationnelles principales : accéder au commutateur et télécharger les interfaces de commutateurs ; reconnaître les informations VLAN du commutateur ; télécharger la table de base de données de réacheminement du commutateur.

«Reconnaissance des passerelles NAT», à la page 390
Il existe plusieurs agents qui téléchargent les informations de conversion d'adresse

réseau (NAT) à partir de passerelles NAT connues.

«Agents de reconnaissance contextuelle», à la page 396
Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

«Base de données de l'auxiliaire Telnet», à la page 308
La base de données de l'auxiliaire Telnet est définie par le fichier de configuration DiscoTelnetHelperSchema.cfg;. Ses noms de table de base de données complets sont : telnetHelper.configuration; telnetHelper.deviceConfig.

Fichier de configuration DiscoXmlRpcHelperSchema.cfg

Le fichier de configuration DiscoXmlRpcHelperSchema.cfg peut être utilisé pour configurer l'auxiliaire XML-RPC, lequel permet à Network Manager de communiquer avec des collecteurs EMS à l'aide de l'interface XML-RPC.

Table de base de données utilisée

Le fichier de configuration DiscoXmlRpcHelperSchema.cfg peut être utilisé pour configurer des insertions dans la table de base de données xmlRpcHelper.configuration.

Cet exemple d'insertion configure l'auxiliaire XML-RPC pour :

- Utiliser une unité d'exécution de processus.
- Autoriser une taille maximale de 1048576 octets pour une réponse XML-RPC.

```
insert into xmlRpcHelper.configuration
(
    m_NumThreads,
    m_MaxResponseSize
)
values
(
    1, 1048576
);
```

Remarque : La taille de réponse maximale par défaut peut être trop petite lors de l'exécution d'une reconnaissance basée collecteurs si ceux-ci génèrent des réponses très volumineuses. Dans de tels cas, augmentez la taille de réponse maximale. Pour augmenter la taille de réponse maximale, attribuez au paramètre **m_MaxResponseSize** une valeur plus élevée. Prenez soin d'affecter à **m_MaxResponseSize** la même valeur dans les deux fichiers suivants :

- `NCHOME/etc/precision/DiscoCollectorFinderSchema.cfg`
- `NCHOME/etc/precision/DiscoXmlRpcHelperSchema.cfg`

Référence associée:

«Base de données de l'auxiliaire XMLRPC», à la page 310
La base de données de l'auxiliaire XMLRPC est définie par le fichier de configuration DiscoXmlRpcHelperSchema.cfg. Son nom de table de base de données complet est xmlRpcHelper.configuration.

Fichier de configuration SnmpStackSecurityInfo.cfg

Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

Tables de base de données utilisées

Ce fichier de configuration peut être utilisé pour configurer des insertions dans les tables de base de données suivantes :

- snmpStack.configuration
- snmpStack.verSecurityTable
- snmpStack.accessParameters

Notez qu'un autre fichier de configuration est associé à la base de données snmpStack, le fichier SnmpStackSchema.cfg, mais vous ne devriez pas avoir à le modifier.

Vous pouvez également 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. Pour plus d'informations, voir *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

Exemple : configuration des versions SNMP

Si la gestion automatique des versions est activée, l'ajustement suivant de la configuration indique qu'un nom de communauté 'public' est utilisé pour les périphériques qui prennent en charge SNMP version 1 et qu'une configuration spécifique est utilisée pour les périphériques qui prennent en charge SNMP version 3. Puisqu'aucune valeur n'a été spécifiée pour m_SnmpPort, cette valeur prend la valeur standard du port SNMP, 161.

```
insert into snmpStack.verSecurityTable
(
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName,
)
values
(
        0,
        'public',
        2,
        {
                        m_AuthPswd="authpassword",
                        m_PrivPswd="privpassword"
        },
        'authPriv'
);
```

Exemple : définition de noms de communauté

Les insertions suivantes définissent des noms de communauté public et crims0n à utiliser pour accéder aux unités SNMP.

Vous pouvez ajouter autant d'insertions au fichier de configuration SnmpStackSecurityInfo.cfg qu'il y a de mots de passe. Toutes les configurations de mot de passe et de sous réseau sont essayées jusqu'à ce qu'une correspondance soit trouvée.

Remarque : Seul un nom de communauté, public, est configuré par défaut.

```
insert into snmpStack.verSecurityTable
(
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName
)
values
(
        0,
        'public',
        2,
        {
                        m_AuthPswd="authpassword",
                        m_PrivPswd="privpassword"
        },
        'authPriv'
);

insert into snmpStack.verSecurityTable
(        m_IpOrSubNetVer,
        m_NetMaskBitsVer,
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName
)
values
(
        "10.10.2.0",
        24,
        0,
        'crims0n',
        2,
        {
                        m_AuthPswd="authpassword",
                        m_PrivPswd="privpassword"
        },
        'authPriv'
);
```

Exemple : spécification d'un port SNMP

Cet exemple configure les mêmes paramètres SNMP que l'exemple précédent sur tous les périphériques du sous-réseau 192.168.64.0 et indique le port SNMP 6161 pour tous les périphériques de ce sous-réseau.

```
insert into snmpStack.verSecurityTable
(
        m_IpOrSubNetVer,
        m_NetMaskBitsVer,
        m_SNMPVersion,
        m_Password,
        m_SNMPVer3Level,
        m_SNMPVer3Details,
        m_SecurityName,
        m_SnmpPort,
```

```
)
values
(
        192.168.64.0,
        24,
        0,
        'public',
        2,
        {
                        m_AuthPswd="authpassword",
                        m_PrivPswd="privpassword"
        },
        'authPriv'
        6161
);
```

Référence associée:

«Reconnaissance de la connectivité pour les commutateurs Ethernet», à la page 376
Les agents de reconnaissance qui reconnaissent les informations de connectivité entre les commutateurs Ethernet disposent de trois étapes opérationnelles principales : accéder au commutateur et télécharger les interfaces de commutateurs ; reconnaître les informations VLAN du commutateur ; télécharger la table de base de données de réacheminement du commutateur.

«Types d'agents», à la page 375
Les agents fournis avec Network Manager peuvent être divisés en catégories en fonction du type de données qu'ils extraient ou de la technologie qu'ils découvrent.

«Connectivité de la couche réseau de couche 3», à la page 381
Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

«Reconnaissance de connectivité pour les périphériques ATM», à la page 386
Le mode de transfert asynchrone (ATM) est un protocole de commutation alternatif pour les données dont le format est mixte (comme les données pures, les voix et les vidéos). Plusieurs types d'agents de reconnaissance peuvent être utilisés pour reconnaître les périphériques ATM sur un réseau.

«Reconnaissance des passerelles NAT», à la page 390
Il existe plusieurs agents qui téléchargent les informations de conversion d'adresse réseau (NAT) à partir de passerelles NAT connues.

«Reconnaissance des informations de confinement», à la page 391
Un principe important utilisé par le modèle de réseau est le confinement. Un conteneur stocke d'autres objets. Vous pouvez placer n'importe quel objet dans un conteneur, voire mélanger plusieurs objets dans le même conteneur.

«Agents de reconnaissance utilisant d'autres protocoles», à la page 393
Network Manager propose des agents reconnaissant des périphériques qui utilisent d'autres protocoles que ceux décrits précédemment

«Agents de reconnaissance spécifiques à une tâche», à la page 397
Il existe un groupe d'agents spécifiques à une tâche.

«Base de données snmpStack», à la page 262
La base de données snmpStack définit le fonctionnement de l'auxiliaire SNMP.

Fichier de configuration TelnetStackPasswords.cfg

Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

Vous pouvez utiliser le fichier de configuration TelnetStackPasswords.cfg pour spécifier une connexion Secure Shell (SSH) lors de la configuration de l'accès au périphérique Telnet. SSH active le chiffrement du mot de passe lorsque vous accédez à Telnet. Les versions 1 et 2 de SSH sont prises en charge (les restrictions s'appliquent en mode FIPS).

Important : Dans Network Manager IP Edition, SSH prend actuellement en charge l'authentification basée sur un mot de passe ou aucune authentification. Il ne prend pas en charge l'authentification de la signature RSA.

Table de base de données utilisée

Le fichier de configuration TelnetStackPasswords.cfg peut être utilisé pour configurer les insertions dans la table de base de données telnetStack.passwords.

Notez qu'il existe un autre fichier de configuration associé à la base de données telnetStack, le fichier TelnetStackSchema.cfg, mais vous n'avez pas besoin de le modifier.

Exemple : configuration des paramètres d'accès Telnet pour un sous-réseau

L'exemple d'insertion suivant configure les paramètres d'accès Telnet pour un sous-réseau. L'insertion spécifie :

- L'adresse de sous-réseau `192.168.200.0` et un masque de réseau de `25`.
- Le mot de passe et le nom d'utilisateur à utiliser pour accéder au périphérique.
- Le mot de passe, la connexion et les invites de console à fournir pour le périphérique.
- Les périphériques de ce sous-réseau prennent en charge SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '192.168.200.0',
        25,
        '3v3rt0n',
        'user',
                '.*assword:.*',
        '.*ogin.*',
                '.*onsole>.*',
        1
);
```

Exemple : configuration des paramètres d'accès Telnet pour une unité

L'exemple d'insertion suivant montre comment vous pouvez configurer les paramètres d'accès pour une adresse IP unique. L'insertion spécifie :

- L'adresse IP unique `172.16.1.21`. L'adresse est identifiée comme adresse unique lorsque `m_NetMaskBits=32`.
- Le mot de passe et le nom d'utilisateur à utiliser pour accéder au périphérique.
- Le mot de passe, la connexion et les invites de console à fournir pour le périphérique.
- Ce périphérique ne prend pas en charge SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '172.16.1.21',
        32,
        '',
        '',
        '.*assword.*',
        '.*sername.*',
        '.*Morr.*',
        0
);
```

Exemple : configuration de l'accès au périphérique Telnet pour un sous-réseau

L'exemple d'insertion suivant configure les paramètres d'accès Telnet pour un sous-réseau. L'insertion spécifie :

- L'adresse de sous-réseau `192.168.200.0` et un masque de réseau de `25`.
- Le mot de passe et le nom d'utilisateur à utiliser pour accéder au périphérique.
- Le mot de passe, la connexion et les invites de console à fournir pour le périphérique.
- Les périphériques de ce sous-réseau prennent en charge SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '192.168.200.0',
        25,
        '3v3rt0n',
        'user',
```

```
                '.*assword:.*',
        '.*ogin.*',
                '.*onsole>.*',
        1
);
```

Exemple : configuration de l'accès au périphérique Telnet pour une adresse IP unique

L'exemple d'insertion suivant montre comment vous pouvez configurer les paramètres d'accès pour une adresse IP unique. L'insertion spécifie :

- L'adresse IP unique `172.16.1.21`. L'adresse est identifiée comme adresse unique lorsque `m_NetMaskBits=32`.
- Le mot de passe et le nom d'utilisateur à utiliser pour accéder au périphérique.
- Le mot de passe, la connexion et les invites de console à fournir pour le périphérique.
- Ce périphérique ne prend pas en charge SSH.

```
insert into telnetStack.passwords
(
        m_IpOrSubNet,
        m_NetMaskBits,
        m_Password,
        m_Username,
        m_PwdPrompt,
        m_LogPrompt,
        m_ConPrompt,
        m_SSHSupport
)
values
(
        '172.16.1.21',
        32,
        '',
        '',
        '.*assword.*',
        '.*sername.*',
        '.*Morr.*',
        0
);
```

Référence associée:

«Reconnaissance de la connectivité pour les commutateurs Ethernet», à la page 376
Les agents de reconnaissance qui reconnaissent les informations de connectivité entre les commutateurs Ethernet disposent de trois étapes opérationnelles principales : accéder au commutateur et télécharger les interfaces de commutateurs ; reconnaître les informations VLAN du commutateur ; télécharger la table de base de données de réacheminement du commutateur.

«Types d'agents», à la page 375
Les agents fournis avec Network Manager peuvent être divisés en catégories en fonction du type de données qu'ils extraient ou de la technologie qu'ils découvrent.

«Connectivité de la couche réseau de couche 3», à la page 381
Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

«Reconnaissance des passerelles NAT», à la page 390
Il existe plusieurs agents qui téléchargent les informations de conversion d'adresse réseau (NAT) à partir de passerelles NAT connues.

«Agents de reconnaissance contextuelle», à la page 396
Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

«Base de données telnetStack», à la page 267
La base de données telnetStack définit les paramètres d'accès Telnet pour les périphériques.

Récupération d'informations supplémentaires

Vous pouvez configurer les agents de reconnaissance de sorte à récupérer des informations supplémentaires provenant d'unités et stocker ces informations dans la colonne ExtraInfo de la base de données topologiques.

Pour indiquer qu'un agent de reconnaissance donné doit récupérer des informations supplémentaires, modifiez le fichier de définition de l'agent ($NCHOME/precision/disco/agents/*.agnt). Tous les agents de reconnaissance disposent d'un fichier de définition dans le répertoire des agents, qu'ils soient textuels ou précompilés.

Les modifications que vous devez apporter à la définition de l'agent sont décrites dans les rubriques suivantes.

Modification du type d'un agent

Vous pouvez modifier le type d'un agent dans le fichier de définition de l'agent.

Au début du fichier de définition d'un agent de reconnaissance, un des types d'agents suivants est identifié :

- `DiscoCompiledAgent{}` : Agent de reconnaissance compilé (doté d'une bibliothèque partagée située dans le répertoire `$NCHOME/precision/lib` directory).
- `DiscoDefinedAgent{}` : Agent textuel de reconnaissance (sans bibliothèque partagée).
- `DiscoCombinedAgent{}` : Agent de reconnaissance mi-textuel, mi-précompilé pour lequel les traitements supplémentaires (tels que la récupération d'informations supplémentaires à partir d'unités) sont définis dans le fichier de définition de l'agent de reconnaissance.

Pour récupérer des informations supplémentaires depuis des unités, le type d'agent doit être `DiscoDefinedAgent{}` ou `DiscoCombinedAgent{}`. Si vous modifiez un agent compilé existant pour qu'il récupère des informations supplémentaires, vous devez donc commencer par modifier le type de l'agent de `DiscoCompiledAgent{}` vers `DiscoCombinedAgent{}`.

Couches médiation et traitement

L'extraction d'informations supplémentaires des périphériques et l'ajout des informations aux enregistrements de l'entité sont effectués par deux couches : la couche médiation et la couche traitement. Dans la couche médiation, les requêtes SNMP réelles d'extraction des variables sont effectuées. Dans la couche traitement, les variables récupérées sont ajoutées aux enregistrements d'entité appropriés. Il existe également un filtre facultatif au niveau de la couche médiation.

Le segment de code suivant est un aperçu de la structure des sections médiation et traitement du fichier de définition de l'agent de reconnaissance.

```
DiscoAgentMediationFilter
            {
                    // Optional section containing filters for the mediation layer.
            }
```

```
DiscoAgentMediationLayer
            {
                                        // Contient les requêtes
SNMP Get et GetNext à effectuer.
                                        // De plus, une trace ICMP
peut être effectuée et les paramètres
                                        // d'accès SNMP peuvent être
extraits dans la couche médiation.
            }

DiscoAgentProcessingLayer
            {
                                        // Ajoute les variables
récupérées dans le(s) enregistrement(s)
                                        // d'entité approprié(s).
            }
```

La couche médiation

La couche médiation est celle où les requêtes SNMP et ICMP sont effectuées.

Dans le code suivant, la règle `DiscoSnmpGetResponse();` effectue une requête SNMP Get et la règle `DiscoSnmpGetNextResponse();` effectue une requête SNMP Get Next. Vous pouvez inclure autant d'occurrences de chaque type de requête que nécessaire.

Vous pouvez également inclure la règle `DiscoSnmpGetAccessParameters();`, qui extrait les détails de l'accès SNMP du périphérique et la règle `DiscoICMPGetTrace();`, qui extrait toutes les adresses IP du chemin d'accès au périphérique.

```
DiscoAgentMediationLayer
  {
        DiscoSnmpRequests
                {
                                        DiscoSnmpGetResponse( ARGUMENT, VARIABLE );
                                        DiscoSnmpGetNextResponse( ARGUMENT, VARIABLE, );
                                        DiscoSnmpGetAccessParameters( VARIABLE );
                }
        DiscoICMPRequests
                {
                                        DiscoICMPGetTrace( VARIABLE );
                }
  }
```

DiscoSnmpGetResponse(); :

DiscoSnmpGetResponse(); exécute une requête SNMP Get. La forme simple de cette règle comprend deux arguments, séparés par une virgule. Le premier argument est la clé à affecter à la réponse. Cette clé est utilisée dans la couche de traitement. Le deuxième argument est l'ID objet à extraire du périphérique.

L'exemple suivant extrait sysUpTime et affecte la clé m_SysUpTime à la valeur renvoyée.

```
DiscoSnmpGetResponse( "m_SysUpTime", sysUpTime );
```

Une forme plus complexe de DiscoSnmpGetResponse(); inclut un troisième argument, l'index d'ID objet. L'exemple suivant extrait ifDescr, affecte la clé m_IfDescr à la valeur renvoyée et utilise l'index d'ID objet 1.

```
DiscoSnmpGetResponse( "m_IfDescr", ifDescr, "1" );
```

DiscoSnmpGetNextResponse(); :

DiscoSnmpGetNextResponse(); exécute une requête SNMP GetNext. Cette règle a les mêmes arguments que DiscoSnmpGetResponse();.

L'exemple suivant extrait ipRouteIfIndex et affecte la clé m_IpRouteIfIndex à la valeur renvoyée.

```
DiscoSnmpGetNextResponse( "m_IpRouteIfIndex", ipRouteIfIndex );
```

DiscoSnmpGetAccessParameters(); :

`DiscoSnmpGetAccessParameters();` extrait les paramètres d'accès SNMP du périphérique.

Si vous configurez l'agent de reconnaissance pour extraire les paramètres d'accès dans la couche médiation, vous devez également configurer l'agent pour ajouter les informations à l'enregistrement de base de données dans la couche de traitement.

```
DiscoSnmpGetAccessParameters( "m_AccessParam" );
```

DiscoICMPGetTrace(); :

`DiscoICMPGetTrace();` extrait les adresses IP dans le chemin d'accès au périphérique.

Si vous configurez l'agent de reconnaissance pour extraire le chemin d'accès au périphérique dans la couche médiation, vous devez également configurer l'agent pour ajouter les informations à l'enregistrement de base de données dans la couche de traitement.

```
DiscoICMPGetTrace( "m_Trace" );
```

Filtre de la couche médiation

Le filtre de la couche médiation est un filtre facultatif qui limite les requêtes SNMP pour des informations supplémentaires vers des périphériques spécifiques. Vous pouvez inclure une condition dans la section DiscoMediationSnmpGetFilter{} de DiscoAgentMediationFilter{}, indiquant que seuls les périphériques qui passent le filtre sont traités par l'agent.

L'exemple suivant garantit que seuls les périphériques dont la valeur d'ipForwarding est 1 sont traités.

```
DiscoAgentMediationFilter
            {
                    DiscoMediationSnmpGetFilter
                    {
                                                          "ipForwarding" = 1 ;
                    }
            }
```

Couche traitement

La couche traitement est la couche dans laquelle les informations récupérées sont ajoutées aux enregistrements d'entité. Les sections DiscoAgentProcLayerAddTags{} et DiscoAgentProcLayerAddLocalTags{} sont facultatives. Toutefois, si les deux sections sont omises, aucune information supplémentaire n'est stockée dans les enregistrements de base de données.

La structure de la couche traitement est indiquée ci-dessous.

```
DiscoAgentProcessingLayer
  {
       DiscoAgentProcLayerAddTags
               {
                                    DiscoAddTagSnmpGet( KEY );
                                  DiscoAddTagSnmpGetNext( KEY );
                                DiscoAddTagSnmpGetAccessParameters( "m_AccessParam" );
                                    DiscoAddTagTrace( "m_Trace" );
               }
       DiscoAgentProcLayerAddLocalTags
               {
                    DiscoAddTagSnmpGet(
                                    BALISE FROM CLE WHERE CONDITION );
                    DiscoAddTagSnmpGetNext(
                                    BALISE FROM CLE WHERE CONDITION );
               }
  }
```

DiscoAgentProcLayerAddTags{} :

Dans la section `DiscoAgentProcLayerAddTags{}`, vous pouvez inclure autant de règles `DiscoAddTagSnmpGet();` ou `DiscoAddTagSnmpGetNext();` que nécessaire. Ces règles ajoutent la variable récupérée à l'enregistrement de base de données pour l'entité reconnue.

Chaque règle de la section `DiscoAgentProcLayerAddTags{}` a un seul argument, qui est la clé affectée à la variable récupérée dans la couche médiation. L'exemple suivant ajoute la valeur de `m_SysUpTime`, extraite dans la couche médiation, à l'enregistrement de l'entité.

```
DiscoAddTagSnmpGet( "m_SysUpTime" );
```

Si vous avez configuré l'agent de reconnaissance pour récupérer les paramètres d'accès SNMP ou le chemin vers le périphérique dans la couche médiation, vous devez inclure la règle `DiscoAddTagSnmpGetAccessParameters();` ou `DiscoAddTagTrace();` dans la section `DiscoAgentProcLayerAddTags{}` pour garantir que les informations récupérées sont ajoutées dans la base de données MODEL.

DiscoAgentProcLayerAddLocalTags{} :

Dans la section `DiscoAgentProcLayerAddLocalTags{}`, vous pouvez inclure autant de règles `DiscoAddTagSnmpGet();` ou `DiscoAddTagSnmpGetNext();` que nécessaire. Ces règles ajoutent la variable récupérée à l'enregistrement de base de données pour un voisin local.

La structure des règles est :

```
DiscoAddTagSnmpGet( BALISE FROM CLE WHERE CONDITION );
DiscoAddTagSnmpGetNext( BALISE FROM CLE WHERE CONDITION );
```

Les arguments qui déterminent le voisin local auquel la balise est ajoutée sont :

- *BALISE* qui indique le nom de zone de la balise à ajouter.
- *CLE* indique la clé affectée à la valeur renvoyée dans la couche médiation.
- *CONDITION* indique une condition qui détermine si la balise est ajoutée ou non.

L'exemple suivant ajoute une zone `m_IfDescr` à l'objet de voisin local (à l'aide de la valeur renvoyée dans la couche médiation, à laquelle a été affectée la clé `m_IfDescr`) où`m_IfIndex=1`.

```
DiscoAddTagSnmpGet( "m_IfDescr" FROM "m_IfDescr"
                                        WHERE ( "m_IfIndex" = "1" )
                          );
```

L'exemple suivant ajoute une zone `m_IfType` à l'objet voisin local en utilisant une liste de valeurs renvoyées par la requête GetNext exécutée dans la couche médiation et à laquelle la clé `m_IfType` a été affectée. La clause `WHERE` indique la valeur particulière requise dans la liste de données. Cette valeur est extraite en recherchant l'entrée dans laquelle la valeur de la zone `m_IfIndex` de l'objet voisin local est égale à `SNMPINDEX(0)`, c'est-à-dire, la première valeur de l'entrée de table SNMP.

```
DiscoAddTagSnmpGetNext( "m_IfType" FROM "m_IfType"
                                        WHERE ( "m_IfIndex" = SNMPINDEX(0) )
                                );
```

Cas particulier : ajout d'informations à la table master.entityByNeighbor

Vous pouvez configurer un agent de reconnaissance pour télécharger des variables MIB et indiquer que les variables complètent la table MODEL `master.entityByNeighbor`.

Si vous configurez un agent de reconnaissance pour télécharger l'une des variables MIB répertoriées dans le tableau 4 et que vous ajoutez ces variables à l'entité portant le nom correspondant, elles sont utilisées pour compléter les colonnes correspondantes dans la table MODEL `master.entityByNeighbor`. Ces colonnes peuvent uniquement être complétées pour les entités contenant la zone `RelatedTo`, c'est-à-dire les entités associées à d'autres entités.

Tableau 4. Variables utilisées pour compléter la table master.entityByNeighbor

Variable MIB	**Nom sous lequel la variable doit être configurée pour être ajoutée à l'entité**	**Colonne à remplir**
ifSpeed	m_IfSpeed	Speed
ifRelType	m_IfRelType	RelType
ifProtocol	m_IfProtocol	Protocole

Configuration du réacheminement des interruptions

Le mutliplexeur d'interruption SNMP, ou processus **`ncp_trapmux`**, est à l'écoute d'un port unique et réachemine toutes les interruptions qu'il reçoit vers un ensemble de paires d'hôtes/paires de sockets.

Restriction : Le multiplexeur d'interruptions SNMP ne réachemine pas les messages SNMPv3 Inform.

A propos de la gestion des interruptions

La gestion des interruptions permet de vous assurer que les interruptions provenant de périphériques réseau sont réacheminées vers les ports, d'où elle peuvent être traitées par le Network Manager ou autres système de gestion réseau.

Dans la plupart des réseaux, les interruptions sont réacheminées vers un seul port par défaut (habituellement, le port 162). Cela peut entraîner des problèmes si Network Manager ou d'autres systèmes de gestion réseau sont installés sur le même serveur. Il se peut que chacun de ces deux systèmes doive être à l'écoute des interruptions ; cependant, seul un processus à la fois peut être lié à un port.

Le multiplexeur d'interruption SNMP est un processus Network Manager qui permet de résoudre ce problème : il est à l'écoute d'un seul port et réachemine toutes les interruptions qu'il reçoit vers un jeu de paires d'hôtes/paires de sockets.

Par défaut, le multiplexeur d'interruption SNMP est à l'écoute d'interruptions sur le port 162, mais vous pouvez modifier ce paramètre en insérant un autre numéro de port dans la table de base de données trapMux.config.

Le processus ncp_trapmux permet également de stocker les événements d'interruption dans un fichier au format binaire (contenant les informations sur l'interruption et l'heure où elle s'est produite), qui permet de reproduire les interruptions, dans le même ordre, à une date ultérieure. Cela est utile notamment pour les débogages.

Démarrage du multiplexeur d'interruptions SNMP

Même s'il est d'usage de vérifier que le processus **ncp_ctrl** est configuré pour lancer et gérer le multiplexeur d'interruptions SNMP, vous pouvez également le démarrer manuellement.

Pour démarrer le processus **ncp_trapmux**, utilisez la commande suivante :

```
ncp_trapmux -domain DOMAIN_NAME
```

Réacheminement d'interruptions

Le multiplexeur d'interruptions SNMP permet de réacheminer des interruptions vers un ou plusieurs serveurs.

Pour configurer le multiplexeur d'interruptions SNMP pour qu'il réachemine des interruptions vers des systèmes de gestion de réseau s'exécutant sur host1 et host2 :

1. Modifiez le fichier de schéma, `$NCHOME/etc/precision/TrapMuxSchema.cfg`, en ajoutant un jeu de paires hôtes/paires de sockets. Par exemple, ajoutez les lignes suivantes au fichier :

   ```
   insert into trapMux.sinkHosts (host, port) values ("host1", 5999);
   insert into trapMux.sinkHosts (host, port) values ("host2", 5999);
   ```

2. Démarrez le multiplexeur d'interruptions SNMP à l'aide des commandes suivantes :

   ```
   ncp_trapmux -domain DOMAIN1
   ncp_trapmux -domain DOMAIN2
   ```

Dans l'exemple ci-dessus, lorsqu'une interruption est envoyée à un serveur exécutant le processus **ncp_trapmux**, elle est réacheminée vers `test-host1`, port `5999` et `test-host2`, port `5999`.

Démarrage d'une capture d'interruption :

Vous pouvez démarrer la capture des interruptions en insérant des commandes dans la base de données SNMP du multiplexeur d'interruptions.

Pour demander à la base de données SNMP du multiplexeur d'interruptions de démarrer la capture des interruptions, procédez comme suit :

1. Connectez-vous au service `TrapMux` à l'aide du fournisseur de services OQL ou de la page Accès à la base de données de gestion.
2. Entrez les commandes suivantes :

```
insert into trapMux.command
(commande) valeurs ( "capture_start" );
go
```

Arrêt de la capture des interruptions :

Vous pouvez arrêter la capture des interruptions en insérant des commandes dans la base de données SNMP du multiplexeur d'interruptions.

Pour demander à la base de données SNMP du multiplexeur d'interruptions d'arrêter la capture des interventions, procédez comme suit :

1. Connectez-vous au service `TrapMux` à l'aide du fournisseur de services OQL ou de la page Accès à la base de données de gestion.
2. Entrez les commandes suivantes :

```
insert into trapMux.command
(commande) valeurs( "capture_stop" );
go
```

Impression d'interruptions sur un fichier :

Vous pouvez imprimer des interruptions sur un fichier en insérant des commandes dans la base de données du multiplexeur d'interruptions SNMP.

Pour demander à **ncp_trapmux** d'imprimer des interruptions :

1. Connectez-vous au service `TrapMux` à l'aide du fournisseur de services OQL ou de la page Accès à la base de données de gestion.
2. Entrez les commandes suivantes :

```
insert into trapMux.command
(command, fileName) values( "print", FILENAME );
go
```

Où *FILENAME* indique le fichier sur lequel la sortie est écrite. Si le fichier n'est pas spécifié, `$NCHOME/etc/precision/trapmux.out` est utilisé.

Relancer les interruptions d'un fichier :

Si vous avez créé un fichier texte lisible pour les interruptions, vous pouvez utiliser le processus **ncp_trapmux** afin de recréer les événements d'interruption dans l'ordre indiqué dans ce fichier.

Le processus **ncp_trapmux** peut relancer les interruptions à l'aide d'un fichier binaire ou d'un fichier lisible par une personne ; toutefois, ce processus peut uniquement générer des fichiers binaires.

Pour demander au processus **ncp_trapmux** de relancer les interruptions d'un fichier, procédez comme suit :

1. Connectez-vous au service TrapMux à l'aide du fournisseur de services OQL ou de la page Accès à la base de données de gestion.
2. Entrez les commandes suivantes :

```
insert into trapMux.command
(command, fileName) valeurs ( "replay", "trapmux.out" );
go
```

Commandes du multiplexeur d'interruptions SNMP

Pour contrôler l'activité du multiplexeur d'interruption SNMP, ou processus ncp_trapmux, vous pouvez saisir des commandes.

Les commandes utilisées pour contrôler le processus ncp_trapmux sont décrites dans le tableau suivant :

Tableau 5. Commandes utilisées pour contrôler le processus ncp_trapmux :

Commande	Fonction et nom de fichier par défaut
capture_start	Démarre la consignation des interruptions dans la mémoire. Le nom de fichier par défaut est NULL (non obligatoire).
capture_stop	Arrête la consignation des interruptions dans la mémoire. Le nom de fichier par défaut est NULL (non obligatoire).
capture_continue	Continue la consignation des interruptions dans la mémoire. Le nom de fichier par défaut est NULL (non obligatoire).
capture_empty	Efface toutes les interruptions consignées de la mémoire. Le nom de fichier par défaut est NULL (non obligatoire).
rehash	Ferme le processus ncp_trapmux et efface la mémoire. Le démon relit alors le fichier de configuration et redémarre le processus. Le nom de fichier par défaut est NULL (non obligatoire).
restart	Définit le démon en mode normal. Le nom de fichier par défaut est NULL (non obligatoire).
replay	Lisez les interruptions dans la mémoire ou lisez les information de paquet d'interruption brutes dans le fichier indiqué et réexécutez les interruptions avec un délai court entre elles. Le nom de fichier par défaut est NULL (exécuté à partir de la mémoire).
replay timed	Lisez les interruptions dans la mémoire ou lisez les information de paquet d'interruption brutes dans le fichier indiqué et réexécutez les interruptions dans l'ordre où elles ont été reçues et avec le même délai entre elles. Le nom de fichier par défaut est NULL (exécuté à partir de la mémoire).
print	Imprimez les interruptions se trouvant dans la mémoire vers le fichier indiqué à un format non-lisible. Les information de temps sont codées avec l'interruption. Le nom de fichier par défaut est $NCHOME/etc/precision/trapmux.out.

Configuration de reconnaissances spécialisées

Vous pouvez configurer le système pour accomplir des reconnaissances plus complexes, comme des reconnaissances MPLS et NAT.

Les reconnaissances spécialisées incluent :

Les reconnaissances EMS (Element Management System)
Collectent des données topologiques à partie des systèmes de gestion d'éléments et les intégrent à la topologie reconnue.

Les reconnaissances MPLS
Reconnaissent les réseaux privés virtuels de couche 3 et les réseaux privés virtuels de couche 2 étendus s'exécutant sur des réseaux principaux MPLS.

Les reconnaissances NAT
Reconnaissent les périphériques de passerelle NAT afin d'extraire les données sur les périphériques dans des espaces adresse privés.

Les reconnaissances de tiers :
Reconnaît les réseaux fournisseurs intervenants en tant qu'objet tiers sur plusieurs réseaux fonctionnant sur un réseau fournisseur. Exemples: réseaux VPN d'entreprise sur un réseau principal MPLS fournisseur.

Fix Pack 4 **Reconnaissances interdomaines**
Relient 2 ou plusieurs domaines reconnus. Les connexions entre les périphériques de différents domaines sont détectées et ajoutées à la topologie.

Configuration des reconnaissances interdomaine

Fix Pack 4

Pour visualiser les liens entre les périphériques dans différents domaines afin de les afficher dans les vues de réseau et de topologie, vous devez configurer et exécuter des reconnaissances interdomaine dans les différents domaines.

La configuration de la reconnaissance interdomaine est une procédure avancée qui nécessite la compréhension des flux de données de reconnaissance, le langage de requête OQL, la structure de la base de données, ainsi que les détails et la composition de la connectivité du réseau.

Pour des raisons de performances ou de mise à l'échelle, ou pour des considérations opérationnelles ou techniques, les réseaux peuvent être partitionnés en domaines distincts. Les considérations opérationnelles comprennent les limites géographiques et de sécurité. Les considérations techniques comprennent le chevauchement des adresses IP. Par défaut, ces domaines sont gérés séparément. Par exemple, si un périphérique du domaine A est connecté à un périphérique du domaine B, cette connexion n'est pas représentée dans la base de données topologiques. En outre, dans les vues de réseau et de topologie, les domaines sont visualisés séparément. Les reconnaissances interdomaine relient tous les domaines reconnus. Les connexions entre les périphériques de différents domaines sont détectées et ajoutées à la topologie du réseau. Un domaine agrégé est créé, dans lequel vous pouvez créer des Vues de réseau provenant de tous les périphériques dans tous les domaines. Dans la Vue tronçon de réseau, les recherches de périphériques peuvent s'étendre sur plusieurs domaines.

Avant de commencer la configuration, exécutez les tâches suivantes :

- Dans les fichiers suivants, reconfigurez la syntaxe qui définit les connexions :
  - `$NCHOME/etc/precision/ModelNcimDb.cfg` et les versions du fichier spécifiques au domaine.
  - `$NCHOME/etc/precision/ModelSchema.cfg`
  - `$NCHOME/etc/precision/StoreSchema.cfg`

  Remplacez 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')",
  ```

  Modifiez cette instruction pour qu'elle se présente de la façon suivante :

  ```
  connects&1 = "eval(list type undef, '&RelatedTo')",
  ```
- Si vous utilisez Tivoli Netcool/OMNIbus version 7.3.1 ou une version antérieure, configurez les automatisations pour prendre en charge la génération des événements affectés par un service (SAE). Dans ces versions de Tivoli Netcool/OMNIbus, cette tâche est requise, même si vous n'utilisez pas d'événements affectés par un service. Si votre environnement utilise la version 7.4, vous pouvez ignorer cette tâche. Pour plus d'informations, recherchez *Configuring automations for service-affected events* dans le manuel *IBM Tivoli Network Manager IP Edition - Guide d'installation et de configuration*.

La procédure globale d'activation et de configuration des reconnaissances interdomaine est la suivante :

1. Déterminez si le réseau bénéficierait d'un partitionnement en plusieurs domaines. Pour plus d'informations sur la détermination du nombre optimal de domaines du système, voir «Instructions relatives au nombre de domaines réseau», à la page 15.
2. Partitionnez le réseau en ajoutant des domaines.
3. Activez la liaison interdomaine pour chaque domaine.
4. Configurez la façon dont les programmes stitcher de reconnaissance tentent de lier les domaines. Exemple :
   - Choisissez les technologies à appliquer aux liens entre vos domaines.
   - Configurez les liens manuels
   - Créez à l'aide d'un programme des liens basés sur des modèles connus dans les descriptions d'interface.
5. Exécutez une reconnaissance sur chaque domaine tour à tour. Les liens entre le premier domaine et les autres domaines sont créés ou induits. Ensuite, les liens entre le second domaine et les autres domaines, et ainsi de suite.
6. Relancez la reconnaissance de chaque domaine. Il est important de reconnaître chaque domaine deux fois, pour que les liens induits de façon erronée entre les domaines soient supprimés. Après la seconde reconnaissance du domaine final, la topologie interdomaine est disponible. L'assemblage de domaines d'agrégation s'exécute chaque fois que la topologie est mise à jour.
7. Créez les vues de réseau souhaitées en spécifiant le domaine AGGREGATION dans les vues. Le domaine AGGREGATION est créé par les programmes stitcher d'agrégation, qui s'exécutent à la fin de la reconnaissance et chaque fois que la topologie est mise à jour. Vérifiez que vous pouvez voir les liens attendus entre les domaines.

Tâches associées:

«Création et configuration de domaines réseau supplémentaires», à la page 12
Pour ajouter des domaines réseau supplémentaires, vous devez configurer le contrôle de processus pour les domaines et enregistrer ces derniers avec la base de données topologiques NCIM. Les configurations et les interrogations peuvent être copiées depuis les domaines existants. Configurez ou reconfigurez les vues de réseau pour afficher les périphériques dans les nouveaux domaines.

Activation de la liaison interdomaine

Fix Pack 4

La première étape de la configuration du lien interdomaine consiste à activer les liens entre les domaines dans le fichier de configuration `DiscoConfig.cfg`. Par défaut, le lien interdomaine est désactivé.

1. Sauvegardez et modifiez le fichier `$NCHOME/etc/precision/DiscoConfig.domain.cfg`.
2. Définissez les paramètres suivants :
   - Affectez à **`m_EnableCrossDomainProcessing`** la valeur `1`.
   - Affectez à **`m_InferPEsUsingBGP`** la valeur `0` pour désactiver l'inférence des périphériques PE (Provider Edge). L'inférence des périphériques PE est incompatible avec les reconnaissances interdomaines. Vous pouvez également définir ce paramètre dans l'onglet Avancé de l'interface graphique Configuration de la reconnaissance réseau en désélectionnant **Enable Inference of PEs using BGP data on CEs**.
3. Répétez ces étapes dans le fichier `DiscoConfig.domain.cfg` de chaque domaine à lier.
4. Dans le fichier du programme stitcher `LinkDomainsPopulateDomainAdjacencies.stch`, définissez les adjacences entre les domaines dans la table tmpDomainAdj.adjacencies. Utilisez des instructions INSERT pour définir les adjacences. Des exemples d'instructions INSERT sont fournis dans le fichier. Chaque instruction INSERT définit une seule adjacence. Vous pouvez placer les instructions INSERT dans n'importe quel ordre. Par exemple, pour définir les adjacences entre les deux domaines NORTH et SOUTH, utilisez l'instruction INSERT suivante :

   ```
   insert into tmpDomainAdj.adjacencies values ('NORTH', 'SOUTH');
   ```

   L'exemple suivant monte les instructions INSERT à utiliser lorsqu'il existe trois domaines : EUROPE, ASIA et AMERICA. EUROPE est adjacent à ASIA et AMERICA.

   ```
   insert into tmpDomainAdj.adjacencies values (EUROPE, ASIA);
   insert into tmpDomainAdj.adjacencies values (EUROPE, AMERICA);
   ```

   Pour définir une adjacence supplémentaire entre ASIA et AMERICA, utilisez une autre instruction INSERT :

   ```
   insert into tmpDomainAdj.adjacencies values (ASIA, AMERICA);
   ```

Tâches associées:

«Configuration de liens interdomaines», à la page 106
Pour configurer des liens interdomaines, déterminez la méthode de liaison appropriée pour votre réseau et configurez les programmes stitcher pertinents.

Configuration de liens interdomaines

Fix Pack 4

Pour configurer des liens interdomaines, déterminez la méthode de liaison appropriée pour votre réseau et configurez les programmes stitcher pertinents.

Une fois les liaisons configurées :

1. Exécutez les reconnaissances pour le premier domaine, le second domaine et les autres domaines.
2. Relancez les reconnaissances sur tous les domaines.
3. Créez des vues de réseau interdomaines.

Tâches associées:

«Démarrage d'une reconnaissance», à la page 52
Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

Configuration des liens interdomaine entre la couche 2 et les périphériques utilisant d'autres technologies : Fix Pack 4

Vous pouvez créer des liens interdomaines entre les périphériques de la couche 2 et ceux qui utilisent des technologies telles que /30 et la pseudo-connexion. Editez les paramètres du fichier stitcher `LinkDomains` pour activer la liaison interdomaine pour une technologie, puis configurez la manière dont les liens interdomaines sont créés en modifiant des paramètres supplémentaires associés.

1. Sauvegardez et modifiez le fichier de programme stitcher `$NCHOME/precision/disco/stitchers/LinkDomains.stch`.
2. Pour créer des liens interdomaines depuis des connexions entre des périphériques de la couche 2 dans différents domaines,définissez le paramètre **`linkViaUnresolvedFDBPort`** sur 1.
3. Activez et configurez ensuite la liaison interdomaine pour les technologies de périphérique dans votre réseau comme indiqué dans les options suivantes :

- Pour créer des liens interdomaines depuis des connexions entre des périphériques /30 de différents domaines, définissez le paramètre **`linkViaSlash30Subnet`** sur 1. Pour contrôler la manière dont les connexions entre les périphériques /30 sont ajoutées à la topologie, définissez les paramètres associés suivants. Si les paramètres sont définis sur `0`, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
`preventLinkPropagation`	Si une connexion de couche 2 entre deux entités est reconnue, la connexion /30 n'est pas ajoutée.
`linkSlash30InLayer2`	Les liens /30 sont ajoutés en tant que liens de couche 2.
`linkSlash30InLayer3`	Les liens /30 sont ajoutés en tant que liens de couche 3.

  Conseil : Pour empêcher la création de liens /30 reconnus, définissez **`linkSlash30InLayer2`** et **`linkSlash30InLayer3`** sur `0`. Cette configuration peut augmenter la durée des reconnaissances. Pour que les liens /30 reconnus soient créés, définissez les deux propriétés sur 1.

- Pour créer des liens interdomaines depuis des pseudo-connexions entre des périphériques de différents domaines, définissez le paramètre

linkViaPseudoWires sur 1. Pour contrôler les services qui sont utilisés pour créer des liens dans la topologie, définissez les paramètres associés suivants. Si les paramètres sont définis sur **0,**, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
resolvePWViaFarEndIP	Des adresses IP de pseudo-connexion d'extrémité éloignée sont utilisées pour créer des liens
resolvePWViaLabels	La recherche d'adresse inverse de pseudo-connexion est utilisée pour créer des liens
resolvePWViaVPLSInterface	Des doublons VPLS sont utilisés pour créer des liens

- Pour utiliser des informations de session BGP téléchargées par des agents BGP pour activer des connexions de session entre des périphériques de différents domaines, définissez le paramètre **linkViaBGPSessions** sur 1. Pour contrôler la couche de la topologie interdomaine sur laquelle les liens BGP sont créés et la manière dont les sessions BGP avec des statuts non définis sont traitées, définissez les paramètres associés suivants. Si les paramètres sont définis sur **0,**, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
linkBGPInLayer2	Les liens BGP reconnus sont placés dans la topologie de couche 2
linkBGPInLayer3	Les liens BGP reconnus sont placés dans la topologie de couche 3
linkEstalbishedSessionsOnly	Connecte deux interfaces BGP si une session BGP interdomaine est reconnue et que le statut ne peut pas être défini.
linkBGPSessionsStrictly	Si une correspondance stricte avec la session BGP échoue, des correspondances IP générales sont utilisées pour créer des liens.

- Pour utiliser les données de renvoi de l'agent CDP pour créer des connexions CDP entre des périphériques de différents domaines, définissez le paramètre **linkViaCDP** sur 1. Pour contrôler la manière dont les connexions CDP sont ajoutées à la topologie, définissez les paramètres associés. Si les paramètres sont définis sur **0,**, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
linkViaCDPAtLowestInterface	Tente une connexion au port ou à l'interface de plus bas niveau.
linkViaCDPAtLayer2	Les liens CDP reconnus entre des domaines sont placés dans la topologie de couche 2
linkViaCDPAtLayer3	Les liens CDP reconnus entre des domaines sont placés dans la topologie de couche 3

- Pour utiliser les données de voisin d'agents MPLS pour résoudre des connexions entre des périphériques de différents domaines, définissez le paramètre **linkViaMPLSTE** sur 1. Pour configurer la création de liens pour les connexions TE MPLS, définissez les paramètres suivants associés. Si les paramètres sont définis sur **0,**, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
linkViaMPLSTEAtLayer2	Place les connexions TE MPLS reconnues entre des domaines dans la topologie de couche 2
linkViaMPLSTEAtLayer3	Place les connexions TE MPLS reconnues entre des domaines dans la topologie de couche 3
linkViaMPLSTEAtMPLSTE	Crée des liens TE MPLS pour les connexions TE MPLS reconnues

- Pour utiliser les données de voisin d'agents OSPF pour résoudre des connexions entre des périphériques de différents domaines, définissez le paramètre **linkViaOSPF** sur 1. Pour configurer la création de liens pour les connexions OSPF, définissez les paramètres suivants associés. Si les paramètres sont définis sur `0`, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
linkViaOSPFAtLayer2	Place les connexions OSPF reconnues dans la topologie de couche 2.
linkViaOSPFAtLayer3	Place les connexions OSPF reconnues dans la topologie de couche 3.
linkViaOSPFAtOSPF	Crée des liens OSPF pour les connexions OSPF reconnues.

- Pour utiliser les données de voisin d'agents PIM pour résoudre des connexions entre des périphériques de différents domaines, définissez le paramètre **linkViaPIM** sur 1. Pour configurer la création de liens interdomaines pour les connexions PIM, définissez les paramètres suivants associés. Si les paramètres sont définis sur `0`, ils sont désactivés.

Paramètre	Effet lorsque la valeur est 1
linkViaPIMAtLayer2	Place les connexions PIM reconnues entre des domaines dans la topologie de couche 2.
linkViaPIMAtLayer3	Place les connexions PIM reconnues entre des domaines dans la topologie de couche 3.
linkViaPIMAtPIM	Crée des liens PIM pour les connexions PIM reconnues.

- Pour prévisualiser les liens interdomaines en les écrivant dans un fichier journal, procédez comme suit :
  1. Définissez le paramètre **previewChanges** sur 1.
  2. Définissez le niveau de journalisation du processus **ncp_disco** sur `debug`. Par exemple, sur un domaine appelé AFRICA, exécutez le processus comme suit :

     ```
     ncp_disco -domain AFRICA -messagelevel debug
     ```

  Les liens interdomaines sont écrits dans le fichier `$NCHOME/log/precision/ncp_disco.`*`DOMAIN`*`.log`. Aucun lien n'est créé.
- S'il existe plusieurs types de connexions entre deux ports, sélectionnez le niveau auquel la connexion est créée en définissant le paramètre **lowLayerResolutionMode**.
  - `0` : Crée uniquement la connexion trouvée par les programmes stitcher interdomaines.

– 1 : Crée uniquement la connexion entre les ports empilés au niveau inférieur sous une interface. Par exemple, si interface POS est empilée par-dessus un port SONET, la connexion est créée uniquement entre les ports SONET. Cette option signifie que le programme de stitcher dure plus longtemps.
– 2 : Crée la connexion entre les interfaces ainsi qu'entre les ports empilés aux niveaux les plus bas. Si une interface POS est empilée par-dessus un port SONET, une connexion est créée entre les ports SONET et une connexion est créée entre les interfaces POS. Cette option signifie que le programme de stitcher dure plus longtemps.

Référence associée:

«Programmes stitcher interdomaine», à la page 426
Les programmes stitcher interdomaine recherchent les liens entre les périphériques dans différents domaines et créent des connexions entre eux dans la topologie.

Configuration manuelle des liens interdomaines : Fix Pack 4

Vous pouvez créer manuellement des liens manuels interdomaine entre les périphériques dont vous savez qu'ils sont connectés. Cette étape est utile si, par exemple, le regroupement des vues de réseau ne montre pas les liens attendus entre les périphériques de domaines différents.

1. Sauvegardez et éditez le fichier de programme stitcher `NCHOME/precision/disco/stitchers/LinkDomainsLoadPresetConnections.stch`.
2. Supprimez la mise en commentaire de l'instruction d'insertion OQL.
3. Copiez une instruction d'insertion OQL pour chaque connexion à créer.
4. Modifiez l'instruction d'insertion OQL et ajoutez les détails de la connexion à créer, à l'aide des paramètres suivants :

   entryNo
   ID numérique unique pour cette ligne. Démarrez à 1 et augmentez jusqu'à *n*.

   action
   Définissez sur `ADD` pour ajouter une connexion.

   aEndDiscoDomainName
   Le domaine dans lequel le périphérique au début de la connexion a été reconnu. Cette connexion est créée uniquement après l'exécution d'une reconnaissance dans ce domaine.

   aEndDiscoEntityName
   entityName périphérique au début de la connexion.

   zEndNCIMDomainName
   Le domaine dans lequel se trouve le périphérique à la fin de la connexion. Si une reconnaissance est exécutée uniquement dans ce domaine, cette connexion n'est pas est créée.

   zEndNCIMEntityName
   entityName du périphérique à la fin de la connexion.

   topologyEntityType
   Type d'entité de la connexion dans la topologie NCIM.

Référence associée:

«Programmes stitcher interdomaine», à la page 426
Les programmes stitcher interdomaine recherchent les liens entre les périphériques dans différents domaines et créent des connexions entre eux dans la topologie.

Configuration des liens interdomaine à l'aide des descriptions d'interface :

Fix Pack 4

Vous pouvez créer des connexions entre toutes les interfaces qui correspondent à une recherche des descriptions d'interface.

Pour rechercher des interfaces et créer des connexions entre ces dernières, procédez comme suit :

1. Sauvegardez et éditez le fichier de programme stitcher `NCHOME/precision/disco/stitchers/LinkDomainsLoadInterfaceDescriptionMatches.stch`.
2. Copiez une seule instruction d'insertion OQL pour chaque connexion à créer.
3. Modifiez l'instruction d'insertion OQL et ajoutez les détails de la connexion que vous voulez créer, à l'aide des paramètres suivants :

   entryNo
   ID numérique unique pour cette ligne. Démarrez à 1 et augmentez jusqu'à n.

   action Définissez sur ADD pour ajouter une connexion.

   onlyAdminUp
   Définissez la valeur `1` pour limiter la recherche aux interfaces dont le statut administratif est Actif. Définissez la valeur `0` pour inclure toutes les interfaces, que leur statut administratif soit Actif ou Inactif.

   Le statut administratif est l'état souhaité de l'interface. Un administrateur réseau peut définir l'un des statuts administratifs d'interface suivants : Actif, Inactif ou Test en cours.

   aEndDiscoMatchType
   Définissez sur EXACT pour exécuter une recherche de texte exacte ou REGEX pour exécuter une recherche de texte régulière des interfaces source dans les bases de données de **`ncp_disco`**.

   aEndDiscoDomainName
   Domaine dans lequel le périphérique au début de la connexion a été reconnu. Cette connexion est créée uniquement après l'exécution d'une reconnaissance dans ce domaine.

   aEndDiscoSearchTerm
   Terme de recherche auquel une interface dans le domaine aEndDiscoDomainName doit correspondre dans les bases de données de **`ncp_disco`**.

   zEndNCIMMatchType
   Définissez sur EXACT pour exécuter une recherche de texte exacte ou REGEX pour exécuter une recherche de texte régulière des interfaces cible dans la base de données NCIM.

   zEndNCIMDomainName
   Domaine NCIM dans lequel rechercher les interfaces cible dans la base de données NCIM.

   topologyEntityType
   entityType de la topologie NCIM de la connexion dans la base de données NCIM.

Toute les interfaces correspondant à la recherche sont connectées les unes aux autres.

L'exemple suivant montre une insertion qui connecte toutes les interfaces du domaine NCOMS dont les descriptions contiennent la chaîne `connection to vmhost_network` à toutes les interfaces du domaine NCOMSADJ dont les descriptions contiennent aussi la chaîne `connection to vmhost_network`:

```
INSERT INTO linkDomains.interfaceDescriptionMatch
(
    entryNo,
    action,
    onlyAdminUp,
    aEndDiscoMatchType,
    aEndDiscoDomainName,
    aEndDiscoSearchTerm,
    zEndNCIMMatchType,
    zEndNCIMDomainName,
    zEndNCIMSearchTerm,
    topologyEntityType
)
VALUES
(
    1,                              // entryNo
    'ADD',                          // action
    1,                              // onlyAdminUp - must be up
    'EXACT',                        // aEndDiscoMatchType
    'NCOMS',                        // aEndDiscoDomainName
    'connection to vmhost_network', // aEndDiscoSearchTerm
    'EXACT',                        // zEndNCIMMatchType
    'NCOMSADJ',                     // zEndNCIMDomainName
    'connection to vmhost_network', // zEndNCIMSearchTerm
    72                              // topologyEntityType
);
```

L'exemple suivant montre une insertion qui connecte toutes les interfaces du domaine NCOMS dont les descriptions contiennent la chaîne régulière `ELON(GW|WR|AR)` à toutes les interfaces du domaine NCOMSADJ dont les descriptions contiennent la chaîne `connection to PE2_ASBR_AS2` :

```
INSERT INTO linkDomains.interfaceDescriptionMatch
(
    entryNo,
    action,
    onlyAdminUp,
    aEndDiscoMatchType,
    aEndDiscoDomainName,
    aEndDiscoSearchTerm,
    zEndNCIMMatchType,
    zEndNCIMDomainName,
    zEndNCIMSearchTerm,
    topologyEntityType
)
VALUES
(
    2,                              // entryNo
    'ADD',                          // action
    1,                              // onlyAdminUp - must be up
    'REGEX',                        // aEndDiscoMatchType
    'NCOMS',                        // aEndDiscoDomainName
    'ELON(GW|WR|AR)',               // aEndDiscoSearchTerm
    'EXACT',                        // zEndNCIMMatchType
    'NCOMSADJ',                     // zEndNCIMDomainName
    'connection to PE2_ASBR_AS2',   // zEndNCIMSearchTerm
    72                              // topologyEntityType
);
```

Référence associée:

«Programmes stitcher interdomaine», à la page 426
Les programmes stitcher interdomaine recherchent les liens entre les périphériques dans différents domaines et créent des connexions entre eux dans la topologie.

Création de vues de réseau interdomaine

Fix Pack 4

Vues de réseau interdomaines pour visualiser le réseau. Vous pouvez créer des vues de réseau standard ou dynamiques. Assurez-vous que chaque domaine a été reconnu deux fois. Dans le cas contraire, les vues peuvent contenir des liens interdomaines erronés.

Avant de créer une vue de réseau interdomaine, vous devez configurer et exécuter deux reconnaissances interdomaines pour chaque domaine à regrouper.

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 un type de vue de réseau. Comme la vue de réseau obtenue contiendra tous les périphériques de tous les réseaux reconnus, réfléchissez à la taille des vues de réseau afin de ne pas surcharger inutilement le serveur.

   Renseignez les autres zones comme il convient pour ce type de vue de réseau.
3. Cliquez sur l'onglet **Filtre**. Renseignez l'onglet comme suit :

   Domaine
   Sélectionnez le domaine **AGGREGATION**.

   Renseignez les autres zones comme il convient pour ce type de vue de réseau.
4. Cliquez sur **OK**. La nouvelle vue est ajoutée à l'arborescence de navigation dans le Panneau de navigation. Si vous ajoutez la vue à un conteneur, développez le noeud du conteneur afin de visualiser la nouvelle vue dans l'arbre.
5. Vérifiez que vous pouvez voir les liens attendus entre les domaines, sinon rectifiez les vues. Les actions possibles sont les suivantes :
   - Vérifiez que les agents correspondants aux technologies et aux périphériques excentrés des domaines sont actifs.
   - Vérifiez que toutes les technologies destinées à pour l'assemblage interdomaine sont actives.

- Si vous savez que des liaisons existent entre les périphériques de domaines différents, mais qu'elles ne sont pas affichées dans les vues de réseau, vous pouvez ajouter ou éditer manuellement les liens.
- Vérifiez l'adéquation des limites entre les domaines et, si nécessaire, repartitionnez le réseau.

Votre vue de réseau affiche les périphériques de tous les domaines reconnus.

Exemple : petit réseau ou validation de concept (POC)

Si vous souhaitez vérifier si plusieurs domaine ont été reconnus et regroupés comme prévu, recréez toutes les vues de réseau qui sont créées automatiquement après la fin d'une reconnaissance. Vérifiez les vues de réseau résultantes n'ont pas d'impact sur les performances. Vous pouvez par exemple procéder de cette façon lorsque vous testez la reconnaissance interdomaine sur un système hors production. Créer des vues de réseau de la façon suivante :

1. Créez une vue réseau de type **Vues dynamiques - Modèle**.
2. Sélectionnez le domaine **AGGREGATION**.
3. Sélectionnez le modèle **IP par défaut**.

Tâches associées:

«Configuration manuelle des liens interdomaines», à la page 109
Vous pouvez créer manuellement des liens manuels interdomaine entre les périphériques dont vous savez qu'ils sont connectés. Cette étape est utile si, par exemple, le regroupement des vues de réseau ne montre pas les liens attendus entre les périphériques de domaines différents.

«Création et configuration de domaines réseau supplémentaires», à la page 12
Pour ajouter des domaines réseau supplémentaires, vous devez configurer le contrôle de processus pour les domaines et enregistrer ces derniers avec la base de données topologiques NCIM. Les configurations et les interrogations peuvent être copiées depuis les domaines existants. Configurez ou reconfigurez les vues de réseau pour afficher les périphériques dans les nouveaux domaines.

Référence associée:

«Programmes stitcher interdomaine», à la page 426
Les programmes stitcher interdomaine recherchent les liens entre les périphériques dans différents domaines et créent des connexions entre eux dans la topologie.

«Fichiers de configuration de la reconnaissance», à la page 58
Dans les fichiers de configuration de la reconnaissance, définissez les paramètres de la reconnaissance en créant ou en éditant les instructions INSERT dans les bases de données des processus de reconnaissance.

Configuration des reconnaissances EMS

Vous pouvez configurer Network Manager pour collecter des données topologiques depuis des EMS (Element Management Systems) et intégrer ces données à la topologie reconnue.

Les rubriques suivantes décrivent comment configurer une reconnaissance EMS.

Pour savoir comment Network Manager collecte des données topologiques depuis des EMS (Element Management Systems) et intègre ces données à la topologie reconnue, voir *IBM Tivoli Network Manager IP Edition - Présentation du produit*.

Concepts associés:

«Processus de reconnaissance avec intégration EMS», à la page 358
Network Manager collecte les données topologiques d'un système de gestion d'éléments à l'aide de collecteurs.

A propos de l'intégration EMS

L'intégration EMS de Network Manager permet au Network Manager de collecter les données topologiques des systèmes de gestion d'éléments.

Le tableau 6 montre les étapes impliquées dans la collecte des données topologiques à partir du système de gestion d'éléments dans le cadre d'une reconnaissance ou d'une reconnaissance partielle. Une fois ces données collectées, Network Manager l'assemble avec la topologie.

Tableau 6. Collecte des données topologiques du système de gestion d'éléments lors de la reconnaissance

Etape	Flot de données
1	A l'aide de l'outil de recherche Collector, le système de reconnaissance interroge le collecteur pour obtenir une liste de périphériques gérés par le système de gestion d'éléments. En cas de reconnaissance partielle, la reconnaissance peut rechercher un seul périphérique ou un seul sous-réseau.
2	L'outil de recherche Collector interroge le système de gestion d'éléments pour obtenir la liste des périphériques.
3	Ce dernier répond et renvoie la liste des périphériques gérés.
4	L'outil de recherche Collector répond en fournissant la liste des périphériques.
5	A l'aide d'agents de reconnaissance de collecteurs spécialisés utilisés à différents moments de la reconnaissance, le système de reconnaissance interroge le collecteur pour obtenir des informations de base et détaillées sur chaque périphérique de la liste. Parmi les informations détaillées recherchées figurent les informations d'inventaire, les détails de connexion de couche 2 et 3 ainsi que les informations sur le réseau privé virtuel.
6	L'outil de recherche Collector répond en fournissant les informations de base et détaillées comme requis.

A propos des collecteurs :

Un collecteur est un module logiciel qui extrait des données topologiques à partir d'une source de données, comme un système de gestion d'éléments (EMS) ou un fichier CSV dont les valeurs sont séparées par des virgules, et rend ces données disponibles pour le processus de reconnaissance en tant qu'ensemble de données XML. Network Manager peut ensuite assembler ces données en topologie reconnue.

Un collecteur convertit les données topologiques à partir du format dans lequel elles sont stockées dans l'EMS de propriété en une structure XML standard qui peut être traitée par Network Manager. Cela signifie qu'un collecteur différent doit être développé pour chaque fournisseur et chaque modèle EMS. Network Manager va de pair avec un collecteur qui traite les données provenant d'un EMS Alcatel 5620 SAM. Ce collecteur est rédigé en langage Perl. Les collecteurs peuvent être rédigés en n'importe quel langage. Néanmoins, Network Manager va de pair avec les modules Perl pour prendre en charge le développement des collecteurs en Perl.

Les collecteurs peuvent s'exécuter sur le même hôte que Network Manager. Ils peuvent également s'exécuter sur un hôte séparé.

Toute interaction entre Network Manager et les conducteurs est menée en XML et se produit sur une interface XML-RPC.

Information associée:

Tivoli Field Guide: EMS Collector Developer Guide

Network Manager est livré avec un collecteur Alcatel 5620 SAM EMS qui est prêt à l'emploi. Consultez le manuel EMS Collector Developer Guide pour plus d'informations sur le développement de collecteurs pour d'autres systèmes de gestion d'éléments.

Collecteurs par défaut :

Un certain nombre de collecteurs sont fournis avec Network Manager.

Chaque collecteur fourni avec Network Manager télécharge les données à partir d'un objet EMS par le biais d'un protocole NBI (Northbound Interface). Chaque EMS gère des périphériques qui prennent en charge certaines technologies.

Le tableau suivant répertorie les collecteurs par défaut.

Tableau 7. Liste des collecteurs par défaut

Collecteur	EMS	Description	Protocole NBI	Technologie
Alcatel5620SamSoap	Alcatel 5620 SAM	Le collecteur extrait et convertit les données XML Alcatel 5620 Sam et rend le contenu disponible par le biais de XML-RPC.	SOAP	OSI Layer 2, OSI Layer 3, Interface Inventory, Physical Entity, VPN Layer 3, VPN Layer 2
Alcatel5620SamSoap FindToFile	Alcatel 5620 SAM	Le collecteur extrait les mêmes données que le collecteur Alcatel5620SamSoap. Le collecteur stocke les données de l'EMS dans les fichiers XML avec le même nom que les objets interrogés. Le collecteur transfère les fichiers XML vers Network Manager en utilisant FTP. Vous devez configurer les détails de la connexion FTP avant d'exécuter le collecteur.	SOAP	Long Term Evolution (LTE), OSI Layer 2, OSI Layer 3, Interface Inventory, Policy and Charging Rules Function (PCRF), Serving Gateway (SGW), Packet Data Network Gateway (PGW), Mobility Management Entity (MME), eNodeB, Physical Entity, VPN Layer 3, VPN Layer 2
Alcatel5620SamCsv	Alcatel 5620 SAM	Ce collecteur récupère des données topologiques de l'EMS depuis une exportation au format CSV du gestionnaire d'administration du système EMS Alcatel 5620.	N/A	Interface Inventory, Physical Entity

Tableau 7. Liste des collecteurs par défaut (suite)

Collecteur	EMS	Description	Protocole NBI	Technologie
Alcatel5529IdmSoap	Alcatel-Lucent 5529 Inventory Data Manager (IDM)	Le collecteur extrait les informations de confinement pour les unités gérées par les services de gestion d'événements (EMS).	SOAP	Interface Inventory, Physical Entity
GenericCsv	Tout EMS prenant en charge la sortie CSV.	Collecteur générique basé sur le format CSV.	N/A	Diverses
Collecteur Huawei U2000 iManager	Huawei iManager U2000	Ce collecteur effectue une reconnaissance des entités réseau logiques et physiques. Les entités de réseau physique identifiées incluent les casiers, les cartes, les ports Ethernet et les ports DSL. Les entités de réseau logique identifiées sont les VLAN.	TL1	Physical Entity, Interface Inventory

Composants de l'intégration EMS :

L'intégration EMS est composée de plusieurs composants qui fournissent une aide lors de la collecte de données topologiques.

Les composants de l'intégration EMS sont décrits dans le tableau 8.

Tableau 8. Composants de l'intégration EMS

Composant	Description
Outil de recherche de collecteurs `ncp_df_collector`	L'outil de recherche de collecteurs lit les valeurs de départ de l'hôte du collecteur à partir d'une table de valeurs de départ figurant dans la base de données `collectorFinder`. Il analyse ensuite les collecteurs indiqués dans cette table afin d'obtenir une liste de périphériques gérés par l'EMS associés à chaque collecteur.
Agents Collector	Extraient des informations de base et détaillées sur les périphériques situés sur le collecteur. Chaque agent utilise l'auxiliaire Collector pour extraire ces informations.
Agent CollectorDetails	Extrait des informations de base sur les périphériques situés sur le collecteur, y compris les données sysObjectId, sysDescr ainsi que les données de désignation.
Agent CollectorInventory	Extrait le voisin local, l'entité et les données d'adresse associées pour chaque périphérique situé sur le collecteur.
Agent CollectorLayer2	Extrait les informations de connectivité de couche 2 pour les périphériques situés sur le collecteur.

Tableau 8. Composants de l'intégration EMS (suite)

Composant	Description
Agent CollectorLayer3	Extrait les informations de connectivité de couche 3 pour les périphériques situés sur le collecteur.
Agent CollectorVpn	Extrait les données du réseau privé virtuel de couches 2 et 3 pour les périphériques situés sur le collecteur.
Auxiliaire Collector `ncp_dh_xmlrpc`	Permet à Network Manager de communiquer avec les collecteurs à l'aide de l'interface XML-RPC.

Référence associée:

«Données topologiques stockées dans un système de gestion d'éléments», à la page 386

Il existe plusieurs agents de reconnaissance qui extraient des informations sur les périphériques gérés par un système de gestion d'éléments.

Configuration d'une reconnaissance EMS

Configurez une reconnaissance EMS pour collecter des données topologiques depuis des EMS (Element Management Systems) et intégrer ces données à la topologie reconnue.

La configuration d'une reconnaissance EMS s'effectue de la même manière que la reconnaissance de n'importe quel autre type de réseau. En plus des activités de configuration des reconnaissances standard, vous devez procéder à des activités de configuration de reconnaissances spécifiques à EMS.

Pour configurer une reconnaissance EMS, exécutez les activités suivantes en plus des activités de configuration de reconnaissance standard :

- Configurer et démarrer les collecteurs EMS
- Définir l'emplacement EMS en définissant l'emplacement de l'outil de recherche Collector
- Activer les agents de reconnaissance des collecteurs

Ces activités de configuration spécifiques à EMS sont décrites dans les rubriques suivantes.

Configuration de collecteurs :

Vous pouvez configurer un collecteur pour qu'il transmette des requêtes et des réponses de données entre Network Manager et l'EMS associé ou une autre source de données.

Fix Pack 4

Les collecteurs SOAP (Simple Object Access Protocol) suivants prennent en charge le protocole de communication HTTPS (Hypertext Transfer Protocol Secure) pour protéger les communications sur le réseau :

- Alcatel5620SamSoap collector
- Alcatel5620SamSoapFindtoFile collector
- Alcatel5529IdmSoap collector

Fix Pack 5 Le collecteur Network Manager EMS se connecte aux collecteurs SOAP ci-dessus via HTTPS, et nécessite d'installer le package OpenSSL 1.0.2g. Le package OpenSSL 1.0.2g peut être téléchargé à partir d'Internet.

Remarque : Fix Pack 5 Ce package est la seule version compatible certifiée.

La configuration du collecteur dépend du type de la source de données :

- Pour un EMS : indiquez le nom d'hôte, le port, le nom d'utilisateur et le mot de passe de l'EMS.
- Pour un fichier CSV : indiquez les détails des fichiers CSV et comment analyser ces fichiers.

Vous devez également indiquer au collecteur sur quel port écouter les requêtes XML-RPC de Network Manager. Cette configuration n'est généralement à faire qu'une fois, lors de l'ajout d'un nouveau collecteur à votre installation Network Manager.

1. Modifiez le fichier de configuration du collecteur. Par exemple, pour configurer le collecteur pour Alcatel 5620 SAM EMS, éditez le fichier `$NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoapCollector.cfg`.
2. Indiquez le port sur lequel le collecteur doit écouter les requêtes XML-RPC de Network Manager.

   Il s'agit également du port que le collecteur utilise pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port `8081`. Pour le changer, recherchez et effectuez la modification dans la section `General` du fichier de configuration. Exemple :

   ```
   General =&gt;
   {
                   Debug =&gt; 0,
                   Listen =&gt; 8081
   },
   ```
3. Indiquez la source de données de ce collecteur. Ce paramètre varie en fonction du type de la source de données que le collecteur utilise :
   - S'il s'agit d'un collecteur SOAP et que la source de données est un service de gestion des événements, spécifiez le nom d'hôte et le port du service de gestion des événements, ainsi que le nom d'utilisateur et le mot de passe à utiliser pour la connexion au service de gestion des événements. Pour ce faire, modifiez la section `DataSource` du fichier de configuration comme suit :

     ```
     DataSource =>
     {
                     Host => 192.168.1.2,
                     Port => 8080

                     Username => 'oss',
                     Password => 'myPa55w0rd'
     &mldr;
     &mldr;
     &mldr;
     },
     ```
   - Fix Pack 4 S'il s'agit d'un collecteur SOAP compatible avec HTTPS et que la source est un service de gestion des événements, définissez le nom d'hôte et le port du service de gestion des services, ainsi que le nom d'utilisateur et le mot de passe de connexion au service de gestion des événements. Vous pouvez également définir un mot de passe chiffré en utilisant la zone **Md5Password** à la place d'un mot de passe non chiffré (la zone **Password**). Vous pouvez également indiquer si le collecteur utilise HTTPS en renseignant les zones **UseSSL** et **SSLCertFile**. Pour ce faire, effectuez les modifications dans la section `DataSource` du fichier de configuration. Exemple :

```
DataSource =&gt;
{
                Host =&gt; 192.168.1.2,


                Username =&gt; 'oss',
                Password =&gt; 'myPa55w0rd',
.
.
.

    UseSSL => 1,
    SSLCertFile => 'certs/alu5620sam.crt',
&mldr;
&mldr;
&mldr;
},
```

- S'il s'agit d'un collecteur CSV et que la source de données est un fichier CSV, indiquez le nom du fichier CSV. Pour ce faire, modifiez la section `DataSource` du fichier de configuration comme suit :

```
DataSource =>
{
                CsvCfg => 'exampleCsv.cfg',
&mldr;
&mldr;
&mldr;
},
```

4. Sauvegardez le fichier de configuration du collecteur.

Configuration du collecteur Alcatel5620SamSoap :

Pour utiliser les données du collecteur Alcatel5620SamSoap dans une reconnaissance de réseau, vous devez configurer les informations de connexion entre les services de gestion d'événements (EMS) et Network Manager.

Vous pouvez également configurer des informations supplémentaires devant être collectées depuis les services de gestion d'événements (EMS). Pour configurer le collecteur Alcatel5620SamSoap, procédez comme suit :

1. Modifiez le fichier de configuration du collecteur : `NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoapCollector.cfg`
2. Modifiez la section `General` du fichier de configuration. Définissez les propriétés suivantes :

   Débogage

   Mode de débogage du collecteur. Définissez la valeur `0` pour désactiver le débogage. Définissez la valeur `4` pour l'activer. La valeur `1`, `2` ou `3` est équivalente à la valeur `0`. Le collecteur affiche debug (stdout).

   Mode écoute

   Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

   Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port `8081`. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier `DiscoCollectorFinderSeeds.cfg` lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

Délai d'attente
Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
                Debug => 0,
                Listen => 8081,
                Timeout => 15
},
```

3. Modifiez la section `DataSource` du fichier de configuration. Définissez les propriétés suivantes :

Host Nom de l'hôte du service de gestion des événements.

Port Port de connexion au service de gestion des événements.

Fix Pack 4

Remarque : Le collecteur est compatible avec le protocole de communication HTTPS (Hypertext Transfer Protocol Secure). (HTTP se trouve au-dessus du protocole SSL (Secure Sockets Layer). Par conséquent, le port SAM n'est plus configurable pour réduire le nombre de modifications à effectuer.

Username
Nom d'utilisateur de connexion au service de gestion des événements.

Password
Mot de passe de connexion non chiffré au service de gestion des événements.

Remarque : Fix Pack 4 Vous pouvez définir un mot de passe non chiffré en utilisant la zone **Mot de passe** ou un mot de passe chiffré MD5 en utilisant la zone **Md5Password**. Si vous utilisez la zone **Mot de passe**, le collecteur sélectionne la valeur définie et la convertit en mot de passe chiffré MD5 avant de former l'en-tête de demande SOAP. Si vous utilisez la zone **Md5Password**, le collecteur n'exécute pas de conversion de mot de passe, mais utilise la valeur définie directement en formant l'en-tête de demande SOAP.

Fix Pack 4 **Md5Password**
Mot de passe chiffré MD5 de connexion au service de gestion des événements.

Timeout
Délai d'attente des communications SOAP entre le collecteur et le service de gestion des applications.

Fix Pack 4 Fix Pack 5 **UseSSL**
Indique si le collecteur doit utiliser SSL. Entrez la valeur 1 pour indiquer qu'il est utilisé. Lorsque SSL est activé, le collecteur utilise TLS pour se connecter à EMS. Entrez la valeur 0 pour indiquer que le collecteur n'utilise pas SSL. La valeur par défaut est que le collecteur n'utilise pas SSL.

Remarque : Si vous configurez le collecteur pour utiliser SSL, le port 8443 est utilisé automatiquement. Dans le cas contraire, le port 8080 est

utilisé. Avant d'exécuter le collecteur dans HTTPS, vérifiez que le serveur Alcatel 5620 SAM est déjà configuré pour fonctionner en mode HTTPS. Consultez la section relative à la configuration de la sécurité SSL dans le document SAM 5620 Installation and Upgrade Guide pour plus d'informations.

Fix Pack 4 **ServerCertificate**

Fichier de certificat SSL qui contient la chaîne HEX du certificat SSL d'Alcatel 5620 SAM. Le fichier doit se trouver dans le répertoire `./certs`.

Les étapes suivantes expliquent les tâches à exécuter pour obtenir la chaîne HEX du certificat SSL. Les informations relatives à la gestion et l'utilisation des certificats SSL dépendent du navigateur que vous utilisez. Consultez la documentation du navigateur pour plus d'informations.

a. Fix Pack 5 En supposant qu'openssl est installé, exécutez la commande suivante pour extraire le certificat de serveur auto-signé pour EMS :

```
openssl s_client -connect SAM5620ServerIPAddress:8443 -showcerts
 -tls1 -no_ssl2 -no_ssl3
```

Où `SAM5620ServerIPAddress` spécifie l'adresse IP du serveur sur lequel Alcatel 5620 SAM est exécuté.

b. Accédez à l'option Certificats du navigateur et sélectionnez l'option qui affiche les noms de certificat des serveurs.

Remarque : Généralement, le navigateur fournit un gestionnaire de certificats que vous pouvez utiliser pour gérer et utiliser les certificats.

c. Suivez les instructions du navigateur pour afficher et exporter le certificat sélectionné vers un fichier (par exemple, `alu5620sam.crt`). Veillez à choisir un certificat associé au serveur cible (celui qui exécute Alcatel 5620). Par exemple, le nom de certificat associé au serveur `10.0.0.55:8443` (dans cet exemple, le serveur sur lequel Alcatel 5620 est exécuté) peut s'appeler `www.alcatel-lucent5620sam.com`. Dans l'exemple, vous exportez le certificat `www.alcatel-lucent5620sam.com` vers le fichier `alu5620sam.crt`. Il est recommandé d'utiliser un nom de fichier qui décrit le certificat. Dans cet exemple, le nom de fichier `alu5620sam.crt` décrit un certificat pour Alcatel-Lucent 5620 SAM.

En outre, veillez à ce que le fichier de certificat se trouve dans le répertoire `./certs` sur le serveur où réside Network Manager.

L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur qui n'est pas compatible avec HTTPS :

```
DataSource =>
{
                Host => 192.168.1.2,
                Port => 8080

                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,
...
...
...
},
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de l'utiliser :

```
DataSource =>
{
                Host => 192.168.1.2,


                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,

    UseSSL => 1,
    SSLCertFile => 'certs/alu5620sam.crt',
...
...
...
},
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de ne pas l'utiliser :

```
DataSource =>
{
                Host => 192.168.1.2,


                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,

    UseSSL => 0,

...
...
...
},
```

4. Modifiez la section `DataAcquisition` du fichier de configuration et définissez les propriétés suivantes :

   GetEntities
   Indicateur pour la reconnaissance des entités physiques, telles que les armoires, les cartes et les ports. Définissez la valeur 1 pour reconnaître les entités physiques. Si vous définissez la valeur 0, seules les informations suivantes sont reconnues : châssis, entités logiques et données pour les autres indicateurs activés dans la section `DataAcquisition`. La valeur par défaut est 1.

   GetVplsVpns
   Indicateur de reconnaissance des données VPN couche 2 basé sur VPLS. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

   GetVllVpns
   Indicateur de reconnaissance des données VPN couche 2 basé sur les epipes uniquement. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

GetLayer3Vpns
Indicateur de reconnaissance des données de la VPN couche 3. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

GetMplsInterfaces
Indicateur de reconnaissance des données d'interface MPLS. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

GetLayer2Connections
Indicateur de reconnaissance des données de liaison physique. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
DataAcquisition =>
{
        GetEntities => 1
        GetVplsVpns => 1,
        GetVllVpns => 1,
        GetLayer3Vpns => 1,
        GetMplsInterfaces => 1,
        GetLayer2Connections => 1,
},
```

5. Modifiez la section `DataProcessing` du fichier de configuration. Définissez la propriété ContainmentMethod.

   La propriété ContainmentMethod contrôle la manière dont les données d'entité sont traitées dans le cas où le confinement est ambigu suite à l'absence ou à la duplication des données d'index, ce qui peut se produire avec les données de module (carte)/emplacement.

   Les valeurs possibles de la propriété ContainmentMethod sont les suivantes :

   0 Ignore les index dupliqués et utilise les emplacements. Les entités emplacement sont stockées, mais les entités module (carte) peuvent être perdues si elles partagent les mêmes données que l'emplacement.

   1 Ignore les index dupliqués et utilise les cartes. Les entités module sont stockées, mais les entités emplacement peuvent être perdues si elles partagent les mêmes données que le module.

   2 Conserve les entités carte et emplacement. Génère un faux index si des doublons sont détectés.

   La valeur par défaut est 2.

6. Facultatif : Si vous désirez extraire depuis les services de gestion d'événements des données personnalisées en plus de celles extraites par défaut, procédez comme suit :
   a. Créez un fichier de configuration dans le répertoire du collecter ou modifiez le fichier par défaut `NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/extraInfo.cfg`.
   b. Définissez les données à extraire, comme dans l'exemple suivant :

```
            Device =>
            {
                extraFields => [ { srcField => 'version', destField =>
 'm_Version', typeField => 'chaîne' }]
            },
```

, où srcField est le nom de l'attribut dans l'objet SAM, destField est le nom de la zone dans laquelle les données seront mappées dans la zone extraInfo, et typeField est un descripteur de type facultatif.

L'attribut à extraire doit faire partie de l'un des objets déjà extraits par le collecteur. Les objets interrogés par le collecteur sont les suivants :

- netw.NetworkElement
- equipment.PhysicalPort
- lag.Interface
- equipment.MediaAdaptor
- equipment.PhysicalPort
- equipment.DaughterCard
- equipment.Equipment
- equipment.Shelf
- vpls.L2AccessInterface
- vll.L2AccessInterface
- l3fwd.ServiceSite
- vprn.L3AccessInterface
- netw.PhysicalLink
- lldp.RemotePeer.

Les types valides sont int et string.

c. Enregistrez et fermez le fichier de configuration.

d. Modifiez la section CustomData du fichier de configuration du collecteur NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoap
Collector.cfg. Indiquez le nom et l'emplacement du fichier de configuration définissant les informations supplémentaires à collecter, comme dans l'exemple suivant :

```
CustomData =>
    {
                ExtraInfoCfg => 'extraInfo.cfg'
},
```

7. Sauvegardez le fichier de configuration du collecteur.

Configuration du collecteur Alcatel5620SamSoapFindToFile :

Pour utiliser les données du collecteur Alcatel5620SamSoapFindToFile dans une reconnaissance de réseau, vous devez configurer les informations de connexion entre le service de gestion des événements et Network Manager, et les informations FTP en utilisant les fichiers XML qui peuvent être envoyés au serveur Network Manager.

Vous pouvez également configurer des informations supplémentaires devant être collectées depuis les services de gestion d'événements (EMS). Pour configurer le collecteur Alcatel5620SamSoapFindToFile, procédez comme suit :

1. Modifiez le fichier de configuration du collecteur : NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap
FindToFile/Alcatel5620SamSoap
FindToFileCollector.cfg
2. Modifiez la section General du fichier de configuration. Définissez les propriétés suivantes :

Débogage
Mode de débogage du collecteur. Définissez la valeur `0` pour désactiver le débogage. Définissez la valeur `4` pour l'activer. La valeur `1`, `2` ou `3` est équivalente à la valeur `0`. Le collecteur affiche debug (stdout).

Mode écoute

Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port `8081`. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier `DiscoCollectorFinderSeeds.cfg` lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

Délai d'attente
Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
                Debug => 0,
                Listen => 8081,
                Timeout => 15
},
```

3. Configurez les paramètres FTP suivants :

FtpUsername
Nom d'utilisateur FTP sur le serveur Network Manager.

FtpPassword
Mot de passe FTP sur le serveur Network Manager.

FtpHost
Adresse IP du serveur Network Manager.

FtpDefaultDirectory
Répertoire par défaut du service FTP sur le serveur Network Manager.

FtpDirectory
Répertoire défini par l'utilisateur du service FTP sur le serveur Network Manager. N'entrez pas de valeur s'il n'est pas utilisé.

Conseil : Lorsque la reconnaissance aboutit, copiez les fichiers XML générés du répertoire FTP défini vers un autre emplacement avant d'exécuter une nouvelle reconnaissance pour que les fichiers XML ne soient pas remplacés.

4. Modifiez la section `DataSource` du fichier de configuration. Spécifiez le nom d'hôte et le port de l'EMS, ainsi que le nom d'utilisateur et le mot de passe pour s'y connecter, comme illustré dans l'exemple suivant :

Host Nom d'hôte du service de gestion des événements.

Port Port de connexion au service de gestion des événements.

Fix Pack 4

Remarque : Le collecteur est compatible avec le protocole de communication HTTPS (Hypertext Transfer Protocol Secure). (HTTP se

trouve au-dessus du protocole SSL (Secure Sockets Layer). Par conséquent, le port SAM n'est plus configurable pour réduire le nombre de modifications à effectuer.

Username
Nom d'utilisateur de connexion au service de gestion des événements.

Password
Mot de passe de connexion non chiffré au service de gestion des événements.

Remarque : Fix Pack 4 Vous pouvez définir un mot de passe non chiffré en utilisant la zone **Mot de passe** ou un mot de passe chiffré MD5 en utilisant la zone **Md5Password**. Si vous utilisez la zone **Mot de passe**, le collecteur sélectionne la valeur définie et la convertit en mot de passe chiffré MD5 avant de former l'en-tête de demande SOAP. Si vous utilisez la zone **Md5Password**, le collecteur n'exécute pas de conversion de mot de passe, mais utilise la valeur définie directement en formant l'en-tête de demande SOAP.

Fix Pack 4 **Md5Password**
Mot de passe chiffré MD5 de connexion au service de gestion des événements.

Timeout
Délai d'attente des communications SOAP entre le collecteur et le service de gestion des applications.

Fix Pack 4 **UseSFTP**
Indique si le collecteur utilise le protocole Secure File Transfer Protocol (SFTP) ou File Transfer Protocol (FTP) pour transférer les fichiers XML entre lui-même et le service de gestion des événements. Pour utiliser SFTP, entrez 1 dans cette zone. Autrement, pour utiliser FTP, entrez la valeur 1 dans la zone. La valeur par défaut est 1 (SFTP).

Fix Pack 5 **UseSSL**
Indique si le collecteur doit utiliser SSL. Entrez la valeur 1 dans cette zone pour indiquer que le collecteur utilise SSL. Lorsque SSL est activé, le collecteur utilise TLS pour se connecter à EMS. Entrez la valeur 0 (zéro) pour indiquer que le collecteur n'utilise pas SSL. Par défaut, le collecteur n'utilise pas SSL.

Remarque : Si vous configurez le collecteur pour qu'il utilise SSL, le port 8443 est utilisé automatiquement. Dans le cas contraire, le port 8080 est utilisé.

Fix Pack 4 Fix Pack 5 **ServerCertificate**
Entrez le nom de fichier et le chemin du fichier de certificat SSL qui contient la chaîne HEX provenant de l'Alcatel 5620 SAM. Le fichier doit être conservé dans le répertoire `./certs`.

Pour obtenir la chaîne HEX du certificat SSL, procédez comme suit :

a. Exécutez les commandes appropriées sur le serveur Alcatel 5620 SAM pour activer ce dernier pour la communication SSL. Pour plus de détails, consultez les informations relatives à la préparation d'un système 5620 SAM pour SSL dans la documentation d'Alcatel 5620 SAM. Vous devez configurer le serveur Alcatel 5620 SAM pour SSL avant d'exécuter le collecteur en mode SSL.

Restriction : Vérifiez que le fichier de clés est généré à l'aide de l'algorithme SHA1. Des versions différentes du logiciel Alcatel 5620 SAM utilisent des algorithmes différents. Le collecteur prend en charge uniquement SHA1. Utilisez une option de ligne de commande telle que `-sigalg SHA1withRSA` lors de la génération du fichier de clés.

b. Fix Pack 5 En supposant qu'openssl est installé, exécutez la commande suivante pour extraire le certificat de serveur auto-signé pour EMS :

```
openssl s_client -connect SAM5620ServerIPAddress:8443 -showcerts
 -tls1 -no_ssl2 -no_ssl3
```

Où `SAM5620ServerIPAddress` spécifie l'adresse IP du serveur sur lequel Alcatel 5620 SAM est exécuté.

c. Exportez le fichier de clés dans un fichier au format BASE64/HEX à l'aide de l'utilitaire de clé Java sur le serveur Alcatel 5620 SAM. Le collecteur lit les certificats SSL uniquement au format BASE64/HEX. Pour plus d'informations sur l'utilisation de l'utilitaire de clé Java, voir le site Web Oracle.

Un certificat au format BASE64/HEX se présente comme suit :

```
-----BEGIN CERTIFICATE-----
[long alphanumeric string]
-----END CERTIFICATE-----
```

d. Copiez le certificat SSL au format BASE64/HEX dans le répertoire suivant sur le serveur Network Manager : `NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoapFindToFile/certs`

L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur qui n'est pas compatible avec HTTPS :

```
DataSource =>
{
                Host => 192.168.1.2,
                Port => 8080

                Username => 'oss',
                Password => 'myPa55w0rd',
                Timeout => 30,

...
...
...
},
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de l'utiliser :

```
DataSource =>
{
                Host => 192.168.1.2,


                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,

    UseSSL => 1,
    SSLCertFile => 'certs/alu5620sam.crt',

   UseSFTP => 1,
```

```
   FtpUsername => 'ftp',
   FtpPassword => 'ftp',
   FtpHost => '192.168.1.5',
   FtpDefaultDirectory => '/var/ftp',
   FtpDirectory => '',
...
...
...
},
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de ne pas l'utiliser :

```
DataSource =>
{
                Host => 192.168.1.2,


                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,

    UseSSL => 0,

UseSFTP => 1,

   FtpUsername => 'ftp',
   FtpPassword => 'ftp',
   FtpHost => '192.168.1.5',
   FtpDefaultDirectory => '/var/ftp',
   FtpDirectory => '',

...
...
...
},
```

5. Modifiez la section `DataAcquisition` du fichier de configuration et définissez les propriétés suivantes :

   GetEntities
   Indicateur pour la reconnaissance des entités physiques, telles que les armoires, les cartes et les ports. Définissez la valeur 1 pour reconnaître les entités physiques. Si vous définissez la valeur 0, seules les informations suivantes sont reconnues : châssis, entités logiques et données pour les autres indicateurs activés dans la section `DataAcquisition`. La valeur par défaut est 1.

   GetVplsVpns
   Indicateur de reconnaissance des données VPN couche 2 basé sur VPLS. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

   GetVllVpns
   Indicateur de reconnaissance des données VPN couche 2 basé sur les epipes uniquement. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

   GetLayer3Vpns
   Indicateur de reconnaissance des données de la VPN couche 3. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

GetMplsInterfaces
Indicateur de reconnaissance des données d'interface MPLS. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

GetLayer2Connections
Indicateur de reconnaissance des données de liaison physique. Définissez la valeur 1 pour activer la reconnaissance de ces données. La valeur par défaut est 1.

L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
DataAcquisition =>
{
        GetEntities => 1
        GetVplsVpns => 1,
        GetVllVpns => 1,
        GetLayer3Vpns => 1,
        GetMplsInterfaces => 1,
        GetLayer2Connections => 1,
},
```

6. Facultatif : Si vous désirez extraire depuis les services de gestion d'événements des données personnalisées en plus de celles extraites par défaut, procédez comme suit :
   a. Créez un fichier de configuration dans le répertoire du collecteur ou modifiez le fichier par défaut `NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/extraInfo.cfg`.
   b. Editez le nouveau fichier et spécifiez les données à extraire, comme dans l'exemple suivant :

```
            Device =>
            {
                extraFields => [ { srcField => 'version', destField =>
 'm_Version', typeField => 'chaîne' }]
            },
```

   , où `srcField` est le nom de l'attribut dans l'objet SAM, `destField` est le nom de la zone dans laquelle les données seront mappées dans la zone extraInfo, et typeField est un descripteur de type facultatif.

   L'attribut à extraire doit faire partie de l'un des objets déjà extraits par le collecteur. Les objets interrogés par le collecteur sont les suivants :

   - netw.NetworkElement
   - equipment.PhysicalPort
   - lag.Interface
   - equipment.MediaAdaptor
   - equipment.PhysicalPort
   - equipment.DaughterCard
   - equipment.Equipment
   - equipment.Shelf
   - vpls.L2AccessInterface
   - vll.L2AccessInterface
   - l3fwd.ServiceSite
   - vprn.L3AccessInterface
   - netw.PhysicalLink
   - lldp.RemotePeer.

   Les types valides sont `int` et `string`.
   c. Enregistrez et fermez le fichier de configuration.

d. Modifiez la section CustomData du fichier de configuration du collecteur NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/Alcatel5620SamSoap
Collector.cfg. Indiquez le nom et l'emplacement du fichier de configuration définissant les informations supplémentaires à collecter, comme dans l'exemple suivant :

```
CustomData =>
    {
                ExtraInfoCfg => 'extraInfo.cfg'
},
```

7. Sauvegardez le fichier de configuration du collecteur.

Configuration du collecteur Alcatel5620Csv :

Pour utiliser les données du collecteur Alcatel5620Csv dans une reconnaissance réseau, vous devez configurer les informations de connexion entre les services de gestion d'événements (EMS) et Network Manager.

1. Modifiez le fichier de configuration du collecteur : NCHOME/precision/collectors/perlCollectors/Alcatel5620SamCsv/Alcatel5620SamCsv Collector.cfg
2. Modifiez la section General du fichier de configuration. Définissez les propriétés suivantes :

   Débogage
   Mode de débogage du collecteur. Définissez la valeur 0 pour désactiver le débogage. Définissez la valeur 4 pour l'activer. La valeur 1, 2 ou 3 est équivalente à la valeur 0. Le collecteur affiche debug (stdout).

   Mode écoute

   Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

   Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port 8081. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier DiscoCollectorFinderSeeds.cfg lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

   Délai d'attente
   Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

   L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
            Debug => 0,
            Listen => 8081,
            Timeout => 15
},
```

3. Modifiez la section DataSource du fichier de configuration en spécifiant le nom du fichier CSV, comme illustré dans l'exemple suivant :

```
DataSource =>
{
            CsvCfg => 'exampleCsv.cfg',
```

```
...
...
...
},
```

4. Sauvegardez le fichier de configuration du collecteur.

Configuration du collecteur HuaweiU2000Imanager :

Pour utiliser les données du collecteur HuaweiU2000Imanager dans une reconnaissance de réseau, vous devez configurer les informations de connexion entre les services de gestion d'événements (EMS) et Network Manager.

1. Modifiez le fichier de configuration du collecteur : `NCHOME/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1/HuaweiU2000iManagerTL1Collector.cfg`
2. Modifiez la section `General` du fichier de configuration. Définissez les propriétés suivantes :

   Débogage
   Mode de débogage du collecteur. Définissez la valeur `0` pour désactiver le débogage. Définissez la valeur `4` pour l'activer. La valeur `1`, `2` ou `3` est équivalente à la valeur `0`. Le collecteur affiche debug (stdout).

   Mode écoute

   Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

   Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port `8081`. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier `DiscoCollectorFinderSeeds.cfg` lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

   Délai d'attente
   Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

   L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
                Debug => 0,
                Listen => 8081,
                Timeout => 15
},
```

3. Modifiez la section `DataSource` du fichier de configuration. Spécifiez le nom d'hôte et le port du système de gestion des événements, ainsi que le nom d'utilisateur et le mot de passe pour vous y connecter. Exemple :

```
DataSource =>
{
                Host => 192.168.1.2,
                Port => 8080

                Username => 'oss',
                Password => 'myPa55w0rd'

        GetEntities => 1

           DataAcquisition =>
           {
```

```
                StoreONTs => 1,
            }
...
...
,
```

- Pour collecter les informations d'entité du collecteur, affectez à la propriété **GetEntities** la valeur 1.
- Pour extraire les données ONT (Optical Network Terminal), affectez à la propriété **StoreONTs** la valeur 1.

Configuration du collecteur Alcatel5529IdmSoap :

Pour utiliser les données du collecteur Alcatel5529IdmSoap dans une reconnaissance de réseau, vous devez configurer les informations de connexion entre les services de gestion d'événements (EMS) et Network Manager.

1. Modifiez le fichier de configuration du collecteur : `NCHOME/precision/collectors/perlCollectors/Alcatel5529IdmSoap/Alcatel5529IdmSoapCollector.cfg`
2. Modifiez la section `General` du fichier de configuration. Définissez les propriétés suivantes :

   Débogage
   Mode de débogage du collecteur. Définissez la valeur `0` pour désactiver le débogage. Définissez la valeur `4` pour l'activer. La valeur `1`, `2` ou `3` est équivalente à la valeur `0`. Le collecteur affiche debug (stdout).

   Mode écoute

   Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

   Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port `8081`. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier `DiscoCollectorFinderSeeds.cfg` lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

   Délai d'attente
   Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

   L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
                Debug => 0,
                Listen => 8081,
                Timeout => 15
},
```

3. Modifiez la section `DataSource` du fichier de configuration. Définissez les propriétés suivantes :

   Hôte
   Nom d'hôte du service de gestion des événements.

   Port
   Port de connexion au service de gestion des événements.

Remarque : Fix Pack 4 Le collecteur est compatible avec le protocole de communication HTTPS (Hypertext Transfer Protocol Secure). (HTTP se trouve au-dessus du protocole SSL (Secure Sockets Layer). Par conséquent, le port SAM n'est plus configurable pour réduire le nombre de modifications à effectuer.

Nom d'utilisateur
Nom d'utilisateur de connexion au service de gestion des événements.

Password
Mot de passe de connexion au service de gestion des événements.

Domain
Domaine du système du service de gestion des applications sur lequel le gestionnaire des données d'inventaire est exécuté.

Timeout
Délai d'attente des communication SOAP entre le collecteur et le service de gestion des applications.

Fix Pack 5 **UseSSL**
Zone qui indique si vous définissez le collecteur pour qu'il utilise SSL. Entrez la valeur 1 pour indiquer que le collecteur utilise SSL. Lorsque SSL est activé, le collecteur utilise TLS pour se connecter à EMS. Entrez `0` pour indiquer que le collecteur n'utilise pas SSL. Par défaut, le collecteur n'utilise pas SSL.

Remarque : Si vous configurez le collecteur pour utiliser SSL, le port 8443 est utilisé automatiquement. Dans le cas contraire, le port 8080 est utilisé. Avant d'exécuter le collecteur dans HTTPs, vérifiez que le serveur EMS est déjà configuré pour fonctionner en mode HTTPs.

Fix Pack 5 **ServerCertificate**
Fichier de certificat SSL qui contient la chaîne HEX du certificat SSL d'Alcatel 5529 IDM. Le fichier doit se trouver dans le répertoire `./certs`. Les étapes suivantes expliquent les tâches à exécuter pour obtenir la chaîne HEX du certificat SSL. Les informations relatives à la gestion et l'utilisation des certificats SSL dépendent du navigateur que vous utilisez. Consultez la documentation du navigateur pour plus d'informations.

a. Fix Pack 5 En supposant qu'openssl est installé, exécutez la commande suivante pour extraire le certificat de serveur auto-signé pour EMS :

```
openssl s_client -connect IDM5529ServerIPAddress:8443 -showcerts
 -tls1 -no_ssl2 -no_ssl3
```

Où `IDM5529ServerIPAddress` spécifie l'adresse IP du serveur sur lequel Alcatel 5529 IDM est exécuté.

b. Accédez à l'option Certificats du navigateur et sélectionnez l'option qui affiche les noms de certificat des serveurs.

Remarque : Généralement, le navigateur fournit un gestionnaire de certificats que vous pouvez utiliser pour gérer et utiliser les certificats.

c. Suivez les instructions du navigateur pour afficher et exporter le certificat sélectionné vers un fichier (par exemple, `aluidm5529.crt`). Veillez à choisir un certificat associé au serveur cible (celui qui exécute Alcatel 5529). Par exemple, le nom de certificat associé au serveur `138.120.29:8443` (dans cet exemple, le serveur sur lequel Alcatel 5529 est exécuté) peut s'appeler `www.alcatel-lucent.com`. Dans l'exemple, vous exportez le certificat `www.alcatel-lucent.com` vers le fichier

`aluidm5529.crt`. Utilisez un nom de fichier qui décrit le certificat. Dans cet exemple, le nom de fichier `aluidm5529.crt` décrit un certificat pour un Alcatel-Lucent 5529.

En outre, veillez à ce que le fichier de certificat se trouve dans le répertoire `./certs` du serveur où réside Network Manager.

GetEntities
Indicateur de la reconnaissance des entités physiques, telles que les armoires, les cartes et les ports. Définissez la valeur 1 pour reconnaître les entités physiques. Si vous définissez `0`, seules les informations de châssis sont reconnues. La valeur par défaut est 1.

GetOnt
Indicateur pour indiquer si le collecteur extrait les informations ONT (Optical Network Terminal). Définissez la valeur 1 pour activer l'extraction des données du module ONT. Cette extraction repose sur les informations des entités physiques. Veillez à affecter à **GetEntities** la valeur 1 si vous voulez affecter à **GetOnt** la valeur 1.

L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur qui n'est pas compatible avec HTTPS :

```
DataSource =>
{
                Host => 192.168.1.2,
                Port => 8080

                Username => 'oss',
                Password => 'myPa55w0rd'

                Timeout => 30

       Domain => 'AMS'

DataAcquisition =>

      GetEntities => 1

DataProcessing =>

       GetOnt => 0,
.
.
.
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de l'utiliser :

```
DataSource =&gt;
{
                Host =&gt; 192.168.1.2,


                Username =&gt; 'oss',
                Password =&gt; 'myPa55w0rd',

                Timeout =&gt; 30,

     Domain => 'AMS'


    UseSSL => 1,
    SSLCertFile => 'certs/alu5529idm.crt',
```

```
&mldr;
&mldr;
&mldr;
},
```

Fix Pack 4 L'exemple suivant montre des exemples de valeurs et les valeurs par défaut de ces propriétés pour un collecteur compatible avec HTTPS et qui choisit de ne pas l'utiliser :

```
DataSource =>
{
                Host => 192.168.1.2,


                Username => 'oss',
                Password => 'myPa55w0rd',

                Timeout => 30,

     Domain =&gt; 'AMS'


    UseSSL =&gt; 0,
&mldr;
&mldr;
&mldr;
},
```

4. Veillez à affecter à **Batchsize** la valeur 500, sauf indication contraire du support IBM. Ce paramètre contrôle la taille de chaque réponse SOAP/XML.
5. Sauvegardez le fichier de configuration du collecteur.

Configuration du collecteur GenericCsv :

Pour utiliser les données issues du collecteur GenericCsv dans une reconnaissance de réseau vous devez configurer les informations de connexion entre le système EMS et Network Manager.

1. Modifiez le fichier de configuration du collecteur : NCHOME/precision/collectors/perlCollectors/GenericCsv/GenericCsv Collector.cfg
2. Modifiez la section General du fichier de configuration. Définissez les propriétés suivantes :

   Débogage

   Mode de débogage du collecteur. Définissez la valeur 0 pour désactiver le débogage. Définissez la valeur 4 pour l'activer. La valeur 1, 2 ou 3 est équivalente à la valeur 0. Le collecteur affiche debug (stdout).

   Mode écoute

   Port qu'écoute le collecteur pour les demandes XML-RPC de Network Manager.

   Ce port est également utilisé par le collecteur pour fournir des réponses XML-RPC à Network Manager. Par défaut, il s'agit du port 8081. Le port doit correspondre à celui que vous avez configuré dans l'insertion dans la table collectorFinder.collectorRules dans le fichier DiscoCollectorFinderSeeds.cfg lors de l'indication de valeurs de départ pour la reconnaissance initiale du collecteur.

Délai d'attente
Délai d'attente de la communication du collecteur vers Network Manager. Le délai est exprimé en secondes. La valeur par défaut est 15 secondes.

L'exemple suivant montre les valeurs par défaut de ces propriétés :

```
General =>
{
                Debug => 0,
                Listen => 8081,
                Timeout => 15
},
```

3. Modifiez la section `DataSource` du fichier de configuration en spécifiant le nom du fichier CSV, comme illustré dans l'exemple suivant :

```
DataSource =>
{
                CsvCfg => 'exampleCsv.cfg',
...
...
...
},
```

4. Sauvegardez le fichier de configuration du collecteur.

Démarrage des collecteurs :

Avant le démarrage de la reconnaissance, tous les collecteurs doivent être en cours d'exécution. Vous devez démarrer les collecteurs ou vous assurez qu'ils sont en cours d'exécution avant de démarrer une reconnaissance qui comprend des collecteurs.

Démarrez un collecteur en accédant à son répertoire, puis en émettant une commande sur l'interface de ligne de commande. Emettez la commande suivante pour démarrer un collecteur (notez que la commande est entrée en une seule ligne. Les options sont expliquées dans le tableau ci-dessous) :

```
ncp_perl script_collecteur -cfg  FICHIER_CONFIG_COLLECTEUR
[ -csvcfg FICHIER_CONFIG_COLLECTEUR ] [ -listen PORT_PRECISION ]
[ -debug DEBUG ] [ -logdir ] [ -nologdir NOMREP ]
[ -help ] [ -version ]
```

Tableau 9. Explication des options de ligne de commande

Option	Explication
script_collecteur	Nom du script perl qui implémente le collecteur, par exemple, `main.pl`.
`-cfg` *FICHIER_CONFIG_COLLECTEUR*	Indique le fichier de configuration du collecteur.
`-csvcfg` *FICHIER_CONFIG_COLLECTEUR_CSV*	Utilisez ce paramètre facultatif pour indiquer le nom d'un fichier CSV à utiliser en tant que source de données. Vous pouvez également indiquer ce paramètre dans le fichier de configuration du collecteur. **Restriction :** Ce paramètre n'est valide que si la source de données est un fichier CSV.
`-listen` *PORT_PRECISION*	Méthode alternative permettant d'indiquer un port sur lequel le collecteur doit écouter les requêtes de Network Manager. N'indiquez une valeur ici que si aucune valeur de port n'a été indiquée dans le fichier de configuration du collecteur basé sur SOAP ou dans celui du collecteur basé sur CSV.

Tableau 9. Explication des options de ligne de commande (suite)

Option	Explication
`-debug DEBUG`	Niveau de la sortie de débogage (1-4, où 4 représente la sortie la plus détaillée).
`-logdir NOMREP`	Dirige les messages de journal de chaque processus démarré par CTRL vers `NCHOME/log/precision`.
`-nologdir NOMREP`	Dirige les messages de journal pour chaque processus démarré par CTRL vers un fichier distinct du dossier indiqué.
`-help`	Tous les composants Network Manager disposent d'une option spéciale `-help` qui permet d'afficher les options de ligne de commande. Le composant n'est pas démarré même si `–help` est utilisé conjointement avec d'autres arguments.
`-version`	Tous les composants Network Manager disposent d'une option spéciale `-version` qui permet d'afficher de numéro de version du composant. Le composant n'est pas démarré même si `–version` est utilisé conjointement avec d'autres arguments.

Définition de l'emplacement d'une reconnaissance EMS :

Définissez l'emplacement d'une reconnaissance EMS en distribuant l'outil de recherche Collector. Cette configuration n'est généralement à faire qu'une fois, lors de l'ajout d'un nouveau collecteur à votre installation.

Pour permettre à Network Manager de rechercher des collecteurs, vous devez définir l'emplacement de l'outil de recherche Collector. Ceci implique la spécification des éléments suivants pour chaque collecteur :

- Le nom d'hôte de l'unité sur laquelle s'exécute le collecteur
- Le port de cette unité sur lequel écoute le collecteur

Si un collecteur s'exécute sur le même hôte que Network Manager, vous n'avez besoin de spécifier que le port.

Remarque : Si vous procédez à la nouvelle reconnaissance d'une unité en utilisant l'outil de recherche Collector, indiquez l'adresse IP de l'unité ou du sous-réseau sur lequel effectuer une nouvelle reconnaissance à l'aide de l'interface graphique de la configuration de la reconnaissance.

Vous pouvez définir l'emplacement de l'outil de recherche Collector pour accomplir une reconnaissance ou une nouvelle reconnaissance partielle d'une unité ou d'un sous-réseau. Si vous définissez l'emplacement de l'outil de recherche Collector pour effectuer une nouvelle reconnaissance partielle, vous pouvez également indiquer une unité ou un sous-réseau récupérés par le collecteur.

Vous devez définir l'emplacement de l'outil de recherche Collector en utilisant le nom d'hôte de l'unité sur laquelle s'exécute le collecteur et le port de cette unité sur lequel écoute le collecteur. Si le collecteur s'exécute sur le même hôte que Network Manager, vous n'avez besoin d'indiquer que le port.

Définition de l'emplacement du collecteur pour une première reconnaissance

Définissez l'emplacement l'outil de recherche Collector pour une première reconnaissance en ajoutant une insertion à la table collectorFinder.collectorRules du fichier de configuration DiscoCollectorFinderSeeds.cfg. L'insertion suivante définit l'emplacement de l'outil de recherche Collector en utilisant le nom d'hôte 172.16.25.1 et le port 8082. Cette insertion signifie que le collecteur s'exécute sur un hôte dont l'adresse IP est 172.16.25.0, ce qui diffère de l'hôte sur lequel s'exécute Network Manager. Le nombre de tentatives pour ce collecteur est de 5.

```
insert into collectorFinder.collectorRules
(
        m_Host,
        m_Port,
        m_NumRetries
)
values
(
        "172.16.25.1",
        8082,
        5
);
```

Activation des agents de reconnaissance des collecteurs :

Par défaut, les agents de reconnaissance des collecteurs ne sont pas activés. Vous devez les activer si vous exécutez une reconnaissance qui inclut une reconnaissance basée sur les collecteurs.

Pour activer les agents de collecteurs :

1. Dans l'interface graphique de la configuration de reconnaissance, sélectionnez l'onglet **Agents de reconnaissance complète**.
2. Sélectionnez les agents suivants en cochant la case située en regard de l'agent :
   - **CollectorDetails**
   - **CollectorInventory**
   - **CollectorLayer2**
   - **CollectorLayer3**
   - **CollectorVpn**

   Conseil : Vous pouvez devoir faire défiler la liste des agents vers le bas pour les trouver.
3. Cliquez sur **Sauvegarder** pour enregistrer ces paramètres de configuration dans le fichier schéma DiscoAgents.*NOM_DOMAINE*.cfg, où *NOM_DOMAINE* est le nom du domaine de reconnaissance, par exemple NCOMS.

Tâches associées:

«Activation des agents», à la page 35
Vous devez activer les agents appropriés pour la reconnaissance que vous souhaitez réaliser. Vous pouvez indiquer des agents pour une reconnaissance complète ou une reconnaissance partielle.

Emplacements et fichiers des collecteurs EMS :

Des scripts Perl et un fichier de configuration au format texte brut sont disponibles pour chaque collecteur par défaut dans un répertoire distinct, sous le répertoire `NCHOME/precision/collectors/perlCollectors/`.

Les utilisateurs expérimentés peuvent développer de nouveaux collecteurs pour activer Network Manager afin d'interagir avec d'autres EMS. Les fichiers de configuration et exécutables de chaque nouveau collecteur doivent être placés dans un répertoire nommé en conséquence sous le répertoire `NCHOME/precision/collectors/perlCollectors/`.

Les collecteurs par défaut sont répertoriés dans le tableau ci-dessous.

Nom	Répertoire	Fichier de configuration
Alcatel5620SamSoap	`NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap/`	`Alcatel5620SamSoap Collector.cfg`
Alcatel5620SamSoapFindToFile	`NCHOME/precision/collectors/perlCollectors/Alcatel5620SamSoap FindToFile/`	`Alcatel5620SamSoap FindToFileCollector.cfg`
Alcatel5620SamCsv	`NCHOME/precision/collectors/perlCollectors/Alcatel5620SamCsv/`	`Alcatel5620SamCsv Collector.cfg`
Alcatel5529IdmSoap	`NCHOME/precision/collectors/perlCollectors/Alcatel5529IdmSoap/`	`Alcatel5529IdmSoap Collector.cfg`
GenericCsv	`NCHOME/precision/collectors/perlCollectors/GenericCsv/`	`GenericCsv Collector.cfg`
Huawei U2000 iManager Collector	`NCHOME/precision/collectors/perlCollectors/HuaweiU2000iManagerTL1/`	`HuaweiU2000iManagerTL1 Collector.cfg`

Configuration d'une reconnaissance contextuelle

Si vous disposez d'unités que vous devez reconnaître, comme des unités périphériques SMS, MPLS ou d'autres unités comportant des routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. La reconnaissance contextuelle garantit une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type d'unité est pris en charge par la reconnaissance.

Dans une reconnaissance contextuelle, les informations concernant un périphérique sont transmises de la table `returns` de l'agent Details à la table `despatch` de l'agent Context adéquat.

Les agents Context utilisent les filtres des fichiers portant l'extension .agent pour déterminer les périphériques à traiter. Ceci est vrai pour tous les agents de reconnaissance. Si le périphérique n'est pas d'un type qui prend en charge les routeurs virtuels, c'est-à-dire qui n'a pas besoin de traitement contextuel, elle est transmise directement à l'agent Associated Address.

Avertissement : L'activation d'une reconnaissance contextuelle active automatiquement tous les agents Contexte. La désactivation d'une reconnaissance contextuelle désactive automatiquement tous les agents Contexte. N'activez ou ne désactivez pas manuellement les agents Contexte, que ce soit via les fichiers de configuration ou l'interface graphique de configuration de la reconnaissance.

Pour activer une reconnaissance contextuelle, ajoutez l'insertion suivante au fichier `DiscoConfig.cfg` :

```
insert into disco.config
(
      m_UseContext
)
values
(
      1
)
```

L'insertion de la valeur `0` désactive la reconnaissance contextuelle.

Concepts associés:

«Reconnaissance des détails des périphériques (contextuels)», à la page 351
La reconnaissance des détails contextuels des périphériques s'effectue en plusieurs étapes.

Référence associée:

«Agents de reconnaissance contextuelle», à la page 396
Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

Configuration des reconnaissances MPLS

Configurez une reconnaissance MPLS pour reconnaître des réseaux MPLS principaux et les VPN qui utilisent ces réseaux principaux. La configuration avancée de la reconnaissance MPLS fournit des éléments de personnalisation supplémentaires.

A propos de la reconnaissance MPLS

Les administrateurs des fournisseurs de services qui proposent des services de réseau privé virtuel MPLS (Multiprotocol Label Switching ou commutation d'étiquettes multi-protocoles) peuvent reconnaître les réseaux principaux MPLS et les réseaux privés virtuels MPLS afin de permettre aux centres de gestion de réseaux des fournisseurs de services de surveiller le bon état de marche des réseaux privés virtuels clients.

Network Manager prend en charge la reconnaissance des réseaux virtuels privés ci-après, s'exécutant sur des réseaux principaux MPLS :

- Réseaux privés virtuels de couche 3
- Réseaux privés virtuels de couche 2 étendus

Pour ces derniers, Network Manager reconnaît les pseudo-connexions point-à-point reliant deux routeurs provider edge (PE).

Les sections suivantes indiquent la terminologie et les conventions de visualisation de la topologie utilisées dans Network Manager pour faire référence aux réseaux MPLS.

Remarque : Les graphiques présentés dans cette section sont des représentations conceptuelles d'un réseau MPLS. Vous ne pouvez pas voir ces vues conceptuelles dans l'interface graphique Vues de réseau.

Réseaux privés virtuels MPLS de couche 3 :

Network Manager peut visualiser les topologies de réseau privé virtuel MPLS de couche 3 dans une vue principale ou secondaire.

Les vues principale et secondaire diffèrent de la manière suivante :

- La vue principale affiche les routeurs provider-edge (PE)et fournit la visibilité des routers provider core (P) et des données LSP (Label Switched Path) au sein du noyau MPLS pour chaque réseau privé virtuel s'exécutant sur le noyau MPLS.
- La vue secondaire affiche uniquement les routeurs PE et le nuage MPLS. Elle ne donne pas de visibilité sur les périphériques du noyau.

Réseaux privés virtuels MPLS de couche 2 étendus :

Pour les réseaux privés virtuels de couche 2 étendus, Network Manager ne fournit qu'une vue secondaire de votre réseau principal MPLS.

Network Manager affiche un réseau privé virtuel étendu de couche 2 en tant que collection de pseudo-connexions point-à-point. Cela signifie que si un réseau privé virtuel étendu de couche 2 contient plus de deux routeurs provider edge (PE), Network Manager affiche ce réseau privé virtuel en plusieurs vues, chacune d'elles consistant en un seul PE vers une connexion PE point-à-point.

Le tableau 10 montre des exemples de réseaux privés virtuels étendus de couche 2 avec deux PE ou plus. Le tableau indique également le nombre de pseudo-connexions et donc le nombre de vues que Network Manager affiche pour chaque réseau privé virtuel.

Tableau 10. Nombre de pseudo-connexions pour un réseau privé virtuel étendu de couche 2

Nombre de PE dans un réseau privé virtuel étendu de couche 2	Nombre de connexions point-à-point	Nombre de vues affichées par Network Manager pour ce réseau privé virtuel
2	1	1
3	3	3
4	6	6

Configuration de la reconnaissance MPLS standard et avancée :

Configurez une reconnaissance MPLS standard afin de reconnaître tous vos réseaux MPLS et utilisez la convention de désignation par défaut pour les réseaux privés virtuels reconnus. La configuration standard de la reconnaissance MPLS permet également l'affichage des événements affectés par un service (SAE) dans le **Liste des événements actifs**. La configuration avancée de la reconnaissance MPLS propose des fonctions de personnalisation supplémentaires.

Les activités de configuration pour le réseau MPLS incluent le processus de distribution, la configuration et les autres activités de reconnaissance standard.

Les configurations standard et avancée de la reconnaissance MPLS diffèrent de la manière suivante :

- Reconnaissance MPLS standard : reconnaît tous vos réseaux MPLS et utilise la convention de désignation par défaut pour les réseaux privés virtuels (VPN) reconnus
- Reconnaissance MPLS avancée : à l'aide des options de configuration avancée, vous pouvez exécuter les tâches suivantes :
  - Limiter la portée de reconnaissance à un VPN ou à un outil de recherche de routeurs virtuels (VRF) spécifique
  - Configurer vos propres conventions de désignation VPN
  - Forcer la reconnaissance de libellé même si vous avez sélectionné une reconnaissance basée sur RT

Après avoir configuré et exécuté une reconnaissance MPLS, vos opérateurs peuvent surveiller les VPN des clients comme suit :

- Afficher les mappes topologiques des VPN sélectionnés, qui montrent l'état d'alerte des VPN et des périphériques situés dans les VPN.
- Identifier des événements affectés par un service (SAE) dans la **Liste des événements actifs**. Un SAE est une alerte qui prévient les opérateurs qu'un service client critique, par exemple un VPN client, a été affecté par un ou plusieurs événements de réseau. Les événements de réseau sous-jacents se produisent sur une interface, sur un routeur PE ou CE.

A propos des événements affectés par le service :

Une alerte d'événement affecté par le service (SAE) avertit les opérateurs qu'un service client critique a été affecté par un ou plusieurs événements de réseau.

Un service SAE est proposé lorsqu'un ou plusieurs événements se produisent sur une interface PE (Provider Edge) ou CE (Customer Edge) dans un réseau privé virtuel (VPN) ou un réseau privé virtuel (VPLS). Les événements de réseau sous-jacents se déroulent sur une interface d'un routeur PE ou CE ou sur le lien existant entre eux. Vous devez configurer la reconnaissance MPLS pour déduire l'existence de routeurs CE afin que tous les SAE possibles soient générés pour vos réseaux privés virtuels clients.

La liste ci-après donne deux exemples de SAE générés sur deux réseaux privés virtuels clients différents :

- SAE généré sur le serveur privé virtuel client-1 en raison d'une interruption `Mpls VRF Down` sur une interface de routeur PE
- SAE généré sur le serveur privé virtuel client-3 en raison d'une interruption `LinkDown` sur une interface de routeur CE

Chaque SAE apparaît en tant qu'alerte dans la liste d'événements actifs. L'apparence du SAE avertit les opérateurs que le réseau privé virtuel client a été affecté, probablement de façon critique, par un ou plusieurs événements de réseau. Les opérateurs peuvent cliquer avec le bouton droit de la souris sur le SAE et émettre une commande pour afficher les événements sous-jacents qui ont causé le SAE.

Pour plus d'informations sur la liste d'événements actifs, voir *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*.

Configuration d'une reconnaissance MPLS standard

Configurez une reconnaissance MPLS pour reconnaître des réseaux MPLS principaux et les VPN qui utilisent ces réseaux principaux.

En plus des activités de configuration des reconnaissances standard, vous devez procéder à des activités de configuration de reconnaissances spécifiques à MPLS :

- Configurer des agents MPLS
- Indiquer les méthodes de reconnaissance, c'est-à-dire s'il faut exécuter une reconnaissance de discriminateurs de route ou de chemin commuté par étiquette (LSP)
- Configurer SNP et Telnet pour garantir que les agents peuvent accéder aux unités réseau
- Configurer Network Manager pour supposer l'existence de routeurs CE. Cette étape est nécessaire pour permettre aux opérateurs de voir les événements affectés par les services dans **Liste des événements actifs**.

Ces activités de configuration spécifiques à EMS sont décrites dans les rubriques suivantes.

Configuration d'agents MPLS :

Lors de la configuration d'une reconnaissance MPLS, vous devez activer un ou plusieurs agents MPLS. Vous pouvez également résoudre la difficulté posée par les adresses IP en double dans différents VPN en configurant l'agent AsAgent.

Les agents MPLS suivants et les fichiers de définitions d'agents (.agnt) correspondants sont fournis :

- Agent Telnet Juniper JuniperMPLSTelnet.agnt)
- Agent de routeur ERX Juniper (UnisphereMPLSTelnet.agnt)
- Agent Telnet MPLS Cisco (CiscoMPLSTelnet.agnt)
- Agent SNMP MPLS Cisco (CiscoMPLSSnmp.agnt)
- Agent Telnet MPLS Laurel (LaurelMPLSTelnet.agnt)

  Remarque : L'agent Telnet MPLS Laurel est destiné aux reconnaissances basées sur RT (RouteTarget).

Ces agents peuvent reconnaître des données de MPLS VPN et Virtual Private LAN Service (VPLS) à partir de périphériques du réseau.

Conseil : Les agents qui extraient des informations VPLS peuvent extraire de grandes quantités de données. L'activation de ces agents peut augmenter considérablement le temps de traitement du processus de reconnaissance. Si vous n'avez pas besoin de redécouvrir les informations VPLS, désactivez ces agents pour une reconnaissance plus rapide.

Remarque : Si vous disposez d'un réseau MPLS qui prend en charge les VPN de couche 3 et de couche 2 améliorée, alors les mêmes agents MPLS reconnaissent les deux types de VPN. Les vues de réseau peuvent également partitionner les VPN de couche 3 et de couche 2 améliorée simultanément sur le même réseau principal MPLS.

Si le réseau MPLS contient du matériel Cisco, activez l'agent Telnet MPLS Cisco et l'agent SNMP MPLS Cisco. Ces deux agents sont complémentaires :

- L'agent SNMP MPLS Cisco cible uniquement les unités dont l'IOS (Internetwork Operating System) prend complètement en charge la reconnaissance MPLS basée sur SNMP
- L'agent CiscoMPLSTelnet cible uniquement les unités dont l'IOS ne prend pas complètement en charge la reconnaissance basée sur SNMP

Avertissement : Soyez prudent lorsque vous modifiez le fichier CiscMPLSSnmp.agnt. Certaines unités de réseau peuvent contenir des versions d'IOS qui comportent un défaut pouvant affecter l'unité lorsque certaines données SNMP MPLS sont demandées. Ces versions d'IOS ont été filtrées par défaut dans le fichier CiscMPLSSnmp.agnt.

En plus de ces activités de configuration de reconnaissance standard, vous pouvez modifier la portée à des VPN ou des VRF spécifiques.

Tâches associées:

«Définition de la portée d'une reconnaissance MPLS/VPN», à la page 152
Lors de la configuration de la reconnaissance d'un ou plusieurs VPN (réseau privé virtuel) qui s'exécutent sur un réseau principal MPLS, vous pouvez limiter la portée de cette reconnaissance à un nom de VPN ou de table VRF (Virtual Routing and Forwarding) particulier.

Configuration d'agents Telnet MPLS :

Les agents CiscoMPLSTelnet, JuniperMPLSTelnet, LaurelMPLSTelnet et UnisphereMPLSTelnet obtiennent des données provenant d'unités, principalement via Telnet. Vous devez activer ces agents et configurer l'accès Telnet pour garantir que ces agents peuvent accéder aux unités et comprendre les sorties de ces unités.

Procédez comme suit pour configurer l'accès Telnet pour des agents Telnet MPLS :

1. Renseignez le fichier de configuration Telnet `TelnetStackPasswords.cfg` de sorte que les agents puissent accéder aux unités cible.
2. Configurez l'auxiliaire Telnet de sorte que les agents puissent comprendre la sortie de ces unités.

Tâches associées:

«Configuration de l'accès aux unités», à la page 30
Indiquez les noms de communauté SNMP et les informations d'accès Telnet pour permettre aux auxiliaires et à l'interrogation Network Manager d'accéder aux unités sur votre réseau.

Référence associée:

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

Configuration d'agents SNMP MPLS :

L'agent CiscoMPLSSnmp obtient des données issues d'unités utilisant SNMP. Vous devez activer cet agent et configurer l'accès SNMP pour garantir que cet agent peut accéder aux unités et comprendre les sorties de ces unités.

Pour configurer l'accès SNMP pour les agents SNMP MPLS :

Remarque : CiscoMPLSSnmp.agnt tente d'extraire les VPN L2 à l'aide des commandes 'show' de telnet si l'agent ne parvient pas à extraire les données via SNMP.

1. Configurez l'accès SNMP aux unités.
2. Configurez l'auxiliaire SNMP de sorte que les agents puissent comprendre la sortie de ces unités.

Tâches associées:

«Configuration de l'accès aux unités», à la page 30
Indiquez les noms de communauté SNMP et les informations d'accès Telnet pour permettre aux auxiliaires et à l'interrogation Network Manager d'accéder aux unités sur votre réseau.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

Configuration de l'agent AsAgent :

Pour éviter les incidents liés aux adresses IP en double dans des VPN différents, activez l'agent AsAgent et fournissez à Network Manager un fichier de mappage, `ASMap.txt`, qui contient une liste complète des unités de chaque VPN, ainsi qu'une étiquette `AddressSpace`, qui définit à quel VPN appartient chaque unité.

Lors d'une reconnaissance MPLS, Network Manager peut reconnaître des unités situées dans des VPN différents, mais disposant de la même adresse IP. Dans ce cas, Network Manager ne peut faire la différence entre ces unités et peut résoudre leur connectivité de manière incorrecte. Les unités en question peuvent être des routeurs CE à la périphérie des VPN ou des unités au sein des VPN.

Dans le fichier de mappage `ASMap.txt`, fournissez une liste complète des unités de chaque VPN, ainsi qu'une étiquette `AddressSpace`, qui définit à quel VPN appartient l'unité.

Le tableau 11, à la page 146 fournit une description de l'agent AsAgent que vous devez activer pour résoudre les incidents liés aux adresses IP en double.

Tableau 11. Agent AsAgent

Nom de l'agent	Fonction
AsAgent	Permet à Network Manager d'identifier les unités situées dans des VPN différents et disposant de la même adresse IP de manière unique et de résoudre ainsi correctement la connectivité des unités. Cet agent fonctionne en association avec le programme stitcher `ASRetprocessing.stch` et le fichier `ASMap.txt` du répertoire `NCHOME/precision/etc`.

Le tableau 12 fournit le format du fichier `ASMap.txt` en donnant un exemple du contenu de ce fichier. Les zones de ce fichier texte doivent être séparées par des tabulations.

Tableau 12. Format du fichier ASMap.txt

Nom de base	Espace adresse	Adresse IP
`CERouter-1`	`CLIENT-1`	`192.168.2.1`
`CEDevice-a`	`CLIENT-1`	`192.168.2.21`
`CEDevice-b`	`CLIENT-1`	`192.168.2.22`
`CEDevice-c`	`CLIENT-1`	`192.168.2.23`
`CERouter-2`	`CLIENT-2`	`192.168.2.1`
`CEDevice-a`	`CLIENT-2`	`192.168.2.31`
`CEDevice-b`	`CLIENT-2`	`192.168.2.32`

Configuration de la méthode de reconnaissance MPLS :

Vous pouvez configurer une reconnaissance MPLS de deux manières : reconnaissance basée cible de routage (RT) ou reconnaissance basée LSP (Label Switched Path).

Méthodes de configuration de la reconnaissance MPLS :

- Reconnaissance basée sur les discriminateurs de route (RT) : Network Manager utilise des informations VRF et RT pour déterminer quels routeurs fournisseurs auxiliaires sont liés à un VPN.
- Reconnaissance basée sur un chemin commuté par étiquette (LSP) : Network Manager utilise des informations VRF et LSP pour déterminer quels routeurs fournisseurs auxiliaires sont liés à un VPN et quels routeurs fournisseurs principaux (P) sont traversés par les LSP dans ce VPN.

Choisissez la méthode de reconnaissance MPLS à utiliser en cochant ou non la case **Activer la reconnaissance de réseau virtuel privé MPLS basée sur RT** dans l'interface graphique de la configuration de la reconnaissance.

- Cochez la case **Activer la reconnaissance de réseau virtuel privé MPLS basée sur RT** pour activer la reconnaissance MPLS basée sur RT.
- Décochez la case **Activer la reconnaissance de réseau virtuel privé MPLS basée sur RT** pour activer la reconnaissance MPLS basée sur LSP.

Vous pouvez également effectuer cette configuration manuellement en définissant la valeur de la zone `m_RTBasedVPNs` de la table `disco.config`.

Remarque : Les reconnaissances basées RT reposent sur une technologie plus récente que les reconnaissances basées LSP et peuvent améliorer les performances

de la reconnaissance. Pour éviter des problèmes de performances liés à des reconnaissances MPLS/VPN basées LSP, utilisez l'option par défaut, à savoir la reconnaissance basée RT. L'option de reconnaissance est celle définie par défaut sur l'onglet **Options avancées** de la page **Configuration de la reconnaissance réseau**. Vous pouvez utiliser des noms VRF avec l'option de reconnaissance basée RT en modifiant le fichier de configuration comme décrit dans la rubrique «Utilisation de noms VRF avec les reconnaissances basées RT».

Le tableau 13 synthétise les différences entre la reconnaissance basée sur RT et la reconnaissance basée sur LSP.

Tableau 13. Reconnaissance basée sur RT et reconnaissance basée sur LSP

Type de reconnaissance	**Données d'étiquette**	**Vue principale**	**Résolution du VPN**
Reconnaissance basée sur RT	Aucune donnée d'étiquette n'est requise pour ce type de reconnaissance La reconnaissance est plus rapide	Se compose de tous les périphériques pour lesquels MPLS est activé	Les VPN sont résolus en fonction des informations RT
Reconnaissance basée sur LSP	Les données d'étiquette sont reconnues afin de tracer les LSP La reconnaissance est plus lente	Se compose des périphériques traversés par les LSP adéquates	Les VPN sont résolus en fonction des informations VRF et des chemins d'étiquette

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

«Table disco.config», à la page 230
La table config configure le fonctionnement général du processus de reconnaissance.

Utilisation de noms VRF avec les reconnaissances basées RT :

Vous préférerez peut-être les reconnaissances basées LSP afin d'utiliser le nom VRF plus familier pour les réseaux privés virtuels. Toutefois, vous pouvez également utiliser des noms VRF avec les reconnaissances basées RT.

Important :

Si des périphériques ont été reconnus précédemment alors que la dénomination VRF était activée, des entités de réseau privé virtuel (VPN) en double peuvent apparaître au cours de la reconnaissance suivante. Par exemple, la même entité VPN peut apparaître deux fois, une avec le nom VRF et l'autre avec le nom RT. Pour éviter des entrées de périphérique en double, associez la valeur zéro à la propriété LingerTime de tous les périphériques de la topologie avant d'exécuter la reconnaissance suivante. Pour cela, procédez comme suit :

1. Connectez-vous au fournisseur de services OQL à l'aide de la commande suivante :

   ```
   ncp_oql -domain NCOMS -service Model
   ```

2. Exécutez la commande suivante pour associer la valeur zéro à LingerTime :

   ```
   update ncimCache.lingerTime set lingerTime = {LINGERTIME=0};
   go
   ```

Pour utiliser des noms VRF avec des reconnaissances basées RT, procédez comme suit :

1. Fermez toutes les instances de l'interface graphique **Configuration de la reconnaissance**.
2. Accédez au répertoire NCHOME/etc/precision.
3. Modifiez le fichier DiscoConfig.*nom_domaine*.cfg comme suit :
   a. Définissez la zone **m_RTVPNResolution** à 2 dans la table disco.config.
   b. Vérifiez que la valeur du paramètre **m_RTBasedVPNs** est définie à 1.
4. Redémarrez les processus ncp pour relire les fichiers de configuration :

   ```
   itnm_stop ncp
   itnm_start ncp
   ```

   Vous avez également la possibilité de redémarrer le processus ncp_config.

Induction de l'existence de routeurs CE :

Vous pouvez induire l'existence des routeurs CE de vos clients en créant des spécifications dans les options de configuration de la reconnaissance avancée de l'interface graphique de la configuration de la reconnaissance.

Si l'hôte sur lequel Network Manager est installé ne dispose d'aucun accès aux routeurs CE de vos clients, Network Manager ne peut pas reconnaître ces routeurs directement. Cette situation se produit généralement lorsque l'entreprise fournissant les services MPLS possède les routeurs PE, mais ne dispose d'aucun accès aux routeurs CE, qui appartiennent aux clients qui exécutent les VPN.

Remarque : Cette situation ne se produit pas si l'entreprise fournissant les services MPLS possède et gère à la fois les routeurs PE et CE, et dispose ainsi d'un accès aux deux ensembles d'unités.

Pour induire l'existence des routeurs CE de vos clients, indiquez ceci dans les options de configuration de la reconnaissance avancée de l'interface graphique de la configuration de la reconnaissance.

Remarque : Ne suivez cette procédure que pour les emplacements où l'interface PE se trouve sur un sous-réseau /30. Dans ce cas, l'autre unité du sous-réseau doit être le routeur CE et l'adresse IP du CE doit être autre l'autre adresse IP du sous-réseau /30.

Limitations de l'induction de l'existence de routeurs CE :

- Evitez d'induire l'existence de routeurs CE si vos routeurs PE sont connectés aux routeurs CE par des liens série et que vous savez qu'il existe des adresse IP en double parmi les routeurs et les périphériques CE du réseau principal MPLS. Network Manager supprime de la topologie tout routeur principal MPLS reconnu qui dispose de la même adresse IP qu'une adresse IP CE induite.
- Si vos routeurs PE sont connectés aux routeurs CE par Ethernet, vous pouvez induire l'existence de routeurs CE sans procéder à des vérifications

supplémentaires. Dans ce cas, Network Manager peut déterminer l'adresse MAC du routeur CE. Si Network Manager a reconnu une autre unité disposant de la même adresse MAC, alors il doit s'agir du réseau CE. Dans ce cas, Network Manager utilise les données du périphérique reconnu et n'induit pas l'existence du CE.

Référence associée:

«Paramètres de reconnaissance avancés», à la page 45
Les paramètres avancés contrôlent les fonctions de la reconnaissance comme les processus et les délais d'attente concomitants. Ces paramètres permettent d'augmenter la vitesse de la reconnaissance, tout en l'équilibrant avec la charge du serveur. Généralement, une reconnaissance plus rapide a pour conséquence l'utilisation d'une plus grande quantité de mémoire sur le serveur.

Configuration d'une reconnaissance MPLS avancée

Configurez une reconnaissance MPLS avancée pour obtenir des fonctions de personnalisation avancées qui ne sont pas incluses dans la reconnaissance MPLS standard.

Lors de la configuration d'une reconnaissance MPLS avancée, vous devez accomplir les activités suivantes en plus des activités nécessaires à une reconnaissance MPLS standard.

- Définir la portée de la reconnaissance MPLS : vous permet de limiter la portée de cette reconnaissance à un VPN ou VRF spécifique.
- Indiquer un nom VPN : vous permet de configurer vos propres conventions d'attribution de nom VPN
- Affiner la reconnaissance de données d'étiquette : vous permet de forcer la reconnaissance LSP, quelle que soit la méthode de reconnaissance MPLS sélectionnée

Configuration de la reconnaissance de tunnels TE (Traffic Engineered) MPLS :

Pour découvrir des tunnels TE (Traffic Engineered) MPLS, activez l'agent StandardMPLSTE, configurez les informations extraites et configurez la portée de la reconnaissance.

Modes de reconnaissance de tunnels TE (Traffic Engineered) MPLS :

Définissez le mode de reconnaissance en fonction du niveau de détail que vous souhaitez extraire.

Un commutateur de mode est fourni dans le fichier de configuration de l'agent de reconnaissance ; il permet de configurer des instances de tunnel spécifiques, qui peuvent être remplacées par des caractères génériques, pour extraire différentes quantités de données de tunnel. Vous pouvez sélectionner l'un des modes suivants.

HeadEndHops (valeur par défaut)

En mode HeadEndHops, l'agent extrait l'extrémité de tête et l'extrémité de queue du tunnel et les LSR en transit et les interfaces de tronçon suivant sont identifiés par la recherche des données de tronçon de route réelle et calculée sur le LSR d'extrémité de tête. Les données de route réelle et calculée sont extraites des tables MIB mplsTunnelARHopTable et mplsTunnelCHopTable respectivement. Ce mode de reconnaissance ne stocke pas d'instances de tunnel de transit et d'extrémité de queue par opposition aux LSR de transit et d'extrémité de queue. Une connexion est créée dans la topologie TE MPLS entre les interfaces LSR d'extrémité de

tête et d'extrémité de queue, lesquelles sont associées à l'objet tunnel LSR d'extrémité de tête pour l'interface de tunnel appropriée.

Les pointeurs d'interconnexion MPLS qui sont reconnus et résolus sur le tunnel de tête seront résolus sur l'ID LSP approprié, si possible.

Vous pouvez utiliser ces informations pour déterminer si le chemin réel emprunté par un tunnel est différent du chemin calculé par Compute Shortest Path First (CSPF). Vous pouvez voir le chemin calculé et le chemin réel, bien qu'il n'y ait aucun moyen de déterminer qu'un LSR agit dans une fonction de transit ou de queue sans observer les données de tunnel LSR d'extrémité de tête.

Remarque : Les données de route réelle sont disponibles uniquement si l'option RRO (Record Route Option) a été indiquée pour l'instance de tunnel.

Dans le schéma de la table scope.mplsTe, le mode HeadEndHops se mappe sur la valeur 1 de m_Mode.

HeadTailEnd

En mode HeadTailEnd, seuls les points d'extrémité de tête et de queue de tunnel TE MPLS sont résolus, par l'interrogation du routeur d'extrémité de tête Label Switching Router (LSR). Ce mode fournit la quantité minimale d'informations sur les tunnels TE MPLS. Une connexion dans la topologie TE MPLS est créée entre les interfaces LSR d'extrémité de tête et d'extrémité de queue. Une instance de ressource de tunnel est associée à l'entité LSR du tunnel d'extrémité de tête.

Dans ce mode, vous ne pouvez pas identifier les LSR en transit et les données de route calculée et réelle ne sont pas extraites.

Les pointeurs d'interconnexion MPLS qui sont reconnus et résolus sur le tunnel de tête seront résolus sur l'ID LSP approprié, si possible.

Dans le schéma de la table scope.mplsTe, le mode HeadTailEnd se mappe sur la valeur 2 de m_Mode.

AllLSRTunnelsAndHops

En mode AllLSRTunnelsAndHops, l'agent extrait l'extrémité de tête et l'extrémité de queue du tunnel et identifie les LSR en transit et les interfaces de tronçon suivant en recherchant des données de tronçon de route réelle et calculée sur le LSR d'extrémité de tête. Les données de route réelle et calculée sont extraites des tables MIB mplsTunnelARHopTable et mplsTunnelCHopTable respectivement. Ce mode de reconnaissance stocke les instances de tunnel de transit et d'extrémité de queue par opposition aux LSR de transit et d'extrémité de queue. Ce mode crée une connexion dans la topologie TE MPLS entre les interfaces LSR d'extrémité de tête et d'extrémité de queue, lesquelles sont associées aux objets tunnel LSR d'extrémité de tête (pour l'interface de tunnel), de transit et d'extrémité de queue. Les connexions de route calculée et réelle sont associées à des types d'entité de connexion calculée et réelle, qui sont regroupés en séquence à partir de l'entité de tunnel LSR d'extrémité de tête. Une instance de ressource de tunnel est associée à l'entité LSR du tunnel d'extrémité de tête.

Vous pouvez utiliser ces informations pour déterminer si le chemin réel emprunté par un tunnel est différent du chemin calculé par CSPF. Vous

pouvez visualiser le chemin calculé et réel et déterminer le rôle de transit ou d'extrémité de queue d'un LSR sans consulter l'instance de tunnel LSR d'extrémité de tête.

Remarque : Les données de route réelle sont disponibles uniquement si l'option RRO (Record Route Option) a été indiquée pour l'instance de tunnel.

Les pointeurs d'interconnexion MPLS qui sont reconnus et résolus sur le tunnel de tête seront résolus sur l'ID LSP approprié, si possible.

Dans le schéma de la table scope.mplsTe, le mode AllLSRTunnelsAndHops se mappe sur la valeur 3 de m_Mode.

Référence associée:

«Table mplsTe», à la page 254
La table mplsTe définit la portée de la reconnaissance de tunnel TE (Traffic Engineered) MPLS et définit les informations à extraire.

Activation de l'agent StandardMPLSTE :

Pour reconnaître des tunnels MPLS TE, vous devez activer l'agent StandardMPLSTE et ajouter les noms de communauté SNMP appropriés.

Pour activer l'agent StandardMPLSTE, procédez comme suit.

1. Cliquez sur **Reconnaissance** > **Configuration de la reconnaissance de réseau**. Dans la liste **Domaine**, sélectionnez le domaine requis.
2. Cliquez sur l'onglet **Agents de reconnaissance complète**. La Liste des agents apparaît, affichant tous les agents de reconnaissance disponibles pour l'option de reconnaissance sélectionnée.
3. Cochez la case située en regard de l'agent StandardMPLSTE.
4. Cliquez sur **Sauvegarder**  .
5. Facultatif : Si vous souhaitez reconnaître des tunnels MPLS TE, activez l'agent StandardMPLSTE pour de nouvelles reconnaissances partielles.
   a. Cliquez sur l'onglet **Agents de nouvelle reconnaissance partielle**.
   b. Cochez la case située en regard de l'agent StandardMPLSTE.
   c. Cliquez sur **Sauvegarder**  .
6. Assurez-vous que les noms de communauté SNMP sont correctement configurés pour pouvoir accéder aux unités des tunnels MPLS TE.

Tâches associées:

«Configuration de l'accès aux unités», à la page 30
Indiquez les noms de communauté SNMP et les informations d'accès Telnet pour permettre aux auxiliaires et à l'interrogation Network Manager d'accéder aux unités sur votre réseau.

Configuration de l'agent StandardMPLSTE :

Configurez les tunnels à découvrir et les détails à extraire.

Pour configurer l'agent StandardMPLSTE, procédez comme suit.

1. Sauvegardez et éditez le fichier `NCHOME/etc/precision/DiscoScope.cfg`.
2. Localisez et éditez l'insertion dans la table scope.mplsTe ou créez une insertion. Créez ou éditez une insertion similaire à la suivante :

```
insert into scope.mplsTe
(
   m_Protocol,
   m_Zones,
   m_Mode,
   m_TunnelFilter
)
values
(
   1,
   [{m_Subnet = '192.168.1.0', m_NetMask = 24 }],
   2,
   1
);
```

   Cette insertion configure l'agent afin qu'il se comporte de la façon suivante :

   - Il utilise IPv4.
   - Il inclut (`m_Tunnelfilter=1`) le sous-réseau 192.168.1.* dans la reconnaissance des têtes de tunnel.
   - Il extrait des données pour la tête et la queue du tunnel mais pas pour les routeurs de transit.
3. Sauvegardez et fermez le fichier.
4. Arrêtez et redémarrez le moteur de reconnaissance, le processus **ncp_disco**, pour que les modifications de configuration soient appliquées.

Référence associée:

«Table mplsTe», à la page 254
La table mplsTe définit la portée de la reconnaissance de tunnel TE (Traffic Engineered) MPLS et définit les informations à extraire.

Définition de la portée d'une reconnaissance MPLS/VPN :

Lors de la configuration de la reconnaissance d'un ou plusieurs VPN (réseau privé virtuel) qui s'exécutent sur un réseau principal MPLS, vous pouvez limiter la portée de cette reconnaissance à un nom de VPN ou de table VRF (Virtual Routing and Forwarding) particulier.

Limitez la portée en configurant la section facultative DiscoAgentDiscoveryScoping du fichier *.agnt. Les options configurables sont décrites dans le tableau 14.

Tableau 14. Définition d'exigences de portée MPLS

Option	Fonction
IncludeVRF	Autorise la reconnaissance du VRF nommé
IncludeVPN	Autorise la reconnaissance du VPN nommé
ExcludeVPN	Ne reconnaît aucun VRF dans le VPN nommé
ExcludeVRF	Ne reconnaît pas le VRF indiqué

L'ordre de priorité de `Exclude` et `Include` dans la section DiscoAgentDiscoveryScoping est le suivant :

1. Exclusion
2. Inclure

L'ordre de priorité de VRF et VPN dans la section DiscoAgentDiscoveryScoping est le suivant :

1. VRF
2. VPN

Par exemple, si vous incluez un VPN, mais qu'un autre filtre exclut un VRF dans votre VPN, le VRF est exclu. Si un VPN est exclu, mais qu'un autre filtre inclut un VRF dans ce VPN, alors le VRF est inclus.

Les noms des VRF sont sensibles à la casse et un astérisque (*) représente un caractère générique pour tout nom VRF ou VPN lorsqu'il est utilisé dans le nom de la configuration. L'astérisque peut être utilisé avec n'importe laquelle des options ci-dessus.

La définition de la portée en fonction des noms VPN ne fonctionne que lorsque les noms VRF configurés sur les périphériques reconnus par les agents MPLS sont au format VRF recommandé par Cisco. Un VRF est nommé d'après le ou les VPN servis et le type de la topologie. Le format des noms VRF se présente comme suit :

```
V [nombre affecté pour rendre le nom VRF unique]: [nom_VPN]
```

Par exemple, dans un VPN appelé `precision`, un VRF pour un routeur de concentrateur périphérique serait nommé :

```
V1:precision
```

Un VRF pour un routeur périphérique de rayon du VPN `precision` serait nommé :

```
V1:precision-s
```

Un VRF pour une topologie de VPN extranet du VPN `precision` serait nommé :

```
V1:precision-etc
```

L'exemple suivant définit la portée d'une reconnaissance dans un système composé de quatre VRF : `V65:Precision-etc`, `V65:Precision-s`, `V65:Precision` et `V44:AcmeSheds`.

```
//2 VRF doivent être inclus
//
DiscoAgentDiscoveryScoping
{
    IncludeVRF = "V65:Precision-etc";
    IncludeVRF = "V44:AcmeSheds";
}
//Les 4 VRF doivent être inclus
//
DiscoAgentDiscoveryScoping
{
    IncludeVPN = "Precision";
    IncludeVRF = "V44:AcmeSheds";
}
```

Référence associée:

«Table disco.config», à la page 230
La table config configure le fonctionnement général du processus de reconnaissance.

Configuration des conventions de dénomination VPN :

Si vous n'utilisez pas la convention de dénomination Cisco VRF, vous pouvez configurer votre propre convention de dénomination VPN en effectuant les insertions appropriées dans le programme stitcher `MPLSAddVPNNames.stch` située dans `$NCHOME/precision/disco/stitchers/`.

Le programme stitcher `MPLSAddVPNNames` extrait et construit un nom VPN à partir de la liste de chemins reconnus par les programmes stitcher de traçage de chemins. Le programme stitcher `MPLSAddVPNNames` peut ensuite ajouter le nom VPN aux interfaces d'unité qui correspondent aux chemins appartenant au VPN.

L'exemple suivant indique où modifier le nom VPN dans le fichier `MPLSAddVPNNames.stch`, situé dans `$NCHOME/precision/disco/stitchers`.

```
//Affectation de nom VPN
//
//Affecte le nom VRF en tant que nom VPN si aucun nom VPN n'a
//été reconnu par l'agent, i.e., si le nom VRF n'était pas au
//format Cisco.
//
vpnName = eval(text, '&m_VPNName');
if (vpnName == NULL)
{
    vpnName = vrfName;    //VPN=VRF, personnalisez en fonction de vos besoins
}
```

Mise au point des données d'étiquette :

La méthode de la reconnaissance MPLS (basée sur RT ou sur LSP) détermine si les agents MPLS récupèrent les données d'étiquette MPLS.

- Si vous choisissez la reconnaissance basée sur RT, les agents MPLS ne récupèrent pas les données d'étiquette.
- Si vous choisissez la reconnaissance basée sur LSP, les agents MPLS récupèrent les données d'étiquette.

Si vous choisissez une reconnaissance basée sur RT, il vous est possible de récupérer manuellement les données d'étiquette en ajoutant l'insertion suivante à la section DiscoAgentDiscoveryScoping du fichier MPLS `.agnt` approprié :

```
DiscoAgentDiscoveryScoping
{
        GetMPLSLabelData = 1;
}
```

Tâches associées:

«Configuration de la méthode de reconnaissance MPLS», à la page 146
Vous pouvez configurer une reconnaissance MPLS de deux manières : reconnaissance basée cible de routage (RT) ou reconnaissance basée LSP (Label Switched Path).

Configuration des reconnaissances NAT

Configurez une reconnaissance NAT afin de reconnaître des environnements NAT en mappant l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associée.

A propos de la conversion d'adresses réseau

Le nombre d'adresses IP disponibles au format 32 octets actuel n'est pas suffisant pour répondre à l'augmentation des demandes d'accès à Internet. La conversion d'adresses réseau a été conçue en tant que solution à court terme à ce problème car elle permet de fournir une méthode pour connecter plusieurs ordinateurs à un réseau IP à l'aide d'une seule adresse IP publique ou d'un faible nombre d'adresses IP publiques uniques.

La conversion d'adresses réseau est fréquemment utilisée dans les entreprises, dans lesquelles un routeur NAT se trouve au bord du réseau privé (appelé dans ce contexte domaine *de raccord*) et convertit les adresses IP annexées aux paquets entrant dans et sortant du domaine de raccord. Le routeur NAT, qui agit en fait en tant qu'agent entre Internet et le réseau local, stocke une liste des mappages entre les adresses publiques et privées.

Remarque : Un domaine de raccord est un réseau local utilisant des adresses IP internes. Le réseau peut utiliser des adresses IP privées, dont l'enregistrement a été annulé, à des fins de communication interne - ces adresses devant être converties en adresses IP uniques, publiques, lorsqu'elles communiquent à l'extérieur du réseau. Les adresses utilisées en interne par un domaine de raccord donné peuvent également être utilisées en interne par un autre domaine de raccord.

Par exemple, lorsqu'un ordinateur du réseau privé demande des informations au réseau public, le routeur NAT convertit automatiquement l'adresse privée de cet ordinateur en l'adresse publique du domaine, qui est la seule adresse transmise au réseau public. Lorsque les informations requises sont renvoyées, le routeur NAT consulte sa liste interne de mappages d'adresses publiques sur des adresses privées afin de réacheminer les informations vers l'ordinateur adéquat.

Il existe plusieurs façons différentes de configurer un environnement NAT. Les descriptions suivantes détaillent les types les plus connus d'environnements NAT.

Environnements NAT statiques :

Dans un envrionnement NAT statique, le routeur NAT mappe les adresses privées et publiques sur une base un à un, c'est-à-dire que l'adresse privée d'un périphérique donnée mappe toujours la même adresse publique. Ce type d'environnement NAT est généralement utilisé pour des périphériques devant être accessibles pour le réseau public.

Environnements NAT dynamiques :

Dans un environnement NAT dynamique, le routeur NAT alloue de manière dynamique les adresses IP publiques d'un groupe d'adresse à des périphériques situés sur le réseau privé qui veulent communiquer avec le réseau public. Une variante sur le NAT dynamique, *surcharge* ou PAT (conversion d'adresse de port), mappe plusieurs adresses privées en une seule et même adresse publique à l'aide de différents ports.

Plages d'adresses privées :

L'IANA (Internet Assigned Numbers Authority) a attribué plusieurs plages d'adresses devant être utilisées par les réseaux privés.

Les plages d'adresses devant être utilisées par les réseaux privés sont les suivantes :

- Classe A : `10.0.0.0` à `10.255.255.255`
- Classe B : `172.16.0.0` à `172.31.255.255`
- Classe C : `192.168.0.0` à `192.168.255.255`

Une adresse IP se trouvant dans ces plages est par conséquent considérée comme étant non routable car elle n'est pas unique. Tout réseau privé devant utiliser des adresses IP en interne peut utiliser toute adresse se trouvant dans ces plages sans nécessiter de coordination avec l'IANA ou un répertoire Internet. Les adresses se trouvant dans cet espace d'adresse privé sont seulement uniques dans un réseau privé donné.

Toutes les adresses extérieures à ces plages sont considérées comme publiques.

A propos de la reconnaissance NAT

Vous pouvez utiliser Network Manager pour gérer les environnements NAT, même s'il existe certaines restrictions sur les types d'environnement NAT actuellement pris en charge.

Network Manager peut interroger des passerelles NAT connues et prises en charge pour obtenir une liste de mappages d'une adresse IP publique sur une adresse IP privée pour des périphériques situés dans les domaines NAT. Sinon, ces mappages peuvent être fournis manuellement. Network Manager peut ensuite reconnaître ces périphériques situés derrière des passerelles NAT et possédant une adresse IP publique.

Chaque domaine NAT dispose d'un identificateur d'espace adresse unique. Chaque périphérique situé dans le domaine NAT dispose de l'identificateur d'espace adresse approprié annexé à son enregistrement. Cela permet aux périphériques d'être gérés (par exemple, interrogés).

Restrictions concernant la reconnaissance NAT :

Il existe plusieurs restrictions dans la gestion des environnements NAT utilisant Network Manager.

La gestion des environnements NAT à l'aide de Network Manager est limitée par les conditions suivantes :

- Network Manager peut reconnaître un ou plusieurs environnements NAT, mais tous utilisent le mappage statique d'adresse NAT.
- Network Manager peut reconnaître des périphériques dans plusieurs domaines NAT, indépendamment du fait de savoir si les adresses IP privées des périphériques sont dupliquées dans d'autres domaines NAT. Néanmoins, l'adresse IP publique de chaque périphérique dans chaque domaine doit être unique.
- Les périphériques situés dans un domaine NAT et ne disposant que d'adresses IP privées ne peuvent pas être reconnus ou gérés par Network Manager.
- Le processus de reconnaissance doit reconnaître l'environnement NAT de l'extérieur, c'est-à-dire à partir du réseau public.
- Les adresses IP virtuelles comme les adresses HSRP (Hot Standby Routing Protocol) ne peuvent pas être mappées. L'adresse physique réelle doit être utilisée.
- Les éléments suivants doivent être indiqués avant l'exécution de la reconnaissance :
  - Les adresses de toutes les passerelles NAT prises en charge.
  - Les conversions de passerelles NAT doivent être reconnues, soit automatiquement, soit en indiquant à l'agent de reconnaissance NATTextFileAgent un fichier à plat de mappages d'adresses IP publiques sur des adresses IP privées.

Différences au sein d'un flux de processus de reconnaissance NAT :

Le flux de processus de reconnaissance NAT diffère de celui d'une reconnaissance normale.

Concepts associés:

«Cycles de reconnaissance», à la page 348
Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

Téléchargement des informations de conversion :

Les informations de conversion NAT sont téléchargées par les agents NAT dans la table de bases de données translations.NATTemp avant que les outils de recherche ne traitent d'autres entités.

Tous les autres périphériques reconnus sont insérés dans la table finders.pending alors que le programme stitcher BuildNATTranslation.stch crée une table de conversion globale et la stocke dans la table de bases de données translations.NAT.

Les outils de recherche, les auxiliaires et autres composants devant accéder aux périphériques peuvent utiliser cette table pour rechercher l'adresse de n'importe quel périphérique se trouvant derrière une passerelle NAT.

Création de la topologie :

Lorsque la topologie est créée, le programme stitcher `AddBaseNATTags.stch` ajoute des informations NAT à l'enregistrement topologique de chaque périphérique contenu dans le domaine NAT.

Le tableau 15 affiche les informations ajoutées à l'enregistrement topologique pour chaque périphérique.

Tableau 15. Informations NAT ajoutées à l'enregistrement de périphérique

Colonne	Description
`ExtraInfo->m_AddressSpace`	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table `translations.NATAddressSpaceIds`. Si la reconnaissance n'utilise pas d'informations NAT, ou si le périphérique se trouve dans le domaine public, cette valeur est NULL (non définie).
`ExtraInfo->m_NATTranslated`	Entier booléen indiquant si le périphérique se situe derrière une passerelle NAT.
`ExtraInfo->m_InsideLocalAddress`	Adresse privée du périphérique.
`ExtraInfo->m_OutsideGlobalAddress`	Adresse publique du périphérique.

Configuration d'une reconnaissance NAT

Configurez une reconnaissance NAT pour reconnaître des environnements NAT et permettre à Network Manager de gérer des environnements NAT.

Vous pouvez définir la plupart des paramètres de reconnaissance NAT depuis l'interface graphique de la configuration de la reconnaissance, à l'exception des tâches suivantes :

- Configurer l'agent NATTextFileAgent afin de fournir une prise en charge pour tout périphérique de passerelle NAT non pris en charge
- Configurer l'agent NATGateway afin de corriger la connectivité incorrecte éventuelle se produisant lorsque la passerelle NAT ne se trouve pas dans l'espace adresse public.

Référence pour la configuration de reconnaissance NAT :

Utilisez ces instructions pas à pas pour configurer une reconnaissance NAT.

Les étapes sont décrites dans le tableau suivant.

Tableau 16. Référence pour la configuration de reconnaissance NAT

Action	Utilisation de l'interface graphique	Utilisation de la ligne de commande
1. Configurez la reconnaissance pour utiliser la conversion d'adresses réseau. Pour ce faire, utilisez l'interface graphique de configuration de reconnaissance ou la ligne de commande.	«Configuration de la conversion NAT», à la page 41	«Activation de la conversion NAT», à la page 161
2. Définissez chaque périphérique de passerelle NAT et son espace adresse correspondant. Pour ce faire, utilisez l'interface graphique de configuration de reconnaissance ou la ligne de commande.		«Définition d'espaces adresse pour des passerelles NAT», à la page 161

Tableau 16. Référence pour la configuration de reconnaissance NAT (suite)

Action	**Utilisation de l'interface graphique**	**Utilisation de la ligne de commande**
3. Indiquez comme valeur de départ de l'outil de recherche PING l'adresse IP de chaque périphérique de passerelle NAT.	«Emplacement de la reconnaissance», à la page 26	Conseils pour déterminer l'emplacement de départ d'une reconnaissance «Fichier de configuration DiscoPingFinderSeeds.cfg», à la page 72 Conseils pour déterminer l'emplacement de départ d'une reconnaissance NAT «Définition de l'emplacement de la reconnaissance à l'aide des adresses de passerelle NAT» , à la page 163

Tableau 16. Référence pour la configuration de reconnaissance NAT (suite)

Action	Utilisation de l'interface graphique	Utilisation de la ligne de commande
4. Définissez une zone de portée pour chaque périphérique de passerelle NAT. **Remarque :** Il n'est pas nécessaire de définir une zone de portée pour les périphériques de passerelle NAT dont l'adresse IP est déjà dans d'autres zones de portée définies pour la reconnaissance. **Remarque :** Ne définissez pas d'espace adresse pour les périphériques de passerelle NAT ou pour les portées de sous-réseau publiques. L'espace adresse peut uniquement être défini pour les sous-réseaux privés.	«Définir la portée de la reconnaissance», à la page 23	Conseils pour déterminer la portée d'une reconnaissance «Fichier de configuration DiscoScope.cfg», à la page 76 Exemple : comment définir une zone de portée pour un sous-réseau NAT privé «Définition d'une zone de portée dans un domaine NAT», à la page 162
5. Définissez les zones de portée pour les sous-réseaux publics associés à chaque espace adresse NAT. **Remarque :** Ne définissez pas d'espace adresse pour les périphériques de passerelle NAT ou pour les portées de sous-réseau publiques. L'espace adresse peut uniquement être défini pour les sous-réseaux privés.		
6. Lorsque cela est possible, définissez les zones de portée pour le sous-réseau privé associé à chaque espace adresse NAT. **Restriction :** Vous pouvez uniquement définir une zone de portée pour un espace adresse NAT privé où la combinaison de sous-réseau et de masque de réseau du sous-réseau privé est unique dans la configuration de reconnaissance. Définissez les paramètres suivants lors de la configuration de cette portée : 1. Désélectionnez l'option **Ajout à la Liste des emplacements de départ de commande PING**. En effet, les sous-réseaux privés n'acceptent pas la commande PING. 2. Définissez un espace adresse pour ce sous-réseau privé. Les avantages d'ajouter une zone de portée pour chaque espace adresse NAT privé sont les suivants : • Seules les adresses de cet espace privé sont commentées en retour pendant la reconnaissance. • Si le périphérique de passerelle NAT et les périphériques dans l'espace adresse NAT associé sont des routeurs, l'ajout d'une zone de portée pour cet espace adresse privé limite le téléchargement de données de routage inutiles.		
7. Activez les agents NAT comme suit : • Pour les périphériques de passerelle NAT, activez l'agent CiscoNATTelnet ou NATNetScreen. • Pour les périphériques de passerelle NAT non pris en charge, créez un fichier de mappage NAT et activez l'agent NATTextFileAgent	«Activation des agents», à la page 35	«Activation d'agents pour les périphériques de passerelle NAT pris en charge», à la page 164 «Activation d'agents pour les périphériques de passerelle NAT non pris en charge», à la page 165

Tâches associées:

«Exemple : Configuration d'une reconnaissance NAT», à la page 167
Cet exemple illustre comment définir des espace adresse à l'aide de l'agent NATTextFileAgent et comment configurer des portées de reconnaissance associées.

Activation de la conversion NAT :

Vous pouvez configurer le système de reconnaissance de sorte qu'il utilise la conversion NAT en modifiant $NCHOME/etc/precision/DiscoConfig.cfg pour créer ou modifier une insertion dans disco.NATStatus et définir m_UsingNAT sur 1 et m_NATStatus sur 0.

L'insertion complète doit ressembler à ceci :

```
insert into disco.NATStatus
(
        m_UsingNAT,
        m_NATStatus
)
valeurs
(
        1,
        0
);
```

Tâches associées:

«Configuration de la conversion NAT», à la page 41
Pour configurer une conversion NAT afin de reconnaître des environnements NAT, mappez l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associé.

«Activation de la conversion NAT»
Vous pouvez configurer le système de reconnaissance de sorte qu'il utilise la conversion NAT en modifiant $NCHOME/etc/precision/DiscoConfig.cfg pour créer ou modifier une insertion dans disco.NATStatus et définir m_UsingNAT sur 1 et m_NATStatus sur 0.

Définition d'espaces adresse pour des passerelles NAT :

Pour indiquer les adresses IP de vos passerelles NAT et l'identificateur de l'espace adresse que vous souhaitez utiliser pour chaque domaine NAT associé, modifiez `DiscoConfig.cfg` afin de créer ou de modifier une insertion dans `translations.NATAddressSpaceIds`.

Respectez les directives suivantes lors de la définition d'espaces adresse pour les passerelles NAT :

- L'adresse IP doit correspondre à l'adresse IP publique accessible depuis le serveur de gestion.
- La zone de l'espace adresse peut être toute chaîne de description. Evitez néanmoins les caractères spéciaux comme les guillemets. Utilisez les règles standard pour les noms DNS de l'espace adresse, car l'espace adresse peut faire partie du nom de ces unités.

L'exemple suivant d'insertion configure le système de reconnaissance pour deux passerelles NAT.

```
insert into translations.NATAddressSpaceIds
(
        m_NATGatewayIP,
        m_AddressSpaceId
)
```

```
values
(
         '172.16.1.112',
        'NATDomain1'
);

insert into translations.NATAddressSpaceIds
(
        m_NATGatewayIP,
        m_AddressSpaceId
)
values
(
         '172.16.1.104',
        'NATDomain2'
);
```

Tâches associées:

«Configuration de la conversion NAT», à la page 41
Pour configurer une conversion NAT afin de reconnaître des environnements NAT, mappez l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associé.

«Activation de la conversion NAT», à la page 161
Vous pouvez configurer le système de reconnaissance de sorte qu'il utilise la conversion NAT en modifiant $NCHOME/etc/precision/DiscoConfig.cfg pour créer ou modifier une insertion dans disco.NATStatus et définir m_UsingNAT sur 1 et m_NATStatus sur 0.

Définition d'une zone de portée dans un domaine NAT :

Vous pouvez personnaliser des zones d'inclusion et d'exclusion pour des domaines NAT individuels en utilisant la colonne `m_AddressSpace` de la table `scope.zones`.

L'exemple d'insertion suivant définit une zone d'inclusion pour un sous-réseau private associé à un domaine NAT.

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="172.16.2.*",
            }
        ],
        "NATDomain1"
);
```

L'exemple ci-dessus définit une zone d'inclusion. Network Manager reconnaît toute unité dont l'adresse IP commence par `"172.16.2"`, c'est-à-dire toute unité du sous-réseau privé `172.16.2.0` dont le masque est `255.255.255.0`, qui appartient également à l'espace adresse NAT `NATDomain1`. Le protocole est défini sur 1, c'est-à-dire sur IP.

Remarque : Ne définissez pas d'espace adresse pour les périphériques de passerelle NAT ou pour les portées de sous-réseau publiques. L'espace adresse peut uniquement être défini pour les sous-réseaux privés.

Tâches associées:

«Configuration de la conversion NAT», à la page 41
Pour configurer une conversion NAT afin de reconnaître des environnements NAT, mappez l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associé.

«Activation de la conversion NAT», à la page 161
Vous pouvez configurer le système de reconnaissance de sorte qu'il utilise la conversion NAT en modifiant $NCHOME/etc/precision/DiscoConfig.cfg pour créer ou modifier une insertion dans disco.NATStatus et définir m_UsingNAT sur 1 et m_NATStatus sur 0.

Définition de l'emplacement de la reconnaissance à l'aide des adresses de passerelle NAT :

Définissez l'emplacement d'une reconnaissance NAT en insérant dans l'outil de recherche Ping les adresses IP des routeurs principaux du système. Vous pouvez également définir l'emplacement de la reconnaissance à l'aide des adresses IP des passerelles NAT.

Dans une reconnaissance NAT, les passerelles NAT doivent être reconnues avant le reste du réseau, elles doivent donc être les premières trouvées par l'outil de recherche.

Network Manager est configuré pour déclencher la définition de l'emplacement de toutes les passerelles NAT si la conversion NAT est activée. Toutefois, l'outil de recherche Ping doit être actif pour que ce déclenchement ait lieu. Si la définition de l'emplacement n'utilise, par exemple, que l'outil de recherche de fichiers, les passerelles NAT ne reçoivent aucune commande PING, même si la conversion a été activée. Il est donc recommandé de définir l'emplacement de la reconnaissance à l'aide de toutes les passerelles NAT. Pour ce faire, utilisez l'outil de recherche de fichiers, l'outil de recherche Ping ou toute autre méthode.

Vous pouvez également définir l'emplacement de la reconnaissance à l'aide de passerelles NAT en utilisant l'interface graphique de la configuration de la reconnaissance.

Tâches associées:

«Configuration de la conversion NAT», à la page 41
Pour configurer une conversion NAT afin de reconnaître des environnements NAT, mappez l'identificateur d'espace adresse pour un domaine NAT à l'adresse IP du périphérique de passerelle NAT associé.

«Activation de la conversion NAT», à la page 161
Vous pouvez configurer le système de reconnaissance de sorte qu'il utilise la conversion NAT en modifiant $NCHOME/etc/precision/DiscoConfig.cfg pour créer ou modifier une insertion dans disco.NATStatus et définir m_UsingNAT sur 1 et m_NATStatus sur 0.

Activation d'agents NAT :

Si vous utilisez un pare-feu NetScreen® ou un routeur Cisco® en tant que passerelle NAT, vous devez utiliser l'agent CiscoNATTelnet ou NATNetScreen.

Assurez-vous d'activer les agents de conversion NAT appropriés. Ces agents doivent s'exécuter pour reconnaître les passerelles NAT. S'ils ne sont pas exécutés, la reconnaissance ne peut se terminer, car elle ne peut pas reconnaître le réseau correctement sans d'abord reconnaître les passerelles NAT.

Les agents NAT sont actuellement CiscoNATTelnet, NATNetScreen et NATTextFileAgent. L'agent CiscoNATTelnet fonctionne sur les routeurs Cisco IOS fournissant une conversion NAT et n'est pas certifié pour les pare-feu PIX. L'agent NATNetScreen est destiné aux pare-feu NetScreen.

Si vous utilisez une passerelle NAT autre qu'un pare-feu NetScreen ou un routeur Cisco, vous devez utiliser l'agent Perl NATTextFileAgent.pl, comme décrit dans «Activation d'agents pour les périphériques de passerelle NAT non pris en charge», à la page 165.

Activation d'agents pour les périphériques de passerelle NAT pris en charge :

Les agents CiscoNATTelnet et NATNetScreen se connectent directement aux passerelles NAT pour télécharger les mappages d'adresses. Vous pouvez configurer ces agents.

Avant d'exécuter ces agents, vous devez accomplir les tâches suivantes :

- Activer la conversion NAT
- Configurer la gestion des interruptions

Pour configurer et exécuter les agents :

1. Activez les agents. Il existe une insertion dans la table disco.agents dans le fichier de configuration DiscoAgents.cfg pour chaque agent de reconnaissance installé. Pour activer un agent, vous devez modifier l'insertion de sorte que la colonne m_Valid de cet agent soit définie sur 1. Pour désactiver un agent, définissez m_Valid=0.

   L'exemple d'insertion suivant active l'agent CiscoNATTelnet.

   ```
   insert into disco.agents
   (
                  m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence,
                  m_DebugLevel, m_LogFile
   )
   valeurs
   (
                  'CiscoNATTelnet', 1, 8, 0, 2, 4,
                  "$NCHOME/log/precision/CiscoNatTelnet.log"
   );
   ```

2. Exécutez une reconnaissance.

Tâches associées:

«Activation des agents», à la page 35
Vous devez activer les agents appropriés pour la reconnaissance que vous souhaitez réaliser. Vous pouvez indiquer des agents pour une reconnaissance complète ou une reconnaissance partielle.

Activation d'agents pour les périphériques de passerelle NAT non pris en charge :

NATTextFileAgent est un agent de secours à utiliser si votre périphérique de conversion NAT n'est pas pris en charge. Vous pouvez le configurer.

Avant d'exécuter l'agent NATTextFileAgent, vous devez accomplir les tâches suivantes :

- Activer la conversion NAT
- Configurer la gestion des interruptions

L'agent NATTextFileAgent lit un fichier à plat appelé NATTranslations.txt qui contient les conversions NAT présentes sur une passerelle NAT particulière. Ceci permet à la reconnaissance de prendre en charge un réseau contenant une passerelle NAT qui n'est pas prise en charge actuellement. Cet agent ne télécharge pas ses informations depuis les passerelles NAT, mais lit une liste de mappages d'adresses IP privées vers des adresses publiques à partir d'un fichier à plat.

Pour configurer et exécuter l'agent :

1. Installez l'interface de programme d'application Perl. L'interface de programme d'application Perl est nécessaire à l'exécution de tous les agents Perl. Cette interface est installée par défaut dans Network Manager.

   Pour vérifier si l'interface de programme d'application est installée, vérifiez que le fichier suivant existe :

   ```
   $NCHOME/precision/bin/ncp_perl
   ```

   Si le fichier est répertorié, l'interface de programme d'application Perl est installée.
2. Créez un fichier de mappage NAT que l'agent contenant les mappages des adresses doit lire. Votre fichier de mappage NAT doit être dans un format qui peut être lu par l'agent : les valeurs doivent être des adresses IP valides spécifiées dans des colonnes, elles-mêmes séparées par des tabulations.

   Par défaut, l'agent utilise le fichier $NCHOME/etc/precision/NATTranslations.txt. Si vous souhaitez créer vos propres mappages, vous devez sauvegarder et modifier ce fichier par défaut. Pour que l'agent utilise un fichier de mappage NAT différent de celui par défaut, modifiez la ligne suivante dans $NCHOME/precision/disco/agents/Perlagents/NATTextFileAgent.pl :

   ```
   my $natFileName  = "$ENV{$NCHOME}/etc/precision/NATTranslations.txt";
   ```
3. Le fichier de mappage NAT contient les colonnes suivantes :
   - Adresse IP de la passerelle NAT du domaine NAT auquel appartient le périphérique. Vous devez indiquer des mappages pour toutes les passerelles NAT dans le même fichier.
   - Adresse globale extérieure du périphérique, c'est-à-dire l'adresse publique du périphérique.
   - Adresse globale intérieure du périphérique, c'est-à-dire l'adresse privée du périphérique.

     L'exemple suivant présente un fichier de mappage NAT pour deux passerelles disposant respectivement de l'adresse IP 1.2.3.4 et 1.2.3.9.

     ```
     // NATGatewayIP              PublicIP                PrivateIP
     1.2.3.4                      2.3.4.5                 10.10.1.1
     1.2.3.4                      2.3.4.6                 10.10.1.2
     1.2.3.9                      2.3.6.1                 10.10.1.1
     1.2.3.9                      2.3.6.2                 10.10.1.2
     ```

Remarque : Pour la station de gestion, l'adresse IP publique d'une passerelle de conversion particulière ne correspond pas nécessairement à celle qu'elle voit. L'adresse publique correspond à l'adresse IP que la passerelle récupère d'un port et qu'elle convertit, puis place sur un autre port. Cette différence est importante lorsque vous disposez de passerelles en chaîne, où une adresse IP peut être convertie plusieurs fois. L'adresse IP publique est l'adresse IP la plus proche du domaine de gestion.

4. Activez l'agent. Il existe une insertion dans la table disco.agents dans le fichier de configuration DiscoAgents.cfg pour chaque agent de reconnaissance installé. Pour activer un agent, modifiez l'insertion de sorte que la colonne m_Valid de cet agent soit définie sur 1. Pour désactiver un agent, définissez m_Valid=0.

   L'exemple d'insertion suivant active l'agent NATTextFileAgent.

   ```
   insert into disco.agents
   (
                  m_AgentName, m_Valid, m_AgentClass, m_IsIndirect,
                  m_Precedence, m_IsPerl
   )
   valeurs
   (
                  'NATTextFileAgent', 1, 8, 0, 2, 1
   );
   ```

5. Vérifiez que le programme stitcher NATTimer.stch a été configuré de sorte à déclencher une nouvelle reconnaissance des passerelles NAT. Par défaut, le programme stitcher NATTimer.stch s'exécute toutes les heures. Vous pouvez modifier cet intervalle en localisant la ligne suivante dans le fichier du programme stitcher et en modifiant la valeur de l'entier :

   ```
   ActOnTimedTrigger( ( m_Interval ) values ( 1 ) ; ) ;
   ```

6. Exécutez une reconnaissance.

Activation de l'agent pour les périphériques de passerelle NAT dans un espace adresse privé :

Lorsque la passerelle NAT n'est pas dans l'espace adresse public, vous pouvez activer l'agent NATGateway pour résoudre la connectivité incorrecte éventuelle.

La reconnaissance part du principe que l'interface de gestion de la passerelle NAT se trouve dans l'espace adresse public. Si ce n'est pas le cas, Network Manager ne peut identifier l'espace adresse des interfaces du périphérique de passerelle NAT, ce qui peut entraîner une connectivité incorrecte. Par exemple, lorsqu'un VPN est utilisé pour accéder à l'interface de gestion, l'interface de gestion de la passerelle NAT ne se trouve pas dans l'espace adresse public.

L'agent NATGateway permet à Network Manager de déterminer si une interface donnée sur un périphérique de passerelle NAT se trouve du côté privé ou public de la passerelle NAT et ainsi de résoudre correctement la connectivité d'unité.

Pour résoudre cette difficulté, activez l'agent NATGateway et fournissez à Network Manager un fichier de mappage, NATGateways.txt. Dans ce fichier, répertoriez toutes les unités de passerelle NAT et des interfaces de chaque unité, ainsi qu'une zone permettant d'indiquer sur l'interface se trouve du côté public ou privé de la passerelle NAT.

Cet agent fonctionne en association avec le programme stitcher NATGatewayRetProcessing.stch et le fichier NATGateways.txt du répertoire NCHOME/precision/etc

Le tableau 17 fournit le format du fichier NATGateways.txt en donnant un exemple du contenu de ce fichier. Les zones de ce fichier texte doivent être séparées par des tabulations.

Tableau 17. Format du fichier NATGateways.txt

Nom de base	A l'intérieur ou à l'extérieur	Adresse IP de l'interface
1.1.1.4	extérieur	172.16.4.10
1.1.1.4	intérieur	10.52.2.10
sca_T1ukP_16	extérieur	192.168.36.93
sca_T1ukP_16	extérieur	192.168.36.98

Exemple : Configuration d'une reconnaissance NAT :

Cet exemple illustre comment définir des espace adresse à l'aide de l'agent NATTextFileAgent et comment configurer des portées de reconnaissance associées.

Effectuez les tâches suivantes avant d'exécuter les étapes de cet exemple :

- Configurez la reconnaissance pour utiliser la conversion d'adresses réseau.
- Indiquez comme valeur de départ de l'outil de recherche PING l'adresse IP de chaque périphérique de passerelle NAT.

Dans cet exemple, les périphériques de passerelle NAT ne sont pas pris en charge. Cela signifie que l'agent NATTextFileAgent doit être utilisé dans cette reconnaissance NAT.

L'agent NATTextFileAgent utilise un fichier de mappage NAT avec le contenu suivant. Il existe trois périphériques de passerelle NAT avec des mappages pour chaque périphérique dans les espaces adresse associés.

```
//First NAT gateway and mappings
//NATGateway            PublicIP              Private IP
201.201.201.201         61.61.61.1             192.168.1.1
201.201.201.201         61.61.61.2             192.168.1.2
201.201.201.201         61.61.61.3             192.168.1.3
201.201.201.201         61.61.61.4             192.168.1.4
201.201.201.201         61.61.61.5             192.168.1.5
201.201.201.201         61.61.61.6             192.168.1.6

//Second NAT gateway and mappings
//NATGateway            PublicIP              Private IP
202.202.202.202         62.62.62.1             192.168.1.1
202.202.202.202         62.62.62.2             192.168.1.2
202.202.202.202         62.62.62.3             192.168.1.3
202.202.202.202         62.62.62.4             192.168.1.4
202.202.202.202         62.62.62.5             192.168.1.5
202.202.202.202         62.62.62.6             192.168.1.6

//Third NAT gateway and mappings
//NATGateway            PublicIP              Private IP
203.203.203.203         63.63.63.1             192.168.3.1
203.203.203.203         63.63.63.2             192.168.3.2
203.203.203.203         63.63.63.3             192.168.3.3
203.203.203.203         63.63.63.4             192.168.3.4
203.203.203.203         63.63.63.5             192.168.3.5
203.203.203.203         63.63.63.6             192.168.3.6
```

Pour les premier et second espaces adresse, l'espace adresse IP privé n'est pas unique. Pour ces deux espaces adresse, l'espace adresse IP privé est défini par une combinaison de sous-réseau et de masque de réseau de 192.168.1.0/29.

En fonction de ce périphérique de passerelle NAT et des données d'espace adresse, définissez les portées de reconnaissance comme suit.

1. Définissez chaque périphérique de passerelle NAT et son espace adresse correspondant. Dans cet exemple, les noms des trois espaces adresse NAT sont RTP1, RTP2 et RTP3. Par exemple, pour le troisième périphérique de passerelle NAT, l'insertion suivante définit le périphérique NAT et son espace adresse associé, RTP3 :

```
insert into translations.NATAddressSpaceIds
(
    m_NATGatewayIP, m_AddressSpaceId
)
values
(
"203.203.203.203", "RTP3"
);
```

2. Définissez une zone de portée pour chaque périphérique de passerelle NAT.

   Remarque : Il n'est pas nécessaire de définir une zone de portée pour les périphériques de passerelle NAT dont l'adresse IP est déjà dans d'autres zones de portée définies pour la reconnaissance.
   Par exemple, pour le premier périphérique de passerelle NAT, l'insertion suivante définit la zone de portée :

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="201.201.201.201",
                m_NetMask=32
            }
        ],
        ""
);
```

3. Définissez les zones de portée pour les sous-réseaux publics associés à chaque espace adresse NAT. Par exemple, pour le troisième sous-réseau public, l'insertion suivante définit la zone de portée :

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="63.63.63.0",
                m_NetMask=29
            }
        ],
        ""
);
```

4. Définissez une zone de portée pour le sous-réseau privé associé au troisième espace adresse NAT uniquement.

   Restriction : Vous pouvez uniquement définir une zone de portée pour un espace adresse NAT privé où la combinaison de sous-réseau et de masque de réseau du sous-réseau privé est unique dans la configuration de reconnaissance. Cela exclut les premier et second sous-réseaux privés.
   Pour le troisième sous-réseau privé, l'insertion suivante définit la zone de portée :

```
insert into scope.zones
(
    m_Protocol, m_Action, m_Zones, m_AddressSpace
)
values
(
        1,
        1,
        [
            {
                m_Subnet="192.168.3.0",
                m_NetMask=29
            }
        ],
        "RTP3"
);
```

5. Activez l'agent NATTextFileAgent.

Vous pouvez à présent lancer la reconnaissance NAT.

Référence associée:

«Référence pour la configuration de reconnaissance NAT», à la page 158
Utilisez ces instructions pas à pas pour configurer une reconnaissance NAT.

Tâches NAT post-configuration

Après avoir configuré les reconnaissances NAT, vous pouvez accomplir plusieurs tâches de post-configuration.

Suivi de l'avancement d'une reconnaissance NAT :

Lors de la reconnaissance d'unités de conversion NAT, vous pouvez suivre l'état de la reconnaissance grâce aux valeurs de disco.NATStatus.

Lors de la reconnaissance, vous ne voyez tout d'abord que les unités de conversion NAT affichées dans les tables d'envoi et de retour de l'agent. Toutes les autres données retournées depuis les outils de recherche sont stockées dans la table de base de données finders.pending pendant la reconnaissance des unités de conversion NAT.

Emettez l'instruction select OQL suivante pour afficher l'état de la reconnaissance :

```
select * from disco.NATStatus;
```

Cette instruction affiche une valeur comprise entre 0 et 4 et signifiant :

- 0 : La reconnaissance NAT est à l'état initial. Les unités NAT n'ont pas été traitées.
- 1 : Reconnaissance NAT initiée. Les adresses IP des passerelles NAT ont été envoyées à l'outil de recherche Ping pour vérifier qu'elles existent
- 2 : La reconnaissance NAT est en cours d'exécution.

- 3: La reconnaissance NAT est en cours de traitement. Toutes les passerelles NAT ont été traitées et la reconnaissance génère la table `translations.NAT`. Cet table permet de garantir une reconnaissance correcte du reste du réseau.
- 4 : Reconnaissance NAT terminée. Les entrées de la table finders.pending ont été déplacées vers la table finders.processing et la reconnaissance se poursuit normalement.

Utilisez les résultats de cette requête pour déboguer une reconnaissance NAT posant problème. La valeur indique si des incidents de reconnaissance sont causés par la conversion d'adresses réseau ou par la partie standard (non-NAT) du processus de reconnaissance.

Débogage d'une reconnaissance NAT :

Pour analyser une reconnaissance NAT, utilisez ncp_oql pour suivre les données du début (outils de recherche) à la fin (topologie de base) jusqu'à ce que vous puissiez déterminer où les données sont incorrectes. Des données incorrectes indiquent que le problème provient d'un agent, d'une unité ou d'un programme stitcher.

Plusieurs requêtes sont utiles lors du débogage d'une reconnaissance, basée sur NAT ou non.

La requête OQL suivante indique les agents qui sont en train d'être démarrés (`m_State=1`), en cours de démarrage (`m_State=2`) ou en cours d'exécution (`m_State=3`):

```
select * from agents.status where m_State <> 0 AND m_State <> 4;
```

Cette requête vous indique quels agents la phase actuelle attend pour se terminer. La reconnaissance attend les agents conçus pour se terminer au cours de la phase actuelle et qui sont dans l'état 1, 2 ou 3.

```
select * from <agentName>.despatch
where m_UniqueAddress NOT IN
      ((
            select m_UniqueAddress from <agentName>.returns where m_LastRecord = 1
      ));
```

En utilisant la première requête, vous pouvez voir quels agents sont toujours en cours d'exécution dans une phase particulière.

La requête suivante permet de déterminer quelle entité cet agent est en train de traiter. Ceci peut se révéler utile pour déterminer si une unité est source d'incidents au sein de votre réseau :

```
select * from translations.ipToBaseName where m_IpAddress = '<ip>';
```

Cette nouvelle requête indique l'adresse et le nom de base utilisés pour une adresse IP particulière. Elle signale également si cette adresse IP est considérée comme faisant partie de la portée.

Activation du modèle de confinement à utiliser avec la conversion d'adresses réseau :

Le programme stitcher `NATAddressSpaceContainers.stch` crée des objets virtuels pour chaque espace adresse qui contient les entités de cet espace adresse. Vous pouvez activer ce programme stitcher en retirant les signes de commentaire de la ligne `// ExecuteStitcher("NATAddressSpaceContainers");`, du fichier `$NCHOME/precision/disco/stitchers/CreateScratchTopology.stch`.

Affichage d'environnements NAT à l'aide de vues de réseau Topoviz :

Utilisez des vues de réseau Topoviz pour créer des vues de réseau basées sur les valeurs de toute colonne de l'enregistrement de topologie d'une entité. Une vue NAT Address Spaces Dynamic Distinct est créée automatiquement si vous avez activé la reconnaissance NAT dans votre configuration de reconnaissance.

Par exemple, vous pouvez créer une vue de réseau filtrée ou une vue Dynamic Distinct dans la zone suivante de la base de données topologiques NCIM :

- table ipEndPoint
- zone addressSpace

Remarque : La vue NAT Address Spaces Dynamic Distinct est créé automatiquement si **Activer la prise en charge de la conversion d'adresses réseau (NAT)** est activé dans votre configuration de reconnaissance.

Chapitre 3. Surveillance de reconnaissances de réseau

Vous pouvez surveiller l'état et la progression de la reconnaissance de réseau à partir de l'interface graphique ou de la ligne de commande.

Surveillance de la reconnaissance de réseau à partir de l'interface graphique

Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

Dans la page Etat de la reconnaissance active, vous pouvez également démarrer et arrêter les reconnaissances.

Tâches associées:

«Démarrage d'une reconnaissance», à la page 52
Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

«Révision de la configuration», à la page 22
Dans la fenêtre Récapitulatif de configuration, passez vos paramètres en revue. Vous pouvez également sauvegarder vos paramètres et, de manière facultative, démarrer la reconnaissance avec les paramètres que vous avez configuré.

«Reconnaissance manuelle d'une unité ou d'un sous-réseau», à la page 200
Pour procéder à une reconnaissance manuelle des unités de sorte que la topologie de réseau de Network Manager corresponde au réseau.

«Démarrage de reconnaissance partielle à partir de l'interface graphique», à la page 203
Le démarrage d'une reconnaissance partielle implique de définir un emplacement de départ et des portées.

Surveillance de l'avancement de la reconnaissance

Fix Pack 4

Vous pouvez utiliser l'onglet **Surveillance** pour surveiller la progression de la reconnaissance au cours de chacune des phases de reconnaissance.

Suivez la procédure ci-dessous pour surveiller la progression de la reconnaissance complète ou partielle en cours.

1. Cliquez sur **Reconnaissance** > **Etat de la reconnaissance réseau**.
2. Sélectionnez un domaine.
3. Cliquez sur l'onglet **Surveillance**.
4. Lancez une reconnaissance complète ou partielle en sélectionnant l'option du bouton Démarrer la reconnaissance  .

Remarque : Si la reconnaissance dynamique est en cours d'exécution, cette table est mise en grisé. Un message indiquant que vous pouvez cliquer sur l'onglet Reconnaissance dynamique pour plus de détails sur la progression de la

reconnaissance dynamique s'affiche. Cliquez sur Démarrer la reconnaissance  pour démarrer une reconnaissance complète. Cela arrête la reconnaissance dynamique.

Les phases suivantes apparaissent dans le tableau.

Interrogation des périphériques
Pendant cette phase, les périphériques sont d'abord reconnus par les outils de recherche, puis les informations sont extraites des périphériques par les agents. Cette phase est également appelée phase 1.

Résolution des adresses
Pendant cette phase, les agent résolvent les conversion d'adresse IP vers MAC. Cette phase est également appelée phase 2.

Téléchargement des connexions
Pendant cette phase, les agents de commutation téléchargent les tables de réacheminement à partir des commutateurs du réseau. Cette phase est également appelée phase 3.

Corrélation des connexions
Pendant cette phase, la connectivité entre les périphériques est calculée, le modèle de confinement est créé et la topologie de réseau est construite. Cette phase est également appelée phase -1.

Vous pouvez consulter à quelle phase est la reconnaissance en cours dans la colonne **État** de la table. Si une phase n'a pas démarré, cette colonne est vide. Si une phase est en cours, cette colonne affiche une icône en forme de rouet. Si une phase s'est terminée correctement, cette colonne contient une icône de forme de coche verte.

État Affiche l'état d'une phase particulière. La colonne montre les types d'état suivants.

Tableau 18. Etat de la phase de reconnaissance

Etat	Icône	Description
Terminé		Si une phase s'est terminée correctement, cette colonne contient une icône de forme de coche verte.
En cours		Si une phase est en cours, cette colonne affiche une icône en forme de rouet.
Non démarré		Si une phase n'a pas démarré, cette colonne est vide.

Vous pouvez savoir combien de temps dure une phase dans la colonne **Durée écoulée** de la table. Le temps nécessaire à chaque phase dépend de la portée de la reconnaissance, de la complexité du réseau et de la quantité de détails extraits des périphériques. Si la durée écoulée augmente et que le travail achevé n'augmente pas, des problèmes liés à la reconnaissance se sont peut-être produits.

A faire : Dans la première phase, le nombre d'adresses IP reconnu cesse de croître en milieu de phase. Il s'agit du fonctionnement normal de la reconnaissance. Le nombre d'adresses IP reconnues augmente uniquement pendant la première partie de la phase, alors que les outils de recherche découvrent de nouveaux périphériques. Dans la dernière partie de la phase, les agents de reconnaissance extraient des informations de ces périphériques et les nouvelles adresses IP ne sont pas reconnues.

La section **Agents de reconnaissance** montre la progression des agents de reconnaissance. Si vous pensez qu'une phase est trop longue, cliquez sur l'onglet **Agents de reconnaissance** pour vérifier les actions des agents de reconnaissance.

Vous pouvez voir la progression d'une phase dans la colonne **Travail terminé** dans la table. Pour la première phase, cette colonne affiche le nombre d'adresses IP trouvées jusqu'à présent. Pour les autres phases, cette colonne montre le pourcentage de travail terminé dans la phase.

Concepts associés:

«Etapes et phases de reconnaissance», à la page 342
Le processus de reconnaissance peut être séparé en deux étapes : collecte et traitement des données. Les étapes se divisent en deux phases.

Comparaison de reconnaissances

Vous pouvez utiliser l'onglet **Surveillance** pour comparer la reconnaissance en cours à la reconnaissance complète précédente.

Vous ne pouvez pas comparer des reconnaissances partielles. Les données de la colonne **Précédente** dans la table concernent la dernière reconnaissance complète.

Fix Pack 4 Pour ouvrir l'onglet **Surveillance**, cliquez sur **Reconnaissance** > **Etat de la reconnaissance réseau**, puis cliquez sur la barre **Surveillance**.

Le temps nécessaire à l'exécution de chaque phase apparaît dans la sous-colonne **Précédente** de la colonne **Durée écoulée**.

Remarque : Fix Pack 3 Pour afficher les durées de reconnaissance de toutes les reconnaissances précédentes, exécutez le script **disco_profiling_data.pl** à partir de la ligne de commande. Pour plus d'informations sur le script **disco_profiling_data.pl**; voir *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Le temps nécessaire à chaque phase dépend de la portée de la reconnaissance, de la complexité du réseau et de la quantité de détails extraits des périphériques. Si le réseau, la portée de reconnaissance et les paramètres n'ont pas changé de manière significative, mais que la durée écoulée pour une phase de la reconnaissance en cours est considérablement supérieure à la durée de la même phase dans la reconnaissance précédente, cela peut signifier que des problèmes se sont produits pendant la reconnaissance.

La colonne **Travail terminé** de la table affiche le nombre d'adresses IP trouvées dans la reconnaissance en cours et le nombre trouvé dans la reconnaissance précédente. Si un nombre très inférieur d'adresses IP est trouvé dans la reconnaissance en cours, il existe peut-être un problème lié à la portée de la reconnaissance ou à l'accès SNMP aux périphériques.

Surveillance de la progression de l'outil de recherche PING

Vous pouvez utiliser la table **Statut de l'outil de recherche PING** pour surveiller la progression de l'outil de recherche PING pendant une reconnaissance.

Pour ouvrir le **Statut de l'outil de recherche PING**, cliquez sur **Reconnaissance** > **Etat de la reconnaissance réseau**, puis cliquez sur l'onglet **Statut de l'outil de recherche PING**.

Vous pouvez utiliser la table **Statut de l'outil de recherche PING** pour savoir quelles adresses IP et quels sous-réseaux ont été découverts jusqu'à présent. Si l'outil de recherche PING est en train de traiter un sous-réseau, vous pouvez également savoir à quelle adresse IP a été envoyée la dernière commande PING.

La table **Statut de l'outil de recherche PING** contient les informations suivantes :

Adresse
Liste des adresses IP et des sous-réseaux reconnus jusqu'à présent.

Masque de réseau
Pour chaque sous-réseau, cette colonne indique la valeur de masque de réseau.

Dernière commande PING
Dernière adresse IP ayant reçu une commande PING.

État Indique si l'outil de recherche Ping lance toujours une commande PING sur cette unité ou ce sous-réseau ou s'il a terminé le lancement des commandes PING.

Tableau 19. Etat de l'Outil de recherche PING

Etat	Icône	Description
Terminé		L'outil de recherche PING a terminé l'envoi de commandes PING sur ce sous-réseau ou cette adresse IP.
Démarré		L'outil de recherche PING est en cours d'envoi de commande PING sur ce sous-réseau ou cette adresse IP.
Arrêté		L'outil de recherche PING n'a pas commencé à envoyer de commandes PING sur ce sous-réseau ou cette adresse IP.
Attente de l'état		Le système attend l'état de l'outil de recherche PING pour ce sous-réseau ou cette adresse IP.

Surveillance de la progression des agents de reconnaissance

Vous pouvez utiliser la section **Statut des agents** pour surveiller la progression des agents de reconnaissance au cours de chacune des phases de reconnaissance.

Les agents de reconnaissance collectent des données sur les périphériques reconnus. Ces données sont utilisées pendant la phase de Connectivité corrélée de la reconnaissance (phase -1) pour construire la connectivité et le confinement du réseau.

Vous pouvez utiliser le **Statut des agents** pour répondre aux questions suivantes notamment, pendant l'exécution de la reconnaissance :

- Tous les agents s'exécutent-ils correctement ?
- Des agents ont-ils échoué ?
- Certains agents ne parviennent-ils pas à terminer leur exécution ?

- Sur quel périphérique un agent spécifique est-il en cours d'exécution ?

1. Pour ouvrir le **Statut des agents**, cliquez sur **Reconnaissance** > **Etat de la reconnaissance réseau**, puis cliquez sur l'onglet **Statut des agents**. La section **Statut des agents** contient deux tables, la table **Statut des agents** dans la partie supérieure et la table **Statut d'adresse IP** dans la partie inférieure. La barre d'outils de la table **Statut des agents** contient les commandes suivantes.

   Filtrer les agents par phase
   Utilisez la liste déroulante de phases pour sélectionner une phase de reconnaissance. La table d'agents affiche alors tous les agents de reconnaissance qui ont démarré pendant la reconnaissance en cours et qui sont planifiés pour se terminer dans la phase de reconnaissance que vous avez sélectionnée.

   Régénération
   Régénère les données dans les tables Statut des agents et Statut de l'adresse IP. L'icône est remplacée par **Régénération** pendant la régénération des données de la table. Pour réactualiser les tables, vous devez attendre la fin de la régénération en cours.

   La table **Statut des agents** répertorie tous les agents qui ont démarré pendant cette reconnaissance et contient les informations suivantes. Ces informations sont mises à jour toutes les 20 secondes. Lorsque vous ouvrez cette table la première fois, elle est triée par ordre décroissant d'**Etat**.

   Agent Agents de reconnaissance qui ont démarré pendant la reconnaissance en cours et qui sont planifiés pour se terminer dans la phase de reconnaissance que vous avez sélectionnée.

   Se termine en phase
   Phase dans laquelle l'agent de reconnaissance se termine.

   Etat Etat en cours de l'agent de reconnaissance. Les états possibles sont répertoriés par ordre décroissant par défaut dans le tableau suivant.

Tableau 20. Etats d'agent

Etat	Valeur	Icône	Description
Mort	5		L'agent s'est terminé de façon inattendue. Il s'agit d'un problème de reconnaissance potentiel.
Terminé	4		L'agent est en cours d'exécution mais a terminé le traitement de toutes les adresses IP de sa file d'attente. L'agent est encore disponible pour traiter les agents supplémentaires placés en file d'attente.
En cours d'exécution	3		L'agent est en cours de traitement des adresses IP.
Démarrage de	2		L'agent est en cours de démarrage.
Non exécuté	1		L'agent n'est pas en cours d'exécution.

   Nombre total d'adresses IP
   Nombre total d'adresses IP que cet agent doit traiter. Ce nombre augmente à mesure que la reconnaissance progresse et que les outils de recherche découvrent davantage de périphériques qui doivent être traités par l'agent.

   Adresses IP en attente
   Nombre d'adresses IP en attente d'être traitées par cet agent. Ce nombre peut augmenter ou décroître pendant la reconnaissance. Ce nombre augmente initialement à mesure que la reconnaissance progresse et que les outils de recherche découvrent davantage de périphériques qui

doivent être traités par l'agent. A mesure que l'agent termine le traitement des adresses IP, ce nombre diminue jusqu'à atteindre la valeur zéro.

Remarque : Si cette valeur n'atteint pas zéro pendant la reconnaissance, cela signifie que l'agent n'a pas pu terminer le traitement d'une ou de plusieurs adresses IP et qu'il existe un problème de reconnaissance potentiel.

2. Cliquez sur un agent dans la table **Statut des agents**. La table **Statut de l'adresse IP** répertorie les adresses IP qui ont été traitées ou sont en cours de traitement par cet agent. La table **Statut de l'adresse IP** répond aux changements effectués dans la table **Statut des agents** . Elle est mise à jour dans les situations suivantes : lorsqu'un nouvel agent est sélectionné dans la table **Statut des agents**, lors du changement de paramètre du filtrage de la table **Statut de l'adresse IP** à **Tout** ou **File d'attente** et lorsque le bouton **Rafraîchir**  de la table **Statut des agents** est activé. Lorsque vous ouvrez cette table la première fois, elle est triée par ordre décroissant d'**Etat**.

Agent_name
Utilisez le bouton d'option pour spécifier s'il convient d'afficher toutes les adresses IP (Toutes) ou uniquement les adresses IP placées en file d'attente pour le traitement (File d'attente). Le paramètre par défaut est File d'attente.

Tous Configurez la table **Détails** pour afficher toutes les adresses IP pour cet agent. Il s'agit des adresses IP qui ont été mises en file d'attente pour le traitement par l'agent, des adresses IP en cours de traitement par l'agent et des adresses IP qui ont déjà été traitées par l'agent.

File d'attente
Configurez la table **Détails** pour afficher uniquement les adresses IP qui ont été placées en file d'attente pour le traitement par cet agent.

Adresse IP
Adresses IP traitées par cet agent. Si l'option **Tous** est sélectionnée, cette colonne affiche les adresses IP traités, en cours de traitement ou placées en file d'attente pour traitement par cet agent. Si l'option **File d'attente** est sélectionnée, cette colonne affiche les adresses IP placées en file d'attente pour traitement par cet agent.

Etat Etat en cours de l'adresse IP. Les états possibles sont répertoriés par ordre décroissant par défaut dans le tableau suivant :

Tableau 21. Etats d'adresse IP

Etat	Valeur	Icône	Description
Mort	5		Le traitement de cette adresse IP s'est terminé de façon inattendue. Il s'agit d'un problème de reconnaissance potentiel.
Terminé	4		Un agent a terminé le traitement de cette adresse IP.
En cours d'exécution	3		Un agent est en train de traiter cette adresse IP.
Démarrage de	2		Un agent commence le traitement de cette adresse IP.
Non exécuté	1		L'adresse IP n'est pas en cours de traitement.

Temps écoulé
Temps nécessaire à l'agent pour traiter cette adresse IP, exprimé HH:MM:SS. Cette valeur est affichée uniquement pour les adresses IP dont le traitement est terminé.

Heure de despatch
Date et heure auxquelles l'agent commence à traiter cette adresse IP. Cette valeur est affichée uniquement pour les adresses IP dont le traitement a commencé ou est terminé.

Temps de retour
Date et heure auxquelles l'agent a extrait des données pour cette adresse IP. Cette valeur est affichée uniquement pour les adresses IP dont le traitement est terminé.

Accès SNMP
Indique si l'agent a pu accéder à cette adresse IP à l'aide du protocole SNMP.

Tâches associées:

«Traitement des incidents liés à une reconnaissance anormalement longue», à la page 210
Une reconnaissance peut être anormalement longue car un agent ne parvient pas à terminer le traitement sur un périphérique spécifique. Utilisez la section **Statut des agents** pour déterminer quel agent est en cause et sur quelle unité s'effectue le traitement.

«Identification des agents en échec», à la page 211
Les agents qui s'interrompent brusquement pendant une reconnaissance peuvent être une cause d'échec de la reconnaissance. Utilisez la section **Statut des agents** pour déterminer si des agents se sont interrompus de manière inattendue.

Surveillance de la reconnaissance à partir de la ligne de commande

Lorsque le processus **ncp_disco** svous pouvez surveiller l'avancement de la reconnaissance en utilisant le fournisseur de services OQL, le processus **ncp_oql**, pour interroger les bases de données de reconnaissance et déterminer ce qui se passe à tout instant.

Les requêtes présentées dans les rubriques suivantes sont généralisées pour tous les scénarios de reconnaissance et ne sont pas limitées à la reconnaissance Couche 3.

Les exemples sont donnés uniquement pour présenter la flexibilité dont vous disposez en utilisant OQL pour la récupération d'informations de bases de données. En utilisant les définitions schématiques de toutes les bases de données et votre connaissance de la syntaxe OQL, vous pouvez construire des requêtes répondant à toute question relative à l'état actuel du processus de reconnaissance.

Vous pouvez émettre des requêtes simples pour, par exemple, savoir ce le processus **ncp_disco** est en train de faire, quels agents de reconnaissance ont reconnu des unités ou combien d'unités ont été reconnues jusqu'ici. Vous pouvez également émettre des requêtes complexes pour découvrir, par exemple, quels périphériques ont été reconnus par un agent de reconnaissance spécifique ou quels agents de reconnaissance ont interrogé un périphérique spécifique.

Pour plus d'informations sur le démarrage du fournisseur de services OQL, et notamment les prérequis, voir *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*.

Tâches associées:

«Reconnaissance du réseau à l'aide de l'interface de ligne de commande», à la page 57

Les utilisateurs expérimentés peuvent configurer et suivre une reconnaissance à l'aide de fichiers de configuration et de requêtes de base de données.

Exemples de requêtes d'état de la reconnaissance

Vous pouvez utiliser des requêtes semblables à ces exemples pour déterminer l'état des différentes parties de la reconnaissance.

Exemple : Détermination des adresses sur lesquelles l'outil de recherche Ping lance des commandes PING

La requête suivante renvoie l'adresse actuelle sur laquelle une commande PING est lancée par l'outil de recherche PING :

```
select m_CurrentAddress from pingFinder.status;
go
.
{
                m_CurrentAddress=192.168.0.1;
}
```

Exemple : identification de la phase de reconnaissance en cours

L'exemple suivant indique comment identifier la phase de reconnaissance en cours. Les résultats de la requête ci-dessus indiquent que le processus de reconnaissance se trouve toujours dans la phase 1 de collecte des données.

```
select * from disco.status;
go
.
{
                m_DiscoveryMode=0;
                m_Phase=1;
                m_BlackoutState=0;
                m_CycleCount=0;
                m_ProcessingNeeded=0;
                m_FullDiscovery=0;
}
```

Exemple : identification de l'état d'une reconnaissance NAT

Cet exemple indique comment identifier l'état de la reconnaissance NAT.

```
select m_NATStatus from disco.NATStatus;
go
.
{
                m_NATStatus=3;
}
```

Exemple : identification des agents activés

Cet exemple indique comment identifier si vous avez activé les agents de reconnaissance appropriés.

```
select m_AgentName, m_Valid from disco.agents
where m_Valid = 1;
go
...
{
                m_AgentName='Details';
```

```
                m_Valid=1;
}
{
                m_AgentName='AssocAddress';
                m_Valid=1;
}
{
                m_AgentName='IpRoutingTable';
                m_Valid=1;
}
{
                m_AgentName='IpForwardingTable';
                m_Valid=1;
}
```

Exemple : identification de l'état des programmes stitcher de reconnaissance

L'exemple suivant indique comment identifier l'état des programmes stitcher en interrogeant la table stitchers.status.

```
select * from stitchers.status
where m_State > 0 ;
go
.........
{
                m_Name='AgentRetToInstrumentationSubnet';
                m_State=3;
}
{
                m_Name='DetailsRetProcessing';
                m_State=3;
}
.....
.....
{
                m_Name='DetectionFilter';
                m_State=3;
}
{
                m_Name='FnderProcToDetailsDesp';
                m_State=3;
}
{
                m_Name='FnderRetProcessing';
                m_State=3;
}
```

Les résultats de la requête indiquent l'état actuel de tous les programmes stitcher appelés par le processus de reconnaissance jusqu'à présent. Notez que les résultats affichés ci-dessus ont été abrégés.

Exemple : identification des agents actifs

L'exemple suivant indique comment demander l'état des agents dans la base de données agents.

```
select * from agents.status
where m_State > 0 ;
go
..
{
                m_Name='Details';
                m_State=3;
                m_NumConnects=1;
```

```
}
{
                m_Name='IpRoutingTable';
                m_State=3;
                m_NumConnects=1;
}
```

Les résultats de la requête ci-dessus indiquent que seuls les agents Details et IpRoutingTable sont actifs (c'est-à-dire que leur état est supérieur à zéro).

Référence associée:

Annexe A, «Bases de données de reconnaissance», à la page 229
Il existe différentes bases de données spécialisées utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue la topologie réseau reconnue.

Exemples de requêtes de périphérique

Vous pouvez utiliser des requêtes similaires à ces exemples pour identifier les périphériques qui correspondent à certains critères, par exemple, les périphériques trouvés par les outils de reconnaissance.

Exemple : identification des périphériques trouvés par les outils de recherche

L'exemple suivant indique comment identifier les périphériques trouvés par les outils de recherche.

```
select * from finders.returns;
go
....
{
                m_UniqueAddress='172.20.12.253';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='172.20.22.61';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='172.20.0.221';
                m_Protocol=1;
                m_Creator='IpRoutingTable';
}
{
                m_UniqueAddress='10.10.35.17';
                m_Creator='PingFinder';
}
```

La requête ci-dessus indique les périphériques reconnus par l'outil de recherche Ping ainsi que ceux signalés comme résultat des connexions reconnues par l'agent Discovery `IpRoutingTable`.

Exemple : identification des périphériques envoyés à l'agent Details.

L'exemple suivant indique comment identifier les périphériques envoyés à l'agent Details.

```
select * from Details.despatch;
go
.............................................................
.............................
{
                m_UniqueAddress='10.10.38.82';
}
{
                m_UniqueAddress='10.10.38.83';
}
.....
.....
{
                m_UniqueAddress='10.10.38.84';
}
{
                m_UniqueAddress='10.10.38.87';
}
{
                m_UniqueAddress='10.10.38.88';
}
{
                m_UniqueAddress='10.10.38.89';
}
{
                m_UniqueAddress='10.10.38.90';
}
```

Exemple : identification des périphériques renvoyés à partir de l'agent Details.

Pour identifier les périphériques renvoyés à partir de l'agent Details, interrogez la table `returns` de l'agent Details, comme indiqué ci-dessous.

```
select * from Details.returns;
go
.............................................................
.............................
{
                m_UniqueAddress='10.10.8.255';
                m_UpdAgent='Details';
                m_HaveAccess=1;
                                m_Description='Ascend Max-HP T1/PRI S/N;
                m_ObjectId='1.3.6.1.4.1.529.1.2.6';
                m_LastRecord=1;
}
{
                m_UniqueAddress='10.10.9.1';
                m_UpdAgent='Details';
                m_Name='minotaur.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
.....
.....
{
                m_UniqueAddress='10.10.9.2';
                m_UpdAgent='Details';
                m_Name='cyclops.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
{
                m_UniqueAddress='10.10.9.3';
                m_UpdAgent='Details';
```

```
                m_Name='centaur.Kazeem.San.COM';
                m_HaveAccess=0;
                m_LastRecord=1;
}
```

Exemple : identification de tous les périphériques reconnus jusqu'à présent

L'exemple suivant indique comment identifier toutes les entités réseau connues.

```
select m_Name, m_ObjectId, m_UniqueAddress
from workingEntities.finalEntity;
go
..............................
{
                m_Name='10.10.8.255';
                m_ObjectId='1.3.6.1.4.1.529.1.2.6';
                m_UniqueAddress='10.10.8.255';
}
{
                m_Name='minotaur.Kazeem.San.COM';
                m_UniqueAddress='10.10.9.1';
}
.....
.....
{
                m_Name='cyclops.Kazeem.San.COM';
                m_UniqueAddress='10.10.9.2';
}
```

Exemple : identification des agents qui ont reconnu des périphériques

L'exemple suivant indique comment identifier les agents qui ont reconnu des périphériques.

```
select m_Name, m_Creator
from workingEntities.finalEntity;
go
..............................
{
                                m_Name='b11-m1-2611.Kazeem.San.COM[ 0 [ 2 ] ]';
                m_Creator='IpRoutingTable';
}
{
                m_Name='b-ayo.Kazeem.San.COM';
                m_Creator='Details';
}
{
                                m_Name='b11-m1-2611.Kazeem.San.COM[ 0 [ 1 ] ]';
                m_Creator='IpRoutingTable';
}
.....
.....
{
                m_Name='b11-m1-2611.Kazeem.San.COM';
```

Exemples de requêtes d'entité réseau

Vous pouvez utiliser des requêtes sur la base de données instrumentation pour identifier si des entités réseau, telles que les sous-réseaux et les VLAN ont été reconnues. Les tables de la base de données instrumentation stockent un enregistrement de chaque périphérique reconnu.

Exemple : identification du nombre de sous-réseaux reconnus

L'exemple de requête suivant renvoie les détails des sous-réseaux reconnus.

```
select * from instrumentation.subNet;
go
.....................................
{
                m_SubNet='172.20.67.0';
                m_NetMask='255.255.255.0';
}
.....
.....
{
                m_SubNet='172.20.70.0';
                m_NetMask='255.255.254.0';
}
{
                m_SubNet='172.20.95.0';
                m_NetMask='255.255.255.0';
}
( 81 record(s) : Transaction complete )
```

Exemple : identification des VLAN reconnus

L'exemple de requête suivant renvoie les détails des ID VLAN reconnus.

```
select * from instrumentation.vlan;
go
.....................................
{
                m_Vlan=23;
}
{
                m_Vlan=65;
}
.....
.....
{
                m_Vlan=677;
}

( 4826 record(s) : Transaction complete )
```

Exemple de requête de reconnaissance par défaut

Vous pouvez utiliser des requêtes similaires à ces exemples pour identifier les périphériques qui correspondent à certaines critères, par exemple, les périphériques trouvés par des agents de reconnaissance particuliers.

Identification des périphériques reconnus par un agent particulier

L'exemple de requête suivant identifie les périphériques reconnus par l'agent IpRoutingTable.

```
select m_Name, m_Creator
from workingEntities.finalEntity
where
m_Creator = 'IpRoutingTable';
go
.............................
{
               m_Name='10.10.63.194';
               m_Creator='IpRoutingTable';
}
.....
.....
{
                                m_Name='b11-m1-2611.Kazeem.San.COM[ 0 [ 1 ] ]';
               m_Creator='IpRoutingTable';
}
{
               m_Name='b11-m1-2611.Kazeem.San.COM';
               m_Creator='IpRoutingTable';
}
```

Identification des périphériques envoyés à un agent spécifique.

L'exemple de requête suivant identifie les périphériques envoyés à l'agent IpRoutingTable.

```
select m_Name, m_ObjectId, m_Description
from IpRoutingTable.despatch;
go
.............................
{
       m_Name='10.10.63.193';
       m_ObjectId='1.3.6.1.4.1.9.1.108';
              m_Description='Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-JS-M), Version 12.0(4)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by Cisco Systems, Inc.
Compiled Thu 29-Apr-99 06:27 by kpma';
}
.....
.....
{
       m_Name='10.10.71.248';
       m_ObjectId='1.3.6.1.4.1.9.1.258';
              m_Description='Cisco Internetwork Operating System Software
IOS (tm) MSFC Software (C6MSFC-IS-M), Version 12.0(7)XE1, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
TAC:Home:SW:IOS:Specials b-ayo k-az-eem for info
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Fri 04-Feb-00 00:';
}
```

Identification des périphériques renvoyés par un agent spécifique.

L'exemple de requête suivant identifie les périphériques renvoyés par l'agent IpRoutingTable.

```
select m_Name from IpRoutingTable.returns;
go
.............................
{
               m_Name='10.10.71.248';
}
.....
.....
{
```

```
                m_Name='10.10.71.248';
}
{
                m_Name='10.10.71.248';
}
```

Identification des périphériques supplémentaires reconnus par un agent spécifique.

Un agent peut reconnaître des périphériques supplémentaires en interrogeant un périphérique. Dans ce cas, le périphérique supplémentaire serait dans la table `returns` de cet agent, mais pas dans la table `despatch`. Vous pouvez identifier les périphériques présents dans la table `IpRoutingTable.returns`, mais pas dans la table `IpRoutingTable.despatch`, en joignant les tables `IpRoutingTable.despatch` et `IpRoutingTable.returns`, comme dans l'exemple suivant.

```
select IpRoutingTable.returns.m_Name from
IpRoutingTable.returns, IpRoutingTable.despatch
where
IpRoutingTable.returns.m_Name <>
IpRoutingTable.despatch.m_Name;
go
.....................................
{
                m_Name='10.10.71.237';
}
.....
.....
{
                m_Name='10.10.71.55';
}
{
                m_Name='10.10.71.51';
}
```

Identification des périphériques qu'un agent a ajouté à la file d'attente

L'exemple suivant renvoie dans la table despatch les périphériques qui n'ont pas encore été renvoyés.

```
select * from <agent>.despatch
where
(
 m_UniqueAddress NOT IN
  (( select m_UniqueAddress from <agent>.returns where m_LastRecord = 1 ))
);
```

Exemples de requêtes de localisation d'un périphérique spécifique

Pour voir si un périphérique spécifique a été reconnu, vous pouvez utiliser des requêtes similaires à ces exemples afin d'effectuer une recherche dans le flux de données de la reconnaissance.

Exemple : identification de la présence ou non d'un périphérique dans la base de données workingEntities

L'exemple de requête suivant détermine si le périphérique est présent dans la base de données workingEntities.

```
select * from workingEntities.finalEntity
where m_UniqueAddress ='10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Exemple : identification du renvoi ou non d'un périphérique à partir de l'agent AssocAddress

Si le périphérique n'est pas présent dans la base de données workingEntities, vous pouvez utiliser l'exemple de requête suivant pour déterminer si le périphérique a été renvoyé à partir de l'agent AssocAddress.

```
select * from AssocAddress.returns
where m_UniqueAddress = '10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Exemple : identification du renvoi ou non d'un périphérique à partir de l'agent Details

Si le périphérique n'a pas été renvoyé à partir de l'agent AssocAddress, vous pouvez utiliser l'exemple de requête suivant pour déterminer s'il a été renvoyé à partir de l'agent Details.

```
select * from Details.returns
where m_UniqueAddress = '10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Exemple : identification de l'envoi ou non d'un périphérique à l'agent Details

Si le périphérique n'a pas été renvoyé à partir de l'agent Details, vous pouvez vérifier s'il a été envoyé à l'agent Details en interrogeant la table `Details.despatch`, comme indiqué ci-dessous. Ce résultat indique que le périphérique a été envoyé à l'agent Details, mais n'a pas encore été traité.

```
select * from Details.despatch
where m_UniqueAddress='10.10.63.239';
go
.
{
                m_UniqueAddress='10.10.63.239';
}
( 1 record(s) : Transaction complete )
```

Exemple : identification de la reconnaissance ou non d'un périphérique par les outils de recherche

Si le périphérique ne se trouve pas dans la table `Details.despatch`, vous pouvez interroger la base de données `finders`, comme indiqué ci-dessous. Ce résultat indique que le périphérique a été reconnu par les outils de recherche.

```
select * from finders.processing
where m_UniqueAddress='10.10.63.239';
go
.
{
                m_UniqueAddress='10.10.63.239';
}
( 1 record(s) : Transaction complete )
```

```
select * from finders.returns
where m_UniqueAddress='10.10.63.239';
go
.
( 0 record(s) : Transaction complete )
```

Chapitre 4. Classification des unités réseau

A la fin de la reconnaissance, Network Manager IP Edition classe automatiquement toutes les unités réseau reconnues en fonction d'une hiérarchie de classes d'unités prédéfinie. Vous pouvez modifier la façon dont les unités réseau sont classées.

Modification de la hiérarchie de classes d'unités

Modifiez la hiérarchie de classes d'unités pour modifier la façon dont les unités réseau sont classées. Par exemple, il est courant de devoir modifier la hiérarchie de classes lorsque le processus de reconnaissance identifie une unité non classée, c'est-à-dire une unité qui n'est pas définie dans la hiérarchie de classes.

Suite à une reconnaissance, vous pouvez vérifier si des unités ne sont pas classées en exécutant les rapports suivants :

- Rapport sur les périphériques contenant des ID objet SNMP non classifiés
- Rapport sur les périphériques contenant des ID objet SNMP inconnus

Liste des classes d'unités existantes

Avant de modifier les définitions AOC et de réinstancier la topologie, répertoriez les classes d'unités en cours d'utilisation.

Répertoriez les classes d'unités existantes en interrogeant les bases de données ncp_model. La requête retourne les noms des AOC auxquels les unités de la topologie actuelle ont été instanciées. Remplacez NCOMS et admin par votre nom de domaine et votre nom d'utilisateur.

1. Connectez-vous au fournisseur de services OQL à l'aide de la commande suivante :

   `ncp_oql -domain` *`NCOMS`* `-username` *`admin`* `service` *`Model`* Vous pouvez également émettre cette requête en utilisant la page Accès à la base de données de gestion.
2. Indiquez le mot de passe adéquat lorsque vous y êtes invité.
3. Entrez la requête suivante :

   ```
   select ClassName from master.entityByName;
   ```

   `go` Voici un exemple de sortie de cette requête :

   ```
   {
    ClassName='Device';
   }
   {
    ClassName='Interface';
   }
   .....
   .....
    ClassName='MainNode';
   }
   {
    ClassName='CiscoSwitch';
   }
   ( 131 record(s) : Transaction complete )
   ```

Création et édition des fichiers AOC

Créez et éditez des fichiers AOC pour classifier les périphériques non classifiés ou modifier la hiérarchie de classe de votre topologie.

Si le processus de reconnaissance a identifié un périphérique non classifié, vous pouvez classifier ce dernier en créant un nouveau fichier AOC qui est spécifique à la classe à laquelle appartient le périphérique.

Vous pouvez éditer les fichiers AOC de l'une des deux façons suivantes : mettre à jour les bases de données **ncp_class** ou modifier les définitions de fichier AOC :

- Si vous souhaitez modifier les définitions AOC en cours en mettant à jour directement la base de données **ncp_class**, utilisez Accès à la base de données de gestion ou le fournisseur de services OQL.
- Si vous souhaitez modifier les définitions de fichiers AOC, procédez comme suit :

1. Accédez au répertoire `NCHOME/precision/aoc`.
2. Sauvegardez les fichiers à éditer.
3. Créez un fichier texte ou modifiez un fichier AOC existant à l'aide d'un éditeur de texte.

   Restriction : Utilisez uniquement des caractères alphanumériques et des traits de soulignement (_) dans les noms de fichier AOC. Tous les autres caractères, par exemple le tiret (-), sont interdits.
4. Si vous avez créé un fichier AOC, ajoutez une insertion à la table de base de données `class.classIds` dans le fichier de configuration `ClassSchema.cfg`.
5. Editez les options de démarrage du processus **ncp_class** et définissez l'option `-read_aocs_from` pour garantir que les fichiers AOC nouveaux ou modifiés sont lus.
6. Redémarrez le processus **ncp_class** après avoir modifié les fichiers AOC. Une fois que **ncp_class** a démarré et est en cours d'exécution, redémarrez le processus **ncp_model**.
7. Vérifiez qu'une version des nouveaux fichiers AOC spécifique au domaine est présente dans le répertoire `NCHOME/precision/aoc`.
8. Sauvegardez et supprimez les fichiers cache de classe dans le répertoire `NCHOME/var/precision`.

   Par exemple, supprimez les fichiers cache suivants :

   ```
   Class.Cache.class.activeClasses.NCOMS
   Class.Cache.class.staticClasses.NCOMS
   ```
9. Exécutez une reconnaissance complète et vérifiez que les résultats correspondent aux modifications que vous avez exécutées.

Référence associée:

«fichier AOC spécifique à une classe de périphériques», à la page 197
Cet échantillon de fichier AOC vous permet de comprendre comment Network Manager attribue les périphériques reconnus à la classe de périphériques située à un niveau inférieur dans la hiérarchie de classes.

Application des modifications AOC à la topologie et aux rapports

Une fois que vous avez mis à jour les définitions AOC et transmis les modifications à **ncp_class**, vous pouvez appliquer les modifications à la topologie en attendant la fin de la prochaine reconnaissance complète ou en redémarrant la reconnaissance à partir du point au niveau duquel la topologie est transmise de ncp_disco vers ncp_model.

A la fin de la prochaine reconnaissance complète, les modifications AOC que vous avez effectuées sont automatiquement appliquées à la topologie du réseau.

Si vous ne souhaitez pas attendre la prochaine reconnaissance complète, utilisez le programme stitcher adapté pour redémarrer la reconnaissance au point souhaité. Pour réinstancier le modèle de confinement, vous devez démarrer le programme stitcher qui envoie la topologie de base de **ncp_disco** vers **ncp_model**.

1. Connectez-vous au fournisseur de services OQL ou accédez au Accès à la base de données de gestion.
2. Emettez la requête suivante vers la table disco.status pour confirmer que le processus **ncp_disco** est en mode de nouvelle reconnaissance : `select * from disco.status;`

   Voici un exemple de réponse.

   ```
   m_DiscoveryMode=1;
   m_Phase=1;
   m_BlackoutState=0;
   m_CycleCount=0;
   m_ProcessingNeeded=0;
   m_FullDiscovery=0;
   ```

   Les résultats retournés par la requête permettent de constater que **ncp_disco** est en mode de nouvelle reconnaissance, c'est à dire que m_DiscoveryMode=1.
3. Démarrez le programme stitcher SendTopologyToModel. SendTopologyToModel envoi la topologie de base depuis ncp_disco vers ncp_model.
   a. Assurez-vous d'être dans le fournisseur de services OQL ou dans le Accès à la base de données de gestion.
   b. Pour insérer le programme stitcher dans la table stitchers.actions, émettez la commande suivante :

      ```
      insert into stitchers.actions
      ( m_Name )
      values
      ( 'SendTopologyToModel' );
      ```

   Une fois votre insertion OQL acceptée, le programme stitcher est appelé et la topologie de réseau envoyée à ncp_model. Lorsque la topologie est envoyée, elle est instanciée en fonction de la hiérarchie AOC modifiée.
4. Afin de s'assurer que les périphériques nouvellement classés soient supprimés du Rapport sur les périphériques contenant des ID objet SNMP non classifiés et du Rapport sur les périphériques contenant des ID objet SNMP inconnus, procédez comme suit :
   a. Clarifiez exactement les nouvelles valeurs sysObjectId qui sont mappées par les nouveaux fichiers AOC ou les fichiers AOC modifiés. Par exemple, les fichiers AOC originaux mappés aux valeurs sysObjectId suivantes :
      - 1.2.3.4
      - 1.5.6.*

Ensuite, deux nouvelles valeurs sysObjectId sont ajoutés au système: 1.9.8 et 1.5.6.7. Dans le fichier AOC, la valeur sysObjectId 1.5.6.7 est couverte par le mappage 1.5.6.*. Cependant, le fichier AOC doit être mis à jour pour ajouter la valeur sysObjectId 1.9.8.

b. Clarifier les fichiers AOC qui sont mappés par la table des mappages de la base de données topologiques NCIM. La table des mappages est utilisée par le Rapport sur les périphériques contenant des ID objet SNMP non classifiés et le Rapport sur les périphériques contenant des ID objet SNMP inconnus pour déterminer les données à afficher dans les rapports. Cette table n'est pas automatiquement mise à jour lorsque vous modifiez les fichiers AOC et redémarrez le gestionnaire de topologie, `ncp_class`, et, par conséquent, ces rapports continuent d'afficher les nouvelles valeurs sysObjectId comme non classifiées et inconnues. Les mappages dans la table des mappages sont également plus spécifiques que les mappages dans les fichiers AOC. Par exemple, la table des mappages de la base de données topologiques NCIM peut contenir les données suivantes :

Tableau 22. Exemple de données dans la table des mappages de la base de données topologiques de la base de données topologiques NCIM

mappingGroup	mappingKey	mappingValue	Description
sysObjectId	1.2.3.4	Type de périphérique A	Description du type de périphérique A
sysObjectId	1.5.6.1	Type de périphérique B	Description du type de périphérique B
sysObjectId	1.5.6.2	Type de périphérique C	Description du type de périphérique C

Dans le fichier AOC, seule la valeur sysObjectId 1.9.8 avait besoin d'être ajoutée vu que le mappage générique 1.5.6.* couvrait la nouvelle valeur sysObjectId 1.5.6.7. Cependant, dans la table des mappages de la base de données topologique NCIM les deux valeurs sysObjectId 1.9.8 et 1.5.6.7 doivent être ajoutées.

c. Depuis la ligne de commande, mettez à jour la table des mappages de la base de données topologiques NCIM avec des enregistrements pertinents pour les nouvelles valeurs sysObjectId. Par exemple, pour ajouter des enregistrements pour les deux nouvelles valeurs sysObjectId 1.9.8 et 1.5.6.7, ajoutez les instructions d'insertion SQL suivantes :

```
insert into mappings (mappingGroup, mappingKey, mappingValue)
values ('sysObjectId', '1.9.8', 'type_périphérique');
insert into mappings (mappingGroup, mappingKey, mappingValue)
values ('sysObjectId', '1.5.6.7', 'type_périphérique');
```

Où *type_périphérique* est le type de périphérique auquel la valeur sysObjectId doit être mappée. Pour plus d'informations sur la table des mappages de la base de données topologiques NCIM, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données topologiques*.

Une fois les modifications AOC appliquées à la topologie, automatiquement en attendant la prochaine reconnaissance ou manuellement en suivant les étapes de cette rubrique, vous remarquerez que les modifications suivantes sont appliquées à l'interrogation et à la visualisation du réseau.

- Lorsque vous définissez une nouvelle règle d'interrogation, les nouvelles classes que vous avez définies sont affichées dans l'onglet Classes dansEditeur de règles d'interrogation.

- Lorsque vous visualisez le réseau en utilisant des vues de réseau, l'arborescence des vues de réseau affiche maintenant les classes définies dans la hiérarchie de classes modifiée.
- Si vous avez mis à jour la table des mappages de la base de données topologiques NCIM, comme indiqué, le Rapport sur les périphériques contenant des ID objet SNMP non classifiés et le Rapport sur les périphériques contenant des ID objet SNMP inconnus ne renvoient plus aucune unité.

exemples de fichier AOC

Les échantillons de fichiers AOC vous permettent de comprendre comment Network Manager attribue les périphériques reconnus aux classes de périphériques dans la hiérarchie de classes.

Classe EndNode

Cet exemple de fichier AOC de classe EndNode vous permet de comprendre comment Network Manager affecte les périphériques reconnus à la classe EndNode.

Exemple

L'exemple de fragment de fichier AOC suivant affecte des périphériques à la classe EndNode à l'aide du filtre défini dans la clause instantiate_rule.

```
//************************************************************
//
// File : EndNode.aoc
//
//************************************************************
active object 'EndNode'
{
super_class = 'Core';
instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.2021\.' OU
EntityOID = '1.3.6.1.4.1.2021' OR
EntityOID = '1.3.6.1.4.1.1575' OR
EntityOID like '1 \.3\.6\.1\.4\.1\.11\.2\.3\.9\.' OU
EntityOID = '1.3.6.1.4.1.11.2.3.9' OR
(EntityType = 1 AND EntityOID IS NULL)
OU
...
OU
(
EntityOID = '1.3.6.1.4.1.1977'
)
OU
(
EntityOID like '1\.3\.6\.1\.4\.1\.2136\.'
)
OU
...
```

La clause instantiate_rule est très longue pour la classe EndNode. Elle comprend plusieurs lignes qui comparent l'ID objet d'entité, (l'ID objet système du périphérique), à différentes valeurs regroupées par un opérateur OU. Il existe différentes versions de la comparaison OR :

EntityOID = '1.3.6.1.4.1.2021'
: Ce filtre recherche une correspondance exacte entre l'ID objet d'entité et la valeur 1.3.6.1.4.1.2021. Si la correspondance n'est pas exacte, la comparaison échoue et le périphérique n'est pas affecté à la classe EndNode.

EntityOID like '1\.3\.6\.1\.4\.1\.11\.2\.3\.9\.'
Ce filtre recherche une correspondance similaire à la valeur 1\.3\.6\.1\.4\.1\.11\.2\.3\.9\. Le caractère \. est requis pour garantir que le . (point) est inclus dans la correspondance. Notez également que la valeur se termine par \. Une correspondance peut ainsi être effectuée aves des ID objet qui commencent par la valeur spécifiée mais ont des valeurs supplémentaires après le dernier . (point) est inclus dans la correspondance.

classe NetworkDevice

Cet exemple de fichier AOC de classe NetworkDevice vous permet de comprendre comment Network Manager affecte les périphériques reconnus à la classe NetworkDevice.

Modèle

L'exemple de fragment de fichier AOC suivant affecte des périphériques à la classe NetworkDevice à l'aide du filtre défini dans la clause instantiate_rule.

```
//************************************************************
//
// File : NetworkDevice.aoc
//
//************************************************************
active object 'NetworkDevice'
{
super_class = 'Core';
instantiate_rule = 'EntityType = 1 OR // Chassis
EntityType = 2 OR // Interface
EntityType = 3 OR // LogicalInterface
EntityType = 5 OR // Card
EntityType = 6 OR // PSU
EntityType = 8 OR // Module
EntityType = 0';
...
```

Pour la classe NetworkDevice, la clause instantiate_rule tente de faire correspondre des types de périphériques. Les exemples suivants sont des filtres utilisés dans la clause instantiate_rule.

EntityType = 1
Correspond à toutes les entités reconnues qui sont des périphériques boîtier. Les périphériques boîtier ont la zone entityType définie sur la valeur 1 dans la table entityData de la base de données topologiques NCIM.

EntityType = 2
Correspond à toutes les entités reconnues qui sont des ports ou des interfaces. Les ports et interfaces ont la zone entityType définie sur la valeur 2 dans la table entityData de la base de données topologiques NCIM.

EntityType = 3
Correspond à toutes les entités reconnues qui sont des interfaces logiques. Les interfaces logiques ont la zone entityType définie sur la valeur 3 dans la table entityData de la base de données topologiques NCIM.

EntityType = 5
Correspond à toutes les entités reconnues qui sont des cartes. Les cartes ont la zone entityType définie sur la valeur 5 dans la table entityData de la base de données topologiques NCIM.

EntityType = 6
Correspond à toutes les entités reconnues qui sont des blocs d'alimentation électriques (PSU). Les PSU ont la zone entityType définie sur la valeur 6 dans la table entityData de la base de données topologiques NCIM.

EntityType = 8
Correspond à toutes les entités reconnues qui sont des modules. Les modules ont la zone entityType définie sur la valeur 8 dans la table entityData de la base de données topologiques NCIM.

fichier AOC spécifique à une classe de périphériques

Cet échantillon de fichier AOC vous permet de comprendre comment Network Manager attribue les périphériques reconnus à la classe de périphériques située à un niveau inférieur dans la hiérarchie de classes.

Modèle

L'échantillon de fichier AOC fragmenté ci-après attribue des périphériques à la classe EWindowsNetHarmoni à l'aide du filtre défini dans la clause instantiate_rule. Il s'agit d'un périphérique EndNode.

```
//************************************************************
//
// Fichier : EWindowsNetHarmoni.aoc
//
//************************************************************
objet actif 'EWindowsNetHarmoni'
{
super_class ='EndNode';

instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.1977\.1\.6\.1279\.'";
...
```

Pour la classe EWindowsNetHarmoni, les paramètres ci-dessous sont définis dans le fichier AOC. Le paramètre instantiate_rule est long. Il s'agit de plusieurs lignes comparant le paramètre EntityOID, (c'est-à-dire l'ID objet système du périphérique), à différentes valeurs, additionnées par un opérateur OR. Il existe différentes versions de la comparaison OR :

super_class ='EndNode'
Ce paramètre établit le périphérique comme appartenant à la classe EndNode. La classe EWindowsNetHarmoni hérite de tous les attributs de la classe EndNode.

instantiate_rule = "EntityOID like '1 \.3\.6\.1\.4\.1\.1977\.1\.6\.1279\.'"
Ce filtre recherche une correspondance à la valeur 1\.3\.6\.1\.4\.1\.11\.2\ .3\.9\. Le caractère \. est requis pour garantir que le . (point) est inclus dans la correspondance. Notez également que la valeur se termine par \. Une correspondance peut ainsi être effectuée aves des ID objet qui commencent par la valeur spécifiée mais ont des valeurs supplémentaires après le dernier . (point) est inclus dans la correspondance.

Chapitre 5. Conservation de la topologie reconnue à jour

A la fin d'une reconnaissance, vous pouvez garder à jour la topologie reconnue en planifiant une reconnaissance, en configurant une reconnaissance automatique, en reconnaissant manuellement des unités et en supprimant des unités.

Planification de reconnaissances

Après l'exécution de la reconnaissance complète, vous pouvez planifier des reconnaissances supplémentaires en insérant l'heure, la date et le jour des reconnaissances à exécuter dans le fichier du programme stitcher `FullDiscovery.stch`.

1. Sauvegardez le fichier `NCHOME/precision/disco/stitchers/FullDiscovery.stch`.
2. Créez des instances distinctes du fichier `FullDiscovery.stch` pour chaque domaine sur le réseau. Pour créer une instance spécifique au domaine, insérez *`.domain`* dans le nom de fichier. Par exemple, `FullDiscovery.NCOMS.stch`. Si vous ne disposez pas de fichiers `FullDiscovery.stch` distincts pour chaque domaine, tous les domaines sur le réseau sont reconnus.
3. Planifiez la reconnaissance du premier domaine. Dans le fichier `FullDiscovery.`*`domain`*`.stch`, supprimez la mise en commentaire de l'une des lignes ActOnTimedTrigger. Ensuite, modifiez-la de sorte que la reconnaissance s'exécute à une heure précise. Par exemple, pour que la reconnaissance s'exécute à 23 h chaque jour, modifiez la ligne comme suit :

   ```
   ActOnTimedTrigger(( m_TimeOfDay ) values ( 2300 ) ; );
   ```
4. Répétez les étapes indiquées dans le fichier `FullDiscovery.stch` de pour chaque domaine sur le réseau.

Exemples

- Pour planifier une reconnaissance pour le sixième jour de la semaine depuis dimanche (à savoir, le samedi) à 23H00 :

  ```
  ActOnTimedTrigger(( m_DayOfWeek , m_TimeOfDay )
   values ( 6 , 2300 ) ; ) ;
  ```

  Sunday = 0, Monday = 1, Tuesday = 2, Wednesday = 3, Thursday = 4, Friday = 5, Saturday = 6.
- Pour planifier une reconnaissance pour le treizième jour de chaque mois à 14H00 :

  ```
  ActOnTimedTrigger(( m_DayOfMonth , m_TimeOfDay )
  values ( 13 , 1400 ) ; );
  ```
- Pour planifier une reconnaissance toutes les 13 heures :

  ```
  ActOnTimedTrigger(( m_Interval ) values ( 13 ) ; );
  ```

Concepts associés:

«A propos des types de reconnaissance», à la page 1
Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Configuration de la reconnaissance automatique

Network Manager fournit un mécanisme permettant de déclencher automatiquement une reconnaissance partielle en fonction de la réception d'une interruption. Cette opération est exécutée par le plug-in Disco sur la Passerelle d'événements. Les interruptions de périphérique peuvent indiquer un changement de périphérique réseau ou la présence d'un nouveau périphérique réseau. Pour plus d'informations sur le plug-in Disco, voir *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

Concepts associés:

«A propos des types de reconnaissance», à la page 1
Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Reconnaissance manuelle d'une unité ou d'un sous-réseau

Pour procéder à une reconnaissance manuelle des unités de sorte que la topologie de réseau de Network Manager corresponde au réseau.

Il peut arriver que vous sachiez que la configuration d'une ou de plusieurs unités a été modifiée et que vous souhaitiez les reconnaître, que le système ait détecté la modification grâce aux interruptions envoyées par les unités ou non.

Vous pouvez procéder à une reconnaissance manuelle d'une unité ou d'un sous-réseau de deux façons :

- Vous pouvez utiliser l'interface graphique de la configuration de la reconnaissance pour indiquer des unités individuelles ou des sous-réseaux complets à découvrir.
- Vous pouvez découvrir des périphériques spécifiques ou des ensembles de périphériques à partir de la vue fractionnée ou des vues de réseau
- Vous pouvez également effectuer des insertions dans la table finders.rediscovery en utilisant ncp_oql et en indiquant l'adresse IP ou le sous-réseau à reconnaître.

Remarque : N'utilisez pas de reconnaissances manuelles pour supprimer des périphériques de la topologie. Les périphériques qui ne sont plus accessibles restent dans la topologie jusqu'à ce que LingerTime atteigne zéro et qu'une autre reconnaissance soit exécutée. Ne procédez à de nouvelles reconnaissances manuelles que pour les périphériques opérationnels dont la configuration a été modifiée.

Tâches associées:

«Suppression d'un périphérique du réseau», à la page 206
Vous pouvez supprimer manuellement un périphérique dont la suppression permanente du réseau est planifiée.

«Surveillance de la reconnaissance de réseau à partir de l'interface graphique», à la page 173
Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

Reconnaissance manuelle d'une unité ou d'un sous-réseau à l'aide de l'interface graphique

Vous pouvez configurer et lancer la reconnaissance d'une unité ou d'un sous-réseau depuis l'interface graphique de la configuration de la reconnaissance. Vous pouvez personnaliser la configuration de la reconnaissance pour rendre la reconnaissance partielle aussi rapide que possible.

Activation des agents de reconnaissance partielle

Vous pouvez configurer une reconnaissance partielle en activant les agents appropriés dans l'onglet **Agents de reconnaissance partielle** de l'interface graphique de configuration de reconnaissance.

Vous pouvez augmenter la vitesse d'une reconnaissance partielle en sélectionnant uniquement les agents essentiels à la reconnaissance de nouveaux périphériques ou des périphériques modifiés.

Référence associée:

«Conseils relatifs à la sélection des agents», à la page 402
Pour reconnaître des technologies de périphériques (c'est-à-dire, utilisant d'autres protocoles qu'IP) sur votre réseau, vous devez vous assurer que les agents appropriés sont actifs.

Configuration des paramètres avancés de reconnaissance partielle

Parmi les paramètres avancés de reconnaissance partielle que vous pouvez configurer se trouvent le retour d'informations, la régénération de couches et les paramètres de voisins distants.

Configuration des paramètres de retour d'informations :

Vous pouvez indiquer des paramètres de retour d'informations lors de la configuration d'une reconnaissance partielle à l'aide de l'interface graphique.

Le retour d'informations est le mécanisme au cours duquel des données retournées par les agents sont utilisées pour rechercher d'autres unités. Parmi les exemples de données de retour d'informations, on trouve l'adresse IP des voisins distants ou le sous-réseau dans lequel un voisin local existe.

Le mécanisme de retour d'informations permet de transmettre toute nouvelle adresse IP à la reconnaissance et ainsi d'augmenter la taille du réseau reconnu. Vous devez trouvez un équilibre entre l'exhaustivité de la topologie reconnue (retour d'informations *activé*) et la rapidité de la reconnaissance (retour d'informations *désactivé*).

Vous pouvez choisir l'une des options suivantes après avoir sélectionné l'onglet **Avancé** dans l'option Configuration de l'interface graphique de la configuration de la reconnaissance :

- **Pas d'appréciations en retour** : Les retours d'informations sont désactivés pour toutes les reconnaissances. Cette option augmente la vitesse de reconnaissance mais ne reconnaît que les périphériques indiqués aux outils de recherche. Dès lors, la topologie générée est incomplète. Toutefois, ce paramètre permet de vérifier que les reconnaissances s'achèvent le plus rapidement possible.

- **Appréciations en retour** : Les retours d'informations sont activés pour les reconnaissances complètes et les nouvelles reconnaissances partielles. Cette option fournit une topologie complète dans toutes les situations, mais est celle qui prend le plus de temps.
- **Appréciations en retour uniquement pour les reconnaissances complètes** : Les retours d'informations sont activés pour les reconnaissances complètes, ce qui garantit une topologie complète. Dans le cas des reconnaissances partielles, le retour d'informations est désactivé. Cela permet d'assurer que son exécution soit la plus rapide possible. Il s'agit du paramètre par défaut.

Configuration des paramètres de la régénération des couches :

Vous pouvez permettre la régénération des couches de la topologie pour afficher une topologie précise lors de la configuration d'une reconnaissance partielle.

Pour régénérer les couches de la topologie après une nouvelle reconnaissance partielle, sélectionnez le paramètre **Activer la régénération des couches suite à une reconnaissance** dans l'onglet **Avancé** de l'option Configuration de l'interface graphique de la configuration de la reconnaissance. Si vous indiquez que les couches topologiques *doivent* être reformées à la suite d'une reconnaissance partielle, la topologie est précise et affiche toutes les données de connectivité. Toutefois, le processus d'ajout de nouvelles unités est plus long.

Concepts associés:

«Option permettant de reformer les couches topologiques», à la page 364
Vous pouvez indiquer si vous voulez reformer les couches topologiques à la suite d'une nouvelle reconnaissance partielle. A l'aide de cette option, vous pouvez augmenter la vitesse de la nouvelle reconnaissance partielle.

Activation de la reconnaissance des voisins distants pour la reconnaissance partielle :

La reconnaissance des voisins distants permet d'améliorer la précision des connexions détectées lors d'une reconnaissance partielle.

Par défaut, la reconnaissance des voisins distants est désactivée. Son activation allonge la durée de la reconnaissance.

En effet, lorsque la fonction est activée, Network Manager vérifie, lors d'une reconnaissance partielle, si des connexions aux voisins distants ont été modifiées. (Dans ce contexte, les voisins distants connectent des périphériques qui se trouvent dans la portée de la dernière reconnaissance complète, mais hors de portée de la reconnaissance partielle en cours.)

Si des connexions ont été modifiées, les périphériques connectés sont inclus dans la reconnaissance partielle, ce qui entraîne une topologie plus précise.

Restriction : Si une connexion entre des périphériques a été modifiée, mais que les informations sur cette connexion sont stockées uniquement sur le périphérique qui se trouve hors de portée, la modification n'est pas enregistrée et les périphériques connectés ne sont pas inclus dans la reconnaissance partielle. L'activation de la reconnaissance des voisins distants améliore la précision de la topologie, en cas de modification, mais ne garantit pas la reconnaissance de toutes les modifications. Pour obtenir une topologie la plus précise possible, exécutez une reconnaissance complète.

Pour activer la reconnaissance des voisins distants, sélectionnez **Activer la reconnaissance de périphériques associés** sur l'onglet Avancé dans l'option Configuration de l'interface graphique de la configuration de la reconnaissance.

Démarrage de reconnaissance partielle à partir de l'interface graphique

Le démarrage d'une reconnaissance partielle implique de définir un emplacement de départ et des portées.

Si une reconnaissance complète n'a pas été exécutée depuis le dernier démarrage du moteur de reconnaissance, **ncp_disco**, vous ne pouvez pas démarrer de reconnaissance partielle.

Vous pouvez démarrer une reconnaissance partielle sur un périphérique ou un sous-réseau à partir de la fenêtre Etat de la reconnaissance active. Vous pouvez également découvrir des périphériques spécifiques en cliquant avec le bouton droit de la souris sur ces périphériques dans les vues tronçon et de réseau.

Pour démarrer une reconnaissance partielle à partir de la fenêtre Etat de la reconnaissance active, effectuez les tâches suivantes.

1. Sélectionnez le domaine dans lequel vous souhaitez exécuter une reconnaissance, dans le menu **Domaine**. Vous pouvez commencer à saisir le nom du domaine et les domaines concordants apparaissent sous la zone **Domaine**.
2. Cliquez sur la flèche vers le bas, située en regard du bouton **Démarrer la reconnaissance**  et sélectionnez **Démarrer la reconnaissance partielle** dans le menu. La fenêtre Reconnaissance partielle s'affiche. Indiquez les adresses IP et les sous-réseaux contenant les périphériques devant être reconnus.
3. Sous **Reconnaissance partielle**, sélectionnez les noeuds et sous-réseaux requis.
4. Pour ajouter un nouveau sous-réseau ou noeud, cliquez sur **Nouveau.**
5. Renseignez les zones comme suit, puis cliquez sur **OK** :

   Nouvelle reconnaissance
   Sélectionnez l'une des options suivantes :

   Adresse IP
   Entrez l'adresse IP requise.

   Sous-réseau
   Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.
6. Pour ajouter de nouvelles zones de portée, cliquez sur **Portée**.

   Remarque : Si vous ajoutez une zone de portée qui n'est pas incluse dans la portée de la dernière reconnaissance complète, les connexions entre les périphériques de la nouvelle et de l'ancienne portée risquent de ne pas être précises jusqu'à la prochaine reconnaissance complète. L'activation de la reconnaissance voisine distante permet d'améliorer la précision de ces connexions.
7. Pour ajouter une nouvelle zone de portée de reconnaissance, cliquez sur **Nouveau**  . Pour éditer une zone de portée existante, cliquez sur l'entrée requise dans la liste.

8. Renseignez les zones comme suit, puis cliquez sur **OK** :

Portée :

Sélectionnez l'une des options suivantes :

Sous-réseau

Entrez le sous-réseau requis et indiquez le nombre d'octets de sous-réseau. La zone **Masque de réseau** est automatiquement mise à jour.

Vous pouvez indiquer une adresse de sous-réseau ou une adresse IP individuelle par le biais de ces zones.

- Par exemple, pour spécifier un sous-réseau de classe C IPv4 10.30.2.0, entrez `10.30.2.0/24`, où `10.30.2.0` correspond au préfixe de sous-réseau et `24` au masque de sous-réseau.
- Pour spécifier un périphérique individuel, entrez une adresse IP IPv4 et un masque de sous-réseau de valeur `32`. Par exemple, entrez `10.30.1.20/32`.
- Si vous utilisez IPv6, utilisez un masque de sous-réseau égal ou supérieur à 112 afin d'éviter des temps de reconnaissance excessifs.

Caractère générique

Utilisez l'astérisque (*) comme caractère générique.

Par exemple, pour spécifier une portée correspondant à toutes les adresses IP commençant par le préfixe de sous-réseau 10.30.200., entrez `10.30.200.*`.

Restriction : Network Manager ne prend pas en charge le format IPv6 mappé IPv4 et exige que toutes les adresses IPv6 soient au format IPv6 standard, séparées par un double point. Par exemple, Network Manager ne prend pas en charge une adresse IPv6 mappé IPv4 comme `::ffff:192.0.2.128`. Vous devez entrer cette adresse au format IPv6 standard, le signe de ponctuation des deux points faisant office de séparateur : `::ffff:c000:280`.

Protocole

Sélectionnez le protocole Internet requis : IPv4 ou IPv6.

Action

Définissez l'intervalle de sous-réseau en tant que zone d'inclusion ou d'exclusion. Si l'intervalle de sous-réseau est une zone d'inclusion sur laquelle vous prévoyez de lancer une commande PING lors de la reconnaissance, cliquez sur **Ajout à la liste des emplacements de départ de commande PING**. Lorsque vous cliquez sur cette option, les périphériques faisant partie de la zone de portée sont ajoutés automatiquement en tant que périphériques de départ de la reconnaissance.

Restriction : L'option `Ajout à la liste des emplacements de départ de commande PING` n'est pas disponible pour les zones de portée IPv6. Cela empêche le balayage des sous-réseaux IPv6 par des commandes ping, ce qui concernerait potentiellement des milliards de périphériques. Une telle opération peut se solder par une reconnaissance inachevée.

9. Cliquez sur **OK**, puis sur **Accéder**. Lorsqu'une reconnaissance partielle s'exécute, le bouton **Démarrer la reconnaissance** est désactivé  .

Concepts associés:

«A propos des types de reconnaissance», à la page 1
Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Tâches associées:

«Démarrage d'une reconnaissance», à la page 52
Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

«Surveillance de la reconnaissance de réseau à partir de l'interface graphique», à la page 173
Dans la page Etat de la reconnaissance active, vous pouvez surveiller l'état et la progression de la reconnaissance en cours, examiner le travail des agents de reconnaissance et afficher les détails de la dernière reconnaissance.

Reconnaissance manuelle d'un périphérique ou d'un sous-réseau depuis la ligne de commande

Vous pouvez procéder à une reconnaissance manuelle d'une unité ou d'un sous-réseau depuis la ligne de commande.

Pour procéder à une reconnaissance manuelle d'une unité ou d'un sous-réseau à partir de la ligne de commande, effectuez des insertions dans la table `finders.rediscovery` en utilisant `ncp_oql` et en spécifiant l'adresse IP ou le sous-réseau pour le ou laquelle effectuer une reconnaissance, comme décrit dans l'exemple suivant.

Reconnaissance manuelle

Pour procéder à une reconnaissance de l'unité disposant de l'adresse IP 192.168.1.2, commencez par démarrer le fournisseur de services OQL à l'aide de la commande suivante :

```
ncp_oql -domain NCOMS -service Disco
```

Une fois connecté au fournisseur OQL, exécutez la requête suivante (notez que la commande est entrée en une seule ligne) :

```
insert into finders.rediscovery (m_Address, m_RequestType) values
("192.168.1.2", 1);
```

Lorsque la reconnaissance d'une unité est ainsi forcée, `ncp_disco` la transmet immédiatement à l'outil de recherche Ping pour confirmer son existence, et ci cette dernière est confirmée, déclenche une nouvelle analyse par les agents appropriés. Si les connexions de l'unité ont été modifiées, les unités voisines peuvent également être reconnues.

Suppression d'un périphérique du réseau

Vous pouvez supprimer manuellement un périphérique dont la suppression permanente du réseau est planifiée.

1. Suspendez l'interrogation du périphérique. Ceci empêche les fausses alertes générées par le système moniteur lors de la mise hors tension du périphérique.
2. Supprimez le périphérique physiquement du réseau.
3. Immédiatement avant la prochaine reconnaissance réseau complète, définissez la durée de temporisation de l'enregistrement du périphérique dans ncp_model à 0.

Tâches associées:

«Reconnaissance manuelle d'une unité ou d'un sous-réseau», à la page 200
Pour procéder à une reconnaissance manuelle des unités de sorte que la topologie de réseau de Network Manager corresponde au réseau.

Définition du délai de latence d'un périphérique

La valeur de la zone LingerTime indique pendant combien de reconnaissances une unité peut ne pas être trouvée avant qu'il ne soir supposé qu'elle a été supprimée du réseau et que son enregistrement soit supprimé de la topologie. Si vous définissez la zone LingerTime sur zéro et que l'unité est introuvable lors de la prochaine reconnaissance, l'enregistrement de cette unité est immédiatement supprimé de la topologie.

Pour définir la zone LingerTime sur zéro :

1. Entrez une commande similaire à celle-ci pour démarrer le fournisseur de services OQL :

   ```
   ncp_oql -domain NCOMS -service Model
   ```

2. Mettez à jour la zone LingerTime dans la table master.entityByName pour toutes les entités qui représentent l'unité. Par exemple, si l'unité est appelée `core-router.abcd.com`, entrez la commande suivante, sur une ligne :

   ```
   update master.entityByName set LingerTime = 0
   where EntityName like 'core-router.abcd.com';
   ```

Mise à jour manuelle des caractéristiques des périphériques

Les caractéristiques de périphérique mises à jour ne sont parfois pas détectées par une reconnaissance.

Parfois, les modifications que vous apportez à un périphérique, par exemple l'attribution d'un nouveau nom, ne sont pas détectées par une reconnaissance ultérieure. Dans ce cas, vous pouvez utiliser l'outil Supprimer un noeud pour supprimer le périphérique de la topologie de réseau, puis effectuer une nouvelle reconnaissance du périphérique, basée sur les nouvelles caractéristiques.

Pour mettre à jour manuellement un périphérique, procédez comme suit :

1. Exécutez le script `RemoveNode.pl` sur le périphérique.
2. Effectuez une nouvelle reconnaissance du périphérique.

Chapitre 6. Traitement des incidents liés à la reconnaissance

Vous pouvez traiter les incidents liés à la reconnaissance en surveillant les événements de reconnaissance et en exécutant des rapports de reconnaissance. Vous pouvez également configurer vos propres événements de reconnaissance.

Traitement des incidents liés à la reconnaissance à l'aide de rapports

Les rapports de traitement des incidents permettent d'améliorer la visibilité des résultats de la reconnaissance et donc de faciliter le traitement des incidents de ces résultats et du réseau lui-même.

Network Manager utilise le composant Tivoli Common Reporting pour générer des rapports. Pour plus d'informations sur Tivoli Common Reporting, voir

- dans le centre de documentation Tivoli Common Reporting
- developerWorks Tivoli Common Reporting

Pour accéder aux rapports dans l'interface graphique de Network Manager, cliquez sur **Reporting** > **Common Reporting** dans le panneau de navigation.

Vous pouvez utiliser des rapports pour vérifier les résultats de la reconnaissance et identifier et résoudre les incidents qui leur sont liés, comme dans les exemples du tableau 23.

Pour plus d'informations sur les rapports Network Manager, reportez-vous à *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tableau 23. Catégories de rapports à utiliser pour le traitement des incidents de la reconnaissance

Tâche de traitement des incidents	**Consulter cette catégorie et ce rapport**	**Avantage du rapport**
Identification de tous les noeuds et interfaces reconnus	Rapports d'utilitaire : Liste des fichiers à plat des interfaces et des noeuds reconnus	Ce rapport répertorie tous les noeuds et interfaces reconnus. Il marque également les interfaces ou ports connectés aux unités réseau. Il vous permet de vérifier que des unités et des interfaces spécifiques ont bien été reconnues.
Résolution de non concordances	Rapports de traitement des incidents : Non concordance de l'interface Duplex connectée	Ce rapport fournit une liste de connexions pour lesquelles il existe une non concordance entre des unités, où une extrémité de la connexion est en semi-duplex et l'autre en duplex intégral. Cette non-concordance est l'un des incidents de configuration clés que les administrateurs réseau doivent détecter pour améliorer la performance et la disponibilité.
Résolution d'unités inaccessibles	Rapports de traitement des incidents : Unités sans accès SNMP	Ce rapport identifie les périphériques qui ne disposent d'aucun accès SNMP. Vous pouvez ensuite la raison de l'échec de l'accès SNMP.

Tableau 23. Catégories de rapports à utiliser pour le traitement des incidents de la reconnaissance (suite)

Tâche de traitement des incidents	**Consulter cette catégorie et ce rapport**	**Avantage du rapport**
Résolution d'unités non connectées	Rapports de traitement des incidents : Unités sans connexion	Ce rapport répertorie les périphériques non connectés. Il s'agit de la première étape de la détermination des raisons pour lesquelles la reconnaissance n'a trouvé aucune connexion réseau pour un périphérique.
Résolution d'unités non classées	Rapports de traitement des incidents : Unités avrc des ID objet SNMP non classifiés	A l'aide de ces rapports, vous pouvez créer des fichiers AOC de noeud terminal pour la nouvelle classe d'unités.
	Relevé de pièce : • Disponibilité de l'interface • Récapitulatif par classe de périphérique • Fournisseur et disponibilité du produit	
Résolution d'unités avec ID objet SNMP non enregistrés	Rapports de traitement des incidents : Unités avrc des ID objet SNMP inconnus	Utilisez les informations de ce rapport pour modifier les fichiers AOC associés aux unités non enregistrées.
Identifications des unités en attente de suppression	Rapports de traitement des incidents : Suppression des unités en attente lors de la prochaine reconnaissance	Ce rapport affiche des informations sur les périphériques à supprimer de la topologie s'ils sont introuvables au cours du prochain cycle de reconnaissance. Il vous permet de vérifier que la suppression de périphériques de la topologie progresse et d'identifier les périphériques dont la suppression a été planifiée par erreur.

Surveillance de l'état de la reconnaissance

Vous pouvez visualiser des messages d'état de la reconnaissance pour comprendre l'état et la progression de la reconnaissance. Vous pouvez également configurer vos propres événements de reconnaissance.

Flux de processus pour la création d'événements de reconnaissance

Les événements de reconnaissance sont créés lors du processus de reconnaissance affichant la progression des agents, des programmes stitcher et des outils de recherche. Ces événements sont envoyés et stockés dans Tivoli Netcool/OMNIbus et peuvent être visualisés à l'aide de l'Interface graphique Web.

Les événements de reconnaissance sont créés lors des étapes suivantes :

- Lors de la phase de collecte de données de la reconnaissance, des programmes stitcher dédiés (AgentStatus et FinderStatus) détectent si des outils de recherches et des agents ont démarrés ou se sont arrêtés.

- Lors de la phase de traitement des données, un programme stitcher dédié (CreateStchTimeEvent) détecte des événements clés ; par exemple, si la reconnaissance a commencé la génération de la table d'entités de travail ou de la table de confinement.
- Lorsque l'un des programmes stitcher ci-dessus détecte un événement, il écrit cet événement dans la table `disco.events`.
- Le programme stitcher DiscoEventProcessing répond à une insertion dans la table `disco.events` et crée et envoie l'événement approprié à la sonde pour Tivoli Netcool/OMNIbus, nco_p_ncpmonitor, qui transmet ensuite l'événement au serveur d'objets.
- Vous pouvez activer ou désactiver la génération d'événements de reconnaissance en définissant la valeur de la zone `m_CreateStchrEvents` dans la table `disco.config`.

Vous pouvez configurer vos propres événements de reconnaissance en écrivant un programme stitcher afin de détecter l'événement souhaité et écrire ces données d'événement dans la table `disco.events`.

Référence associée:

«Table disco.events», à la page 247
La table d'événements limite des événements de reconnaissance générés à un format standard. Un événement est généré par l'insertion d'un enregistrement dans cette table.

«Principaux programmes stitcher de reconnaissance», à la page 409
Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

Surveillance des messages d'état de la reconnaissance

Vous pouvez visualiser des messages d'état de la reconnaissance pour comprendre l'état et la progression de la reconnaissance.

Les processus de reconnaissance, y compris les agents, les programmes stitcher et les outils de recherche envoient des messages à IBM Tivoli Netcool/OMNIbus lorsqu'ils démarrent et s'arrêtent. Vous pouvez visualiser ces messages pour savoir si les processus de reconnaissance s'exécutent comme prévu et pour évaluer la progression globale de la reconnaissance.

Pour visualiser les messages d'état des processus de reconnaissance, effectuer les tâches suivantes.

1. Cliquez sur **Disponibilité** > **Evénements** > **Liste des événements actifs** pour afficher **Liste des événements actifs**.
2. Appliquez un filtre à la liste des événements actifs afin que seuls les événements dont l'`Agent` est `ncp_disco` soient affichés.
3. Facultatif : Détaillez le filtre ou triez **EventId** pour afficher uniquement des types spécifiques d'événements de reconnaissance.
4. Vérifiez que les colonnes **LocalPriObj** et **LocalSecObj** sont affichées dans la liste des événements actifs. Ces colonnes contiennent des informations sur les événements de reconnaissance. (Certaines colonnes ne sont pas utilisées par tous les événements.)

Traitement des incidents liés aux agents de reconnaissance

Vous pouvez utiliser l'interface graphique d'état de reconnaissance pour identifier et résoudre les problèmes associés aux agents de reconnaissance.

Traitement des incidents liés à une reconnaissance anormalement longue

Une reconnaissance peut être anormalement longue car un agent ne parvient pas à terminer le traitement sur un périphérique spécifique. Utilisez la section **Statut des agents** pour déterminer quel agent est en cause et sur quelle unité s'effectue le traitement.

Pour utiliser la section **Statut des agents** afin de déterminer si la cause du problème est un agent bloqué sur un périphérique, procédez comme suit :

1. Ouvrez la section **Statut des agents** en cliquant sur **Reconnaissance** > **Etat de la reconnaissance réseau**, puis cliquez sur l'onglet **Statut des agents**.
2. Définissez la liste déroulante Phases située au-dessus de la table Agents supérieure par Interrogation des périphériques. La table Agents supérieure affiche à présent uniquement les agents qui sont planifiés pour s'exécuter dans la première phase de reconnaissance, Interrogation des périphériques.

   Remarque : Ce problème se produit généralement pendant la première phase de reconnaissance, Interrogation des périphériques.
3. Vérifiez que la colonne **Etat** est classée par ordre décroissant. Les agents apparaissent par défaut par ordre décroissant d'état d'agent, comme répertorié dans le tableau suivant.

Tableau 24. Etats d'agent

Etat	Valeur	Icône	Description
Mort	5		L'agent s'est terminé de façon inattendue. Il s'agit d'un problème de reconnaissance potentiel.
Terminé	4		L'agent est en cours d'exécution mais a terminé le traitement de toutes les adresses IP de sa file d'attente. L'agent est encore disponible pour traiter les agents supplémentaires placés en file d'attente.
En cours d'exécution	3		L'agent est en cours de traitement des adresses IP.
Démarrage de	2		L'agent est en cours de démarrage.
Non exécuté	1		L'agent n'est pas en cours d'exécution.

4. Faites défiler le tableau vers le bas pour identifier les agents dont l'état est En cours d'exécution  . Il s'agit des agents qui continuent de traiter des périphériques. Si la reconnaissance s'est exécutée pendant un temps anormalement long, il n'y a peut-être qu'un seul agent dont l'état est En cours d'exécution  . Il s'agit de l'agent bloqué.
5. Sélectionnez l'un des agents avec l'état En cours d'exécution  . Par défaut, le tableau au bas de la page affiche à présent toutes les adresses IP qui se trouvent encore en file d'attente pour cet agent.
6. Cliquez sur le bouton d'option **Tous** situé au-dessus du tableau inférieur. Le tableau de bas de page contient à présent toutes les adresses IP qui ont été traitées par cet agent, qui sont toujours traités par ces agents ou qui se trouvent dans la file d'attente de l'agent.

7. Vérifiez que la colonne **Etat** est classée par ordre décroissant. Les adresses IP apparaissent par défaut par ordre décroissant d'état d'agent, comme répertorié dans le tableau suivant.

Tableau 25. Etats d'adresse IP

Etat	Valeur	Icône	Description
Mort	5		Le traitement de cette adresse IP s'est terminé de façon inattendue. Il s'agit d'un problème de reconnaissance potentiel.
Terminé	4		Un agent a terminé le traitement de cette adresse IP.
En cours d'exécution	3		Un agent est en train de traiter cette adresse IP.
Démarrage de	2		Un agent commence le traitement de cette adresse IP.
Non exécuté	1		L'adresse IP n'est pas en cours de traitement.

8. Faites défiler le tableau vers le bas pour identifier les adresses IP dont l'état est En cours d'exécution  . Ces adresses IP sont en cours de traitement par cet agent. Si l'agent est bloqué sur un périphérique, il n'existe qu'une seule adresse IP avec l'état En cours d'exécution  .
9. Consultez les autres informations de la table pour en savoir plus sur cette adresses IP. La colonne Délai écoulé indique la durée de traitement du périphérique par l'agent. La colonne Accès SNMP indique si l'agent a disposé de l'accès SNMP vers ce périphérique.

Si l'agent n'a pas disposé de l'accès SNMP vers ce périphérique, un problème s'est peut-être produit sur les paramètres de nom de communauté SNMP. Une analyse approfondie de ce périphérique est requise.

Tâches associées:

«Surveillance de la progression des agents de reconnaissance», à la page 176
Vous pouvez utiliser la section **Statut des agents** pour surveiller la progression des agents de reconnaissance au cours de chacune des phases de reconnaissance.

Identification des agents en échec

Les agents qui s'interrompent brusquement pendant une reconnaissance peuvent être une cause d'échec de la reconnaissance. Utilisez la section **Statut des agents** pour déterminer si des agents se sont interrompus de manière inattendue.

Pour utiliser la section **Statut des agents** afin de déterminer si des agents de reconnaissance ne s'exécutent pas correctement, procédez comme suit :

1. Ouvrez la section **Statut des agents** en cliquant sur **Reconnaissance** > **Etat de la reconnaissance réseau**, puis cliquez sur l'onglet **Statut des agents**.
2. Vérifiez que la liste déroulante Phases située au-dessus de la table Agents supérieure est définie par Toutes les phases. La table Agents supérieure affiche à présent tous les agents qui ont démarré dans cette reconnaissance.
3. Cliquez sur la colonne **Etat** dans la table Agents supérieure afin que les agents soient classés par ordre décroissant d'**Etat**. Les agents apparaissent à présent dans la table par ordre alphabétique de statut.
4. Les agents s'étant interrompus brusquement se trouvent au début de la table et ont le statut Mort.

Une analyse plus poussée est requise afin de déterminer pourquoi cet agent s'est interrompu brusquement.

Tâches associées:

«Surveillance de la progression des agents de reconnaissance», à la page 176
Vous pouvez utiliser la section **Statut des agents** pour surveiller la progression des agents de reconnaissance au cours de chacune des phases de reconnaissance.

Traitement des incidents liés aux périphériques manquants

Si un périphérique qui doit figurer dans la topologie de réseau est absent, procédez comme suit pour traiter le problème.

Avant d'effectuer ces étapes, exécutez une reconnaissance complète en activant le retour d'informations.

Pour rechercher des causes communes de l'absence d'un périphérique dans les mappes de réseau, procédez comme suit.

1. Vérifiez que le périphérique que vous recherchez s'exécute et est connecté au réseau.
2. Recherchez le périphérique.
   a. Recherchez le périphérique dans les mappes de réseau par nom d'hôte, puis par adresse IP.
   b. Si vous savez à quels périphériques il est connecté, tentez de trouver l'un des périphériques connectés dans la Vue tronçon de réseau. Définissez ensuite le nombre de tronçons par 1 et vérifiez si le périphérique est représenté comme étant connecté.
3. Vérifiez si le périphérique est dans la portée. Vérifiez la portée de la reconnaissance, y compris les zones d'exclusion, dans l'onglet **Portée** de l'interface graphique Configuration de la reconnaissance réseau.
4. Vérifiez si le périphérique est exclu de la reconnaissance.
   a. Cliquez sur **Filtres**.
   b. Vérifiez les filtres de pré-reconnaissance et de post-reconnaissance pour vous assurer que rien n'empêche le périphérique d'être reconnu ou instancié.

Tâches associées:

«Définition des filtres de reconnaissance», à la page 36
Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Traitement des incidents liés à une reconnaissance en veille

Si vous démarrez la reconnaissance et qu'après quelques minutes aucun périphérique n'a été découvert, exécutez les étapes de traitement des incidents suivantes.

Si l'état de la reconnaissance reste en phase zéro (inactif) après le démarrage et qu'aucun périphérique n'a été découvert, exécutez les étapes suivantes de traitement des incidents.

1. Si vous utilisez l'outil de recherche de fichiers, vérifiez que vous avez correctement spécifié quelle zone du fichier de départ contient l'adresse IP et quelle zone contient le nom d'hôte. Vous pouvez vérifier ces paramètres dans l'interface graphique de configuration de reconnaissance.
2. Si vous utilisez l'outil de recherche PING et que vous envoyez la commande PING sur des adresses IP individuelles, vérifiez que ces adresses IP sont accessibles. Si tel n'est pas le cas, il peut s'agir d'une indisponibilité du réseau ou d'un problème de pare-feu.
3. Vérifiez que les adresses IP de départ sont dans la portée. Même si vous ajoutez une adresse à l'outil de recherche PING ou à l'outil de recherche de fichiers, le périphérique n'est pas atteint par la commande PING ni instancié s'il ne se trouve pas dans la portée. Par exemple, si la portée de reconnaissance est 172.16.1.0 /24 et que les emplacements de départ sont dans le réseau 192.168.1.0 /24, les outils de recherche ne peuvent pas les trouver.
4. Si vous envoyez la commande PING sur un sous-réseau étendu et peu peuplé, par exemple un sous-réseau de classe B ne contenant que 10 périphériques, il est possible qu'un assez long laps de temps s'écoule avant que l'outil de recherche PING ne trouve le premier périphérique.

Si vous devez consulter les journaux de reconnaissance, reportez-vous aux informations sur la localisation des fichiers journaux et la modification des niveaux de journalisation dans *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Tâches associées:

«Démarrage d'une reconnaissance», à la page 52
Une fois la reconnaissance configurée, vous pouvez la démarrer et, le cas échéant, l'arrêter.

Suppression de fichiers cache de reconnaissance

Supprimez les fichiers cache de reconnaissance pour effectuer une nouvelle reconnaissance propre.

Pour supprimer la reconnaissance de réseau en cours sur un domaine, vous devez supprimer tous les fichiers cache de cette reconnaissance. Vous pouvez effectuer cette opération lorsque vous devez effacer toutes les données d'une reconnaissance précédente ou lorsque le support IBM vous le demande.

Cette procédure supprime tous les fichiers cache de la reconnaissance en cours et efface la base de données de la reconnaissance, en réinitialisant la reconnaissance. Après cette procédure, vous devez exécuter une nouvelle reconnaissance complète de votre réseau.

Remarque : Etant donné que la topologie de réseau est stockée séparément dans la base de données NCIM, cette procédure ne supprime pas vos mappes de réseau.

Toutefois, les modifications apportées au réseau depuis la dernière reconnaissance sont représentées dans la reconnaissance suivante.

Exécutez la procédure suivante pour supprimer tous les fichiers cache de reconnaissance :

1. Arrêtez tous les processus Network Manager à l'aide du script `itnm_stop`.
2. Accédez au répertoire `$NCHOME/var/precision` et supprimez tous les fichiers qui appartiennent au domaine que vous souhaitez supprimer. Les fichiers qui appartiennent à un domaine donné comportent le domaine dans leur nom. Par exemple, un fichier de configuration appartenant au domaine NCOMS est appelé `nom_fichier.NCOMS.cfg`.
3. Facultatif : Vous pouvez archiver ou supprimer les fichiers journaux existants et démarrer la nouvelle reconnaissance avec de nouveaux fichiers journaux. Les fichiers journaux et les traitements suivants sont importants :
   - **ncp_disco**
   - **ncp_df_***
   - **ncp_agent***
   - **ncp_disco_perl_agent***
4. Redémarrez les processus Network Manager à l'aide du script `itnm_start`.

   De nouveaux fichiers journaux vides sont automatiquement créés lorsque les processus Network Manager sont redémarrés à l'aide des scripts `itnm_start`.
5. Effectuez une nouvelle reconnaissance réseau.

Traitement des incidents causés par des caractères non autorisés

Si vous voyez un message d'erreur sur des caractères non autorisés dans les instructions d'insertion dans la base de données topologique, procédez comme suit pour identifier le problème.

Si vous avez des périphérique réseau dont les descriptions comportent des caractère non autorisés dans le jeu local de la base de données, un message d'erreur du type suivant peut s'afficher :

```
Warning: W-RIV-002-206: [4115626896t] CMdlDbEntityMgr.cc(647)
A database 'execute' operation has failed :
SQLRETURN = -1 CNcpODBCSth.cc line 233 : [Informix][Informix ODBC Driver][Informix]
An illegal character has been found in the statement.
```

1. Sauvegardez et modifiez le fichier de configuration `SnmpStackSchema.cfg`.
2. Recherchez la ligne qui configure une insertion dans la table `snmpStack.conversionCfg` et modifiez-la comme suit :

   ```
   insert into snmpStack.conversionCfg values (1);
   ```
3. Sauvegardez et fermez le fichier.

L'Auxiliaire SNMP substitue les caractères non autorisés dans l'environnement local de la base de données et qui sont renvoyés par des périphériques par le caractère du point d'interrogation : '?'.

L'Auxiliaire SNMP substitue les caractères uniquement dans les objets configurés dans la table snmpStack.multibyteObjects.

Chapitre 7. Enrichissement de la topologie

Vous pouvez enrichir la topologie en ajoutant du contexte supplémentaire aux informations découvertes par le processus de reconnaissance. Par exemple, vous pouvez ajouter des balises personnalisées aux unités afin d'afficher le client, l'emplacement ou d'autres informations associées à ce périphérique. Vous pouvez ensuite utiliser ces informations personnalisées pour visualiser ou interroger votre réseau.

Cette section présente différents exemples d'enrichissement de la topologie. Vous pouvez les consulter pour vous faire une idée des différentes manières dont vous pouvez enrichir la topologie et des méthodes disponibles pour ce faire.

Ajout de balises aux entités

Vous pouvez ajouter une ou plusieurs balises de paire nom-valeur aux entités reconnues.

Le tableau suivant présente un exemple d'unité avec comme adresse IP 172.20.3.20, avec deux balises de paires nom-valeur associées.

Tableau 26. Exemple de balises de paires nom-valeur

Adresse IP	**Nom**	**Valeur**
172.20.3.20	customer	acme
172.20.3.20	location	london

Une fois que la reconnaissance a balisé vos adresses IP avec des informations de paires nom-valeur personnalisées, vous pouvez utiliser ces informations pour effectuer des tâches de visualisation et d'interrogation personnalisées. Par exemple, vous pourriez créer une vue réseau personnalisée affichant toutes les adresses IP référencées avec l'emplacement "london".

Personnalisation de la reconnaissance

Utilisez l'une des méthodes suivantes pour personnaliser la reconnaissance en ajoutant des balises de paires nom-valeur aux entités identifiées à l'aide de l'outil de recherche de fichiers ou de tables de balises personnalisées. Si vous utilisez les tables de balises personnalisées, vous pouvez également utiliser la logique définie dans le programme stitcher GetCustomTag pour évaluer la valeur de la balise de paire nom-valeur ajoutée.

Ajout de balises aux entités à l'aide de l'outil de recherche de fichiers

Si vous utilisez l'outil de recherche de fichiers pour lancer la reconnaissance, vous pouvez ajouter des balises de paire nom-valeur aux entités en ajoutant des colonnes supplémentaires au fichier de départ lu par l'outil.

L'exemple de procédure ci-après suppose que vous ajoutez les colonnes supplémentaires suivantes à votre fichier de départ de recherche de fichiers :

- customer
- location

L'exemple de fragment de fichier texte suivant présente l'apparence possible du fichier de départ :

```
vi /var/tmp/logged_hosts

172.16.1.21       lnd-dharma-acme       acme        london
172.16.1.201      lnd-phoenix-acme      acme        london
172.16.1.25       prs-sun-acme          acme        paris
172.16.2.33       ranger1               telecorp    newyork
172.16.2.34       ranger2               telecorp    newyork
~
"/var/tmp/logged_hosts" [Read only] 4 lines, 190 characters
```

Dans ce fragment, la troisième colonne héberge des informations sur le client et la quatrième colonne, sur son emplacement.

1. Modifiez le fichier de configuration DiscoFileFinderParseRules.cfg.
2. Dans ce fichier, configurez l'outil de recherche de fichiers à l'aide d'une insertion similaire à celle de l'exemple afin d'analyser le fichier de départ. Prenez soin de configurer la zone `m_ColDefs` afin qu'elle corresponde aux nouvelles colonnes de balises personnalisées.

```
insert into fileFinder.parseRules
(
            m_FileName,
            m_Delimiter,
            m_ColDefs
)
values
(
            "/var/tmp/logged_hosts",
            "[     ]",
            [
                {
                    m_VarName="m_UniqueAddress",
                    m_ColNum=1
                },
                {
                    m_VarName="m_Name",
                    m_ColNum=2
                }
                {
                    m_VarName="m_CustomTags->customer",
                    m_ColNum=3
                },
                {
                    m_VarName="m_CustomTags->location",
                    m_ColNum=4
                }
            ]
);
```

Cette insertion indique à l'outil de recherche de fichiers d'effectuer les opérations suivantes :

- Analyse de `/var/tmp/logged_hosts`.
- Traitement des espaces en tant que séparateurs de données.
- Utilisation des définitions de colonnes suivantes :
  - `m_UniqueAddress` pour la première colonne
  - `m_Name` pour la seconde colonne
  - `m_CustomTags->customer` pour la troisième colonne
  - `m_CustomTags->location` pour la quatrième colonne

3. Editez le fichier DbEntityDetails.cfg et configurez une insertion similaire à la suivante :

```
insert into dbModel.entityDetails
(
    EntityType,
    EntityDetails
)
values
(
    1,  -- chassis
    {
        Customer = "eval(text, '&ExtraInfo->m_CustomTags->customer')",
        Location = "eval(text, '&ExtraInfo->m_CustomTags->location')"
    }
);
insert into dbModel.entityDetails
(
     EntityType,
     EntityDetails
)
values
(
     2,  -- port/interface
     {
         Customer = "eval(text, '&ExtraInfo->m_CustomTags->customer')",
         Location = "eval(text, '&ExtraInfo->m_CustomTags->location')"
     }
);
```

4. Redémarrez Network Manager pour propager les modifications du fichier de configuration :

```
itnm_start ncp -domain domaine
```

Tâches associées:

«Ajout de balises personnalisées à la table NCIM entityDetails», à la page 223
Vous pouvez configurer la base de données topologiques NCIM pour stocker des balises personnalisées associées aux périphériques ou aux interfaces dans la table entityDetails. Cela permet aux opérateurs de réseau de visualiser les périphériques dans la vue Tronçon et de créer des vues dans vues de réseau en fonction de ces données personnalisées.

Ajout de balises aux entités à l'aide de tables de balises personnalisées

Vous pouvez ajouter des balises de paire nom-valeur à des entités par la création d'insertions contenant les données de paires nom-valeur dans la table disco.ipCustomTags ou dans la table disco.filterCustomTags.

Ajout de balises aux entités à l'aide de la table disco.ipCustomTags :

Vous pouvez associer des balises de paires nom-valeur à des adresses IP uniques à l'aide de la table disco.ipCustomTags.

L'exemple de procédure ci-après suppose que vous ajoutez aux entités les balises de paires nom-valeur suivantes lors de votre reconnaissance :

- customer
- location

Cet exemple utilise la table disco.ipCustomTags pour configurer les balises de paires nom-valeur suivantes :

Tableau 27. Exemple de balises de paires nom-valeur

Adresse IP	Nom	Valeur
172.16.1.21	customer	acme
172.16.1.21	location	london
172.16.1.201	customer	acme
172.16.1.201	location	london
172.16.1.25	customer	acme
172.16.1.25	location	paris
172.16.2.33	customer	telecorp
172.16.2.33	location	newyork
172.16.2.34	customer	telecorp
172.16.2.34	location	newyork

1. Modifiez le fichier de configuration DiscoConfig.cfg.
2. Dans ce fichier de configuration, ajoutez une insertion similaire à la suivante :

```
insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.1.21',
            {
                customer="acme",
                location="london"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
```

```
            '172.16.1.201',
            {
                customer="acme",
                location="london"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.1.25',
            {
                customer="acme",
                location="paris"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.2.33',
            {
                customer="telecorp",
                location="newyork"
            }
);

insert into disco.ipCustomTags
(
            m_UniqueAddress,
            m_CustomTags
 )
values
(
            '172.16.2.34',
            {
                customer="telecorp",
                location="newyork"
            }
);
```

3. Sauvegardez le fichier de configuration DiscoConfig.cfg.

Vous devez maintenant configurer le fichier de configuration DbEntityDetails.cfg pour garantir que, à la suite de la reconnaissance, la table entityDetails de la base de données topologique de NCIM soit mise à jour avec les balises personnalisées.

Tâches associées:

«Ajout de balises personnalisées à la table NCIM entityDetails», à la page 223
Vous pouvez configurer la base de données topologiques NCIM pour stocker des balises personnalisées associées aux périphériques ou aux interfaces dans la table entityDetails. Cela permet aux opérateurs de réseau de visualiser les périphériques dans la vue Tronçon et de créer des vues dans vues de réseau en fonction de ces données personnalisées.

Ajout de balises aux entités à l'aide de la table disco.filterCustomTags :

Vous pouvez associer des balises de paires nom-valeur à à un ensemble filtré d'adresses IP uniques à l'aide de la table disco.filterCustomTags.

Vous pouvez filtrer des adresses IP d'après un large éventail de critères. Vous pouvez, par exemple, les filtrer d'après le nom de l'unité, l'adresse IP ou un identificateur de réseau local virtuel (VLAN). L'exemple de procédure ci-dessous applique un filtre basé sur l'adresse IP et utilise la table disco.filterCustomTags pour configurer les balises de paires nom-valeur suivantes sur toutes les adresses IP dans le sous-réseau 172.20.3.0/24:

Tableau 28. Exemple de balises de paires nom-valeur

Adresse IP	Nom	Valeur
172.20.3.0/24	customer	acme
172.20.3.0/24	location	london

1. Modifiez le fichier de configuration DiscoConfig.cfg.
2. Dans ce fichier de configuration, ajoutez l'insertion suivante :

```
insert into disco.filterCustomTags
(
            m_Filter,
            m_CustomTags
 )
values
(
            "m_UniqueAddress LIKE '172.20.3'",
            {
                customer="acme",
                location="london"
            }
);
```

3. Sauvegardez le fichier de configuration DiscoConfig.cfg.

Autres exemples de filtres

La procédure ci-dessus s'applique un filtre basé sur l'adresse IP : `"m_UniqueAddress LIKE '172.20.3'"`.

Vous pouvez créer un filtre basé sur n'importe quels attributs associés à des entités reconnues. Vous pourriez, par exemple, appliquer les filtres suivants :

- Filtre basé sur le nom de l'entité : `"m_Name LIKE 'lon'"`
- Filtre basé sur l'identificateur de réseau local virtuel d'une entité de réseau local virtuel : `"m_LocalNbr->m_VlanID = 102"`

Vous devez maintenant configurer le fichier de configuration DbEntityDetails.cfg pour garantir que, à la suite de la reconnaissance, la table entityDetails de la base de données topologique de NCIM soit mise à jour avec les balises personnalisées.

Tâches associées:

«Ajout de balises personnalisées à la table NCIM entityDetails», à la page 223
Vous pouvez configurer la base de données topologiques NCIM pour stocker des balises personnalisées associées aux périphériques ou aux interfaces dans la table entityDetails. Cela permet aux opérateurs de réseau de visualiser les périphériques dans la vue Tronçon et de créer des vues dans vues de réseau en fonction de ces données personnalisées.

Enrichissement de la topologie à l'aide du programme stitcher GetCustomTag :

Vous pouvez utiliser le programme stitcher GetCustomTag afin d'utiliser une logique pour évaluer la partie valeur d'une paire nom-valeur.

L'exemple de procédure ci-dessous utilise la logique par défaut dans le programme stitcher GetCustomTag.stch pour ajouter la balise de paire nom-valeur personnalisée suivante à toutes les adresses IP du sous-réseau 172.20.3.0/24 :

Tableau 29. Exemple de balises de paires nom-valeur

Adresse IP	Nom	Valeur
172.20.3.0/24	Customer	A-Z Inc., London

1. Modifiez le fichier de configuration DiscoConfig.cfg.
2. Dans ce fichier de configuration, ajoutez l'insertion suivante :

```
insert into disco.filterCustomTags
(
            m_Filter,
            m_StitcherTagName,
 )
values
(
            "m_UniqueAddress LIKE '172.20.3'",
            'Customer'
);
```

   Cette insertion configure le système pour exécuter l'action suivante pour chaque adresse IP dans le sous-réseau 172.20.3.0/24 : appel du programme stitcher GetCustomTag.stch et transmission de la partie nom de la balise Customer à ce programme. Le programme stitcher GetCustomTag.stch évaluera alors la valeur de la balise Customer.
3. Sauvegardez le fichier de configuration DiscoConfig.cfg.

Vous devez maintenant configurer le fichier de configuration DbEntityDetails.cfg pour garantir que, à la suite de la reconnaissance, la table entityDetails de la base de données topologique de NCIM soit mise à jour avec les balises personnalisées.

Tâches associées:

«Ajout de balises personnalisées à la table NCIM entityDetails», à la page 223
Vous pouvez configurer la base de données topologiques NCIM pour stocker des balises personnalisées associées aux périphériques ou aux interfaces dans la table entityDetails. Cela permet aux opérateurs de réseau de visualiser les périphériques dans la vue Tronçon et de créer des vues dans vues de réseau en fonction de ces données personnalisées.

Exemple : programme stitcher GetCustomTag.stch :

Cette rubrique décrit le fonctionnement du programme stitcher GetCustomTag.stch.

Programme stitcher AddCustomTags.stch

Le programme stitcher GetCustomTag.stch est appelé par le programme stitcher AddCustomTags.stch.

Le programme stitcher AddCustomTags.stch effectue des boucles entre les balises et les entités des tables disco.ipCustomTags et disco.filterCustomTags. Si, dans l'une de ces tables, la zone `m_StitcherTagName` est définie, AddCustomTags.stch appelle alors le programme stitcher GetCustomTag.stch et lui transmet le nom

d'entité pertinent et la zone m_StitcherTagName en tant que paramètres. La zone m_StitcherTagName contient la partie nom d'une balise de paire nom-valeur. Cette zone pourrait, par exemple, contenir la valeur 'Customer'. Une fois que le programme stitcher AddCustomTags.stch a construit toutes les paires nom-valeur pour les adresses IP définies dans les tables disco.ipCustomTags et disco.filterCustomTags, il transmet ces informations en aval.

Remarque : Le programme stitcher AddCustomTags.stch extrait le nom d'entité en effectuant une recherche dans la table workingEntities.finalEntity à l'aide des informations d'adresse IP fournie dans la table disco.ipCustomTags ou disco.filterCustomTags.

Programme stitcher GetCustomTag.stch

Le programme stitcher GetCustomTag.stch reçoit en entrée un seul nom d'entité et une zone m_StitcherTagName, puis utilise une logique pour évaluer la partie valeur de la paire nom-valeur. Par défaut, le programme stitcher contient le code décrit ici. Vous pouvez personnaliser ce programme afin qu'il utilise des paires nom-valeur différentes et aussi modifier la logique définissant comment la valeur est calculée.

Tableau 30. Description ligne par ligne du programme stitcher GetCustomTag.stch

Numéros de ligne	Description
15	Définit la valeur de la variable entityName (nom entité) d'après le premier argument reçu du programme stitcher AddCustomTags.stch. Cette variable héberge le nom d'entité associé à l'adresse IP pour laquelle le programme stitcher évalue la valeur d'une balise de paire nom-valeur.
16	Définit la valeur de la variable tagName (nom balise) d'après le premier argument reçu du programme stitcher AddCustomTags.stch. Il s'agit du nom de la balise dont la valeur sera évaluée.
18	Définissez la variable valeur à zéro. La variable valeur sera renvoyée par le programme stitcher et contiendra la valeur évaluée de la balise de paire nom-valeur.
20-29	Si le nom de la balise à évaluer est 'Customer', calcul de la valeur de la balise. Calcul de la valeur de la manière suivante : si le nom d'entité contient le texte lon, définition de la variable valeur d'après le nom de client "A-Z Inc. London".
31	Renvoie la valeur de la balise.

```
1]    //
2]    // Ce programme stitcher extrait la valeur pour un nom de balise personnalisée
3]    //
4]    UserDefinedStitcher
5]    {
6]     StitcherTrigger
7]     {
8]      //
9]      // Appelé à partir d'un autre programme stitcher
10]     //
11]    }
12]
13]    StitcherRules
14]    {
15]     text entityName = eval(text,'$ARG_1');
16]     text tagName = eval(text,'$ARG_2');
17]
18]     text value = NULL;
19]
20]     if(tagName == "Customer")
21]     {
22]      // insertion de la logique pour extraction de balise personnalisée
23]      // Dans cet exemple, extraction de la partie nom d'hôte du nom
24]      int count = MatchPattern(entityName, '(lon)');
25]      if (count == 1)
26]      {
27]       value = "A-Z Inc., London";
28]      }
29]     }
30]
31]     SetReturnValue(value);
32]    }
33]   }
```

Ajout de balises personnalisées à la table NCIM entityDetails

Vous pouvez configurer la base de données topologiques NCIM pour stocker des balises personnalisées associées aux périphériques ou aux interfaces dans la table entityDetails. Cela permet aux opérateurs de réseau de visualiser les périphériques dans la vue Tronçon et de créer des vues dans vues de réseau en fonction de ces données personnalisées.

Pour configurer la base de données topologiques NCIM pour stocker des balises personnalisées dans la table entityDetails, procédez comme suit :

1. Accédez au répertoire `$NCHOME/etc/precision` et modifiez le fichier `DbEntityDetails.cfg`.
2. Supprimer la mise en commentaire de l'instruction **`insert`**. Pour un exemple de l'instruction **`insert`**, voir «Exemple d'instruction insert», à la page 224.

MODEL vérifie la section ExtraInfo de chaque enregistrement d'interface pour les zones suivantes :

- m_CustomerName
- m_CustomerType

Si l'une de ces zones est trouvée, sa valeur est insérée dans la table entityDetails de la base de données topologiques NCIM et associée à un entityId égal à la valeur spécifiée dans l'enregistrement d'interface MODEL actuel. Pour plus d'informations sur la table entityDetails, reportez-vous au manuel *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données topologiques*.

Lorsqu'un enregistrement d'interface MODEL ne contient pas d'attribut m_CustomerType ou m_CustomerName dans la section ExtraInfo, ou si l'une de ces zones a une valeur NULL, aucune ligne n'est ajoutée à la table entityDetails pour cet enregistrement d'interface.

Exemple d'instruction insert

```
////////////////////////////////////////////////////////
//
// Ce fichier fournit un moyen permettant d'étendre le schéma de base de données
// NCIM par ajout des données paire clé-valeur à la table de base de données
// nommée entityDetails.
//
//
//
//L'exemple suivant suppose qu'un stitcher personnalisé a été créé
//  avec la possibilité de renseigner la section ExtraInfo des entités chassis
// avec le nom et le type de chaque client.
//
//  insert into dbModel.entityDetails
//  (
//      EntityType,
//      EntityDetails
//  )
//  valeurs
//  (
//      1,  -- chassis
//      {
//          CustomerName = "eval(text, '&ExtraInfo->m_CustomerName')",
//          CustomerType = "eval(text, '&ExtraInfo->m_CustomerType')"
//      }
//  );
```

Vous pouvez maintenant exécuter une reconnaissance complète de votre réseau avec les balises personnalisées.

Visualisation de la topologie enrichie

Après avoir créé une topologie dans laquelle une ou plusieurs paires nom-valeur sont associées à certaines entités, vous pouvez créer une vue réseau personnalisée afin d'afficher les entités comportant ces balises. Vous pouvez également utiliser la vue de réseau fractionnée pour rechercher des entités avec ces balises.

Dans cet exemple, vous créez une vue de réseau dynamique distincte qui classe les périphériques d'après le client. Cet exemple suppose que vous avez balisé des adresses IP avec une paire nom-valeur unique contenant le nom du client associé à cette adresse. Le programme stitcher GetCustomTag.stch contient un exemple de la procédure à suivre.

Pour plus d'informations sur la création de vues de réseau, reportez-vous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*.

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 `Vues dynamiques – Distinctes`.

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. Cliquez sur l'onglet **Filtre**. Dans la liste **Domaine**, sélectionnez votre domaine réseau.
4. Dans la liste **Zones**, sélectionnez la table de base de données topologiques et la zone correspondant aux catégories et aux sous-catégories que vous désirez définir.
   a. Cliquez sur **Ajouter...**.
   b. Dans la liste **Table**, sélectionnez la table de base de données `entityDetails`. La liste **Zone** est renseignée automatiquement en fonction de votre sélection.
   c. Sélectionnez la zone `nom_clé` dans la liste **Zone**.
   d. Cliquez sur **OK**.

Au fur et à mesure que vous sélectionnez des zones, la liste **Prévisualisation** est mise à jour et affiche les relations existant entre les catégories que vous avez sélectionnées.

5. Dans la liste **Noeuds d'extrémité**, indiquez si vous voulez que des noeuds d'extrémité, tels que des imprimantes ou postes de travail, soient affichés dans la vue.
6. Dans la liste **Connectivité**, sélectionnez la connectivité requise.

Option	Description
Sous-réseaux IP	Affiche l'appartenance du périphérique par le sous-réseau. Pour simplifier la vue et clarifier l'appartenance du périphérique par le sous-réseau, ce type de connectivité n'affiche pas toutes les connexions.
Couche 2	Affiche toutes les connexions de liaison de données. Aucune connexion logique ne s'affiche.
Couche 3	Affiche toutes les connexions logiques. Les routeurs s'affichent. Les commutateurs ne s'affichent pas, à moins qu'ils aient une connexion active qui implique une interface de couche 3. Les connexions entre les périphériques de couche 3 s'affichent. Les connexions entre une interface de couche 3 et une de couche 2 s'affichent entre l'interface de couche 3 et le sous-réseau auquel appartient l'interface de couche 2.
OSPF	Affiche les connexions basées sur les informations OSPF reconnues incluant le rôle du routeur, l'appartenance à la zone et la connectivité.
PIM	Affiche les connexions basées sur les informations adjacentes PIM.
IPMRoute	Affiche les connexions basées sur les informations de routage en amont et en aval IP Multicast.
Sans connexions	Ne présente aucune des connexions reconnues pour les noeuds affichés dans la vue.

7. Cliquez sur **OK**. La nouvelle vue est ajoutée à l'arborescence de navigation dans le Panneau de navigation. Si vous ajoutez la vue à un conteneur, développez le noeud du conteneur afin de visualiser la nouvelle vue dans l'arbre.

Maintenant que vous avez créé une vue de réseau dynamique distincte qui classe les périphériques par client, vous pouvez créer une règle d'interrogation qui renvoie certains ou tous les clients.

Tâches associées:

«Enrichissement de la topologie à l'aide du programme stitcher GetCustomTag», à la page 221
Vous pouvez utiliser le programme stitcher GetCustomTag afin d'utiliser une logique pour évaluer la partie valeur d'une paire nom-valeur.

Interrogation de la topologie enrichie

Maintenant que vous avez créé une vue de réseau dynamique distincte qui classe les périphériques par client, vous pouvez créer une règle d'interrogation qui renvoie certains ou tous les clients.

Dans cet exemple, l'assistant de règles d'interrogation est utilisé pour vous guider lors de la création d'une règle d'interrogation. Au cours de cette procédure, vous avez la possibilité de spécifier les vues réseau à interroger. En sélectionnant les vues réseau dynamiques distinctes que vous avez créées en fonction des balises de paires nom-valeur du client, vous pouvez interroger les unités compte tenu du nom de client associé à ces unités.

Si vous avez besoin d'une règle d'interrogation complète comportant plusieurs définitions d'interrogation et des caractéristiques de portée complètes, utilisez l'Editeur de règles d'interrogation. Pour plus d'informations sur la création de règles d'interrogation, reportez-bous à la rubrique *IBM Tivoli Network Manager IP Edition - Guide de gestion des événements*.

1. Cliquez sur **Administration** > **Réseau** > **Interrogation du réseau**.
2. Cliquez sur **Lancer l'assistant de configuration d'interrogation** .
3. Cliquez sur **Suivant**. Renseignez la page Détails de la règle d'interrogation comme suit :

   Nom Indiquez un nom pour la règle d'interrogation. Seuls des caractères alphanumériques et des traits de soulignement sont autorisés.

   Intervalle
   Spécifiez l'intervalle requis (en secondes) entre les opérations d'interrogation. Cliquez sur les flèches modifier la valeur.

   Interrogation activée
   Indiquez si l'interrogation doit être activée. Elle est activée par défaut. Pour la désactiver, décochez cette case.

   Stocker les données d'interrogation
   Cochez cette case pour stocker les données d'interrogation afin qu'elles soient ensuite récupérées pour la génération de rapports. Les données sont stockées dans la base de données ncpolldata.

   Restriction : Le stockage de données interrogées n'est pas pris en charge pour le PING distant Cisco, le PING distant Juniper et les définitions d'interrogation de seuil générique.

   Définition
   Sélectionnez une définition d'interrogation dans la liste.
4. Cliquez sur **Suivant**. Sur la page Vues de réseau, naviguez dans l'arborescence des vues de réseau vers le noeud contenant les vues de réseau dynamiques distinctes que vous avez créées. Ouvrez le noeud et sélectionnez les périphériques client que vous souhaitez interroger à l'aide de cette règle d'interrogation.
5. Cliquez sur **Suivant**. Sur la page Récapitulatif de la règle de définition, consultez les informations que vous avez indiquées et cliquez sur **Terminer**.

Annexe A. Bases de données de reconnaissance

Il existe différentes bases de données spécialisées utilisées par ncp_disco, le composant qui effectue la reconnaissance de l'existence et de la connectivité des périphériques réseau, et par ncp_model, le composant qui gère, stocke et distribue la topologie réseau reconnue.

Les composants ncp_disco et ncp_model stockent des informations de configuration, de gestion et opérationnelles dans les bases de données. Vous pouvez interroger ces bases de données en vous connectant au service DISCO ou MODEL via le fournisseur de services OQL.

Les bases de données ncp_disco peuvent être actives ou passives. Lorsque des données sont insérées dans une base de données active, une action est automatiquement déclenchée ; par exemple, une autre table est remplie avec des données, un script ou un programme stitcher est lancée.

Concepts associés:

«Filtres», à la page 6
Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

Tâches associées:

«Définition des filtres de reconnaissance», à la page 36
Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Base de données du moteur de reconnaissance

La base de données du moteur de reconnaissance (ncp_disco) vous permet de configurer les options générales du processus de reconnaissance et d'effectuer un suivi de ce dernier.

La base de données du moteur de reconnaissance, DISCO, est définie dans le fichier $NCHOME/etc/precision/DiscoSchema.cfg. Les noms qualifiés complets de ses tables sont les suivants : disco.config, disco.managedProcesses, disco.status, disco.agents et disco.NATStatus.

Table disco.config

La table config configure le fonctionnement général du processus de reconnaissance.

Tableau 31. Schéma de table de base de données disco.config

Nom de colonne	Contraintes	Type de données	Description
m_NothngFndPeriod		Float	L'intervalle de temps maximum, en secondes, entre la reconnaissance d'un périphérique et la reconnaissance du périphérique suivant dans la phase de reconnaissance du périphérique.
m_PendingPerCent		Entier	Le nombre maximum autorisé de périphériques en attente par rapport aux périphériques en cours de traitement. La violation de ce seuil entraîne l'exécution d'une reconnaissance complète (et non d'une nouvelle reconnaissance partielle).
m_CycleLimit		Entier	Le nombre de cycles de reconnaissance à effectuer avant de lancer une nouvelle reconnaissance complète (utilisée par le programme stitcher FinalPhase).
m_RestartAgents		Entier	Un indicateur déterminant si DISCO tente de redémarrer les agents de reconnaissance subissant un échec au cours de leur fonctionnement.
m_RestartFinders		Entier	Indicateur pour déterminer s'il est nécessaire de redémarrer un outil de recherche ayant subi un échec.
m_DirScanIntvl		Entier	La durée s'écoulant entre les analyses permettant de rechercher si des modifications doivent être apportées aux fichiers du programme stitcher et de l'agent. Si l'analyse détecte des modifications à effectuer, les définitions du programme stitcher et de l'agent sont chargées et les modifications adéquates sont apportées aux programmes stitcher et aux agents.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_WriteTablesToCache	Type de données Boolean défini en externe	Entier booléen	Indicateur spécifiant s'il convient d'écrire un cache des tables du moteur de reconnaissance, ncp_disco, sur le disque. **Remarque :** La définition de cet indicateur entraîne des reconnaissances plus lentes qu'une reconnaissance standard. • 1 : Ecrire le cache des tables ncp_disco sur le disque. Les tables définies dans la base de données de reprise sont placées dans la mémoire cache et ncp_disco peut être redémarré à n'importe quel moment. • 0 : Ne pas écrire le cache des tables ncp_disco sur le disque. Aucune table n'est placée dans la mémoire cache durant la reconnaissance et ncp_disco ignore les fichiers cache existants s'il est redémarré.
m_MinResidentSize		Entier	La taille minimale initiale de DISCO en kilooctets (Ko). La valeur maximale que vous pouvez indiquer est 500 Mo (512 000 Ko). La spécification d'une valeur initiale augmente la vitesse de la reconnaissance en allouant la mémoire de DISCO en un seul bloc.
`m_UseContext`		Entier booléen	Indicateur signalant si la reconnaissance est contextuelle. • 1 : Indique que la reconnaissance est contextuelle. • 0 : Indique que la reconnaissance n'est pas contextuelle.
`m_RebuildLayers`	Type de données Boolean défini en externe	Entier booléen	Indicateur signalant s'il est nécessaire de reformer les couches topologiques après une nouvelle reconnaissance partielle. • 1 : Reformer les couches. Après une nouvelle reconnaissance partielle, les programmes stitcher de couches topologiques sont exécutés. La nouvelle reconnaissance partielle prend plus de temps mais permet une topologie complète. • 0 : Ne pas reformer les couches. Après une nouvelle reconnaissance partielle, les programmes stitcher de couches topologiques ne sont pas exécutés. La reconnaissance partielle est alors plus rapide. Toutefois, les données de connectivité associées au périphérique récemment reconnu ne sont pas totalement visibles dans la topologie.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_DiscoProfiling		Entier booléen	Indicateur signalant si un profil doit être établi pour la reconnaissance. • 1 : Profiler la reconnaissance. • 0 : Ne pas profiler la reconnaissance.
m_ModelVlans	Type de données Boolean défini en externe	Entier booléen	Indicateur signalant s'il est nécessaire d'arrêter la modélisation VLAN. 1 : Ce paramètre *met en marche* la modélisation VLAN. Lorsque vous définissez ce paramètre sur 1, les programmes stitcher AddGlobalVlans, CreateTrunkConnections et AddVlanContainers *sont* appelés. 0 : Ce paramètre *arrête* la modélisation VLAN. Lorsque vous définissez ce paramètre sur 0, les programmes stitcher AddGlobalVlans, CreateTrunkConnections et AddVlanContainers ne sont *pas* appelés.
m_DisplayMode		Entier	Indique la manière dont les vues panoramiques réseau et l'étiquette d'affichage utilisée pour l'interface doivent être renseignées pour les noeuds principaux. • 0 - Utiliser le nom d'entité (valeur par défaut) • 1 - Utiliser SysName. Cette option se révèle particulièrement utile lorsqu'il n'est pas nécessaire de nommer les entités par sysName dans la base de données (voir m_UseSysName), mais qu'il est nécessaire d'afficher les entités dans les vues de l'interface avec un sysName.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_RTBasedVPNs	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur précisant le type de reconnaissance MPLS à effectuer. • 1 : Définissez cette valeur pour sélectionner la reconnaissance MPLS basée sur le protocole RT (route target). Dans ce type de reconnaissance, aucune étiquette de données n'est obligatoire. La reconnaissance est donc plus rapide. La vue principale MPLS affiche tous les périphériques activés pour le protocole MPLS. • 0 : Définissez cette valeur pour sélectionner la reconnaissance MPLS basée sur le protocole LSP (label switch path). Dans ce type de reconnaissance, les étiquettes de données sont reconnues car elles sont requises pour effectuer le suivi des chemins commutés par étiquette (LSP). La vue principale MPLS présente les routeurs PE (provider edge) et P (provider) extraits lors du traçage des LSP dans la portée des réseaux privés virtuels.
m_UseIfName	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur précisant la stratégie de désignation à utiliser lors de la création des interfaces. • 1 : ce paramètre indique que vous voulez utiliser ifName ou ifDescr pour nommer les interfaces et non leur ifIndex, leurs informations de carte ou de port. • 0 : ce paramètre indique que vous voulez utiliser la convention de désignation par défaut pour chaque interface de périphérique : `baseName[<card>[<port>]`
Fix Pack 4 m_UseIPName	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur précisant la stratégie de désignation à utiliser pour les périphériques. • 1 : Utilise l'adresse IP pour l'attribution de nom au périphérique. • 0 (par défaut) : N'utilise l'adresse IP pour l'attribution de nom au périphérique. Le nom DNS est utilisé le cas échéant.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_UseSysName	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur précisant la stratégie de désignation à utiliser lors de la désignation des périphériques. • 1 : ce paramètre indique que vous voulez nommer les périphériques en utilisant la valeur de la variable SNMP sysName comme source principale pour les informations de désignation. La variable sysName doit être définie et doit être unique dans le réseau. • 0 : ce paramètre indique que vous ne voulez pas nommer les périphériques en utilisant la valeur de la variable SNMP sysName comme source principale pour les informations de désignation.
m_CheckFileFinderReturns	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur signalant s'il est nécessaire d'utiliser l'outil de recherche Ping pour vérifier les périphériques indiqués dans le fichier à plat fourni à l'outil de recherche File. • 1 : ce paramètre commande à l'outil de recherche Ping de vérifier les périphériques indiqués dans le fichier à plat fourni à l'outil de recherche File. Ce paramètre est recommandé si vous avez des raisons de penser que certains périphériques indiqués dans le fichier à plat sont toujours connectés au réseau. • 0 : ce paramètre signale que vous ne voulez pas effectuer de vérification des périphériques indiqués dans le fichier à plat fourni à l'outil de recherche File.
m_InferCEs	Type de données Boolean défini en externe défaut = 0	Entier booléen	Indicateur précisant s'il est nécessaire de déduire l'existence de routeurs CE (customer-edge). Lorsque ce paramètre est activé, DISCO crée une entité de routeur CE pour chaque interface de routeur PE (provider-edge) se trouvant sur un sous-réseau /30 et ne disposant pas d'informations CE provenant d'une autre source. • 1 : DISCO doit déduire l'existence de routeurs CE. • 0 : DISCO ne doit pas déduire l'existence de routeurs CE.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_FeedbackCtrl	défaut = 0	Entier	Indicateur signalant s'il est nécessaire d'utiliser le mécanisme de retour d'informations lors de la reconnaissance. Ce mécanisme permet le retour d'informations concernant toute nouvelle adresse IP et ainsi, l'augmentation de la taille du réseau reconnu. Des commandes PING sont émises par l'outil de recherche Ping à l'attention des périphériques ayant fait l'objet d'un retour d'informations. **Remarque :** Pour que le retour d'informations fonctionne, l'outil de recherche ping doit être activé. • 0 : Le retour d'informations est désactivé pour toutes les reconnaissances/nouvelles reconnaissances. Cette option augmente la vitesse de reconnaissance mais ne reconnaît que les périphériques indiqués aux outils de recherche. Dès lors, la topologie générée est incomplète. Toutefois, ce paramètre permet de vérifier que les reconnaissances et les nouvelles reconnaissances s'achèvent le plus rapidement possible. • 1 : Le retour d'informations est activé pour les reconnaissances complètes et les nouvelles reconnaissances complètes ou partielles. Des commandes PING sont émises à l'attention de toutes les adresses IP. Cette option fournit une topologie complète dans toutes les situations, mais est celle qui prend le plus de temps. • 2 : Le retour d'informations est activé pour les reconnaissances et les nouvelles reconnaissances complètes, assurant ainsi la génération d'une topologie complète dans ces cas. Dans le cas de la nouvelle reconnaissance partielle, le retour d'informations est désactivé. Cela permet d'assurer que son exécution soit la plus rapide possible. Il s'agit du paramètre par défaut.
m_AllowVirtual	Valeur par défaut = 1	Entier	Indicateur signalant s'il est nécessaire d'autoriser les adresses IP virtuelles dans le cadre de la reconnaissance. • 0 : Ne pas effectuer la reconnaissance des adresses IP virtuelles. • 1 : Effectuer la reconnaissance des adresses IP virtuelles. Il s'agit du paramètre par défaut. • 2 : Effectuer la reconnaissance des adresses IP virtuelles uniquement si elles sont définies dans la table scope.special. Cette table définit les adresses IP de gestion.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_PingVerification	défaut = 2	Entier	Option permettant de vérifier si une interface parvient à recevoir des commandes PING. Si le périphérique ne peut pas recevoir de commandes PING, Network Manager ne l'interroge pas pour rechercher des alertes. • 0 : Ne pas vérifier si une commande PING peut être lancée : Network Manager ne vérifie pas si une commande PING peut être lancée sur l'une des interfaces reconnues. Les interfaces seront interrogées sans tenir compte de leur capacité à recevoir une commande PING au moment de la reconnaissance. • 1 : Vérifier si une commande PING peut être lancée : permet de vérifier si une commande PING peut être lancée sur toutes les interfaces reconnues à la suite de la reconnaissance. • 2 : Déterminer la meilleure méthode : définit l'indicateur d'interrogabilité d'une interface en fonction de l'état du mécanisme de retour d'informations (activé/désactivé) lors de la reconnaissance.
m_CreateStchrEvents	Type de données Boolean défini en externe défaut = 1	Entier booléen	Indique s'il convient de créer des événements de reconnaissance à envoyer à ObjectServer. Cette zone accepte les valeurs suivantes : • 0 : Ne pas générer d'événement de reconnaissance. • 1 : Générer des événements de reconnaissance.
m_RTVPNResolution		Entier	Indique si un contrôle précis doit être appliqué sur la résolution VPN de couche 3 et sur la désignation dans un répertoire cible de routage : • 1 : Utiliser la cible de routage (valeur par défaut). • 2 : Utiliser VRF.
m_InferPEsUsingBGP		Entier booléen	Indicateur précisant s'il est nécessaire d'induire l'existence de routeurs PE (provider-edge) à l'aide des informations BGP sur les routeurs CE (customer-edge) : • 0 : Ne pas induire l'existence des PE. • 1 : Induire l'existence des PE.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_BuildLogicalCollections		Entier booléen	Indique s'il est nécessaire de créer des entités de collection logiques afin de regrouper les éléments, tels que les domaines VTP, les zones OSPF et les VPN MPLS : • 0 : Ne pas créer d'entité de collection logique. • 1 : Créer des entités de collection logiques.
m_RediscoverRelatedDevices		Entier booléen	Dans le cadre d'un changement de périphérique lors d'une nouvelle reconnaissance partielle, indique s'il est nécessaire d'effectuer une nouvelle reconnaissance des périphériques connexes en cas de modification de la connexion : • 0 : Ne pas effectuer de nouvelle reconnaissance des périphériques connexes en cas de modification de la connexion. • 1 : Effectuer une nouvelle reconnaissance des périphériques connexes en cas de modification de la connexion.
m_DiscoOnStartup		Entier booléen	Indique si une reconnaissance démarre automatiquement lors de l'exécution du moteur de reconnaissance, ncp_disco : • 0 : Ne pas démarrer automatiquement une reconnaissance. • 1 : Démarrer automatiquement une reconnaissance.
m_FindersOnStartup		Entier booléen	Indique si les outils de recherche démarrent automatiquement lors de l'exécution du moteur de reconnaissance, ncp_disco : • 0 : Ne pas démarrer automatiquement les outils de recherche. • 1 : Démarrer automatiquement les outils de recherche.
Fix Pack 4 m_EnableCrossDomainProcessing		Entier booléen	Attribuez la valeur 1 pour activer le traitement interdomaine. Si vous procédez à une reconnaissance interdomaine, vous devez également réaliser d'autres étapes de configuration.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
m_SubnetFiltering		Entier	Modifie les interfaces à inclure dans les connexions de sous-réseau : • 0 : Aucun filtrage • 1 : Filtrage des interfaces VRF (pensez à utiliser m_VpnASTagging à la place de ce mode, compte tenu qu'il améliore la connectivité de toutes les couches, et pas seulement de la couche 3). • 2 : Filtrage des interfaces connues se trouvant dans le périmètre de la portée afin de conserver les IP inaccessibles en double. • 3 : Automatique. La meilleure approche est déterminée en fonction d'autres options de configuration.
m_VerifyCDPUsingDeviceId		Entier booléen	Indique s'il est nécessaire de vérifier les liens CDP à l'aide de l'ID de périphérique CDP. L'ID de périphérique CDP n'est pas toujours fiable à 100%. L'utilisation de m_VerifyCDPUsingDeviceId permet d'améliorer la connectivité CDP si l'ID de périphérique est exact, mais la dégrade dans le cas contraire. • 0 : Ne pas vérifier les liens CDP à l'aide de l'ID de périphérique CDP. • 1 : Vérifier les liens CDP à l'aide de l'ID de périphérique CDP.
m_UseIfIndex		Entier booléen	Indique s'il est nécessaire de nommer les interfaces à l'aide du paramètre ifIndex uniquement. Ce paramètre supplante le paramètre m_UseIfName. • 0 : Ne pas nommer les interfaces à l'aide du paramètre ifIndex uniquement. • 1 : Nommer les interfaces à l'aide du paramètre ifIndex uniquement.
m_AddIntDisplayLabel		Entier booléen	Indique s'il est nécessaire d'ajouter une étiquette d'affichage d'interface : • 0 : Ne pas ajouter d'étiquette d'affichage d'interface. • 1 : Ajouter une étiquette d'affichage d'interface.
m_Use_dNCIM		Entier booléen	Par défaut, cette zone est définie sur 0. **Important :** Ne modifiez pas cette valeur et conservez le paramètre 0.Cette zone fait partie de l'aperçu technique dNCIM. Pour en savoir plus à ce sujet, prenez contact avec le support IBM.

Tableau 31. Schéma de table de base de données disco.config (suite)

Nom de colonne	Contraintes	Type de données	Description
Fix Pack 3 m_RefreshDiscovery	défaut = 0	Entier booléen	Spécifie si le programme stitcher FullDiscovery redémarre la reconnaissance lorsqu'il est appelé après qu'une reconnaissance complète initiale a été effectuée. La valeur par défaut est 0 : ne pas redémarrer le processus de reconnaissance. Définissez la valeur à 1 pour redémarrer le processus de reconnaissance à l'aide du programme stitcher RestartDiscoProcess.stch . L'activation de cette option peut être utile si la reconnaissance charge des données personnalisées dans le fichier DiscoContrib.cfg. Le nouveau processus de reconnaissance lit à nouveau le fichier. Cela peut aussi aider si le processus de reconnaissance a accumulé des éléments dans la mémoire car le processus nouvellement démarré réinitialise le processus à son état initial. **Remarque :** Même lorsqu'il est activé, le programme stitcher FullDiscovery arrête et démarre le processus de reconnaissance seulement s'il n'y a pas de reconnaissance en cours au moment où il est appelé.
m_UnmanagedSubInts	défaut = 0	Entier booléen	Indique s'il convient de définir automatiquement des sous-interfaces comme étant non gérées lorsque l'interface spécifique propriétaire est marquée comme étant non gérée par `TagManagedEntities.stch` : • 0 : Ne pas définir automatiquement les sous-interfaces comme étant non gérées. • 1 : Définir automatiquement les sous-interfaces comme étant non gérées si l'interface propriétaire est définie comme étant non gérée par le programme stitcher. • .
m_VpnASTagging		Entier	Indique si vous devez attribuer un espace d'adresse privé aux interfaces CE/PE : • 0 : Oui. • 1 : Non. • 2 : Automatique. La meilleure approche est déterminée en fonction d'autres options de configuration.

Tâches associées:

«Définition de la portée d'une reconnaissance MPLS/VPN», à la page 152
Lors de la configuration de la reconnaissance d'un ou plusieurs VPN (réseau privé virtuel) qui s'exécutent sur un réseau principal MPLS, vous pouvez limiter la portée de cette reconnaissance à un nom de VPN ou de table VRF (Virtual Routing and Forwarding) particulier.

Référence associée:

«Fichier de configuration DiscoConfig.cfg», à la page 74
Le fichier de configuration DiscoConfig.cfg permet à l'outil de recherche Ping de vérifier automatiquement les unités découvertes par l'outil de recherche de fichiers et de permettre une reconnaissance contextuelle.

Table disco.managedProcesses

La table managedProcesses est un référentiel pour tous les sous-processus gérés par DISCO, comme les outils de recherche. A condition que CTRL soit en cours d'exécution, les processus insérés dans la table sont démarrés et gérés par DISCO.

Tableau 32. Schéma de table de base de données disco.managedProcesses

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Le nom du processus à gérer.
m_Args		Liste de textes	Une liste d'arguments de ligne de commande envoyés à l'exécutable.
m_Host		Texte	Le nom de l'hôte sur lequel exécuter l'exécutable.
m_LogFile		Texte	Le nom du fichier journal dans lequel les résultats sont inscrits.

Table disco.status

La table disco.status permet de surveiller la progression du processus **ncp_disco** durant le processus de reconnaissance.

Avertissement : La table disco.status est utilisée et mise à jour de manière interne. Vous ne devez pas faire d'insertions dans cette table.

Tableau 33. Schéma de table de base de données disco.status

Nom de colonne	Contraintes	Type de données	Description
m_DiscoveryMode		Entier	Mode de reconnaissance actuel : • 0 : Reconnaissance complète • 1 : Reconnaissance partielle

Tableau 33. Schéma de table de base de données disco.status (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Phase		Entier	La phase en cours du cycle de reconnaissance actuel. Lors de l'étape de collecte des données, les phases sont les suivantes : • 0 : la reconnaissance n'a pas encore démarré. • 1 : phase principale de reconnaissance durant laquelle les données de périphériques sont extraites. La plupart des agents de reconnaissance s'achèvent durant cette phase. • 2 - n : les phases durant lesquelles les données topologiques sont extraites pour les objets actuellement reconnus. Le nombre de phases requis dépend de la configuration de votre reconnaissance. Par défaut, dans une reconnaissance de couche 2, la phase 2 consiste en l'extraction des conversions d'adresses IP en adresses MAC et la phase 3, en l'extraction des informations topologiques sur les commutateurs Ethernet. Lors de l'étape de traitement des données, la phase ci-dessous est entreprise. • 3 : la phase durant laquelle les données collectées sont traitées. Les couches sont créées et les données envoyées à MODEL. Vous pouvez obtenir plus d'informations détaillées sur les phases de reconnaissance dans la rubrique «Etapes et phases de reconnaissance», à la page 342.
m_BlackoutState	Type de données booléennes défini de manière externe	Entier booléen	Indicateur précisant si le processus de reconnaissance est en mode inactif, c'est-à-dire si DISCO accepte ou non de nouveaux périphériques signalés par les outils de recherche au cours de ce cycle de reconnaissance : • 0 : Faux (accepte de nouveaux périphériques) • 1 : Vrai (n'accepte pas de nouveaux périphériques)

Tableau 33. Schéma de table de base de données disco.status (suite)

Nom de colonne	Contraintes	Type de données	Description
m_CycleCount		Entier	Le cycle de nouvelle reconnaissance Current, c'est-à-dire le nombre actuel de cycles effectués par DISCO sans création de topologie. En mode nouvelle reconnaissance, DISCO crée uniquement une topologie à l'issue du dernier cycle (déterminé par l'absence de périphériques en attente de traitement dans la table `finders.pending`).
m_ProcessingNeeded	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant si la topologie actuelle doit faire l'objet d'un nouveau traitement. Cet indicateur est vérifié lorsque DISCO se trouve en mode nouvelle reconnaissance afin de déterminer si des périphériques détectés récemment (et se trouvant maintenant dans la table finders.pending) nécessitent un nouveau traitement de toute la topologie : • 0 : la topologie ne doit pas être à nouveau traitée • 1 : la topologie doit être à nouveau traitée
m_FullDiscovery	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant que le programme stitcher FullDiscovery.stch a été appelée lors de la reconnaissance. Si le programme stitcher est appelé, l'indicateur est défini sur 1 pour vérifier que le programme stitcher FullDiscovery.stch est exécuté lorsque la reconnaissance en cours se termine (entraînant le démarrage d'une autre reconnaissance complète). Si l'indicateur est défini sur une autre valeur, aucune action n'est effectuée.
m_DiscoveryCycle Requested	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant qu'une reconnaissance est requise par l'interface graphique.
m_DiscoveryCycle RequestTime		Entier	Heure de la demande de reconnaissance, en temps Unix.

Table disco.agents

La table Agents indique les agents de reconnaissance utilisés par DISCO. Chaque agent à exécuter doit avoir une insertion dans la table disco.agents du fichier de configuration DiscoAgents.cfg qui l'active (définissez m_Valid=1). Si m_Valid=0, l'agent n'est pas exécuté.

Tableau 34. Schéma de table de base de données disco.agents

Nom de colonne	Contraintes	Type de données	Description
m_AgentName	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Le nom unique de l'agent de reconnaissance.
m_Valid		Entier	Un indicateur précisant si l'agent de reconnaissance doit être utilisé ou non : • (1) Exécuter l'agent de reconnaissance • (0) Ne pas exécuter l'agent de reconnaissance
m_AgentClass		Entier	La catégorie à laquelle l'agent de reconnaissance appartient : • (0) Agent de routage • (1) Agent de commutation • (2) Agent de concentration • (3) Agent ILMI • (4) Agent FDDI • (5) Agent PNNI • (6) Agent de relai de trame • (7) Agent CDP • (8) Agent NAT
m_IsIndirect		Entier	Un indicateur précisant le type d'informations de connectivité renvoyées par l'agent de reconnaissance : • (0) Connectivité directe ; par exemple, les agents de routage • (1) Informations de connectivité indirecte ; par exemple, les agents de commutation
m_Precedence		Entier	Une représentation entière du niveau de priorité des informations renvoyées par l'agent de reconnaissance ; plus le nombre entier est élevé, plus la pondération des informations renvoyées est élevée. La priorité est uniquement utilisée lorsqu'il existe un conflit entre les informations de périphériques en cours de fusion en vue de générer la table de base de données workingEntities.finalEntity.
m_HostName		Texte	Le nom de la machine hôte sur laquelle exécuter l'agent.

Tableau 34. Schéma de table de base de données disco.agents (suite)

Nom de colonne	Contraintes	Type de données	Description
m_DebugLevel		Entier	Le niveau de débogage de l'agent.
m_LogFile		Texte	Le fichier texte dans lesquels les résultats de débogage sont inscrits.
m_NumThreads		Entier	Le nombre d'unités exécutées par l'agent. Si ce paramètre n'est pas renseigné, le nombre par défaut est 10 et le maximum autorisé est 900.
m_ValidOnPartial		Entier	Indique si l'agent doit être utilisé dans une reconnaissance partielle : • 0 : L'agent ne doit *pas* être utilisé dans une reconnaissance partielle. • 1 : L'agent doit être utilisé dans une reconnaissance partielle.
m_MessageLevel		Texte	Indique le niveau de message (la valeur par défaut est l'avertissement). Les options incluent : • débogage • informations • avertissement • erreur • fatal

La table disco.agents indique également la priorité de l'agent, qui peut être utilisée lors de la fusion des informations de périphériques en vue de générer la table workingEntities.finalEntity. La priorité détermine les enregistrements utilisés lorsque des enregistrements en double ou entrant en conflit sont signalés par divers agents de reconnaissance.

Les règles de priorité suivantes s'appliquent :

- L'agent Details se situe au niveau de priorité le plus faible car il est conçu pour n'extraire que les informations de base sur les périphériques.
- Les agents de routage se situent à un niveau de priorité d'un cran plus élevé. Leurs informations de connectivité se trouvent uniquement au niveau de la couche IP, c'est pourquoi elles ne sont pas aussi précises que celles renvoyées par les agents de commutation.
- Les agents de commutation se situent à un niveau de priorité supérieur à celui des agents de routage car ils peuvent renvoyer des informations sur la couche support (couche 2), qui sont plus précises que les informations de couche 3.

Référence associée:

«Fichiers de définition des agents de reconnaissance», à la page 60
Les fichiers de définition des agents de reconnaissance définissent le fonctionnement des agents de reconnaissance.

«Fichier de configuration Agents.cfg», à la page 63
Le fichier de configuration DiscoAgents.cfg définit les agents exécutés pendant une reconnaissance.

Table disco.NATStatus

La table NATStatus permet de configurer le système de reconnaissance pour utiliser NAT.

Tableau 35. Schéma de table de base de données disco.NATStatus

Nom de colonne	Contraintes	Type de données	Description
m_NATChecks		Entier	Compteur des passerelles NAT qui ne répondent pas et qui ont été configurées pour la reconnaissance. **Important :** Ne modifiez pas la valeur de cette zone si Service de support IBM ne le demande pas.
m_NATStatus	• UNIQUE • NON NULL	Entier	Cette colonne est remplie automatiquement par le processus de reconnaissance et peut être utilisée pour effectuer un suivi du processus de reconnaissance NAT. Pour effectuer des insertions dans cette table, définissez la valeur `0`. Les valeurs possibles sont les suivantes : • `0` : Uninitialized • `1` : Seeded discovery with gateways • `2` : Awaiting gateway returns • `3` : Processing NAT translations • `4` : NAT translations complete
m_UsingNAT	• UNIQUE • NON NULL	Entier booléen	Indique si la reconnaissance utilise plusieurs espaces adresse. Si tel est le cas, définissez la valeur 1. Dans le cas contraire, définissez la valeur `0`.

Table disco.dynamicConfigFiles

La table dynamicConfigFiles stocke les noms des fichiers de configuration qui doivent être relus chaque fois qu'une reconnaissance complète est lancée.

Tableau 36. Schéma de table de base de données disco.dynamicConfigFiles

Nom de colonne	Contraintes	Type de données	Description
`m_Name`	Clé primaire Non null	`Texte`	Nom du fichier de configuration devant être relu,
`m_UpdTime`		`Horodatage`	Date et heure de dernière mise à jour de ce fichier de configuration.

Table disco.tempData

La table tempData est utilisée par les programmes stitcher de profilage de la reconnaissance afin d'enregistrer le temps et la mémoire utilisés pour effectuer la reconnaissance.

Tableau 37. Schéma de table de base de données disco.tempData

Nom de colonne	Contraintes	Type de données	Description
m_Phase1TmpTime		Entier	Temps pris par la phase 1 de la reconnaissance, également dénommée phase Interrogation des périphériques.
m_Phase2TmpTime		Entier	Temps pris par la phase 2 de la reconnaissance, également dénommée phase Résolution des adresses.
m_Phase3TmpTime		Entier	Temps pris par la phase 3 de la reconnaissance, également dénommée phase Téléchargement des connexions.
m_ProcPhaseTmpTime		Entier	Temps pris par la phase -1, à savoir la phase de traitement des données de la reconnaissance, également dénommée phase Corrélation des connexions.
m_Phase1TmpMem		Chaîne de 64 caractères	Mémoire utilisée au cours de la phase 1 de la reconnaissance.
m_Phase2TmpMem		Chaîne de 64 caractères	Mémoire utilisée au cours de la phase 2 de la reconnaissance.
m_Phase3TmpMem		Chaîne de 64 caractères	Mémoire utilisée au cours de la phase 3 de la reconnaissance.
m_ProcPhaseTmpMem		Chaîne de 64 caractères	Mémoire utilisée au cours de la phase -1 de la reconnaissance.

Table disco.profilingData

La table profilingData est utilisée par les programmes stitcher de profilage de la reconnaissance afin d'enregistrer les données concernant le temps et la mémoire utilisés pendant la reconnaissance.

Tableau 38. Schéma de table de base de données disco.profilingData

Nom de colonne	Contraintes	Type de données	Description
m_Phase1StartTime		Entier	Date et heure du déclenchement de la phase 1 de la reconnaissance. La phase 1 est également appelée phase Interrogation des périphériques.
m_Phase2StartTime		Entier	Date et heure du déclenchement de la phase 2 de la reconnaissance. La phase 2 est également appelée phase Résolution des adresses.
m_Phase3StartTime		Entier	Date et heure du déclenchement de la phase 3 de la reconnaissance. Cette phase est également dénommée Téléchargement des connexions.
m_ProcPhaseStartTime		Entier	Date et heure du déclenchement de la phase -1 de la reconnaissance, à savoir la phase de traitement des données. La phase 1 est également dénommée Corrélation des connexions.
m_CompletionTime		Entier	Date et heure d'achèvement de la phase -1.

Tableau 38. Schéma de table de base de données disco.profilingData (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Phase1StartMem		Chaîne de 64 caractères	Mémoire utilisée au déclenchement de la phase 1 de la reconnaissance.
m_Phase2StartMem		Chaîne de 64 caractères	Mémoire utilisée au déclenchement de la phase 2 de la reconnaissance.
m_Phase3StartMem		Chaîne de 64 caractères	Mémoire utilisée au déclenchement de la phase 3 de la reconnaissance.
m_ProcPhaseStartMem		Chaîne de 64 caractères	Mémoire utilisée au déclenchement de la phase -1 de la reconnaissance.
m_CompletionMem		Chaîne de 64 caractères	Mémoire utilisée à l'achèvement de la phase -1 de la reconnaissance.
m_NumFinderInserts		Entier	Nombre total d'insertions par l'outil de recherche au cours de la reconnaissance.
m_NumDetailsReturns		Entier	Nombre total de renvois depuis la table 'details' au cours de la reconnaissance.
m_NumMainNodes		Entier	Nombre total de noeuds principaux reconnus.
m_NumMainNodesWithAccess		Entier	Nombre total de noeuds principaux reconnus et sans accès SNMP.
m_NumIPs		Entier	Nombre total d'adresses IP reconnues.
m_NumSwitches		Entier	Nombre total de commutateurs reconnus.
m_NumRouters		Entier	Nombre total de périphériques de routage reconnus.
m_NumEntities		Entier	Nombre total d'entités dans la base de données scratchTopology.
m_SoftwareVersion		Texte	Version logicielle utilisée.
m_DiscoveryMode		Entier	Type de reconnaissance : • 0 : Reconnaissance complète • 1 : Reconnaissance partielle

Table disco.events

La table d'événements limite des événements de reconnaissance générés à un format standard. Un événement est généré par l'insertion d'un enregistrement dans cette table.

Tableau 39. Schéma de table de base de données disco.events

Nom de colonne	Contraintes	Type de données	Description
m_EventName	Non nul	Texte	Nom de l'événement
m_EntityName	Non nul	Texte	Nom de l'entité sur lequel l'événement se produit.
m_EventType	Non nul	Entier	Cette zone accepte l'une des valeurs suivantes : • 1 : Problème • 2 : Résolution • 13 : Informatif

Tableau 39. Schéma de table de base de données disco.events (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Severity	Non nul	Entier	Cette zone accepte l'une des valeurs suivantes : • 0: CLEAR • 1: INDETERMINATE • 2: WARNING • 3: MINOR • 4: MAJOR • 5: CRITICAL Il est possible de définir plusieurs valeurs.
m_Description	Non nul	Texte	Description de l'événement de reconnaissance
m_ExtraInfo	Type de donnée vblist défini en externe		Fournit une liste d'informations supplémentaires.

Concepts associés:

«Flux de processus pour la création d'événements de reconnaissance», à la page 208

Les événements de reconnaissance sont créés lors du processus de reconnaissance affichant la progression des agents, des programmes stitcher et des outils de recherche. Ces événements sont envoyés et stockés dans Tivoli Netcool/OMNIbus et peuvent être visualisés à l'aide de l'Interface graphique Web.

Table disco.ipCustomTags

La table ipCustomTags stocke des balises personnalisées, pouvant être associés à des entités uniques identifiées lors de la reconnaissance et utilisés pour effectuer des tâches de visualisation et d'interrogation personnalisées.

Tableau 40. Schéma de table de base de données disco.ipCustomTags

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	Non null	Texte	Adresse IP à laquelle associer les balises de paires nom-valeur dans m_CustomTags.
m_StitcherTagName	Non null	Texte	Nom d'une balise à évaluer à l'aide du programme stitcher GetTagStitcher.stch.
m_CustomTags	Non null	Type d'objet vblist	Liste de balises de paires nom-valeur.

Tâches associées:

«Ajout de balises aux entités à l'aide de tables de balises personnalisées», à la page 218

Vous pouvez ajouter des balises de paire nom-valeur à des entités par la création d'insertions contenant les données de paires nom-valeur dans la table disco.ipCustomTags ou dans la table disco.filterCustomTags.

Table disco.filterCustomTags

La table filterCustomTags stocke des balises personnalisées, pouvant être associés à un ensemble filtré d'entités identifiées lors de la reconnaissance et utilisées pour effectuer des tâches de visualisation et d'interrogation personnalisées.

Tableau 41. Schéma de table de base de données disco.filterCustomTags

Nom de colonne	Contraintes	Type de données	Description
m_Filter	Non null	Texte	Définition de filtre extrayant un ensemble d'adresses IP auxquelles associer les balises de paires nom-valeur dans m_CustomTags. Vous pouvez créer un filtre basé sur n'importe quels attributs associés à des entités reconnues. Vous pourriez, par exemple, appliquer les filtres suivants : • Filtre basé sur l'adresse IP de l'entité : "m_UniqueAddress LIKE '172.20.3'" • Filtre basé sur le nom de l'entité : "m_Name LIKE 'lon'" • Filtre basé sur l'identificateur de réseau local virtuel d'une entité de réseau local virtuel : "m_LocalNbr->m_VlanID = 102"
m_StitcherTagName	Non null	Texte	Nom d'une balise à évaluer à l'aide du programme stitcher GetTagStitcher.stch.
m_CustomTags	Non null	Type d'objet vblist	Liste de balises de paires nom-valeur.

Tâches associées:

«Ajout de balises aux entités à l'aide de tables de balises personnalisées», à la page 218

Vous pouvez ajouter des balises de paire nom-valeur à des entités par la création d'insertions contenant les données de paires nom-valeur dans la table disco.ipCustomTags ou dans la table disco.filterCustomTags.

Exemple de configuration de la table disco.config

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans la table disco.config.

- La période maximale entre la reconnaissance de périphériques est de 300 secondes. Cette condition ainsi que la suivante doivent être respectées afin de procéder à la phase suivante du cycle de reconnaissance.
- Le rapport maximal autorisé de périphériques est de 20 pour cent. Si ce seuil est dépassé, une reconnaissance complète est lancée.
- La limite des cycles est de 5, ce qui signifie qu'un maximum de cinq cycles de reconnaissance est nécessaire pour achever le processus de reconnaissance. Si le seuil de 5 cycles de reconnaissance est dépassé, une reconnaissance complète est lancée.
- L'indicateur de redémarrage de l'agent est 1, ce qui signifie que DISCO est mandaté pour redémarrer chaque agent de reconnaissance dont le fonctionnement échoue.
- L'indicateur de redémarrage de l'outil de recherche est 1, ce qui signifie que DISCO est mandaté pour redémarrer chaque outil de recherche dont le fonctionnement échoue.

- Les analyses pour rechercher des mises à jour pour les agents et les programmes stitcher ont été désactivés. C'est généralement le cas lorsque vous ne voulez pas modifier le flot de données de reconnaissance.
- N'écrivez pas de cache des tables du moteur de reconnaissance, ncp_disco, sur le disque.

```
insert into disco.config
(
            m_NothngFindPeriod,
            m_PendingPerCent,
            m_CycleLimit,
            m_RestartAgents,
            m_RestartFinders,
            m_DirScanIntvl
            m_WriteTablesToCache
)
values
(
            300,
            20,
            5,
            1,
            1,
            0,
            0
);
```

Exemple de configuration de la table disco.managedProcesses

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans la table disco.managedProcesses. Si le programme CTRL est en cours d'exécution, vous pouvez configurer, lancer et gérer les sous-processus des outils de recherche File et Ping.

```
insertion dans disco.managedProcesses
(
                        m_Name, m_Args, m_Host
)
values
(
                        "ncp_df_file", [ ], "othello"
);

insertion dans disco.managedProcesses
(
                        m_Name, m_Args, m_Host
)
values
(
                        "ncp_df_ping", [ ], "othello"
);
```

Exemple de configuration de la table disco.agents

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans la table disco.agents.

- L'agent de reconnaissance ArpCache est activé pour s'exécuter lors de la reconnaissance (m_Valid=1). Il appartient à la classe de routage (m_AgentClass=0), renvoie des informations de connectivité directes (m_IsIndirect=0) et dispose d'un niveau de priorité de 2.
- L'agent de reconnaissance AtmForumPnni est désactivé pour cette reconnaissance (m_Valid=0). Il appartient à la classe PNNI (m_AgentClass=5), renvoie des informations de connectivité directes (m_IsIndirect=0) et dispose d'un niveau de priorité de 5.
- L'agent de reconnaissance BayEthernetHub est désactivé pour cette reconnaissance (m_Valid=0). Il appartient à la classe de concentrateur (m_AgentClass=2), renvoie des informations de connectivité indirectes (m_IsIndirect=1) et dispose d'un niveau de priorité de 3.

```
insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
valeurs
(
                'ArpCache', 1, 0, 0, 2
);

insert into disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
valeurs
(
                'AtmForumPnni', 0, 5, 0, 5
);

insertion dans disco.agents
(
                m_AgentName, m_Valid, m_AgentClass, m_IsIndirect, m_Precedence
)
valeurs
(
                'BayEthernetHub', 0, 2, 1, 3
);
```

Base de donnée de portée de la reconnaissance

La base de donnée de portée limite l'étendue ou la portée de la reconnaissance. La base de donnée de portée vous permet de configurer une gamme de protocoles et d'attributs qui définissent les zones à inclure ou à exclure du processus de reconnaissance.

La plage des adresses IP et des périphériques pouvant potentiellement être pris en compte par le processus de reconnaissance est illimitée, donc, à moins de restreindre la portée de la reconnaissance, ncp_disco tenterait éventuellement de reconnaître l'Internet entier.

Vous pouvez par exemple spécifier ces périphériques sensibles qui ne doivent pas être reconnus et par conséquent instanciés. Un périphérique sensible est un

périphérique que vous ne voulez pas interroger. Cela peut être dû à un risque de sécurité impliqué par l'interrogation du périphérique, ou car l'interrogation est susceptible de surcharger le périphérique.

Référence associée:

«Fichier de configuration DiscoScope.cfg», à la page 76
Le fichier de configuration DiscoScope.cfg permet de configurer la portée d'une reconnaissance.

Schéma de base de données disco.scope

La base de données de portée est définie dans $NCHOME/etc/precision/DiscoSchema.cfg et $NCHOME/etc/precision/DiscoScope.cfg. Ses noms de table de base de données complets sont : scope.zones; scope.detectionFilter; scope.instantiateFilter; scope.special.

Table scope.detectionFilter

Si vous spécifiez un filtre dans la table detectionFilter, seuls les périphériques correspondants sont reconnus. La colonne m_Protocol devant être unique, il ne doit exister qu'une seule insertion dans cette table pour tout protocole donné. Plusieurs filtres doivent être définis dans une seule insertion.

Tableau 42. Schéma de table de base de données scope.detectionFilter

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• CLE PRIMAIRE • UNIQUE • NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par la zone actuellement définie. Actuellement, seul le protocole IP est pris en charge : • 0 : Non défini • 1 : IP
m_Filter		Texte	Une représentation textuelle d'un filtre d'attribut par rapport aux colonnes de la table Details.returns ; par exemple, m_UniqueAddress ou m_ObjectId.

Bien que vous puissiez configurer la condition de filtre pour tester une colonne quelconque dans la table Details.returns, vous devrez peut-être utiliser l'adresse IP comme base pour le filtre si vous devez restreindre la détection d'un périphérique particulier. Si le périphérique n'octroie pas d'accès SNMP à l'agent Details, ce dernier peut être incapable d'extraire les variables MIB, telles que l'ID objet. Le renvoi de l'adresse IP au minimum est toutefois garanti lorsque le périphérique est détecté.

Table inferMPLSPEs

Utilisez la table inferMPLSPE lorsque vous déduisez des périphériques PE (provider-edge) inaccessibles à l'aide de données BGP sur les périphériques CE (customer-edge). Cette table vous permet, le cas échéant, de spécifier les zones à traiter pour déterminer quels sont les périphériques PE déduits qui sont valides.

Pour spécifier les zones à traiter pour déterminer quels périphériques PE déduits sont valides, remplissez la table scope.inferMPLSPEs en utilisant des entrées de portée de format standard, comme dans la table scope.zones. Utilisez cette option lorsque vous disposez de périphériques inaccessibles qui sont connectés par BGP mais ne sont pas réellement des périphériques PE.

Si les conditions suivantes ont la valeur true, le système crée un objet réseau «tiers» pour modéliser ce réseau fournisseur inaccessible.

- Un routeur se trouve dans cette portée.
- Le routeur a des homologues BGP en dehors du réseau reconnu.
- m_InferMPLSPEsUsingBGP est activé. Il peut également être défini à l'aide de l'onglet **Avancé** dans l'interface graphique de la configuration de reconnaissance.

Tableau 43. schéma de table de base de données scope.inferMPLSPEs

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• CLE PRIMAIRE • NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par la zone actuellement définie. Actuellement, seul le protocole IP est pris en charge : • 0 : Non défini • 1 : IP
m_Action	• NON NULL • Type de données filtAction défini en externe	Entier	Action à réaliser pour la zone active : • 0 : Non défini • 1 : Inclure • 2 : Exclure
m_Zones	NON NULL	Liste de types de zone	Liste de varbinds (nom=valeur) qui définit la zone de reconnaissance actuelle.

Exécuter uniquement des interfaces du réseau 199.220.*

L'exemple suivant montre comment indiquer au système de n'exécuter que des interfaces du réseau 199.220.*.

```
insert into scope.inferMPLSPEs
(
     Protocol,
     m_Action,
     m_Zones
)
values
(
```

```
    1,
    1,
    [ { m_Subnet = "199.220.*" } ]
//);
```

Table scope.instantiateFilter

Lorsque vous spécifiez un filtre dans la table instantiateFilter, seuls les périphériques qui correspondent à ce critère sont instanciés, c'est-à-dire envoyés à MODEL. Si aucun filtre n'est spécifié, tous les périphériques reconnus sont instanciés.

Notez que la colonne m_Protocol devant être unique, il ne doit exister qu'une seule insertion dans cette table pour tout protocole donné. Plusieurs filtres doivent être définis dans une seule insertion.

Tableau 44. Schéma de table de base de données scope.instantiateFilter

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• CLE PRIMAIRE • UNIQUE • NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par la zone actuellement définie. Actuellement, seul le protocole IP est pris en charge : • 0 : Non défini • 1 : IP
m_Filter		Texte	Une représentation textuelle d'un filtre d'attribut par rapport aux colonnes de la table scratchTopology.entityByName ; par exemple, EntityOID ou Address.

Table mplsTe

La table mplsTe définit la portée de la reconnaissance de tunnel TE (Traffic Engineered) MPLS et définit les informations à extraire.

Le tableau suivant décrit le schéma de la table scope.mplsTe.

Tableau 45. Schéma de table de base de données scope.zones

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par la zone actuellement définie. Les valeurs suivantes sont possibles : • 0 : Non défini • 1 : Internet Protocol (IP) • 2 : Network Address Translation (NAT) • 3 : IPv6
m_Zones	NON NULL	Liste de types de zone	Définit la portée dans laquelle les têtes de tunnel sont découvertes
m_AddressSpace		Texte	Espace adresse facultatif

Tableau 45. Schéma de table de base de données scope.zones (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Mode		Entier	Le mode de reconnaissance de tunnel TE définit les informations à extraire. Les valeurs possibles sont les suivantes : • 0: Inconnu (non défini) • 1: Tête/queue de tunnel avec liste de tronçons de transit • 2: Tête/queue de tunnel (pas de liste de tronçons) • 3: Tête de tunnel, queues et périphériques de transit
m_TunnelFilter		Entier	Filtre de tunnel TE. Les valeurs possibles sont les suivantes : • 0: Inconnu (non défini) • 1: Inclure les tunnels avec cette tête • 2: Exclure les tunnels avec cette tête

Tâches associées:

«Configuration de l'agent StandardMPLSTE», à la page 152
Configurez les tunnels à découvrir et les détails à extraire.

Table scope.multicastGroup

La table scope.multicastGroup définit quels groupes de multidiffusion reconnaître et quels détails extraire de ces groupes.

Le tableau suivant décrit le schéma de la table scope.multicastGroup.

Tableau 46. schéma de table de base de données scope.multicastGroup

Nom de colonne	Contraintes	Type de données	Description
m_AddressSpace		Texte	Espace adresse facultatif
m_GroupName		Texte	Nom descriptif d'un groupe
m_Groups	Non nul	liste de zone de type	La zone définit les sous-réseaux de multidiffusion auxquels s'appliquent les options de portée.
m_IGMPMode		Entier	Mode de reconnaissance du groupe IGMP • 0 - Inconnu (utiliser la valeur par défaut) • 1 - Inclure un groupe • 2 - Exclure un groupe

Tableau 46. schéma de table de base de données scope.multicastGroup (suite)

Nom de colonne	Contraintes	Type de données	Description
m_IPMRouteMode		Entier	Mode de reconnaissance du groupe de route de multidiffusion IP : • 0 - Inconnu (utiliser la valeur par défaut) • 1 - Inclure un groupe • 2 - Exclure un groupe
m_PimMode		Entier	Le mode de reconnaissance multidiffusion PIM définit les informations à extraire. Les valeurs admises sont les suivantes : • 0 : Inconnu (utiliser la valeur par défaut) • 1 : Extraire des données de groupe PIM • 2 : Ne pas extraire de données de groupe PIM. Les groupes dans lesquels cette option est appliquée ne sont pas représentés dans les données service/point d'extrémité PIM.
m_Protocol	• NON NULL • Type de données netProtocol défini en externe (IPv4 [1] uniquement pour le moment)	Entier	Une représentation par un entier du protocole réseau utilisé par le groupe actuellement défini. Les valeurs suivantes sont possibles : • 0 : Non défini • 1 : IP • 2 : NAT • 3 : IPv6

Tâches associées:

«Configuration d'une reconnaissance multidiffusion», à la page 42
Configurez une reconnaissance multidiffusion en activant les agents obligatoires et en sectorisant la reconnaissance.

Table scope.multicastSource

La table scope.multicastSource définit les routes IPM à reconnaître. Cette table est particulièrement utile si vous disposez de plusieurs sources de route IPM car cela vous permet de définir la portée de la reconnaissance multidiffusion en fonction de la source de la route IPM afin qu'elle porte sur les sources pertinentes.

Le tableau suivant décrit le schéma de la table scope.multicastSource.

Tableau 47. schéma de table de base de données scope.multicastSource

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par le groupe actuellement défini. Les valeurs suivantes sont possibles : • 0 : Non défini • 1 : IP • 2: NAT • 3 : IPv6
m_Source	NON NULL	liste de zone de type	Source multidiffusion à inclure ou exclure
m_IPMRouteMode		Entier	Une représentation par un entier du protocole réseau utilisé par le groupe actuellement défini. Les valeurs suivantes sont possibles : • Mode de reconnaissance de la source de route de multidiffusion IP • 0 - Inconnu (utiliser la valeur par défaut) • 1 - Inclure la source • 2 - Exclure la source
m_Groups		liste de zone de type	Sous-réseaux du groupe de multidiffusion auxquels s'applique l'option de portée de la source

Tâches associées:

«Configuration d'une reconnaissance multidiffusion», à la page 42
Configurez une reconnaissance multidiffusion en activant les agents obligatoires et en sectorisant la reconnaissance.

Table scope.special

La table special définit la gestion des adresses IP. Une adresse de gestion est une adresse IP sur un périphérique, utilisée pour gérer le périphérique. Les adresses de gestion ne gèrent pas le trafic réseau.

Tableau 48. Schéma de table de base de données scope.special

Nom de colonne	Contraintes	Type de données	Description
m_Zones	NON NULL	Liste de zone de type	Liste de varbinds (nom=valeur) qui définit la zone de reconnaissance actuelle. Elle prend la forme d'une liste d'adresses IP de sous-réseau et de sous-réseaux.
m_AddressSpace		Texte	Identificateur d'espace adresse facultatif pour une entrée de portée particulière.

Tableau 48. Schéma de table de base de données scope.special (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Protocol		Entier	Protocole du réseau. Prend l'une des valeurs suivantes : • `0` : Indéfini • `1` : IP • `2` : NAT • `3` : IPv6
m_OutOfBand		Type d'entier booléen	Indique si la zone de gestion est hors bande. Prend l'une des valeurs suivantes : • `0` : Intrabande • `1` : Hors bande
m_IsManagement		Type d'entier booléen	Indique si l'adresse est une adresse de gestion.
m_IsValidVirtual		Type d'entier booléen	Indique si l'adresse est une une adresse IP virtuelle valide.
Fix Pack 4 m_Identifier		Texte	Identificateur facultatif pour le suivi.
Fix Pack 4 m_Priority		Ent	Priorité utilisée s'il existe plusieurs correspondances. L'entrée scope.special ayant la priorité la plus élevée est sélectionnée. Cette priorité doit avoir au minimum la valeur 1.
Fix Pack 4 m_NonPingable		Ent	Si la valeur est 1, l'adresse est sélectionnée, même si elle ne peut pas être contactée (ping.
Fix Pack 4 m_AdminInterface		Type d'entier booléen	Indique si l'adresse est une interface.
Fix Pack 4 m_ExtraInfo		Type d'objet vblist	Zones facultatives avec lesquelles l'entité cible peut être enrichie.

Table scope.zones

La table zones permet de définir des zones du réseau à inclure ou à exclure du processus de reconnaissance. Une zone est généralement définie comme une liste de varbinds. Les varbinds sont des paires `name = value`.

Vous pouvez définir plusieurs zones et combiner les zones d'inclusion et d'exclusion. Toutefois, si vous définissez une combinaison de zones d'inclusion et d'exclusion, les zones d'exclusion doivent se trouver dans la portée des zones d'inclusion.

Tableau 49. Schéma de table de base de données scope.zones

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• CLE PRIMAIRE • NON NULL • Type de données netProtocol défini en externe	Entier	Une représentation par un entier du protocole réseau utilisé par la zone actuellement définie. Actuellement, seul le protocole IP est pris en charge : • 0 : Non défini • 1 : IP
m_Action	• NON NULL • Type de données filtAction défini en externe	Entier	Action à réaliser pour la zone active : • 0 : Non défini • 1 : Inclure • 2 : Exclure
m_Zones		Liste de types de zone	Liste de varbinds (nom=valeur) qui définit la zone de reconnaissance actuelle.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Exemple de configuration de la base de données de portée

Les exemples d'insertions OQL dans les tables de la base de données de portée de cette rubrique seraient ajoutés au fichier de configuration DiscoScope.cfg pour configurer DISCO lors de son lancement.

Conseil : Dans les tables detectionFilter et instantiateFilter de la base de données de portée, la colonne m_Protocol est UNIQUE. Par conséquent, il ne doit pas y avoir plus d'une insertion par protocole dans ces tables.

Configuration de la table scope.zones

Les informations ci-dessous vous permettent de comprendre comment configurer la table scope.zones.

Création de deux zones d'inclusion

Cet exemple de configuration de la table scope.zones crée deux zones d'inclusion pour la reconnaissance en cours. Les deux zones sont définies à l'aide d'une seule insertion.

```
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
```

```
(
        1,
        1,
        [
            {
                                m_Subnet="172.16.1.0",
                                m_NetMask=24
            },
            {
                    m_Subnet="172.16.2.*"
            }
        ]
);
```

L'insertion OQL précédente spécifie les conditions suivantes :

- Le réseau utilise le protocole IP (m_Protocol=1).
- Tout périphérique qui entre dans la zone présente doit être inclus dans la reconnaissance (m_Action=1).
- La reconnaissance inclut :
  - Tout périphérique inclus dans le sous-réseau 172.16.1.0 (avec un masque de sous-réseau de 24, c'est-à-dire, 24 bits activé et 8 bits désactivé, qui implique un masque de réseau 255.255.255.0).
  - Tout périphérique dont l'adresse IP commence par 172.16.2, c'est-à-dire, dans le sous-réseau 172.16.2.0 avec un masque de 255.255.255.0.

Création d'une zone au sein d'une autre zone

Il est possible de spécifier des zones dans d'autres zones : dans une zone d'inclusion donnée, vous pouvez indiquer les périphériques ou sous-réseaux ne devant pas être détectés. Ces périphériques ne sont pas recherchés par l'outil de recherche PING ni interrogés par les agents de reconnaissance. Par exemple, vous pouvez définir une zone de portée d'inclusion constituée du sous-réseau 1.2.0.0/16 de classe B, au sein de laquelle vous pouvez définir une zone de portée d'exclusion composée du sous-réseau 172.20.32.0/19. Et enfin, au sein de la zone de portée d'exclusion, vous pouvez spécifier une zone de portée d'inclusion 172.20.33.0/24.

```
// Include all IP addresses in this range
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
              [{m_Subnet = '172.20.0.0', m_NetMask = 16 }]
);

// Apart from the IP addresses in this range
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        2,
                [{m_Subnet = '172.20.32.0' , m_NetMask = 19 }]
```

```
);
// Except for these IP addresses which we do want to include
insert into scope.zones
(
        m_Protocol,
        m_Action,
        m_Zones
)
values
(
        1,
        1,
                [{m_Subnet = '172.20.33.0' , m_NetMask = 24 }]
);
```

L'insertion SQL précédente spécifie les trois zones de portée suivantes :

- Toutes les zones indiquent que le réseau utilise le protocole IP (m_Protocol=1).
- Les zones d'inclusion et d'exclusion sont définies comme suit :
  - Tout périphérique qui appartient à la première zone, 172.20.0.0/16, doit être inclus dans la reconnaissance (m_Action=1).
  - Tout périphérique qui appartient à la deuxième zone, 172.20.32.0/19, totalement incluse dans la première zone, doit être exclu de la reconnaissance (m_Action=2).
  - Tout périphérique qui appartient à la troisième zone, 172.20.33.0/24, totalement incluse dans la deuxième zone, doit être inclus dans la reconnaissance (m_Action=1).

Interdiction de la détection de périphériques avec un filtre

Cet exemple d'insertion définit un filtre de détection. Etant donné que la table scope.detectionFilter ne doit contenir qu'une seule insertion, plusieurs conditions pour IP doivent être définies à l'aide d'une insertion. Les conditions du filtre peuvent être combinées à l'aide des mots-clés booléens OQL `AND` et `OR`.

```
insert into scope.detectionFilter
(
        m_Protocol, m_Filter
)
values
(
        1,
        "(
                ( m_UniqueAddress <> '10.10.63.234' )
                AND
                ( m_ObjectId not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

L'exemple de filtre ci-dessus garantit que seuls les périphériques suivants sont encore interrogés par la reconnaissance :

- Les périphériques qui n'ont pas l'adresse IP suivante `10.10.63.234`.
- Les périphériques qui n'ont pas l'ID objet `1.3.6.1.4.1.*`.

Dans l'exemple ci-dessus, la barre oblique inversée (`\`) est utilisée conjointement avec la comparaison `not like` pour l'échappement du caractère `.`, qui serait traité comme caractère générique dans le cas contraire.

Restriction de l'instanciation basée sur l'ID objet

Cet exemple d'insertion définit un filtre d'instanciation. Cet exemple empêche l'instanciation de périphériques correspondant à un ID objet donné.

Le filtre (m_Filter) utilise des valeurs de colonne de la table scratchTopology.entityByName.

Remarque : Pour vous assurer que des alertes ne soient pas émises pour des *interfaces* exclues par le filtre d'instanciation, vous devez définir la variable `RaiseAlertsForUnknownInterfaces`. Pour ce faire, procédez comme suit :

1. Modifiez le fichier de configuration `$NCHOME/etc/precision/NcPollerSchema.cfg`.
2. Ajoutez la ligne suivante au fichier :

   ```
   update config.properties set RaiseAlertsForUnknownInterfaces = 1;
   ```

Restriction de l'instanciation basée sur l'ID objet

La clause OQL `not like` indique que seuls les périphériques qui passent le filtre (c'est-à-dire, ceux pour lesquels l'ID objet est différent de 1.3.6.1.4.1.*) sont instanciés.

```
insert into scope.instantiateFilter
(
        m_Protocol,
        m_Filter
)
values
(
                1,          // The backslash is used here to escape the .
                "(          // which would otherwise be treated
                                    // as a wildcard.
                ( EntityOID not like '1\.3\.6\.1\.4\.1\..*' )
        )"
);
```

Bases de données d'accès

Plusieurs bases de données contrôlent l'accès aux périphériques réseau : les bases de données snmpStack et telnetStack.

Base de données snmpStack

La base de données snmpStack définit le fonctionnement de l'auxiliaire SNMP.

Description

La base de données snmpStack est définie dans le fichier `SnmpStackSchema.cfg`.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

Table de base de données snmpStack.accessParameters

La table de base de données snmpStack.accessParameters permet de configurer la façon dont l'auxiliaire SNMP gère l'extraction de vastes variables non scalaires pour des unités ou des sous-réseaux spécifiques.

Description

Les valeurs insérées dans cette table remplacent les valeurs de `m_GetNextBoundary` et `m_GetNextSlowDown` définies dans la table `snmpHelper.configuration`.

Schéma

Le tableau suivant décrit le schéma de la table de base de données snmpStack.accessParameters :

Tableau 50. Schéma de la table de base de données snmpStack.accessParameters

Nom de colonne	Contraintes	Type de données	Description
`m_NetAddress`	NON NULL	Texte	Adresse IP sur laquelle remplacer les valeurs de limite et de ralentissement.
`m_NetMask`		Texte	Masque réseau. Si aucun masque réseau n'est défini, `m_NetAddress` est considéré comme une adresse IP unique. Dans le cas contraire, `m_NetAddress` est considéré comme une adresse de sous-réseau.
`m_GetNextSlowDown`	NON NULL	Entier	Durée (en millisecondes) à respecter entre chaque requête GetNext SNMP lorsque le nombre de requêtes GetNext distinctes envoyées lors de l'extraction d'une variable SNMP non scalaire dépasse `m_GetNextBoundary`.
`m_GetNextBoundary`	NON NULL	Entier	Lors de l'extraction d'une variable SNMP non scalaire à partir d'une unité, nombre minimal de requêtes GetNext à envoyer avant que la durée définie par `m_GetNextSlowDown` ne soit insérée.
`m_GeneralSlowDown`	NON NULL	Entier	Durée totale de laquelle différer une requête (en millisecondes). Un ralentissement général ne doit être utilisé que lorsque cela est absolument nécessaire car cela peut augmenter de façon significative la durée de reconnaissance globale.
`m_useGetBulk`	NON NULL	Entier booléen	Indique si l'auxiliaire SNMP doit utiliser GetBulk lors du traitement de périphériques via SNMP v2 ou SNMP v3. Cette zone peut avoir les valeurs suivantes : • 0 : Ne pas utiliser GetBulk • 1 : Utiliser GetBulk

Table de base de données snmpStack.configuration

La table snmpStack.configuration contrôle le fonctionnement général de l'auxiliaire SNMP.

Schéma

Le tableau suivant décrit le schéma de la table de base de données snmpStack.configuration :

Tableau 51. Schéma de la table de base de données snmpStack.configuration

Nom de colonne	Contraintes	Type de données	Description
m_AutoVersion	Type de données booléen défini en externe	Entier booléen	Indicateur contrôlant la gestion automatique des versions SNMP : • 1 : Utilisation de la gestion automatique des versions SNMP. L'auxiliaire SNMP tente d'abord d'utiliser SNMP V3 pour accéder aux unités. S'il n'y parvient pas, il utilise alors SNMP V2, puis SNMP V1. • 0 : Gestion automatique des versions non utilisée. L'auxiliaire SNMP ignore les entrées de la table versions.
m_AllowOQL	Type de données booléen défini en externe	Entier booléen	Indicateur contrôlant l'accès OQL à la base de données SnmpHelper : • 1 : Accès OQL autorisé aux noms de communauté en cache pour les unités reconnues. • 2 : Accès OQL non autorisé.
m_ExpireAfter		Long	Durée, en secondes, après laquelle le nom de communauté en cache de l'unité expire s'il n'a pas été utilisé. La valeur par défaut zéro permet de conserver les noms de communauté en cache.

Table de base de données snmpStack.conversion

La table de base de données snmpStack.conversion configure l'auxiliaire SNMP pour remplacer les caractères non autorisés dans l'environnement local de la base de données NCIM par des points d'interrogation : '?'.

Description

L'auxiliaire SNMP substitue les caractères uniquement dans les objets configurés dans la table snmpStack.multibyteObjects.

Les insertions dans cette table de base de données sont configurées dans le fichier SnmpStackSchema.cfg.

Schéma

Le schéma de table de base de données snmpStack.conversion est décrit dans le tableau suivant :

Tableau 52. Schéma de table de base de données snmpStack.conversion

Nom de colonne	Contraintes	Type de données	Description
m_SubstituteInvalidUTF8	NON NULL	Entier	Si la valeur est 1, l'auxiliaire SNMP remplace les caractères qui ne sont pas autorisés dans l'environnement local de la base de données NCIM par un point d'interrogation : '?'. Si la valeur est 0, aucune action n'est effectuée concernant les caractères non valides.

Table snmpStack.multibyteObjects

La table snmpStack.multibyteObjects définit les objets MIB vérifiés afin de s'assurer qu'il s'agit de chaîne à plusieurs octets.

Description

L'envoi d'une chaîne ASCII brute au serveur auxiliaire peut provoquer des problèmes si la chaîne contient des caractères avec une signification ASCII spéciale. Si les objets MIB contiennent des chaînes à plusieurs octets, l'auxiliaire SNMP les code.

Schéma

Le schéma de table de base de données snmpStack.multibyteObjects est décrit dans le tableau suivant :

Tableau 53. Schéma de la table de base de données snmpStack.multibyteObjects

Nom de colonne	Contraintes	Type de données	Description
m_ObjectName	NON NULL	Texte	Nom d'objet MIB à vérifier.

Table de base de données snmpStack.verSecurityTable

La table snmpStack.verSecurityTable mappe une adresse IP ou de sous-réseau avec une version de SNMP (1, 2 ou 3).

Description

Les paramètres de sécurité doivent être configurés, comme indiqué pour la version de SNMP, pour pouvoir obtenir l'accès SNMP à l'unité réseau. Par exemple, l'utilisation de noms de communauté pour SNMP versions 1 et 2, ainsi que la spécification des différents niveaux de sécurité proposés par SNMP V3.

Schéma

Le tableau suivant décrit le schéma de la table de base de données snmpStack.verSecurityTable :

Tableau 54. Schéma de la table de base de données snmpStack.verSecurityTable

Nom de colonne	Contraintes	Type de données	Description
m_IpOrSubNetVer		Texte	Adresse IP ou de sous-réseau à laquelle la configuration de l'accès aux unités spécifiée par cet enregistrement est applicable. L'interprétation de cette zone en tant qu'adresse IP ou de sous-réseau dépend de la valeur de la zone m_NetMaskBitsVer.
m_NetMaskBitsVer		Entier	Masque de sous-réseau pour l'adresse indiquée dans la zone m_IpOrSubNetVer. Si cette zone est définie sur 32, m_IpOrSubNetVer est considéré comme une adresse IP unique.
m_SNMPVersion		Entier	Version de SNMP à laquelle la configuration s'applique. • 0 : SNMP V1 • 1 : SNMP V2 • 2 : SNMP V3
m_Password		Texte	Mot de passe à saisir pour l'adresse IP ou de sous-réseau, par exemple, un nom de communauté.
m_Type		Entier	Entier permettant de classer le type de mot de passe, par exemple : (2) Mot de passe Get SNMP.
m_SNMPVer3Level		Entier	Entier représentant le niveau de sécurité pour SNMP V3.
m_SNMPVer3Details		Objet de type V3SecInfo	Objet représentant les informations de mot de passe d'authentification et/ou de mot de passe privé pour SNMP V3.
m_SecurityName		Texte	Mot de passe de sécurité pour SNMP V3.
m_SnmpPort		Entier	Port SNMP sur l'unité cible ou les unités cibles si la configuration de l'accès aux unités indiquée par l'enregistrement est applicable à un sous-réseau. Si aucune valeur n'est définie pour m_SnmpPort, la valeur par défaut utilisée correspond au port SNMP standard 161.

Base de données telnetStack

La base de données telnetStack définit les paramètres d'accès Telnet pour les périphériques.

Description

La base de données telnetStack est définie dans le fichier TelnetStackSchema.cfg. Elle contient les tables suivantes :

- telnetStack.configuration
- telnetStack.passwords

Référence associée:

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

Table de base de données telnetStack.passwords

La table de base de données telnetStack.passwords définit les paramètres d'accès Telnet pour les unités.

Schéma

Le tableau suivant décrit le schéma de la table de base de données telnetStack.passwords :

Tableau 55. Schéma de la table de base de données telnetStack.passwords

Nom de colonne	Contraintes	Type de données	Description
m_IpOrSubNet		Texte	Adresse IP ou de sous-réseau dépendant de la valeur de m_NetMaskBits.
m_NetMaskBits		Entier	Masque de sous-réseau. Si la valeur définie est 32, m_IpOrSubNet est considéré comme une adresse IP unique.
m_Password	NON NULL	Texte	Mot de passe à saisir pour l'adresse IP ou de sous-réseau. Valeur par défaut = "\n" (retour chariot).
m_Username		Texte	Nom d'utilisateur à saisir pour l'adresse IP ou de sous-réseau. Valeur par défaut = "".
m_PwdPrompt		Texte	Invite de mot de passe à attendre de l'unité distante. Valeur par défaut = ".*assword:.*".
m_LogPrompt		Texte	Invite de connexion à attendre de l'unité distante. Valeur par défaut = ".*ogin:.*".
m_ConPrompt		Texte	Invite de console à attendre de l'unité distante. Valeur par défaut = "^.*[a-zA-Z0-9].*[$%>#]$".

Tableau 55. Schéma de la table de base de données telnetStack.passwords (suite)

Nom de colonne	Contraintes	Type de données	Description
m_SSHSupport		Entier booléen	Indicateur spécifiant l'utilisation ou non du support SSH pour l'unité : • 1 : Utilisation du support SSH pour l'unité. • 0 : Support SSH non utilisé pour l'unité. Si aucune valeur n'est définie pour m_SSHSupport, la valeur par défaut utilisée est 0, soit aucun support SSH.

Bases de données de gestion des processus

Au démarrage, le moteur de reconnaissance, ncp_disco, remplit les bases de données d'agent et de programme stitcher avec les informations extraites des fichiers de l'agent et du programme stitcher de reconnaissance. Pendant le fonctionnement, ncp_disco analyse les fichiers d'agent et de programme stitcher pour rechercher des modifications et met à jour les bases de données d'agent et de programme stitcher, le cas échéant. La fréquence des analyses est définie dans la base de données disco.

Les bases de données d'agent et de programme stitcher contiennent des informations de définition et de configuration pour les agents et les programmes stitcher, telles qu'une liste des types de périphériques envoyés à tout agent donné. Les informations de ces bases de données sont extraites par le moteur de reconnaissance dans les répertoires suivants :

- /precision/disco/agents
- /precision/disco/stitchers

Les bases de données de programmes stitcher contiennent également des informations sur le moment où un programme stitcher donné est déclenché ; par exemple "lancer le programme stitcher X à la fin de l'agent Y," ou "lancer le programme stitcher X à l'insertion d'une entrée dans la table de base de données Z." Il est par conséquent possible de démarrer des programmes stitcher sur demande en insérant leur nom dans la table actions appropriée à l'aide d'OQL. Les agents nécessaires sont démarrés automatiquement lorsqu'un périphérique est inséré dans la table despatch de l'agent.

Configuration du flux de données : démarrage de programmes stitcher sur demande

Les informations extraites par DISCO contiennent les définitions complètes des agents et des programmes stitcher, y compris les conditions de déclenchement. En changeant ces conditions, vous pouvez modifier le flux de données du processus de reconnaissance.

Vous pouvez lancer le cycle de reconnaissance à partir d'un point quelconque du flux de données configuré en plaçant un programme stitcher dans la table actions de la base de données des programmes stitcher.

Schéma de la base de données agents

La base de données agents est définie dans `$NCHOME/etc/precision/DiscoSchema.cfg`. Ses noms de table de base de données complets sont : agents.definitions; agents.victims; agents.status

Table agents.definitions

La table agents.definitions contient les informations de planification pour chaque agent de reconnaissance, extraites des informations du fichier de l'agent de reconnaissance.

Tableau 56. Schéma de la table de base de données agents.definitions

Nom de colonne	Contraintes	Type de données	Description
`m_Name`	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom de l'agent.
`m_Type`	Type de données agentType défini en externe	Entier	Type d'agent : • 0 : Non défini • 1 : Précompilé • 2 : Défini par texte • 3 : Combinaison
`m_Text`	NON NULL	Texte	Description textuelle des règles de l'agent.
`m_ExecuteOn`		Texte	L'hôte sur lequel l'agent doit être exécuté.
`m_Phase`	Valeur par défaut = 1	Entier	Phase de la reconnaissance à la fin de laquelle l'agent doit avoir terminé.
`m_UpdTime`		Entier long	Heure de la dernière modification, qui détermine si l'agent a été modifié depuis le stockage de sa définition.

Table agents.victims

La table agents.victims contient une extraction des critères qui déterminent les périphériques envoyés à l'agent.

Tableau 57. Schéma de la table de base de données agents.victims

Nom de colonne	Contraintes	Type de données	Description
`m_Name`	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom de l'agent.
`m_Filter`		Texte	La condition de filtre qui détermine les périphériques envoyés à l'agent.

Table agents.status

La table agents.status contient des informations sur l'état actuel de l'agent.

Tableau 58. Schéma de la table de base de données agents.status

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom de l'agent.
m_State	Type de données agentState défini en externe Valeur par défaut = 0	Entier	Etat actuel de l'agent : • 0 : Non défini • 1 : Non exécuté • 2 : Démarrage • 3 : En cours d'exécution • 4 : Terminé • 5 : Inactif
m_NumConnects	défaut = 0	Entier	Nombre de connexions de DISCO à l'agent.

Schéma de la base de données des programmes stitcher

La base de données des programmes stitcher est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Ses noms de tables de base de données complets sont : stitchers.definitions; stitchers.triggers; stitchers.status; stitchers.actions.

Table stitchers.definitions

La table stitchers.definitions contient les informations de planification pour chaque programme stitcher reconnu.

Tableau 59. Schéma de la table de base de données stitchers.definitions

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom du programme stitcher.
m_Type	Type de données stitcherType défini en externe	Entier	Type de programme stitcher : • 0 : Non défini • 1 : Précompilé • 2 : Défini par texte
m_Text		Texte	Description textuelle des règles de programme stitcher.
m_Phase	défaut = 0	Entier	Phase de la reconnaissance à la fin de laquelle le programme stitcher doit avoir terminé.
m_UpdTime		Entier long	Heure de la dernière modification du programme stitcher.

Table stitchers.triggers

La table stitchers.triggers contient une extraction des critères qui déterminent le déclencheur du programme stitcher.

Tableau 60. schéma de la table de base de données stitchers.triggers

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom du programme stitcher.
m_Type		Entier	Type de déclencheur du programme stitcher : • 0 : Non défini • 1 : A la fin d'une autre activité, par exemple, un autre programme stitcher ou une phase de la reconnaissance • 2 : Sur insertion dans la table • 3 : Sur demande • 4 : Sur un temporisateur
m_Trigger	Type de données ruleTrigger défini en externe	Objet	Description du déclencheur du programme stitcher.

Table stitchers.status

La table stitchers.status contient les informations sur l'état actuel du programme stitcher.

Tableau 61. Schéma de la table de base de données stitchers.status

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom du programme stitcher.
m_State	Type de données stchrState défini en externe Valeur par défaut = 0	Entier	Etat actuel du programme stitcher : • 0 : Non défini • 1 : Démarrage • 2 : En cours d'exécution • 3 : Terminé • 4 : Non géré (l'état du programme stitcher n'est pas géré)

Table stitchers.actions

Si un programme stitcher est inséré dans la table stitchers.actions, DISCO l'exécute. Une fois que le programme stitcher s'est terminé, son entrée est supprimée de la table stitchers.actions. Tout programme stitcher déclenché pour être exécuté à partir du programme stitcher inséré, ou à la fin du programme stitcher, est également exécuté.

Vous pouvez également configurer d'autres actions à effectuer à la fin du programme stitcher, pour que le cycle de reconnaissance se termine à partir de ce point.

Tableau 62. Schéma de la table de base de données stitchers.actions

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL	Texte	Nom du programme stitcher.

Concepts associés:

«Flot de données de reconnaissance configurable», à la page 357
Le flot de données du processus de reconnaissance est configurable par l'utilisateur. Les programmes stitcher contrôlent le déplacement des données entre les bases de données, et vous pouvez personnaliser le processus de reconnaissance en changeant la manière dont les programmes stitcher sont déclenchés et fonctionnent.

Bases de données de sous-processus

Les bases de données d'outils de recherche, Details et agent sont utilisées au cours de la reconnaissance par les sous-processus du moteur de reconnaissance pour stocker les informations extraites du réseau. Les bases de données sont définies dans le fichier de configuration DiscoSchema.cfg.

Les bases de données de sous-processus incluent :

- La base de données d'outils de recherche, utilisée par les outils de recherche pour stocker les informations sur l'existence des périphériques.
- La base de données Details, utilisée par l'agent Details pour stocker les informations de base des périphériques.
- Les bases de données d'agent de reconnaissance, créées à l'aide d'un modèle.

Les outils de recherche, agents Details et AssocAddress doivent toujours être exécutés pour que leurs bases de données soient définies dans le fichier de configuration DiscoSchema.cfg. Les bases de données des agents de reconnaissance restants sont créés en se basant sur un modèle défini dans le fichier de configuration DiscoSchema.cfg.

Schéma de base de données d'outils de recherche

La base de données d'outils de recherche est définie dans $NCHOME/etc/precision/DiscoSchema.cfg.

Les noms de table de base de données complets de la base de données d'outils de recherche sont :

- finders.despatch
- finders.returns
- finders.pending
- finders.processing
- finders.rediscovery

La base de données d'outils de recherche est le point de gestion et de surveillance central pour les outils de recherche qui fonctionnement au cours de la reconnaissance. Les outils de recherche reconnaissent l'existence de périphériques et signalent ces derniers dans la base de données des outils de recherche, mais ne reconnaissent pas les connexions.

Les entités réseau signalées par les outils de recherche sont généralement envoyées à l'agent Details pour l'extraction des informations de base sur le périphérique, bien que le flux de données de reconnaissance soit entièrement configurable.

Concepts associés:

«Cycles de reconnaissance», à la page 348
Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

Table finders.despatch

La table finders.despatch contient un enregistrement de toutes les requêtes envoyées aux outils de recherche ainsi que l'état actuel des requêtes.

Tableau 63. Schéma de la table de base de données finders.despatch

Nom de colonne	Contraintes	Type de données	Description
m_Finder	• CLE PRIMAIRE • NON NULL	Texte	Nom de l'outil de recherche responsable de la requête.
m_FindRequest	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Requête OQL envoyée à l'outil de recherche mentionné ci-dessus.
m_Request Status		Entier	Etat actuel de la requête envoyée à l'outil de recherche.

Table finders.returns

Lorsqu'un outil de recherche trouve un périphérique, il renvoie les informations à la table finders.returns, à condition que la reconnaissance se trouve toujours à la phase de reconnaissance de périphériques, c'est-à-dire la première phase de collecte de données. Si la reconnaissance est en état d'inactivité, les outils de recherche renvoient les informations à la table pending.

La table returns sert de point de transfert en notifiant au système qu'un périphérique existe. Par défaut, un programme stitcher envoie les informations sur le périphérique à l'agent Details afin de reconnaître les informations de base.

Tableau 64. Schéma de la table de base de données finders.returns

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Adresse IP de l'entité réseau reconnue.
m_Name		Texte	Nom unique de l'entité réseau.
m_Creator		Texte	Outil de recherche qui a créé cet enregistrement.
m_Protocol		Entier	Protocole du périphérique reconnu : • 1 : IP • 2 : IP-NAT

Table finders.pending

La table pending accepte les informations de périphérique lorsque la table returns a été verrouillée par DISCO. La table returns doit être verrouillée pendant le traitement des données car, bien que l'étape de collecte des données soit terminée, cela ne signifie pas nécessairement que tous les périphériques du réseau ont été reconnus.

Les entités réseau envoyées à la table pending sont traitées après la fin du cycle de reconnaissance en cours.

Tableau 65. Schéma de la table de base de données finders.pending

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Adresse IP de l'entité réseau reconnue.
m_Name		Texte	Nom unique de l'entité réseau.
m_Creator		Texte	Outil de recherche qui a créé cet enregistrement dans la table.
m_Protocol		Entier	Protocole du périphérique reconnu : • 1 : IP • 2 : IP-NAT

Tableau 65. Schéma de la table de base de données finders.pending (suite)

Nom de colonne	Contraintes	Type de données	Description
m_AddressSpace		Texte	Le nom de l'espace d'adresse NAT auquel appartient le périphérique. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table finders.processing

La table processing contient un enregistrement de toutes les entités reconnues, actuellement traitées par DISCO. Tout périphérique signalé à la table returns et en attente de la prochaine action a une entrée dans la table processing.

Tableau 66. Schéma de la table de base de données finders.processing

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • UNIQUE • NON NULL	Texte	Adresse IP de l'entité réseau reconnue.
m_Name		Texte	Nom unique de l'entité réseau.
m_Creator		Texte	Outil de recherche qui a créé cet enregistrement dans la table.
m_Protocol		Entier	Protocole du périphérique reconnu : (1) IP (2) IP-NAT
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table finders.rediscovery

La table rediscovery peut contenir les noeuds et les sous-réseaux pour lesquels vous voulez effectuer une nouvelle reconnaissance. Tout périphérique inséré dans cette table est envoyé à l'outil de recherche Ping.

Tableau 67. Schéma de la table de base de données finders.rediscovery

Nom de colonne	Contraintes	Type de données	Description
m_Address	• CLE PRIMAIRE • NON NULL	Texte	Adresse sur laquelle exécuter la commande PING.

Tableau 67. Schéma de la table de base de données finders.rediscovery (suite)

Nom de colonne	Contraintes	Type de données	Description
m_RequestType		Int	Type d'adresse IP : • 1 : Individuelle • 2 : Sous-réseau
m_NetMask		Texte	Masque de réseau si l'adresse fait référence à un sous-réseau.
m_Protocol	NON NULL	Int	Protocole de cette adresse IP : • 1 : IPv4 • 3 : IPv6

Schéma de base de données Details

La base de données Details est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Ses noms de table de base de données complets sont : Details.despatch; Details.returns.

L'agent Details extrait les informations de base sur les périphériques reconnus par les outils de recherche lorsque les informations de ces outils sont placées dans la table despatch. L'agent Details extrait les informations de périphérique appropriées et place les résultats dans la table returns.

Un programme stitcher prend les informations de la table Details.returns et les envoie à l'agent Associated Address et finalement à l'agent de reconnaissance approprié.

Table details.despatch

La table despatch contient des informations de base sur les périphériques détectés par les outils de recherche. Lorsque des données sont placées dans cette table, l'agent Details interroge automatiquement le réseau pour obtenir des informations plus détaillées sur le périphérique.

Tableau 68. Schéma de table de base de données Details.despatch

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • NON NULL	Texte	Adresse IP unique de l'entité réseau.
m_Name		Texte	Nom unique d'une entité sur le réseau.
m_Protocol		Entier	Protocole du périphérique reconnu : • 1 : IP • 2 : IP-NAT
m_AddressSpace		Texte	Le nom de l'espace d'adresse NAT auquel appartient le périphérique. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table details.returns

La table returns contient des informations de périphérique détaillées, récupérées par l'agent Details. Les informations insérées dans cette table sont traitées automatiquement par les programmes stitcher pour que la connectivité du périphérique soit reconnue par l'agent de reconnaissance approprié.

Tableau 69. Schéma de table de base de données Details.returns

Nom de colonne	Contraintes	Type de données	Description
m_Name		Texte	Nom unique d'une entité sur le réseau.
m_UniqueAddress	NON NULL	Texte	Adresse de couche 3.
m_Protocol		Entier	Protocole du périphérique reconnu : • 1 : IP • 2 : IP-NAT
m_ObjectId		Texte	Représentation textuelle de la classe d'unités (une adresse ASN.1).
m_Description		Texte	Valeur de la variable MIB sysDescr de l'entité.
m_HaveAccess	Type de données booléennes défini de manière externe	Entier	Indicateur d'accès SNMP au périphérique : • 1 : Accès • 0 : Pas d'accès
m_UpdAgent		Texte	Agent ayant mis à jour ce périphérique.
m_LastRecord	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant s'il s'agit du dernier enregistrement pour cette entité (c'est-à-dire, si l'entité a été entièrement traitée) : • 1 : True • 0 : False
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.
m_ExtraInfo	Type de donnée vblist défini en externe	Objet	Toute information supplémentaire.

Bases de données d'outils de recherche

Les outils de recherche déterminent l'existence de périphériques. Chaque outil de recherche utilise une méthode différente pour reconnaître les périphériques réseau. Vous pouvez activer les outils de recherche pour votre reconnaissance en les configurant en tant que processus gérés de DISCO dans leurs fichiers de configuration respectifs. Les outils de recherche sont automatiquement lancés au moment opportun, à condition que CTRL soit en cours d'exécution.

Chaque outil de recherche doit être configuré en éditant son fichier de configuration. Les outils de recherche reconnaissent l'existence de périphériques et signalent ces derniers dans la base de données des outils de recherche, mais ne reconnaissent pas les connexions.

Notez que la base de données des outils de recherche est distincte des bases de données associées aux outils de recherche individuels.

Les outils de recherche sont décrits dans le tableau ci-dessous avec leur nom exécutable et l'emplacement de leur fichier de configuration. $NCHOME est la variable d'environnement qui contient le chemin d'accès au répertoire netcool.

Tableau 70. Description des outils de recherche

Outil de recherche	Exécutable	Fichier de configuration	Description
Ping	ncp_df_ping	$NCHOME/etc/precision/DiscoPingFinderSchema.cfg $NCHOME/etc/precision/DiscoPingFinderSeeds.cfg	Effectue une demande d'écho ICMP simple sur des adresses de diffusion ou de multidiffusion, des adresses IP individuelles ou tous les périphériques du sous-réseau.
Fichier	ncp_df_file	$NCHOME/etc/precision/DiscoFileFinderSchema.cfg $NCHOME/etc/precision/DiscoFileFinderParseRules.cfg	Analyse un fichier, tel que /etc/hosts, pour trouver des périphériques sur le réseau.
Collector	ncp_df_collector	$NCHOME/etc/precision/DiscoCollectorFinderSchema.cfg $NCHOME/etc/precision/DiscoCollectorFinderSeeds.cfg	Un collecteur EMS est un module logiciel qui extrait et stocke des données de topologie d'un EMS (Element Management System). L'outil de recherche Collector interroge un collecteur et obtient une liste d'adresses IP gérées par l'EMS associé à ce collecteur.

Base de données collectorFinder

La base de données collectorFinder définit le fonctionnement des outils de recherche Collector.

Description

La base de données collectorFinder est définie dans le fichier de configuration `DiscoCollectorFinderSchema.cfg`. Elle contient les tables suivantes :

- collectorFinder.collectorRules
- collectorFinder.configuration

Référence associée:

«Fichier de configuration DiscoCollectorFinderSeeds.cfg», à la page 67
Le fichier de configuration `DiscoCollectorFinderSeeds.cfg` définit la façon dont les données topologiques sont acquises depuis les collecteurs Element Management System (EMS) lors de la reconnaissance.

Table de base de données collectorFinder.collectorRules

La table de base de données collectorFinder.collectorRules permet de configurer le fonctionnement de l'outil de recherche Collector.

Description

Vous pouvez modifier certains des paramètres pour des collecteurs particuliers dans la table collectorFinder.configuration. La table collectorRules peut contenir plusieurs enregistrements.

Schéma

Le tableau suivant décrit le schéma de la table de base de données collectorFinder.collectorRules :

Tableau 71. Schéma de la table de base de données collectorFinder.collectorRules

Nom de colonne	Contraintes	Type de données	Description
`m_Host`		Texte	Adresse hôte sur laquelle s'exécute le collecteur. Cette zone a la valeur NON NULL uniquement si le collecteur s'exécute sur un autre hôte de Network Manager. Cette zone peut être configurée pour une première ou une nouvelle reconnaissance.
`m_Port`	• CLE PRIMAIRE • NON NULL	Texte	Port sur lequel le collecteur est en écoute. Si le collecteur s'exécute sur le même hôte que Network Manager, il s'agit d'un port Network Manager. Cette zone peut être configurée pour une première ou une nouvelle reconnaissance.

Tableau 71. Schéma de la table de base de données collectorFinder.collectorRules (suite)

Nom de colonne	Contraintes	Type de données	Description
m_RequestType		Entier	Indicateur identifiant les données topologiques à télécharger à partir de la source de données. Cet indicateur fonctionne avec les zones m_Address et m_NetMask. Il accepte les valeurs suivantes : • 0 : Reconnaissance de toutes les unités. Toutes les unités extraites par le collecteur sont reconnues. Les zones m_Address et m_NetMask sont ignorées. • 1 : Reconnaissance d'une seule unité. Seule une des unités extraites par le collecteur est reconnue. La zone m_Address indique l'unité tandis que la zone m_NetMask est ignorée. • 2 : Reconnaissance d'un sous-réseau. Un des sous-réseaux extraits par le collecteur est reconnu. La zone m_Address indique le sous-réseau et la zone m_NetMask le masque de sous-réseau. Cette zone est configurée pour une nouvelle reconnaissance uniquement.
m_DataSourceId		Entier	Limite la reconnaissance à une seule source de données prise en charge par le collecteur. Cette zone est rarement utilisée car les collecteurs ne prennent généralement en charge qu'une seule source de données. Cette zone est configurée pour une nouvelle reconnaissance uniquement.
m_Address		Texte	Utilisée en conjonction avec les zones m_RequestType et m_NetMask lors de la spécification d'une unité ou d'un sous-réseau pour la reconnaissance. Consultez l'entrée relative à m_RequestType pour plus d'informations. Cette zone est configurée pour une nouvelle reconnaissance uniquement.
m_NetMask		Texte	Utilisée en conjonction avec les zones m_RequestType et m_Address lors de la spécification d'une unité ou d'un sous-réseau pour la reconnaissance. Consultez l'entrée relative à m_RequestType pour plus d'informations. Cette zone est configurée pour une nouvelle reconnaissance uniquement.

Tableau 71. Schéma de la table de base de données collectorFinder.collectorRules (suite)

Nom de colonne	Contraintes	Type de données	Description
m_NumRetries		Entier	Nombre de tentatives d'exécution d'une requête XML RPC sur le collecteur. Cette zone est facultative. Lorsqu'elle est définie, cette zone remplace la valeur par défaut indiquée dans la table collectorFinder.configuration. Elle peut être configurée pour une première ou une nouvelle reconnaissance.

Table de base de données collectorFinder.configuration

La table collectorFinder.configuration regroupe les règles générales de méthodologie du collecteur EMS (Element Management System). Elle ne doit contenir qu'un enregistrement.

Schéma

Le tableau suivant décrit le schéma de la table de base de données collectorFinder.configuration :

Tableau 72. Schéma de la table de base de données collectorFinder.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads		Entier	Nombre d'unités d'exécution à utiliser par l'outil de recherche Collector.
m_TimeOut		Entier	Temps d'attente maximal pour la réponse d'un collecteur (délai d'attente).
m_NumRetries		Entier	Nombre de fois où une requête XML-RPC doit être envoyée à un collecteur.
m_MaxResponseSize		Entier	Taille maximale, en octets, d'une réponse XML-RPC. **Remarque :** La taille de réponse maximale par défaut peut être trop petite lors de l'exécution d'une reconnaissance basée collecteurs si ceux-ci génèrent des réponses très volumineuses. Dans de tels cas, augmentez la taille de réponse maximale. Pour augmenter la taille de réponse maximale, attribuez au paramètre **m_MaxResponseSize** une valeur plus élevée. Prenez soin d'affecter à **m_MaxResponseSize** la même valeur dans les deux fichiers suivants : • NCHOME/etc/precision/DiscoCollectorFinderSchema.cfg • NCHOME/etc/precision/DiscoXmlRpcHelperSchema.cfg

Base de données fileFinder

La base de données fileFinder définit le fonctionnement de l'outil de recherche File.

Description

La base de données fileFinder est définie dans le fichier DiscoFileFinderParseRules.cfg. Elle contient les tables suivantes :

- fileFinder.configuration
- fileFinder.parseRules

Référence associée:

«Fichier de configuration DiscoFileFinderParseRules.cfg», à la page 69
Le fichier DiscoFileFinderParseRules.cfg file peut être utilisé pour indiquer les fichiers à analyser pour une liste d'adresses IP d'unités du réseau.

Table de base de données fileFinder.configuration

Vous pouvez configurer l'outil de recherche File à l'aide de la table fileFinder.configuration, qui définit le nombre d'unités d'exécution à utiliser par l'outil de recherche.

Schéma

Le tableau suivant décrit la table de base de données fileFinder.configuration.

Tableau 73. Schéma de la table de base de données fileFinder.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads	NON NULL	Entier	Nombre d'unités d'exécution à utiliser par l'outil de recherche File.

Table de base de données fileFinder.parseRules

En configurant des insertions dans la table fileFinder.parseRules, vous pouvez définir les fichiers à analyser pour une liste d'adresses IP d'unités sur le réseau.

Description

La table fileFinder.parseRules regroupe les règles pour l'analyse de fichiers.

Vous pouvez, par exemple, analyser le fichier `/etc/hosts` situé sur la machine exécutant DISCO. Vous pouvez également distribuer la reconnaissance en analysant le fichier `/etc/defaultrouter`.

Schéma

Le tableau suivant décrit le schéma de la table de base de données fileFinder.parseRules :

Tableau 74. Schéma de la table de base de données fileFinder.parseRules

Nom de colonne	Contraintes	Type de données	Description
m_FileName	• NON NULL • UNIQUE	Texte	Chemin d'accès complet unique et nom du fichier à analyser, par exemple, `/etc/hosts`.

Tableau 74. Schéma de la table de base de données fileFinder.parseRules (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Delimiter		Texte	Délimiteur séparant les zones de données au sein du fichier. Les expression d'appariement de formes régulières sont également acceptées en tant que délimiteurs valides. **Remarque :** \t n'est pas pris en charge en tant que valeur valide pour le caractère <tab>.
m_ColDefs		Liste d'atomes	Liste de règles indiquant les variables à extraire et les colonnes les contenant.

Base de données pingFinder

La base de données pingFinder définit le fonctionnement de l'outil de recherche Ping.

Description

La base de données pingFinder est définie dans le fichier DiscoPingFinderSeeds.cfg. Elle contient les tables suivantes :

- pingFinder.configuration
- pingFinder.pingFilter
- pingFinder.pingRules
- pingFinder.scope

Référence associée:

«Fichier de configuration DiscoPingFinderSeeds.cfg», à la page 72
Le fichier de configuration DiscoPingFinderSeeds.cfg permet de définir l'emplacement de l'outil de recherche Ping et de restreindre la détection des unités.

Table de base de données pingFinder.configuration

La table pingFinder.configuration regroupe les règles générales de méthodologie d'exécution de la commande PING. Cette table ne doit contenir qu'un seul enregistrement.

Description

La table pingFinder.configuration permet de configurer la façon dont la commande PING est exécutée sur les unités, notamment pour l'activation de la commande PING sur la diffusion ou la multidiffusion. Bien que l'exécution de la commande PING sur les adresses de diffusion/multidiffusion permet la reconnaissance rapide des unités par rapport aux autres méthodes de détection, cette méthode est parfois moins conseillée pour certaines conditions réseau, par exemple, lorsque le réseau est fortement chargé. En général, on exécute une commande PING sur des adresses de diffusion sur des réseaux inconnus faiblement chargés. Vous ne devez exécuter une commande PING sur des adresses de multidiffusion que si elles ont été configurées sur le réseau.

Schéma

Le tableau suivant décrit le schéma de la table de base de données pingFinder.configuration :

Tableau 75. Schéma de la table de base de données pingFinder.configuration

Nom de colonne	Type de données	Description
m_NumThreads	Entier	Nombre d'unités d'exécution à utiliser par l'outil de recherche PING.
m_TimeOut	Entier	Temps d'attente maximal pour la réponse d'une adresse après l'exécution d'une commande PING (délai d'attente).
m_InterPingTime	Entier	Intervalle entre les commandes PING sur les adresses d'un réseau.
m_NumRetries	Entier	Nombre de fois qu'une commande PING doit être exécutée sur un périphérique.
m_Broadcast	Entier	Indicateur permettant d'activer ou de désactiver l'exécution de la commande PING sur les adresses de diffusion : • 1 : Activation • 0 : Désactivation
m_Multicast	Entier	Indicateur permettant d'activer ou de désactiver l'exécution de la commande PING sur les adresses de multidiffusion : • 1 : Activation • 0 : Désactivation

Table de base de données pingFinder.pingFilter

La table pingFinder.pingFilter permet d'empêcher l'exécution de la commande PING par l'outil de recherche PING sur des unités ou des sous-réseaux spécifiques.

Description

Vous pouvez exclure certaines interfaces, telles que les interfaces ISDN et de modem, car l'exécution de la commande PING sur ces interfaces génère des appels téléphoniques onéreux. Si vous configurez l'outil de recherche PING pour utiliser les tables scope.zones et pingFinder.pingFilter, celui-ci exécute la commande PING sur les unités ou les sous-réseaux avec lesquels il a été distribué s'ils se trouvent dans la portée de la reconnaissance ou de l'outil de recherche PING.

Schéma

Le tableau suivant décrit le schéma de la table de base de données pingFinder.pingFilter :

Tableau 76. Schéma de la table de base de données pingFinder.pingFilter

Nom de colonne	Contraintes	Type de données	Description
m_Protocol	• CLE PRIMAIRE • NON NULL • Type de données netProtocol défini en externe	Entier	Entier représentant le protocole de réseau utilisé par la zone de l'outil de recherche PING définie. Actuellement, seul le protocole IP est pris en charge : • 0 : Non défini • 1 : IP
m_Action	• NON NULL • Type de données netProtocol défini en externe	Entier	Action à effectuer pour la zone actuelle : • 0 : Non défini • 1 : Inclusion • 2 : Exclusion
m_Zones		Liste de zones de type	Liste des liaisons de variables (nom=valeur) définissant la zone active.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table de base de données pingFinder.pingRules

La table pingFinder.pingRules regroupe les différentes adresses et sous-réseaux sur lesquels l'outil de recherche PING doit exécuter la commande PING.

Description

La table pingRules peut contenir plusieurs enregistrements.

Schéma

Le tableau suivant décrit la table pingFinder.pingRules.

Tableau 77. Schéma de la table de base de données pingFinder.pingRules

Nom de colonne	Contraintes	Type de données	Description
m_Address	• CLE PRIMAIRE • NON NULL	Texte	Adresse sur laquelle exécuter la commande PING.
m_RequestType		Entier	Indicateur identifiant le type d'adresse : • 1 : Individuelle • 2 : Sous-réseau

Tableau 77. Schéma de la table de base de données pingFinder.pingRules (suite)

Nom de colonne	Contraintes	Type de données	Description
m_NetMask		Texte	Masque de sous-réseau. Si une valeur est définie pour cette zone, cela implique automatiquement que l'adresse correspond à un sous-réseau.
m_TimeOut		Entier	Temps d'attente maximal pour une réponse. Cette valeur remplace le délai d'attente par défaut défini dans la table de configuration.
m_NumRetries		Entier	Nombre maximal de tentatives d'exécution de la commande PING. Cette valeur remplace la valeur par défaut.

Table de base de données pingFinder.scope

La table pingFinder.scope définit la portée de l'outil de recherche PING.

Description

Vous pouvez utiliser la table pingFinder.scope pour configurer la façon dont l'outil de recherche PING contrôle si l'exécution de la commande PING est autorisée pour une unité. Vous pouvez empêcher l'exécution de la commande PING par l'outil de recherche PING sur des unités ou des sous-réseaux spécifiques.

Schéma

Le tableau suivant décrit le schéma de la table de base de données pingFinder.scope :

Tableau 78. Schéma de la table de base de données pingFinder.scope

Nom de colonne	Contraintes	Type de données	Description
m_UseScope		Entier	Indicateur spécifiant l'utilisation ou non des entrées de la table scope.zones lors de la sélection des unités sur lesquelles exécuter la commande PING : • 0 : L'outil de recherche PING ignore la table scope.zones lors de la sélection des unités. • 1 : Il s'agit de la valeur par défaut. L'outil de recherche PING utilise la table scope.zones pour identifier les unités pour lesquelles il est possible d'exécuter la commande PING. Si vous effectuez une reconnaissance non sectorisée (une reconnaissance sans entrée dans la table scope.zones), il est préférable de définir m_UseScope sur zéro afin de réduire la charge de traitement.

Tableau 78. Schéma de la table de base de données pingFinder.scope (suite)

Nom de colonne	Contraintes	Type de données	Description
m_UsePingEntries		Entier	Indicateur spécifiant l'utilisation ou non des entrées de la table pingFinder.pingFilter lors de la sélection des unités sur lesquelles exécuter la commande PING : • 0 : Il s'agit de la valeur par défaut. L'outil de recherche PING ignore les entrées de la table pingFinder.pingFilter lors de la sélection des unités. • 1 : L'outil de recherche PING contrôle la table pingFinder.pingFilter avant d'exécuter la commande PING sur une unité afin de voir si cette action est possible.

Bases de données du serveur auxiliaire

Lorsque le serveur auxiliaire démarre, il crée une base de données pour chaque auxiliaire qui doit être exécuté.

Conseil : La bonne pratique est de configurer le serveur auxiliaire pour qu'il démarre automatiquement, via l'insertion OQL appropriée dans la table services.inTray de CTRL. Vous pouvez également démarrer le serveur manuellement à l'aide de la commande ncp_d_helpserv dans la ligne de commande.

Référence associée:

«Fichier de configuration DiscoHelperServerSchema.cfg», à la page 71
Le fichier de configuration DiscoHelperServerSchema.cfg définit le contenu des diverses bases de données auxiliaires.

La base de données ARPhelper

La base de données ARPHelper stocke des informations sur les requêtes émises par l'auxiliaire ARP à partir du réseau. Elle est définie dans le fichier $NCHOME/etc/precision/ DiscoHelperServerSchema.cfg et les noms qualifiés complets de ses tables sont les suivants : ARPHelper.ARPHelperTable et ARPHelper.ARPHelperConfig.

La table de base de données ARPHelperTable, décrite dans le tableau 79, configure le fonctionnement général de l'auxiliaire ARP.

Tableau 79. Schéma de table de base de données ARPHelper.ARPHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Une interface clé unique pour les bases de données du serveur auxiliaire en cas de requêtes Reply.

Tableau 79. Schéma de table de base de données ARPHelper.ARPHelperTable (suite)

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestGetKey	NON NULL	Texte	Une interface clé unique pour les bases de données du serveur auxiliaire en cas de requêtes Get.
RivHelperDbTimeToDie		Long64	Indique la durée de vie de l'information requise dans le serveur auxiliaire.
m_HostIp	NON NULL	Texte	Adresse IP du périphérique à interroger.
m_HostSubnet		Texte	Sous-réseau du périphérique hôte à interroger.
m_HostMask		Texte	Le masque de sous-réseau du périphérique hôte à interroger.
m_HostMac		Texte	L'adresse physique du périphérique (adresse MAC).

La table ARPHelperConfig, décrite dans le tableau 80, contient des informations de configuration pour l'auxiliaire ARP.

Tableau 80. Schéma de table de base de données ARPHelper.ARPHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Le délai d'attente de la base de données auxiliaire, c'est-à-dire le temps s'écoulant avant l'expiration de la base de données en l'absence de toute activité.
m_HelperReqTimeout		Long64	Le délai d'attente des requêtes auxiliaires, c'est-à-dire le temps s'écoulant avant l'expiration de chaque requête.
m_HelperStartupTimeout		Long64	Le délai d'attente de démarrage par défaut de l'auxiliaire, c'est-à-dire la durée maximale à attendre pour qu'un auxiliaire démarre lorsqu'on lui en fait la requête.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou le réseau à l'aide d'un auxiliaire : (0) Ne pas utiliser le cache (1) Utilise le cache

Tableau 80. Schéma de table de base de données ARPHelper.ARPHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
`m_HelperDoQueryVBs` Facultatif		Liaisons de variables de type d'objet	Liste des entrées de l'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est détecté dans la base de données, le réseau n'est pas interrogé.
`m_HelperDoNotQueryVBs` Facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaires qui n'interrogent pas la base de données. Cette zone remplace la valeur indiquée dans `m_HelperDoWeQuery`.
`m_HelperDoWeStore`		Entier	Indique si le serveur auxiliaire stocke des réponses des auxiliaires dans sa base de données : (0) Ne stocke pas de réponses dans la base de données (1) Stocke des réponses dans la base de données
`m_HelperDoStoreVBs` Facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaires qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace la valeur de `m_HelperDoWeStore`.
`m_HelperDoNotStoreVBs` Facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaires qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace la valeur de `m_HelperDoWeStore`.
`m_HelperDebugLevel` Facultatif		Entier	Définit le niveau de débogage de l'auxiliaire et l'imprime dans `m_HelperLogfile`.
`m_HelperLogfile` Facultatif		Texte	Le chemin d'accès complet et le fichier de journal de l'auxiliaire en cours.

Les zones m_HelperDoWeQuery et m_HelperDoWeStore disposent chacune de deux zones facultatives. Un enregistrement entré dans la zone m_HelperDoWeQuery ou m_HelperDoWeStore constitue le paramètre par défaut auquel l'auxiliaire répond si aucun enregistrement n'est entré dans les zones facultatives. Toutefois, un enregistrement entré dans l'une des zones facultatives connexes remplace le paramètre par défaut.

Par exemple, si la zone m_HelperDoWeQuery est définie pour interroger le réseau et non le cache (c'est-à-dire m_HelperDoWeQuery=0) et si une adresse IP de 192.168.0.1 est indiquée dans la zone m_HelperDoQueryVBs, un enregistrement de requête dans lequel `m_IpAddress = 192.168.0.1` entraîne l'interrogation du cache à

la place de celle du réseau. Le réseau est uniquement interrogé si les informations ne sont pas actuellement stockées dans le cache.

Configuration de la base de données ARPhelper

L'exemple d'insertion ci-après présente une configuration typique de l'auxiliaire ARP.

```
insertion dans ARPHelper.ARPHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
values
(
                259200, 1200, 90, 0, 0
);
```

Schéma de la base de données de l'auxiliaire DNS

La base de données DNSHelper est définie dans $NCHOME/etc/precision/DiscoHelperServerSchema.cfg. Ses noms de table de base de données complets sont : DNSHelper.DNSHelperTable; DNSHelper.DNSHelperConfig

La table de base de données DNSHelper stocke des informations sur les requêtes effectuées par l'auxiliaire ARP à partir du réseau.

Tableau 81. Schéma de table de base de données DNSHelper.DNSHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Clé unique pour les requêtes Reply.
RivHelperRequestGetKey	NON NULL	Texte	Clé pour les requêtes Get.
RivHelperDbTimeToDie		Long64	Durée de vie de l'information demandée dans le serveur auxiliaire.
m_HostName		Texte	Nom d'hôte pour cette adresse IP.
m_HostIp		Texte	Adresses IP pour cet hôte.
RivHelperRequestOutput		Atom	Données de réponse.

La table DNSHelperConfig contient les informations de configuration de l'auxiliaire DNS.

Tableau 82. Schéma de la table de base de données DNSHelper.DNSHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Délai d'attente de la base de données auxiliaire, c'est-à-dire, le délai d'expiration de la base de données.
m_HelperReqTimeout		Long64	Le délai d'attente de la requête de l'auxiliaire, c'est-à-dire, le délai d'expiration de chaque requête.
m_HelperStartupTimeout		Long64	Délai d'attente par défaut du démarrage de l'auxiliaire, c'est-à-dire, la durée d'attente maximale du démarrage d'un auxiliaire sur demande.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou s'il interroge le réseau à l'aide d'un auxiliaire : • 0 : Ne pas utiliser le cache • 1 : Utiliser le cache
m_HelperDoNotQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui n'interrogent pas la base de données. Cette zone remplace la valeur de m_HelperDoWeQuery.
m_HelperDoQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est trouvé dans la base de données, le réseau n'est pas interrogé.
m_HelperDoWeStore		Entier	Indique si le serveur auxiliaire stocke les réponses des auxiliaires dans sa base de données : • 0 : Ne pas stocker les réponses dans la base de données • 1 : Stocker les réponses dans la base de données

Tableau 82. Schéma de la table de base de données DNSHelper.DNSHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
m_HelperDoStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDoNotStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDebugLevel facultatif		Entier	Définit le niveau de débogage de l'auxiliaire, impression dans le fichier m_Logfile.
m_HelperLogfile facultatif		Texte	Chemin complet et fichier journal de l'auxiliaire actuel.

Configuration de la base de données de l'auxiliaire DNS

L'exemple d'insertion suivant montre une configuration type de l'auxiliaire DNS.

```
insert into DNSHelper.DNSHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
values
(
                259200, 1200, 90, 0, 0
);
```

Schéma de la base de données de l'auxiliaire Ping

La base de données de l'auxiliaire Ping est définie dans `$NCHOME/etc/precision/DiscoHelperServerSchema.cfg`. Ses noms de table de base de données complets sont : PingHelper.PingHelperTable; PingHelper.PingHelperConfig; pingHelper.configuration

Le schéma de la table de base de données PingHelper.PingHelperTable est décrit dans tableau 83, à la page 293.

Tableau 83. Schéma de la table de base de données PingHelper.PingHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Interface clé vers les bases de données du serveur auxiliaire pour les requêtes Reply.
RivHelperRequestGetKey	NON NULL	Texte	Une interface clé unique pour les bases de données du serveur auxiliaire en cas de requêtes Get.
RivHelperDbTimeToDie		Long64	Durée de vie de l'information demandée dans le serveur auxiliaire.
m_HostIp		Atom	Adresse IP sur laquelle lancer les commandes PING.
m_HostSubnet		Texte	Sous-réseau de l'adresse IP sur laquelle envoyer des commandes PING.
m_HostMask		Texte	Masque de sous-réseau de l'adresse sur laquelle envoyer des commandes PING.
m_PingRequestType		Entier	Type de requête PING : • 1 : Adresse individuelle • 2 : Sous-réseau
m_PingResponseType		Entier	Type de réponse à la commande PING.
m_PingRetries		Entier	Nombre de nouvelles tentatives pour la commande PING.
m_PingTimeout		Entier	Durée d'attente maximale de la réponse.
RivHelperRequestOutput		Atom	Données de réponse.

Le schéma de la table de base de données PingHelper.PingHelperConfig est décrit dans tableau 84, à la page 294.

Tableau 84. Schéma de la table de base de données PingHelper.PingHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Délai d'attente de la base de données auxiliaire, c'est-à-dire, le délai d'expiration de la base de données.
m_HelperReqTimeout		Long64	Le délai d'attente de la requête de l'auxiliaire, c'est-à-dire, le délai d'expiration de chaque requête.
m_HelperStartupTimeout		Long64	Délai d'attente par défaut du démarrage de l'auxiliaire, c'est-à-dire, la durée d'attente maximale du démarrage d'un auxiliaire sur demande.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou le réseau à l'aide d'un auxiliaire : • 0 : Ne pas utiliser le cache • 1 : Utiliser le cache
m_HelperDoNotQueryVBs facultatif		Type d'objet varbinds	Liste des entrées d'auxiliaires qui n'interrogent pas la base de données. Cette zone remplace m_HelperDoWeQuery.
m_HelperDoQueryVBs facultatif		Type d'objet varbinds	Liste des entrées de l'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est détecté dans la base de données, le réseau n'est pas interrogé.
m_HelperDoWeStore		Entier	Indique si le serveur auxiliaire stocke des réponses des auxiliaires dans sa base de données : • 0 : Ne pas stocker les réponses dans la base de données • 1 : Stocker les réponses dans la base de données

Tableau 84. Schéma de la table de base de données PingHelper.PingHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
`m_HelperDoStoreVBs` facultatif		Type d'objet varbinds	Liste des entrées d'auxiliaires qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
`m_HelperDoNotStoreVBs` facultatif		Type d'objet varbinds	Liste des entrées d'auxiliaires qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
`m_HelperDebugLevel` facultatif		Entier	Définit le niveau de débogage de l'auxiliaire, impression dans le fichier spécifié dans m_HelperLogfile.
`m_HelperLogFile` facultatif		Texte	Le chemin d'accès complet et le fichier de journal de l'auxiliaire en cours.

Le schéma de la table de base de données pingHelper.configuration est décrit dans le tableau 85. Elle ne doit contenir qu'un seul enregistrement.

Bien que le lancement de commandes PING sur des adresses de diffusion et de multidiffusion permette une reconnaissance plus rapide des périphériques que les autres méthodes, il n'est pas conseillé de procéder ainsi dans certaines conditions réseau, par exemple lorsque le réseau est très encombré.

Tableau 85. Schéma de la table de base de données pingHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads		Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.
m_TimeOut		Entier	Durée d'attente maximale d'une réponse à partir d'une adresse sur laquelle a été envoyée une commande PING, en millisecondes. Si vous exécutez l'agent TraceRoute, vous devrez peut-être augmenter cette valeur en fonction des conditions réseau.

Tableau 85. Schéma de la table de base de données pingHelper.configuration (suite)

Nom de colonne	Contraintes	Type de données	Description
m_NumRetries		Entier	Nombre de nouveaux lancements de commandes PING sur un périphérique.
m_InterPingTime		Entier	L'intervalle en millisecondes entre des tentatives de lancement de commandes PING successives des adresses de sous-réseau.
m_Broadcast		Entier	Indicateur utilisé pour activer ou désactiver l'exécution de la commande PING sur les adresses de diffusion : • (1) Activer • (0) Désactiver
m_Multicast		Entier	Indicateur utilisé pour activer ou désactiver l'exécution de la commande PING sur les adresses de multidiffusion : • (1) Activer • (0) Désactiver

Configuration de la base de données de l'auxiliaire PING

L'insertion suivante fournit un exemple de configuration type de la base de données PingHelper.

```
insert into PingHelper.PingHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
values
(
                259200, 1200, 90, 0, 0
);
```

Schéma de base de données d'auxiliaire SNMP

La base de données SnmpHelper est définie dans $NCHOME/etc/ precision/ DiscoHelperServerSchema.cfg. Ses noms de table de base de données complets sont : SnmpHelper.SnmpHelperTable; SnmpHelper.SnmpHelperConfig.

Le schéma de la table de base de données SNMPHelperTable est décrit dans le tableau 86, à la page 297.

Tableau 86. Schéma de la table de base de données SnmpHelper.SnmpHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Interface clé vers les bases de données du serveur auxiliaire pour les requêtes Reply.
RivHelperRequestGetKey	NON NULL	Texte	Interface clé vers les bases de données du serveur auxiliaire pour les requêtes Get.
RivHelperDbTimeToDie		Long64	Durée de vie de l'information demandée dans le serveur auxiliaire.
m_HostIp	NON NULL	Texte	Adresse IP du périphérique à interroger.
m_CommunitySuffix		Texte	Suffixe du nom de communauté.
m_OID	NON NULL	Atom	ID objet pour la requête Get.
m_SnmpIndex		Atom	Index de la requête Get (s'il s'agit d'une requête Get).
m_RequestType		Entier	Type de requête : • 0 : Get • 1 : GetNext • 2 : GetBulk
RivHelperRequestOutput		Atom	Données de réponse.

Le schéma de la table de base de données SNMPHelperConfig est décrit dans le tableau 87.

Tableau 87. Schéma de la table de base de données SnmpHelper.SnmpHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Délai d'attente de la base de données auxiliaire, c'est-à-dire, le délai d'expiration de la base de données.
m_HelperReqTimeout		Long64	Le délai d'attente de la requête de l'auxiliaire, c'est-à-dire, le délai d'expiration de chaque requête.

Tableau 87. Schéma de la table de base de données SnmpHelper.SnmpHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
m_HelperStartupTimeout		Long64	Délai d'attente par défaut du démarrage de l'auxiliaire, c'est-à-dire, la durée d'attente maximale du démarrage d'un auxiliaire sur demande.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou s'il interroge le réseau à l'aide d'un auxiliaire : • 0 : Ne pas utiliser le cache • 1 : Utiliser le cache
m_HelperDoNotQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui n'interrogent pas la base de données. Cette zone remplace m_HelperDoWeQuery.
m_HelperDoQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est trouvé dans la base de données, le réseau n'est pas interrogé.
m_HelperDoWeStore		Entier	Indique si le serveur auxiliaire stocke les réponses des auxiliaires dans sa base de données : • 0 : Ne pas stocker les réponses dans la base de données • 1 : Stocker les réponses dans la base de données
m_HelperDoStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.

Tableau 87. Schéma de la table de base de données SnmpHelper.SnmpHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
m_HelperDoNotStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDebugLevel facultatif		Entier	Définit le niveau de débogage de l'auxiliaire, impression dans le fichier m_HelperLogfile.
m_HelperLogfile facultatif		Texte	Chemin complet et fichier journal de l'auxiliaire actuel.

Configuration de la base de données de l'auxiliaire SNMP

L'insertion suivante fournit un exemple de configuration de la base de données de l'auxiliaire SNMP.

```
insert into SnmpHelper.SnmpHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
values
(
                259200, 1200, 90, 0, 0
);
```

Schéma de la base de données de l'auxiliaire Telnet

La base de données TelnetHelper est définie dans $NCHOME/etc/ precision/ DiscoHelperServerSchema.cfg. Ses noms de table de base de données complets sont : TelnetHelper.TelnetHelperTable; TelnetHelper.TelnetHelperConfig.

Le schéma de la table de base de données `TelnetHelperTable` est décrit dans le tableau 88.

Tableau 88. Schéma de la table de base de données TelnetHelper.TelnetHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Une interface clé unique de réponse à une requête vers les bases de données du serveur auxiliaire.

Tableau 88. Schéma de la table de base de données TelnetHelper.TelnetHelperTable (suite)

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestGetKey	NON NULL	Texte	Une interface clé de requête get vers les bases de données du serveur auxiliaire.
RivHelperDbTimeToDie		Long64	Durée de vie de l'information demandée dans le serveur auxiliaire.
m_HostIp	NON NULL	Texte	Adresse IP du périphérique à interroger.
m_TelnetCommand		Texte	La commande Telnet.
RivHelperRequestOutput		Atom	Données de réponse.

Le tableau 89 donne le schéma de la table TelnetHelperConfig.

Tableau 89. Schéma de la table de base de donnée TelnetHelper.TelnetHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Délai d'attente de la base de données auxiliaire, c'est-à-dire, le délai d'expiration de la base de données.
m_HelperReqTimeout		Long64	Le délai d'attente de la requête de l'auxiliaire, c'est-à-dire, le délai d'expiration de chaque requête.
m_HelperStartupTimeout		Long64	Délai d'attente par défaut du démarrage de l'auxiliaire, c'est-à-dire, la durée d'attente maximale du démarrage d'un auxiliaire sur demande.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou s'il interroge le réseau à l'aide d'un auxiliaire : • 0 : Ne pas utiliser le cache • 1 : Utiliser le cache
m_HelperDoNotQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui n'interrogent pas la base de données. Cette zone remplace m_HelperDoWeQuery.

Tableau 89. Schéma de la table de base de donnée TelnetHelper.TelnetHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
m_HelperDoQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est trouvé dans la base de données, le réseau n'est pas interrogé.
m_HelperDoWeStore		Entier	Indique si le serveur auxiliaire stocke les réponses des auxiliaires dans sa base de données : • 0 : Ne pas stocker les réponses dans la base de données • 1 : Stocker les réponses dans la base de données
m_HelperDoStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDoNotStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDebugLevel facultatif		Entier	Définit le niveau de débogage de l'auxiliaire, impression dans le fichier m_HelperLogfile.
m_HelperLogfile facultatif		Texte	Chemin complet et fichier journal de l'auxiliaire actuel.

Configuration de la base de données d'auxiliaire Telnet

L'exemple d'insertion suivant montre une configuration type de la base de données de l'auxiliaire Telnet.

```
insert into TelnetHelper.TelnetHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
```

```
values
(
                259200, 1200, 90, 0, 0
);
```

Schéma de base de données d'auxiliaire XMLRPC

La base de données de l'auxiliaire XmlRpcHelper est définie dans $NCHOME/etc/precision/DiscoHelperServerSchema.cfg. Ses noms de table de base de données complets sont : XmlRpcHelper.XmlRpcHelperTable; XmlRpcHelper.XmlRpcHelperConfig.

Le schéma de la table de base de données XmlRpcHelper.XmlRpcHelperTable est décrit dans le tableau 90.

Tableau 90. Schéma de la table de base de données XmlRpcHelper.XmlRpcHelperTable

Nom de colonne	Contraintes	Type de données	Description
RivHelperRequestReplyKey	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Interface clé vers les bases de données du serveur auxiliaire pour les requêtes Reply.
RivHelperRequestGetKey	NON NULL	Texte	Une interface clé unique pour les bases de données du serveur auxiliaire en cas de requêtes Get.
RivHelperDbTimeToDie		Texte	Durée de vie de l'information demandée dans le serveur auxiliaire.
m_port		Atom	Port du périphérique physique.
m_DataSourceId		Entier	Source de données voulue.
m_MethodCalled		Texte	Méthode appelée.
m_MethodSignature		Entier	Signature de la méthode.
RivHelperRequestOutput		Atom	Données de réponse.

Le schéma de la table de base de données XmlRpcHelper.XmlRpcHelperConfig est décrit dans le tableau 91.

Tableau 91. Schéma de la table de base de données XmlRpcHelper.XmlRpcHelperConfig

Nom de colonne	Contraintes	Type de données	Description
m_HelperDbTimeout	UNIQUE	Long64	Délai d'attente de la base de données auxiliaire, c'est-à-dire, le délai d'expiration de la base de données.
m_HelperReqTimeout		Long64	Le délai d'attente de la requête de l'auxiliaire, c'est-à-dire, le délai d'expiration de chaque requête.

Tableau 91. Schéma de la table de base de données XmlRpcHelper.XmlRpcHelperConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
m_HelperStartupTimeout		Long64	Délai d'attente par défaut du démarrage de l'auxiliaire, c'est-à-dire, la durée d'attente maximale du démarrage d'un auxiliaire sur demande.
m_HelperDoWeQuery		Entier	Indique si le serveur auxiliaire interroge sa base de données ou s'il interroge le réseau à l'aide d'un auxiliaire : • 0 : Ne pas utiliser le cache • 1 : Utiliser le cache
m_HelperDoNotQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui n'interrogent pas la base de données. Cette zone remplace m_HelperDoWeQuery.
m_HelperDoQueryVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui interrogent toujours la base de données avant d'interroger le réseau. Si l'élément est trouvé dans la base de données, le réseau n'est pas interrogé.
m_HelperDoWeStore		Entier	Indique si le serveur auxiliaire stocke des réponses des auxiliaires dans sa base de données : • 0 : Ne pas stocker les réponses dans la base de données • 1 : Stocker les réponses dans la base de données
m_HelperDoStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui stockent toujours des données dans la base de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDoNotStoreVBs facultatif		Liaisons de variables de type d'objet	Liste des entrées d'auxiliaire qui ne stockent jamais de données dans les bases de données du serveur auxiliaire. Cette zone remplace m_HelperDoWeStore.
m_HelperDebugLevel facultatif		Entier	Définit le niveau de débogage de l'auxiliaire, impression dans le fichier spécifié dans m_HelperLogfile.
m_HelperLogFile facultatif		Texte	Chemin complet et fichier journal de l'auxiliaire actuel.

Configuration de la base de données de l'auxiliaire XMLRPC

L'insertion suivante fournit un exemple de configuration type de la base de données XmlRpcHelper. Elle spécifie les paramètres suivants :

- La base de données de l'auxiliaire expire après 3 jours.
- Chaque délai d'attente de requête de base de données d'auxiliaire expire après 20 minutes.
- La durée d'attente maximale du démarrage de l'auxiliaire sur demande est de 90 secondes.
- Le serveur auxiliaire n'interroge pas sa base de données.
- Le serveur auxiliaire ne stocke pas de réponses des auxiliaires dans sa base de données.

```
insert into XmlRpcHelper.XmlRpcHelperConfig
(
        m_HelperDbTimeout,
        m_HelperReqTimeout,
        m_HelperStartupTimeout,
        m_HelperDoWeQuery,
        m_HelperDoWeStore
)
values
(
        259200,
 1200,
 90,
 0,
0
);
```

Bases de données des auxiliaires individuels

En plus de DiscoHelperServerSchema.cfg, chacun des auxiliaires dispose d'un fichier de configuration qui détermine son comportement. Les rubriques suivantes décrivent les bases de données des fichiers de configuration individuels.

Base de données de l'auxiliaire ARP

La base de données de l'auxiliaire ARP est définie par le fichier de configuration DiscoARPHelperSchema.cfg. Le nom qualifié complet de sa table est ARPHelper.configuration.

La base de données ARPHelper.configuration, décrite dans le tableau 92, définit le nombre d'unité utilisées par l'auxiliaire.

Tableau 92. Schéma de table de base de données ARPHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads	Aucun(e)	Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.

Référence associée:

«Fichier de configuration DiscoARPHelperSchema.cfg», à la page 66
Le fichier de configuration DiscoARPHelperSchema.cfg accomplit la résolution de l'adresse IP en adresse MAC.

Base de données de l'auxiliaire DNS

La base de données de l'auxiliaire DNS est définie par le fichier de configuration DiscoDNSHelperSchema.cfg; Ses noms de table de base de données complets sont : DNSHelper.configuration; DNShelper.methods.

La table `DNSHelper.configuration` décrite ne doit contenir qu'un seul enregistrement.

Tableau 93. Schéma de la table de base de données DNSHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
`m_NumThreads`		Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.
`m_MethodList`		Liste de textes	Liste ordonnée des méthodes de récupération de nom.
`m_TimeOut`		Entier	Durée d'attente maximale d'une réponse d'un périphérique (en secondes).

Tableau 94. Schéma de table de base de données DNShelper.methods

Nom de colonne	Contraintes	Type de données	Description
`m_MethodName`	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom de la méthode.
`m_MethodType`		Entier	Type de méthode : • 0 : Système • 1 : DNS • 2 : Fichier
`m_NameServerAddr`		Texte	Adresse IP du serveur DNS (indiquée sous forme de chaîne de texte). Si aucune valeur n'est spécifiée, `/etc/resolv.conf` est lu.
`m_NameDomain`		Texte	Nom de domaine ; par exemple `abcd.com`.
`m_NameDomainList`		Texte	Contient une liste des suffixes de domaines prévus. Si vous vous attendez à ce que la reconnaissance renvoie une partie ou la totalité des noms de périphériques avec les suffixes de domaine déjà présents, vous pouvez spécifier une liste des suffixes de domaine prévus dans cette colonne. **Remarque :** La valeur de suffixe de domaine spécifiée dans `m_NameDomain` n'est pas ajoutée aux noms de périphériques renvoyés par la reconnaissance et comportant l'un des suffixes répertoriés dans `m_NameDomainList`.

Tableau 94. Schéma de table de base de données DNShelper.methods (suite)

Nom de colonne	Contraintes	Type de données	Description
m_FileName		Texte	Le nom du fichier, le cas échéant.
m_FileOrder		Entier	L'ordre des fichiers : • 0 : Nom en premier puis adresse IP • 1 : Adresse IP puis nom
m_TimeOut		Entier	Délai d'attente de la requête en secondes.

Référence associée:

«Fichier de configuration DiscoDNSHelperSchema.cfg», à la page 67
Le fichier de configuration DiscoDNSHelperSchema.cfg définit l'accès au système d'adressage par domaines, qui permet à la reconnaissance de rechercher des noms de domaine, en configurant l'auxiliaire DNS.

Base de données de l'auxiliaire Ping

La base de données de l'auxiliaire Ping est définie par le fichier de configuration DiscoPingHelperSchema.cfg;. Son nom de table de base de donnée complet est pingHelper.configuration.

Le schéma de la table de base de données pingHelper.configuration est décrit dans le tableau 85, à la page 295. Elle ne doit contenir qu'un seul enregistrement.

Bien que le lancement de commandes PING sur des adresses de diffusion et de multidiffusion permette une reconnaissance plus rapide des périphériques que les autres méthodes, il n'est pas conseillé de procéder ainsi dans certaines conditions réseau, par exemple lorsque le réseau est très encombré.

Tableau 95. Schéma de table de base de données pingHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads		Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.
m_TimeOut		Entier	Durée d'attente maximale d'une réponse à partir d'une adresse sur laquelle a été envoyée une commande PING, en millisecondes. Si vous exécutez l'agent TraceRoute, vous devrez peut-être augmenter cette valeur en fonction des conditions réseau.
m_NumRetries		Entier	Nombre de nouveaux lancements de commandes PING sur un périphérique.
m_InterPingTime		Entier	L'intervalle en millisecondes entre des tentatives de lancement de commandes PING successives des adresses de sous-réseau.

Tableau 95. Schéma de table de base de données pingHelper.configuration (suite)

Nom de colonne	Contraintes	Type de données	Description
m_Broadcast		Entier	Indicateur utilisé pour activer ou désactiver l'exécution de la commande PING sur les adresses de diffusion : • (1) Activer • (0) Désactiver
m_Multicast		Entier	Indicateur utilisé pour activer ou désactiver l'exécution de la commande PING sur les adresses de multidiffusion : • (1) Activer • (0) Désactiver

Référence associée:

«Fichier de configuration DiscoPingHelperSchema.cfg», à la page 74
Le fichier de configuration DiscoPingHelperSchema.cfg définit la manière dont les commandes PING doivent être lancées sur les périphériques.

Base de données de l'auxiliaire SNMP

La base de données de l'auxiliaire SNMP est définie par le fichier de configuration DiscoSnmpHelperSchema.cfg. Son nom de table de base de données complet est snmpHelper.configuration.

La base de données de l'auxiliaire SNMP comprend la table snmpHelper.configuration, décrite dans le tableau 96, qui ne doit contenir qu'un seul enregistrement.

Tableau 96. Schéma de la table de base de données snmpHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
`m_NumThreads`	Aucun(e)	Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.
`m_TimeOut`	Aucun(e)	Entier	Durée d'attente maximale d'une réponse à partir d'un périphérique, en millisecondes.
`m_NumRetries`	Aucun(e)	Entier	Nombre de tentatives de récupération de la/des variable(s) SNMP à partir d'un périphérique.

Référence associée:

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Base de données de l'auxiliaire Telnet

La base de données de l'auxiliaire Telnet est définie par le fichier de configuration DiscoTelnetHelperSchema.cfg;. Ses noms de table de base de données complets sont : telnetHelper.configuration; telnetHelper.deviceConfig.

La table telnetHelper.configuration indique les règles générales de réception d'informations des périphériques distants.

Tableau 97. Schéma de la table de base de données telnetHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads		Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire. Si vous modifiez cette valeur, vérifiez que votre système est configuré pour autoriser au moins ce nombre de sessions Telnet simultanées.
m_TimeOut		Entier	Durée d'attente maximale de l'accès à un périphérique (en millisecondes).
m_Retries		Entier	Nombre de tentatives sur l'unité.

La table telnetHelper.deviceConfig définit des options de configuration spécifiques au périphérique.

Tableau 98. Schéma de la table de base de données telnetHelper.deviceConfig

Nom de colonne	Contraintes	Type de données	Description
m_SysObjectId facultatif		Texte	La variable MIB sysObjectID avec laquelle la correspondance doit être effectuée pour cette entrée de configuration. L'entrée ayant la correspondance d'ID objet la plus longue sera utilisée. Par exemple, si vous spécifiez une valeur de 1.3.6.1.4.1.9.1, tous les périphériques ayant des ID objet de forme 1.3.6.1.4.1.9.1.* seront appariés. Les périphériques IOS Cisco ont des ID objets de forme 1.3.6.1.4.1.9.1.*. Cette zone est ignorée si m_IpOrSubNet est spécifié.
m_IpOrSubNet		Texte	L'adresse IP ou l'adresse de sous-réseau qualifiée complète correspondant à une configuration particulière. Si elle n'est pas indiquée, la configuration est utilisée comme adresse de sous-réseau par défaut.
m_NetMaskBits		Entier	Nombre de bits de poids fort dans le masque de réseau. Ce nombre doit être indiqué si m_IpOrSubNet est spécifié.
m_PageLengthCmd		Texte	Commande à émettre pour définir la longueur de page de sortie.

Tableau 98. Schéma de la table de base de données telnetHelper.deviceConfig (suite)

Nom de colonne	Contraintes	Type de données	Description
`m_PageLength`		Entier	Taille de longueur de page de sortie. Définie par défaut sur 0, c'est-à-dire aucune pagination. Si vous définissez une taille de longueur de page, vous devez également insérer une valeur dans la colonne `m_PageLengthCmd` afin de définir une commande de longueur de page.
`m_ContinueMsg`		Texte	Invite du périphérique distant attendue entre une sortie paginée, par exemple, "`Voulez-vous continuer`". Les expressions régulières sont des entrées valides.
`m_ContinueCmd`		Texte	La réponse à envoyer au périphérique distant pour qu'il puisse poursuivre la sortie paginée. Elle est généralement définie sur "`y`". Vous devez faire attention en définissant cette valeur, car certains périphériques requièrent un retour chariot après la commande et d'autres non. Par défaut, un tel retour n'est pas ajouté afin d'offrir une souplesse maximale. Il doit être spécifié explicitement à l'aide de `Ctrl-M` à la fin de la chaîne.
`m_TransmissionDelay`		Entier	Cette option vous permet de personnaliser le retard utilisé par `ncp_dh_telnet` lors de la transmission de données à un périphérique. Cela peut être utile en cas de perte de données ou de problèmes de périphérique lors de l'utilisation du paramètre de retard de transmission par défaut.

Référence associée:

«Fichier de configuration DiscoTelnetHelperSchema.cfg», à la page 85
Le fichier de configuration DiscoTelnetHelperSchema.cfg définit le fonctionnement de l'auxiliaire Telnet, qui retourne les résultats d'une opération Telnet dans un périphérique indiqué.

Base de données de l'auxiliaire XMLRPC

La base de données de l'auxiliaire XMLRPC est définie par le fichier de configuration DiscoXmlRpcHelperSchema.cfg. Son nom de table de base de données complet est xmlRpcHelper.configuration.

Le schéma de la table de base de données xmlRpcHelper.configuration est décrit dans tableau 99. Elle ne doit contenir qu'un seul enregistrement.

Tableau 99. Schéma de la table de base de données xmlRpcHelper.configuration

Nom de colonne	Contraintes	Type de données	Description
m_NumThreads	Aucun(e)	Entier	Nombre d'unités d'exécution devant être utilisées par l'auxiliaire.
m_TimeOut	Aucun(e)	Entier	Durée d'attente maximale d'une réponse d'un collecteur EMS, en millisecondes. Si vous exécutez l'agent TraceRoute, vous devrez peut-être augmenter cette valeur en fonction des conditions réseau.

Référence associée:

«Fichier de configuration DiscoXmlRpcHelperSchema.cfg», à la page 88
Le fichier de configuration DiscoXmlRpcHelperSchema.cfg peut être utilisé pour configurer l'auxiliaire XML-RPC, lequel permet à Network Manager de communiquer avec des collecteurs EMS à l'aide de l'interface XML-RPC.

Bases de données de suivi de la reconnaissance

Au cours du processus de reconnaissance, le moteur de reconnaissance, ncp_disco, enregistre chaque élément reconnu dans le réseau, qu'il ait été traité ou non. Les bases de données d'instrumentation et des conversions sont utilisées à cet effet. Elles peuvent être interrogées à tout moment pour afficher le nombre de types et de catégories de périphériques reconnus.

Les bases de données des conversions, instrumentation, et workingEntities enregistrent les entités réseau et technologies connues et peuvent être utilisées pour suivre la progression de la reconnaissance.

Base de données des translations

La base de données des translations est définie dans le fichier `$NCHOME/etc/precision/DiscoSchema.cfg`. Elle a plusieurs noms de table de base de données complets.

Les noms complets des tables de la base de données des translations sont les suivants :

- translations.ipToBaseName
- translations.vlans
- translations.NAT
- translations.NATtemp
- translations.NATAddressSpaceIds
- Fix Pack 4 specialManagementIPs

Table translations.ipToBaseName

La table ipToBaseName est un registre de périphériques reconnus et d'adresses IP associées à ces périphériques.

Lorsqu'un périphérique a plusieurs interfaces, et par conséquent plusieurs adresses IP, l'agent Associated Address télécharge toutes les adresses associées, les stocke dans la table ipToBaseName et permet aux agents de reconnaissance appropriés de reconnaître le périphérique. Toute tentative ultérieure de reconnaissance du périphérique au moyen d'une autre de ses adresses IP est bloquée lorsque l'agent Associated Address vérifie la table ipToBaseName, c'est-à-dire avant que les détails du périphérique soient transmis à l'agent de reconnaissance approprié.

Tableau 100. Schéma de la table de base de données translations.ipToBaseName

Nom de colonne	Contraintes	Type de données	Description
m_BaseName	NON NULL	Texte	Nom de base de l'entité reconnue.
m_BaseAddress	NON NULL	Texte	Adresse de base de l'entité reconnue.
m_WorkAddress	NON NULL	Texte	Adresse utilisée pour l'extraction des données.
m_IpAddress	NON NULL	Texte	Adresse IP de l'entité.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.
m_InScope		Entier booléen	Indique si la valeur de la zone m_IpAddress se trouve dans la portée.
m_Protocol	NON NULL	Entier	Protocole pour cette adresse. Cette zone admet les valeurs suivantes : • 1 : *IPv4* • 3 : *IPv6*
m_IsManagementIP		Entier booléen	Indique s'il s'agit d'une adresse IP de gestion.
m_IsOutOfBand		Entier booléen	Indique s'il s'agit d'une adresse hors bande.
Fix Pack 3 m_Name		Texte	Nom de l'interface avec adresse IP, si connue.

Table translations.vlans

La table vlans contient une liste de périphériques faisant partie des réseaux VLAN (Virtual Local Area Networks). Chaque enregistrement dans la table vlans mappe le périphérique au VLAN auquel il appartient.

Tableau 101. Schéma de la table de base de données translations.vlans

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL	Texte	Nom du périphérique associé à cette entrée.

Tableau 101. Schéma de la table de base de données translations.vlans (suite)

Nom de colonne	Contraintes	Type de données	Description
m_VlanID	• CLE PRIMAIRE • NON NULL	Texte	Identificateur VLAN sur le périphérique.
m_Subnet		Texte	Sous-réseau auquel le VLAN semble associé.
m_NetMask		Texte	Masque de sous-réseau.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table translations.NAT

La table NAT est utilisée pour contenir les mappages de conversion NAT statique. Les périphériques mappés sont reconnus, même s'ils se trouvent en-dehors de la portée de la reconnaissance.

Tableau 102. Schéma de la table de base de données translations.NAT

Nom de colonne	Contraintes	Type de données	Description
m_OutsideGlobalAddr	• CLE PRIMAIRE • NON NULL	Texte	L'adresse publique.
m_InsideLocalAddr	NON NULL	Texte	L'adresse privée.
m_InsideGlobalAddr		Texte	Cette colonne est actuellement inutilisée.
m_OutsideLocalAddr		Texte	Cette colonne est actuellement inutilisée.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table translations.NATtemp

La table NATtemp est utilisée pour contenir les mappages de conversion NAT d'une passerelle NAT précise. Le processus de reconnaissance peut ainsi comparer les nouveaux mappages de conversion NAT aux anciens et initier une nouvelle reconnaissance partielle ou complète, si nécessaire.

Tableau 103. Schéma de la table de base de données translations.NATtemp

Nom de colonne	Contraintes	Type de données	Description
m_OutsideAddr	• CLE PRIMAIRE • NON NULL	Texte	Adresse publique du périphérique.
m_InsideAddr	NON NULL	Texte	Adresse privée du périphérique.

Tableau 103. Schéma de la table de base de données translations.NATtemp (suite)

Nom de colonne	Contraintes	Type de données	Description
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Table translations.NATAddressSpaceIds

La table NATAddressSpaceIds est utilisée pour identifier les adresses IP des passerelles NAT et pour spécifier un identificateur d'espace adresse pour chacune d'entre elles.

Tableau 104. Schéma de la table de base de données translations.NATAddressSpaceIds

Nom de colonne	Contraintes	Type de données	Description
m_NATGatewayIP	• CLE PRIMAIRE • NON NULL	Texte	L'adresse IP de la passerelle.
m_AddressSpaceId		Texte	L'identificateur d'espace adresse à utiliser pour tous les périphériques du domaine NAT appartenant à la passerelle dont l'adresse IP est spécifiée dans m_NATGatewayIP.

Tâches associées:

«Définition d'espaces adresse pour des passerelles NAT», à la page 161
Pour indiquer les adresses IP de vos passerelles NAT et l'identificateur de l'espace adresse que vous souhaitez utiliser pour chaque domaine NAT associé, modifiez `DiscoConfig.cfg` afin de créer ou de modifier une insertion dans `translations.NATAddressSpaceIds`.

Table specialManagementIPs

Fix Pack 4

Après la phase de traitement de la reconnaissance, cette table contient une entrée pour chaque adresse IP qui figurait dans la portée, en fonction des entrées dans la table scope.special.

Tableau 105. Table specialManagementIPs

Colonne	Contraintes	Type de données	Description
m_IpAddress	Non null	Texte	Adresse IP de l'entité.
m_WorkAddress	Non null	Texte	Adresse qui a été utilisée pour l'extraction des données.

Tableau 105. Table specialManagementIPs (suite)

Colonne	Contraintes	Type de données	Description
m_AdminInterfaceIP		Type entier booléen	Indique si l'adresse est une interface, comme défini dans la table scope.special.
m_IsManagementIP		Type entier booléen	Indique si l'adresse est une adresse de gestion, comme indiqué dans la table scope.special.
m_ExtraInfo		Liste VB de types d'objets	Informations supplémentaires qui enrichissent l'entité cible, comme défini dans la table scope.special.
m_AddressSpace		Texte	Espace adresse de l'adresse IP, comme défini dans la table ipToBaseName.
m_Identifier		Texte	Identificateur, comme défini dans la table scope.special.
m_Priority		Ent	Priorité, comme indiqué dans la table scope.special.
m_NonPingable		Ent	Indique si l'adresse est sélectionnée, même si elle ne peut pas être contactée (ping), comme indiqué dans la table scope.special
m_UsedForChassis		Ent	Si la valeur est 1, cela implique que l'adresse IP a été définie pour être utilisée comme adresse d'accès de l'entité châssis.

Schéma de la base de données instrumentation

La base de données instrumentation est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Elle répertorie les périphériques reconnus en les regroupant par technologie. Vous pouvez exécuter des requêtes OQL pour extraire les noms de tous les sous-réseaux, VLAN, périphériques de relais de trame, etc. reconnus.

Les noms de table de base de données complets de la tableinstrumentation sont :

- instrumentation.ipAddresses
- instrumentation.name
- instrumentation.subNet
- instrumentation.vlan

- instrumentation.frameRelay
- instrumentation.ciscoFrameRelay
- instrumentation.hsrp
- instrumentation.pnniPeerGroup
- instrumentation.fddi

Table instrumentation.ipAddresses

La table ipAddresses contient un enregistrement des adresses IP uniques reconnues dans le réseau.

Tableau 106. Schéma de la table de base de données instrumentation.ipAddresses

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Adresse IP d'une entité réseau reconnue.

Table instrumentation.name

La table name contient un enregistrement du nom unique de chaque périphérique reconnu.

Tableau 107. Schéma de la table de base de données instrumentation.name

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom d'une entité réseau reconnue.

Table instrumentation.subNet

La table subNet contient un enregistrement de chaque adresse et masque de sous-réseau reconnus.

Tableau 108. Schéma de la table de base de données instrumentation.subNet

Nom de colonne	Contraintes	Type de données	Description
m_SubNet	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Adresse de sous-réseau d'un sous-réseau reconnu.
m_NetMask	• NON NULL • UNIQUE	Texte	Masque de sous-réseau d'un sous-réseau reconnu.

Table instrumentation.vlan

La table vlan contient un enregistrement de chaque VLAN reconnu.

Tableau 109. Schéma de la table de base de données instrumentation.vlan

Nom de colonne	Contraintes	Type de données	Description
m_Vlan	UNIQUE	Entier	ID du VLAN reconnu.

Table instrumentation.frameRelay

La table frameRelay contient un enregistrement de chaque périphérique de relais de trame reconnu.

Tableau 110. Schéma de la table de base de données instrumentation.frameRelay

Nom de colonne	Contraintes	Type de données	Description
m_IfDlci	• CLE PRIMAIRE • NON NULL • UNIQUE	Entier	L'identificateur de connexion de liaison de données du périphérique de relais de trame.
m_IfIndex	• CLE PRIMAIRE • NON NULL	Entier	Valeur unique pour chaque interface de périphérique.

Table instrumentation.ciscoFrameRelay

La table ciscoFrameRelay contient un enregistrement de chaque périphérique de relais de trame Cisco reconnu.

Tableau 111. Schéma de la table de base de données instrumentation.ciscoFrameRelay

Nom de colonne	Contraintes	Type de données	Description
m_UniqueKey	• NON NULL • UNIQUE	Texte	Combinaison de l'adresse IP, de FRIfIndex et de FRDlci.
m_FRIfIndex	• CLE PRIMAIRE • NON NULL	Entier	Valeur unique pour chaque interface de périphérique.
m_FRDlci	• CLE PRIMAIRE • NON NULL • UNIQUE	Entier	L'identificateur de connexion de liaison de données du périphérique de relais de trame.

Table instrumentation.hsrp

La table hsrp contient un enregistrement de chaque périphérique HSRP (Hot Standby Router Protocol) reconnu.

Tableau 112. Schéma de la table de base de données instrumentation.hsrp

Nom de colonne	Contraintes	Type de données	Description
m_GroupAddress	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Adresse de groupe du périphérique.
m_PrimaryAddress		Texte	Adresse principale du périphérique.
m_StandbyAddress		Texte	Adresse de secours du périphérique.

Table instrumentation.pnniPeerGroup

La table pnniPeerGroup contient les identificateurs de groupe d'homologues du niveau le plus bas des périphériques PNNI reconnus. Les ID groupes d'homologues PNNI logiques ne sont pas stockés.

Tableau 113. Schéma de la table de base de données instrumentation.pnniPeerGroup

Nom de colonne	Contraintes	Type de données	Description
m_PeerGroupId	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	L'identificateur de groupe homologue PNNI de niveau le plus bas.

Table instrumentation.fddi

La table fddi contient les noeuds FDDI (Fibre Distributed Data Interface) reconnus.

Tableau 114. Schéma de la table de base de données instrumentation.fddi

Nom de colonne	Contraintes	Type de données	Description
m_UniqueAddress	• CLE PRIMAIRE • NON NULL	Texte	Adresse unique du noeud.
m_StationManagmentTask	• CLE PRIMAIRE • NON NULL	Entier	Tâche de gestion de station pour ce noeud.

Base de données workingEntities

La base de données workingEntities est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Ses noms de tables de base de données complets sont : workingEntities.finalEntity; workingEntities.containment.

La base de données workingEntities fournit un référentiel central pour les informations sur les entités reconnues et les détails de confinement associés à chaque entité. Cette base de données n'est cependant remplie qu'a la fin du processus de reconnaissance.

Table workingEntities.finalEntity

La table finalEntity est un référentiel central pour les informations sur les entités reconnues.

Tableau 115. Schéma de la table de base de données workingEntities.finalEntity

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom unique de l'entité reconnue.
m_Creator	NON NULL	Texte	Nom de l'agent (ou outil de recherche) qui a reconnu l'entité.
m_ObjectId		Texte	Classe d'unités (représentation textuelle de l'adresse ASN.1).
m_Description		Texte	Description du périphérique, extraite de la variable MIB sysDescr pour l'entité.
m_UniqueAddress		Texte	Adresse IP de l'entité réseau.
m_IsActive	Type de données booléennes défini de manière externe	Entier booléen	Indique si l'entité est active : (2) Indique que l'entité est reconnue mais hors de portée. Les entités hors de portée ne sont pas surveillées par Network Manager. (1) L'entité est active. (0) L'entité est *in*active.
m_HaveAccess	Type de données Boolean défini en externe	Entier booléen	Indicateur signalant la disponibilité d'un accès SNMP au périphérique : • 1 : accès SNMP disponible • 0 : pas d'accès SNMP
m_EntityType	Type de données entityType défini en externe	Entier	Description de type d'élément de l'entité reconnue : • 0 : Type inconnu • 1 : Entité de base • 2 : Voisin local • 3 : Voisin distant
m_BaseName		Texte	Nom de l'Entité de base pour ce périphérique.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Tableau 115. Schéma de la table de base de données workingEntities.finalEntity (suite)

Nom de colonne	Contraintes	Type de données	Description
m_ExtraInfo	Type de donnée vblist défini en externe	Objet	Informations supplémentaires requises par l'agent.
m_LocalNbr	Type de donnée vblist défini en externe	Objet	Informations sur le voisin local.

Table workingEntities.containment

La table containment est un référentiel central d'informations sur les informations de confinement des entités reconnues. Elle indique les relations de confinement entre toutes les entités de la table finalEntity.

Pour avoir un exemple du fonctionnement de la table containment, supposez que la table finalEntity inclue les entités distinctes suivantes :

- Un périphérique dont l'adresse IP est `1.2.3.4`
- Une interface sur ce périphérique `1.2.3.4[0[1]]`

La table finalEntity ne fournit aucune information de confinement pour ces deux entités. En d'autres termes, elle n'indique pas que l'interface 1.2.3.4[0[1]] est contenue physiquement dans le périphérique 1.2.3.4. Ces informations de confinement sont incluses dans la table containment comme suit :

```
m_Container='1.2.3.4'
m_Part='1.2.3.4[0[1]]'
m_IsPhysical=1
m_LinkType=1
```

Notez que m_Container et m_Part sont des noms uniques d'entité sur le réseau, ayant chacune un m_Name unique dans la table finalEntity.

Tableau 116. Schéma de la table de base de données workingEntities.containment

Nom de colonne	Contraintes	Type de données	Description
m_Container	• CLE PRIMAIRE • NON NULL	Texte	Nom d'un objet qui contient quelque chose. Cet objet fait référence à une entité sur le réseau et correspond à une entité ayant ses propres entrée et m_Name unique dans la table workingEntities.finalEntity.
m_Part	• CLE PRIMAIRE • NON NULL	Texte	Nom de l'objet qui est contenu. Cet objet fait référence à une entité sur le réseau et correspond à une entité ayant ses propres entrée et m_Name unique dans la table workingEntities.finalEntity.
m_IsPhysical		Entier booléen	Indicateur signalant si le confinement est physique ou logique : • 1 : Confinement physique • 0 : Confinement logique

Tableau 116. Schéma de la table de base de données workingEntities.containment (suite)

Nom de colonne	Contraintes	Type de données	Description
m_LinkType		Entier	Valeur indiquant le mode de transfert de données entre m_Container et m_Part. Les valeurs suivantes sont possibles : • 0 : Aucune donnée n'est transmise. • 1 : Des données sont transmises dans les deux sens. • 2 : Des données sont transmises de m_Container à m_Part. • 3 : Des données sont transmises de m_Part à m_Container

workingEntities.interfaceMapping

Fix Pack 3

La table interfaceMapping active l'assemblage afin d'identifier rapidement les interfaces.

Le tableau ci-dessous répertorie les colonnes de la table interfaceMapping.

Remarque : Les zones de cette table ne sont pas toutes remplies ; toutefois, l'utilisation de cette table permet de consulter les données rapidement.

Tableau 117. Schéma de la table de base de données workingEntities.interfaceMapping

Nom de colonne	Contraintes	Type de données	Description
m_Name	Non null	Texte	Nom unique d'une interface sur le réseau.
m_IfIndex		Entier	ifIndex du protocole SNMP.
m_InterfaceId		Texte	Identificateur de l'interface.
m_EntPhysIndex		Entier	Index physique MIB d'entité si présent.
m_IfDescr		Texte	ifDescr RFC de l'interface.
m_IfName		Texte	ifName RFC de l'interface.
m_IfAlias		Texte	Zone ifAlias RFC de l'interface.
m_IfType		Entier	ifType RFC de l'interface.
m_PhysAddress		Texte	Adresse MAC pour cette entité si présente.
m_BaseName	Non null	Texte	Nom de l'entité de base pour ce périphérique.
m_AddressSpace		Texte	Nom de l'espace adresse dans lequel se trouve ce périphérique. Pour les périphériques publics, la zone a pour valeur null.

Bases de données topologiques de travail

Le moteur de reconnaissance, ncp_disco, utilise une série de bases de données pour exécuter les étapes de traitement de données du cycle de reconnaissance. Les programmes stitcher fonctionnent sur ces bases de données pour rassembler une topologie de réseau et créer le modèle de confinement.

Les programmes stitcher créent les différentes topologies de réseau, telles que les topologies de couche 2 et 3, en fusionnant les informations des tables returns des agents de reconnaissance en une seule topologie cumulative dans la base de données fullTopology.

Schéma de la base de données fullTopology

La base de données fullTopology est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Son nom de table de base de données complet est fullTopology.entityByNeighbor.

La base de données fullTopology contient la topologie générée. A la fin de la phase de collecte des données de la reconnaissance, les programmes stitcher fusionnent les informations récupérées par les agents de reconnaissance pour former une seule topologie, qui est au format nom-vers-nom à ce stade.

Table fullTopology.entityByNeighbor

La table entityByNeighbor contient les informations sur la connectivité entre les périphériques reconnus.

Tableau 118. Schéma de la table de base de données fullTopology.entityByNeighbor

Nom de colonne	Contraintes	Type de données	Description
m_Name	• CLE PRIMAIRE • NON NULL	Texte	Nom unique d'une entité sur le réseau.
m_NbrName	• CLE PRIMAIRE • NON NULL	Texte	Nom du périphérique connecté à l'entité réseau unique.
m_NbrType	Type de données connectionType défini en externe	Entier	Représentation par un entier du type de connexion entre l'entité réseau et son voisin : • 2 : Principal-vers-local • 3 : Local-vers-distant

Schéma de la base de données scratchTopology

La base de données scratchTopology est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Son nom de table de base de données complet est : scratchTopology.entityByName.

La base de données scratchTopology contient le modèle de confinement dérivé de la base de données fullTopology (et créé par des programmes stitcher). Il s'agit de la version de la topologie envoyée au composant MODEL.

Concepts associés:

«Filtres», à la page 6
Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de

reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

Tâches associées:

«Définition des filtres de reconnaissance», à la page 36
Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Table scratchTopology.entityByName

La table entityByName contient le modèle réseau dérivé de la base de données fullTopology.

Tableau 119. Schéma de la table de base de données scratchTopology.entityByName

Nom de colonne	Contraintes	Type de données	Description
`Address`		Liste de textes	Liste d'adresses de couche 1 à 7 du modèle OSI de l'entité.
`BaseName`		Texte	Nom de base unique d'une entité.
`Inclure`		Liste de textes	Liste d'éléments ou d'autres conteneurs contenus dans l'entité réseau actuelle.
`Description`		Texte	Valeur de la variable MIB sysDescr ou autre description appropriée de l'entité.
`EntityName`	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom unique de l'entité réseau.
`EntityOID`		Texte	Classe d'unités à laquelle appartient l'entité réseau. Il s'agit d'une représentation textuelle de l'adresse ASN.1.
`EntityType`	Type de données entityTypes défini en externe	Entier	Type d'élément de l'entité : • 0 : Inconnu • 1 : Boîtier • 2 : Interface • 3 : Interface logique • 4 : Objet Vlan • 5 : Carte • 6 : PSU • 7 : Sous-réseau • 8 : Module

Tableau 119. Schéma de la table de base de données scratchTopology.entityByName (suite)

Nom de colonne	Contraintes	Type de données	Description
`ExtraInfo`	Type de donnée vblist défini en externe		Toute information supplémentaire.
`IsActive`	Type de données booléennes défini de manière externe	Entier booléen	Défini par le programme stitcher CheckInterfaceStatus. Dérivé des valeurs d'ifAdminStatus et d'ifOperStatus de l'entité. Indique si une classe d'objet active est nécessaire : • 1 : Classe d'objet active requise • 0 : Classe d'objet active non requise
`LingerTime`		Entier	Vous pouvez définir la valeur LingerTime d'une entité dans des programmes stitchers personnalisés pour déterminer comment ncp_model gère l'entité lorsque ncp_disco envoie la topologie à ncp_model. La valeur LingerTime détermine le nombre de reconnaissances dans lesquelles une entité ne se trouve pas pour être considérée avoir été retirée du réseau et son enregistrement supprimé de la topologie. Si la valeur est zéro, l'entité est supprimée immédiatement de ncp_model lorsque le processus de reconnaissance met à jour la topologie dans ncp_model.
`RelatedTo`		Liste de textes	Liste d'entités connectées à l'entité réseau.
`Statut`	Type de données booléennes défini de manière externe	Entier booléen	Cette zone est remplie par le moteur de reconnaissance ncp_disco avec la valeur de la zone m_HaveAccess. Elle indique donc si ncp_disco a acquis un accès SNMP à l'unité.
`UpwardConnections`		Liste de textes	Liste de conteneurs qui contiennent cette entité.

Base de données rediscoveryStore

La base de données rediscoveryStore est utilisée à des fins de comparaison en mode nouvelle reconnaissance. Elle est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Ses noms de tables de base de données complets sont : rediscoveryStore.dataLibrary; rediscoveryStore.rediscoveredEntities

La base de données rediscoveryStore contient des informations de cycles de reconnaissance précédents, pouvant être utilisées à des fins de comparaison pendant une nouvelle reconnaissance complète ou partielle.

Table rediscoveryStore.dataLibrary

La table dataLibrary est utilisée comme point de référence en mode nouvelle reconnaissance pour comparer l'état précédent à l'état actuel.

Tableau 120. Schéma de la table de base de données rediscoveryStore.dataLibrary

Nom de colonne	Contraintes	Type de données	Description
m_Name		Texte	Nom unique d'une entité sur le réseau.
m_UniqueAddress		Texte	Adresse IP d'une entité réseau reconnue.
m_CompareDb	NON NULL	Texte	Entité utilisée pour comparer cette entité réseau.

Table rediscoveryStore.rediscoveredEntities

La table rediscoveredEntites stocke les entités trouvées lors d'une nouvelle reconnaissance.

Tableau 121. Schéma de la table de base de données rediscoveryStore.rediscoveredEntities

Nom de colonne	Contraintes	Type de données	Description
m_Name		Texte	Nom unique d'une entité sur le réseau.
m_UniqueAddress		Texte	Adresse IP d'une entité réseau reconnue.
m_PhysAddr		Texte	Adresse physique de l'entité.
m_OldBaseName			Nom de base de l'entité avant la nouvelle reconnaissance
m_NewBaseName			Nom de base de l'entité après la nouvelle reconnaissance.

Base de données du gestionnaire de topologie

Le gestionnaire de topologie, ncp_model, stocke les données de topologie suite à une reconnaissance et envoie ces données à la base de données topologiques (NCIM), où elles peuvent être interrogées à l'aide de SQL. Lorsque ncp_model démarre, il attend que le moteur de reconnaissance termine le processus de reconnaissance, crée la topologie et l'insère dans la base de données ncp_model.

Tableau 122. Bases de données MODEL (ncp_model)

Base de données	Description
master	Stockage central de la topologie du réseau.
model	Utilisée pour le suivi des mises à jour de la topologie.

Schéma de base de données master

La base de données master est définie dans $NCHOME/etc/precision /ModelSchema.cfg. Ses noms de tables de base de données complets sont : master.entityByName; master.entityByNeighbor; master.containers. La base de données master contient les entités réseau, leur confinement et leurs connexions.

Table master.entityByName

La table entityByName contient des informations sur toutes les entités réseau reconnues. Cette table est active, remplie avec les informations reçues de DISCO. Les entrées effectuées dans la table entityByName sont également utilisées pour renseigner la table containers.

Tableau 123. Schéma de la table de base de données master.entityByName

Nom de colonne	Contraintes	Type de données	Description
`ActionType`	Type de données d'action défini en externe	Entier	La valeur de cette zone a une signification lorsque l'enregistrement est diffusé sur le bus de messages. Elle indique le type de mise à jour de topologie en cours de diffusion. Cette zone accepte les valeurs suivantes : **0** Nouveau **1** Mise à jour **2** Supprimer **3** Non défini
`Adresse`		Liste de textes	Liste d'adresses de couche 1 à 7 du modèle OSI de l'entité.
`ChangeTime`		Heure	Heure de dernière modification de l'enregistrement de l'entité réseau.
`NomdeClasse`		Texte	Nom de classe de l'entité réseau (le cas échéant).
`Inclure`		Liste de textes	Liste d'éléments ou d'autres conteneurs contenus dans l'entité réseau actuelle.
`CreateTime`		Heure	Heure de création de l'enregistrement de l'entité réseau dans la table.

Tableau 123. Schéma de la table de base de données master.entityByName (suite)

Nom de colonne	Contraintes	Type de données	Description
Description		Texte	Valeur de la variable MIB sysDescr ou autre description appropriée de l'entité.
EntityName	• CLE PRIMAIRE • NON NULL • UNIQUE	Texte	Nom descriptif unique de l'entité réseau.
EntityOID		Texte	Valeur de la variable MIB sysOID de l'entité.
EntityType	Type de données entityTypes défini en externe	Entier	Typé d'élément de l'entité. • 0 : Inconnu • 1 : Boîtier • 2 : Interface • 3 : Interface logique • 4 : Objet VLAN • 5 : Carte • 6 : PSU • 7 : Collection logique • 8 : Module
ExtraInfo	Type de donnée vblist défini en externe	Objet	Liste d'informations supplémentaires.
IsActive	Type de données booléennes défini de manière externe	Entier booléen	Défini par le programme stitcher CheckInterfaceStatus. Dérivé des valeurs d'ifAdminStatus et d'ifOperStatus de l'entité. Indique si une classe d'objet active est nécessaire : • 1 : Classe d'objet active requise • 0 : Classe d'objet active non requise
LingerTime	NON NULL Valeur par défaut = 3	Entier	La durée de temporisation est utilisée lors de la nouvelle reconnaissance pour que la nouvelle topologie puisse être fusionnée avec la topologie existante. La valeur de LingerTime est décrémentée si l'entité n'est pas présente dans la nouvelle topologie. L'entité est uniquement supprimée de la topologie lorsque la valeur de LingerTime atteint 0.
ObjectId	• CLE PRIMAIRE • NON NULL • UNIQUE	Entier long	ID objet unique de l'entité réseau.
RelatedTo		Liste de textes	Liste d'entités connectées à l'entité réseau.

Tableau 123. Schéma de la table de base de données master.entityByName (suite)

Nom de colonne	Contraintes	Type de données	Description
Security		Texte	Mot de passe pour accéder à l'entité réseau (le cas échéant).
Statut	Type de données d'état défini en externe	Entier	Cette zone est remplie par le moteur de reconnaissance ncp_disco avec la valeur de la zone m_HaveAccess. Elle indique donc si ncp_disco a acquis un accès SNMP à l'unité.
UpwardConnections		Liste de textes	Liste de conteneurs qui contiennent cette entité.

Table master.entityByNeighbor

La table entityByNeighbor contient les informations de connectivité de chaque entité réseau.

Tableau 124. Schéma de la table de base de données master.entityByNeighbor

Nom de colonne	Contraintes	Type de données	Description
LeftId	• CLE PRIMAIRE • NON NULL	Entier long	ID objet de la connexion côté gauche.
LeftName	• CLE PRIMAIRE • NON NULL	Texte	Nom d'entité de la connexion côté gauche.
RightName	• CLE PRIMAIRE • NON NULL	Texte	Nom d'entité de la connexion côté droit.
Speed		Long64	Vitesse de la connexion en bits par seconde (bps).
Protocole	Type de données protocole défini en externe	Entier	Type de protocole de transmission utilisé par la connexion.
RelType	Type de données connectionType défini en externe	Entier	Type de relation.
Duplex	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant si la liaison est bidirectionnelle (c'est-à-dire, duplex complet) : • 1 : Liaison bidirectionnelle. • 0 : Liaison non bidirectionnelle.

Table master.containers

La table containers utilise le modèle de confinement pour considérer chaque entité réseau comme étant confinée par d'autres entités réseau. La table, remplie automatiquement en résultat des entrées effectuées dans la table entityByName, montre le parent de chaque entité, c'est-à-dire l'objet qui contient l'entité présente.

Tableau 125. Schéma de la table de base de données master.containers

Nom de colonne	Contraintes	Type de données	Description
ObjectId	• CLE PRIMAIRE • NON NULL	Entier long	ID objet unique de l'entité réseau.
EntityName	• CLE PRIMAIRE • NON NULL	Texte	Nom descriptif de l'entité réseau conteneur.
MemberName	NON NULL	Texte	Nom de membre de l'objet contenu.

Schéma de la base de données model

La base de données model est définie dans $NCHOME/etc/precision/ModelSchema.cfg. Ses noms de tables de base de données complets sont : model.config; model.statistics. Cette base de données stocke des informations sur la topologie pour permettre une fusion efficace des topologies lors de la nouvelle reconnaissance.

Table model.config

La table model.config stocke les informations de configuration utilisées par MODEL au cours de la nouvelle reconnaissance.

Tableau 126. Schéma de la table de base de données model.config

Nom de colonne	Contraintes	Type de données	Description
LingerTime	• CLE PRIMAIRE • NON NULL • UNIQUE	Entier	Valeur de la durée de temporisation pour la topologie.
ChassisCreation Evénements	NON NULL	Entier booléen	Génère les événements ItnmEntityCreation et ItnmEntityDeletion pour les entités de boîtier.
IpInterfaceCreation Evénements	NON NULL	Entier booléen	Génère les événements ItnmEntityCreation et ItnmEntityDeletion pour les interfaces ayant leur propre adresse IP.
MaintenanceState Evénements	NON NULL	Entier booléen	Génère les événements ItnmMaintenanceState pour les entités de boîtier et les interfaces ayant leur propre adresse IP.
ManagedStatusUpdate Intervalle	NON NULL	Entier	Intervalle, en secondes, auquel le processus ncp_model recherche les modifications dans la table managedStatus NCIM. Durée maximale pour la réaction de l'interrogateur aux modifications apportées au statut géré dans une des interfaces graphiques suivantes : vues réseau, vue Tronçon réseau, navigateur de structure. Valeur par défaut : 30 secondes.

Tableau 126. Schéma de la table de base de données model.config (suite)

Nom de colonne	Contraintes	Type de données	Description
DiscoveryUpdateMode	NON NULL	Entier	Pour une utilisation système interne uniquement. Avant la mise à jour par lots, **ncp_disco** définit cette valeur sur 1 pour une reconnaissance partielle ou sur 0 pour une reconnaissance complète.

Toutes les combinaisons des indicateurs ChassisCreationEvents, IpInterfaceCreationEvents et MaintenanceStateEvents peuvent être activées ou désactivées. Par défaut, ces trois indicateurs sont désactivés.

Remarque : Si votre réseau contient des routeurs avec un grand nombre d'adresses IP, l'activation de l'indicateur IpInterfaceCreationEvents peut générer un grand nombre d'événements dans Object Server.

Table model.profilingData

Fix Pack 3

La table model.profilingData stocke les données associées au temps et à la mémoire utilisés lors de la reconnaissance. Elle inclut des informations sur le temps de transfert des données de profilage de reconnaissance dans la base de données topologiques NCIM.

Tableau 127. Schéma de la table de base de données model.profilingData

Nom de colonne	Contraintes	Type de données	Description
BatchStartTime	• CLE PRIMAIRE • NON NULL • UNIQUE	Entier	Durée écoulée depuis le démarrage d'une mise à jour par lots depuis le moteur de reconnaissance.
BatchStartSize	NON NULL	Entier	Nombre d'enregistrements dans le lot reçu.
BatchStartMem	NON NULL	Entier 64 bits	Utilisation de la mémoire au démarrage du lot.
BatchEndTime		Entier	Heure de fin d'une mise à jour par lots depuis le moteur de reconnaissance ncp_disco.
BatchEndSize		Entier	Nombre d'enregistrements à la fin. **Remarque :** Cette valeur peut être supérieure à la valeur de début si des lots consécutifs ont été fusionnés.
BatchEndMem		Entier 64 bits	Utilisation de la mémoire à la fin du lot.
EntityCount		Entier	Nombre d'entités après la mise à jour par lots.
ChassisCount		Entier	Nombre de périphériques de boîtier après la mise à jour par lots.
InterfaceCount		Entier	Nombre d'interfaces après la mise à jour par lots.

Table model.statistics

La table model.statistics stocke les informations relatives aux reconnaissances précédentes.

Tableau 128. Schéma de la table de base de données model.statistics

Nom de colonne	Contraintes	Type de données	Description
TopologyCount	• CLE PRIMAIRE • NON NULL • UNIQUE	Long	Comptage du nombre d'envois de la topologie de DISCO à MODEL.
TopologySendFinished		Entier	Indique si DISCO a terminé le transfert de la topologie à MODEL. Cette colonne est définie sur 0 lorsque le programme stitcher SendTopologyToModel.stch commence à envoyer la topologie et sur 1 lorsque l'envoi de la topologie est terminé.
InsertCount		Long	Nombre d'entités insérées dans la topologie.
UpdateCount		Long	Nombre d'entités mises à jour dans la topologie.
DeleteCount		Long	Nombre d'entités supprimées de la topologie.

Base de données de reprise après incident

La reprise après incident avec la base de données de reprise ne doit pas être confondue avec la reprise d'agent et d'outil de recherche, configurée directement à partir de la table disco.config. Si elle est sélectionnée, la reprise d'agent et d'outil de recherche fonctionne que la reprise avec la base de données de reprise soit implémentée ou pas.

Si la colonne m_WriteTablesToCache de la table disco.config est définie sur 1 (true), les données sont mises en mémoire cache pendant le processus de reconnaissance pour activer la restauration des données en cas d'échec du moteur de reconnaissance ncp_disco. Une reconnaissance exécutée dans ce mode est plus lente qu'une reconnaissance standard, en raison du temps supplémentaire requis pour le stockage de données sur le disque tout au long du processus de reconnaissance.

Données en mémoire cache ignorées

Si DISCO est redémarré en mode reprise après incident, les données en mémoire cache d'un groupe de tables sont ignorées.

Les données en mémoire cache des tables suivantes sont ignorées lorsque DISCO est redémarré en mode reprise après incident :

- disco.config
- disco.managedProcesses
- disco.agents
- L'ensemble de la base de données de portée
- failover.config
- failover.doNotCache
- failover.restartPhaseAction

Pour les tables ci-dessus, seules les insertions spécifiées dans le fichier de schéma au moment du redémarrage sont enregistrées.

Schéma de base de données de reprise en ligne

La base de données de reprise en ligne est définie dans $NCHOME/etc/precision/DiscoSchema.cfg. Ses noms de tables de base de données complets sont : failover.config; failover.status; failover.findRateDetails; failover.doNotCache; failover.restartPhaseAction.

Table failover.config

La table failover.config ne doit jamais contenir plus d'une insertion.

Tableau 129. Schéma de la table de base de données failover.config

Nom de colonne	Contraintes	Type de données	Description
m_InitialiseFromCache	Type de données booléennes défini de manière externe	Entier booléen	Indicateur signalant si les données qui existent déjà dans le cache doivent être utilisées ou non : • 0 : Ne pas utiliser les données en cache • 1 : Utiliser les données en cache le cas échéant
m_NumberOfRetries		Entier	Nombre de tentatives d'utilisation des données en cache avant d'abandonner (c'est-à-dire, le nombre de redémarrages successifs de DISCO avant de démarrer sans données). Si aucune valeur n'est spécifiée, DISCO démarre toujours avec des bases de données vides.
m_StoreEveryNthDevice	Valeur par défaut = 10	Entier	Fréquence de mise à jour de la table findRateDetails. Une fois le nombre spécifié de périphériques trouvé, la table est mise à jour.

Table failover.status

La table failover.status affiche le nombre de tentatives de redémarrage du processus DISCO avec des données en cache. Cette table est active, vous ne devez donc pas y configurer d'insertions.

Tableau 130. Schéma de la table de base de données failover.status

Nom de colonne	Contraintes	Type de données	Description
m_NumberOfAttempts	• NON NULL • CLE PRIMAIRE	Entier	Nombre de tentatives de redémarrage du processus DISCO avec des données en cache. Cette colonne est définie sur 1 lors de la première exécution de DISCO en mode reprise après incident et incrémentée à chaque exécution suivante de DISCO dans ce mode.

Table failover.findRateDetails

La table findRateDetails détaille les périphériques trouvés à un certain moment de la reconnaissance. Cette table est active et les insertions ne doivent pas être effectuées dans le fichier de schéma ; la table est remplie automatiquement.

Tableau 131. Schéma de la table de base de données failover.findRateDetails

Nom de colonne	Contraintes	Type de données	Description
m_StartTime	• NON NULL • CLE PRIMAIRE	Texte	Heure à laquelle le premier périphérique a été trouvé.
m_LastFindTime		Texte	Heure à laquelle le dernier périphérique a été trouvé.
m_DevicesFound		Entier	Nombre de périphériques trouvés à l'heure actuelle.

Table failover.doNotCache

Pour empêcher la mise en mémoire cache d'une table donnée, vous pouvez spécifier son nom dans la table doNotCache. Ainsi, aucun fichier cache inutile n'est créé, tels que ceux pour les tables temporaires définies dans des programmes stitcher.

Tableau 132. Schéma de table de base de données failover.doNotCache

Nom de colonne	Contraintes	Type de données	Description
m_DatabaseName	NON NULL	Texte	Nom de toute base de données qui ne doit pas être mise en mémoire cache pendant la reprise après incident. Les tables suivantes doivent être mises en cache afin d'utiliser le mode de reprise après incident et par conséquent ne doivent pas être répertoriées dans cette table : • disco.status • failover.status Les tables suivantes doivent être mises en cache et par conséquent ne doivent pas être répertoriées dans cette table : • Les tables despatch et returns de l'agent. • finders.processing • translations.ipToBaseName
m_TableName	NON NULL	Texte	Nom de la table dans la base de données spécifiée dans m_DatabaseName qui ne doit pas être mise en cache. Utilisez * pour indiquez toutes les tables de la base de données.

Table failover.restartPhaseAction

La table restartPhaseAction contient l'ensemble de programmes stitcher exécutés lors du redémarrage dans une phase de reconnaissance donnée. Plusieurs programmes stitcher peuvent être spécifiés, mais leur ordre d'exécution est arbitraire. Il est recommandé d'exécuter au moins le programme stitcher FinalPhase lors du redémarrage dans la phase de création de la topologie.

Tableau 133. Schéma de la table de base de données failover.restartPhaseAction

Nom de colonne	Contraintes	Type de données	Description
m_RestartPhase	NON NULL	Entier	Phase dans laquelle DISCO est redémarré.
m_ExecuteStitcher	NON NULL	Texte	Programme stitcher à exécuter dans cette phase.

Exemple de configuration de la base de données de reprise en ligne

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans les tables de base de données de reprise en ligne ajoutées au fichier DiscoConfig.cfg pour configurer DISCO lors de son lancement.

Exemple de configuration de la table failover.config

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans la table failover.config.

Pour cette configuration de la table failover.config, les données en mémoire cache sont utilisées. Le moteur de reconnaissance, ncp_disco, peut être redémarré jusqu'à trois fois avant que des données en mémoire cache soient ignorées. Ces valeurs sont uniquement utilisées lorsque disco.config.m_WriteTablesToCache=1.

```
insert into failover.config
(
        m_InitialiseFromCache,
        m_NumberOfRetries
)
values
(  1, 3  );
```

Exemple de configuration de la table failover.doNotCache

Cet exemple utilise des commandes OQL pour insérer des valeurs de configuration dans la table failover.doNotCache. La table disco.config ainsi que toutes les tables de la base de données d'instrumentation ne sont pas mises en mémoire cache.

```
insert into failover.doNotCache
(
        m_DatabaseName,
        m_TableName
)
values
(
                'disco', 'config'
);

insert into failover.doNotCache
(
                m_DatabaseName, m_TableName
)
values
(
                'instrumentation', '*'
);
```

Base de données agentTemplate

Les bases de données de chaque agent de reconnaissance sont basées sur un modèle appelé base de données agentTemplate.

La base de données agentTemplate est définie dans le fichier $NCHOME/etc/precision/DiscoSchema.cfg et les noms qualifiés complets de ses tables sont les suivants : agentTemplate.despatch et agentTemplate.returns.

Référence associée:

«Fichiers de définition des agents de reconnaissance», à la page 60
Les fichiers de définition des agents de reconnaissance définissent le fonctionnement des agents de reconnaissance.

Reconnaissance de la table .despatch de l'agent

Lorsqu'un périphérique a été interrogé par l'agent Details, il est transmis à l'agent Associated Address afin de vérifier s'il a déjà été reconnu. Si ce n'est pas le cas, les détails du périphérique sont traités et envoyés par un programme stitcher à la table .despatch de l'agent approprié.

La table .despatch est décrite dans le tableau 134.

Lorsque les détails du périphérique sont placés dans la table .despatch, l'agent tente d'extraire les informations de connectivité afférents au périphérique.

Tableau 134. Schéma de la table de base de données agentTemplate.despatch

Nom de colonne	Contraintes	Type de données	Description
m_Name	CLE PRIMAIRE NON NULL	Texte	Nom unique d'une entité sur le réseau.
m_UniqueAddress	NON NULL	Texte	Adresse IP unique de l'entité réseau.
m_ManagerId	CLE PRIMAIRE NON NULL	Texte	Gestionnaire du périphérique. Si l'accès au périphérique est direct, cette propriété est définie sur " ". Par défaut, elle est définie sur " ".
m_Protocol		Entier	Protocole du périphérique reconnu : • (1) IP • (2) IP-NAT
m_ObjectId		Texte	Représentation textuelle de la classe d'unités (une adresse ASN.1).
m_SnmpAccessIP		Texte	Si cette propriété est définie, elle remplace l'adresse IP utilisée pour l'accès SNMP aux périphériques à l'aide du serveur auxiliaire.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.
m_HaveAccess	Type de données booléennes défini de manière externe	Entier booléen	Indicateur précisant si l'accès SNMP au périphérique : • (1) Est activé • (0) N'est pas activé

Reconnaissance de la table .returns de l'agent

Les détails de connectivité renvoyés pour le périphérique sont placés dans la table .returns de l'agent. Ces détails sont utilisés pour remplir la base de données topologiques.

La table .returns est décrite dans le tableau 135.

Tableau 135. Schéma de la table de base de données agentTemplate.returns

Nom de colonne	Contraintes	Type de données	Description
m_Name	NON NULL	Texte	Nom unique d'une entité sur le réseau.
m_UniqueAddress	NON NULL	Texte	Adresse de couche 3 de cette entité.
m_Protocol		Entier	Protocole du périphérique reconnu : • (1) IP • (2) IP-NAT
m_ObjectId		Texte	Représentation textuelle de la classe d'unités (une adresse ASN.1).
m_HaveAccess	Type de données booléennes défini de manière externe	Nombre entier booléen	Indicateur d'accès SNMP au périphérique : • (1) Est activé • (0) N'est pas activé
m_ExtraInfo	Type de donnée vblist défini en externe	Objet	Toute information supplémentaire indiquée par l'utilisateur dans le fichier de définitions de l'agent.
m_LocalNbr	Type de données du voisin défini de manière externe	Objet	Voisins directs (interfaces).
m_RemoteNbr	Type de données nbrsNeighbor défini de manière externe	Objet	Voisins distants connectés aux interfaces.
m_UpdAgent		Texte	Agent ayant mis à jour ce périphérique.
m_SnmpAccessIP		Texte	Si cette propriété est définie, elle remplace l'adresse IP utilisée pour l'accès SNMP aux périphériques à l'aide du serveur auxiliaire.
m_AddressSpace		Texte	Nom de l'espace d'adresses NAT auquel appartient l'unité. Cette valeur est définie dans la table translations.NATAddressSpaceIds. Si la reconnaissance n'utilise pas NAT ou si l'unité se trouve dans le domaine public, cette valeur est NULL.

Tableau 135. Schéma de la table de base de données agentTemplate.returns (suite)

Nom de colonne	Contraintes	Type de données	Description
m_LastRecord	Type de données booléennes défini de manière externe	Entier booléen	Est-ce le dernier enregistrement pour cette entité : • (1) Vrai • (0) Faux

Annexe B. Processus de reconnaissance

Le processus de reconnaissance Network Manager produit une topologie de réseau qui inclut les données de connectivité et de confinement.

Sous-processus de reconnaissance

Le processus de reconnaissance se subdivise en plusieurs sous-processus qui oeuvrent ensemble pour reconnaître les périphériques et l'interconnectivité entre ces derniers.

Lorsque vous lancez une reconnaissance, le moteur de reconnaissance interne Network Manager (`ncp_disco`) est exécuté. Le moteur ncp_disco gère le processus de reconnaissance de l'existence des périphériques et de leur interconnectivité.

Chaque fois que vous lancez une reconnaissance complète, le moteur de reconnaissance, ncp_disco, relit ses fichiers de configuration. Le moteur de reconnaissance instruit également le serveur auxiliaire et les auxiliaires individuels de relire leurs fichiers de configuration. Cette opération est contrôlée par la règle `DiscoReadConfig()` dans le fichier du programme stitcher FullDiscovery.

Remarque : Lorsque vous lancez une reconnaissance partielle, ncp_disco ne lit pas ses fichiers de configuration.

Il détecte l'existence d'un périphérique sur le réseau et en extrait des informations d'inventaire et de connectivité, qui sont ensuite traitées ou 'piquées' ensemble afin de générer un modèle de connectivité ou topologique. Ses composants sont décrits dans le tableau 136.

Tableau 136. Composants de reconnaissance

Nom	Description
Outils de recherche	Les outils de recherche reconnaissent l'existence de périphériques mais n'extraient pas d'informations de connectivité.
Agents	ncp_disco utilise les agents de reconnaissance pour demander des informations de connectivité aux périphériques reconnus par les outils de recherche. Il existe différents agents, chaque agent étant spécialisé pour extraire des informations de différents périphériques et, dans certains cas, pour utiliser différents protocoles. Les agents n'interagissent pas directement avec le réseau mais ils extraient des informations via le serveur auxiliaire. Ils peuvent consister en des bibliothèques ou des fichiers texte et sont spécialisés pour un protocole, des périphériques ou des classes spécifiques.
Serveur auxiliaire	Le serveur auxiliaire gère les auxiliaires et stocke les informations extraites du réseau. Les agents de reconnaissance extraient leurs informations via ce serveur afin de réduire la charge sur le réseau. Le serveur auxiliaire peut traiter directement les requêtes à l'aide des données recueillies ou transmettre la requête à l'auxiliaire approprié.
Auxiliaires	Les auxiliaires extraient des informations du réseau pour le compte des agents de reconnaissance. Ils convertissent également les requêtes des agents en protocole de réseau approprié et posent des requêtes aux périphériques.

Tableau 136. Composants de reconnaissance (suite)

Nom	Description
Programmes stitcher	Les programmes stitcher sont des processus qui transfèrent, manipulent et distribuent les données entre les bases de données. Les programmes stitcher de reconnaissance sont également responsables du traitement des informations collectées par les agents et de leur utilisation pour créer la topologie du réseau. Un jeu prédéfini de programmes stitcher est inclus avec Network Manager. Vous pouvez modifier les programmes stitcher existants ou rédiger de nouveaux programmes stitcher afin d'effectuer la personnalisation de votre topologie de réseau. Par exemple, vous pouvez rédiger un programme stitcher permettant de faire apparaître vos interfaces de périphériques avec une convention de désignation personnalisée. Les programmes stitcher sont codés à l'aide d'un langage qui leur est spécifique.

Minutage de la reconnaissance

Chaque reconnaissance complète consiste en un ou plusieurs cycles de reconnaissance. La division d'une reconnaissance complète en plusieurs cycles de reconnaissance permet à la reconnaissance de s'achever au moment opportun.

Durant le premier cycle de reconnaissance, Network Manager reconnaît l'existence d'une majorité de périphériques prédéterminée sur le réseau et achève la collecte de données et le traitement des opérations associées à ces périphériques. Lorsque Network Manager a reconnu l'existence d'une majorité de périphériques prédéterminée sur le réseau, il entre en *état inactif*.

Les périphériques reconnus par Network Manager à l'état inactif sont placés dans une table de base de données appelée finders.pending. Ces périphériques ne seront traités que lors du cycle de reconnaissance suivant. Cela signifie que le processus de reconnaissance ne doit pas attendre que tous les périphériques soient reconnus avant de commencer les opérations de collecte et de traitement des données plus détaillées.

Remarque : Idéalement, une reconnaissance doit se terminer dans un même cycle. Toutefois, il se peut que le système ne parvienne pas à reconnaître l'existence des entités suffisamment vite. Dans ce cas, des cycles de reconnaissance supplémentaires sont nécessaires. Les raisons pour lesquelles le système ne reconnaît pas assez vite l'existence des entités sont les suivantes : balayage des sous-réseaux peu peuplés et absence d'accès aux périphériques. Les premières reconnaissances sont souvent associées à plusieurs cycles. Cette situation peut être atténuée en utilisant le script BuildSeedList.pl pour créer une liste de départ à l'issue des reconnaissances initiales. Cette liste sera ensuite utilisée dans les reconnaissances suivantes afin de rechercher plus rapidement les périphériques.

Par défaut, chaque cycle de reconnaissance est composé d'une étape de collecte et d'une étape de traitement des données. L'étape de collecte des données est à son tour subdivisée en trois phases. La figure 1, à la page 341 montre un diagramme de minutage qui nécessite deux cycles de reconnaissance pour venir à échéance.

Les étapes de collecte et de traitement des données sont brièvement décrites dans le tableau 137, à la page 341.

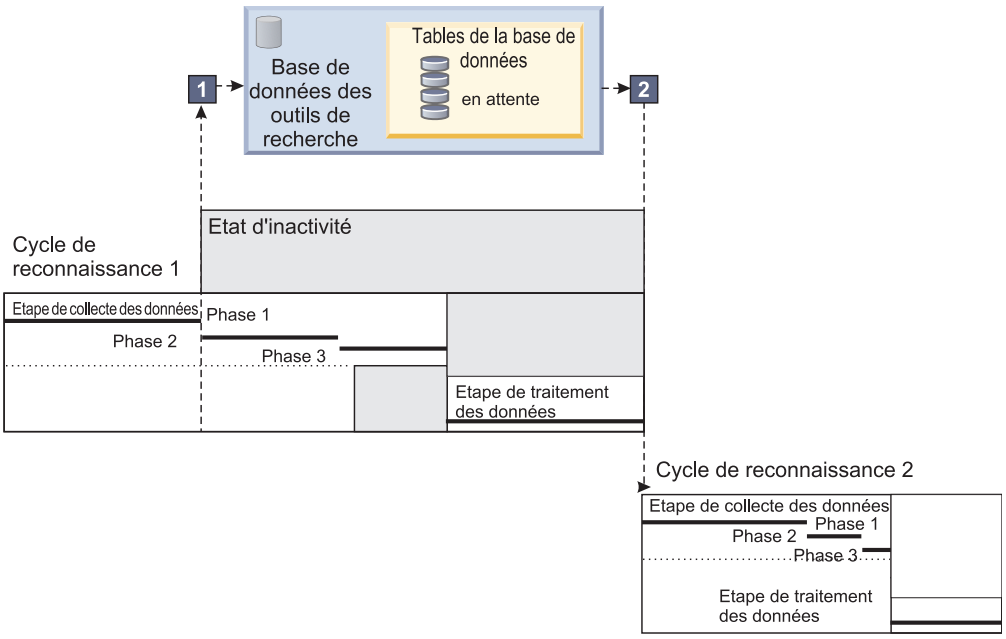

Figure 1. Minutage pour une reconnaissance complète composée de deux cycles de reconnaissance

Dans la figure 1, l'état inactif pour le premier cycle de reconnaissance débute et se termine aux moments respectivement indiqués par les numéros 1 et 2 :

1 : *Début de l'état inactif*. Une majorité prédéterminée de périphériques situés sur le réseau n'ont pas été reconnus. Tous les périphériques reconnus après ce moment sont placés dans la table finders.pending afin d'être traités lors du cycle de reconnaissance suivant.

2 : *Fin de l'état inactif*. Les périphériques stockés dans la table finders.pending sont maintenant traités lors du cycle de reconnaissance suivant.

Remarque : Si le réseau en cours de reconnaissance est particulièrement important ou complexe, il se peut que vous ayez besoin de plus de deux cycles de reconnaissance pour parvenir à une reconnaissance complète. Dans ce cas, chaque cycle de reconnaissance, sauf le dernier, dispose de son propre état inactif.

Tableau 137. Etapes de collecte et de traitement des données

Etape ou phase	Description
Etape de collecte des données	Durant cette étape, Network Manager interroge le réseau pour obtenir des informations sur le périphérique à l'aide des composants outil de recherche, agent et auxiliaire de DISCO. L'étape de collecte de données est subdivisée en trois phases qui sont décrites dans cette table.
Collecte de données : phase une	Durant cette phase, les outils de recherche identifient les périphériques sur le réseau. La phase une se termine lorsque le *taux de recherche* du périphérique descend sous un certain niveau. Pour chaque périphérique reconnu, les agents extraient les détails, les adresses IP associées au périphérique et les informations de connectivité.
Collecte des données : phase deux	Durant cette phase, un agent extrait les données de mappage d'adresses IP sur des adresses MAC.

Tableau 137. Etapes de collecte et de traitement des données (suite)

Etape ou phase	Description
Collecte de données : phase trois	Durant cette phase, les agents téléchargent toutes les informations concernant les tables de base de données de réacheminement des commutateurs de réseau et émettent des commandes PING à l'attention de tous les périphériques afin de confirmer la précision des contenus de ces tables.
Etape de traitement des données	Durant cette étape, Network Manager déduit la topologie du réseau sur la base des données collectées durant l'étape de collecte des données. Les programmes stitcher analysent les données collectées et génèrent une topologie du réseau qui inclut les données de connectivité et de confinement.

Concepts associés:

«Etapes et phases de reconnaissance»
Le processus de reconnaissance peut être séparé en deux étapes : collecte et traitement des données. Les étapes se divisent en deux phases.

«Cycles de reconnaissance», à la page 348
Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

«Etape de collecte des données», à la page 343
L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

«Etape de traitement des données», à la page 343
La déduction de la topologie a lieu lors de l'étape de traitement des données, alors que les informations provenant de la collecte des données sont analysées, interprétées et traitées par les programmes stitcher. L'étape de traitement des données atteint son paroxysme avec la génération du modèle de confinement.

Etapes et phases de reconnaissance

Le processus de reconnaissance peut être séparé en deux étapes : collecte et traitement des données. Les étapes se divisent en deux phases.

Concepts associés:

«Minutage de la reconnaissance», à la page 340
Chaque reconnaissance complète consiste en un ou plusieurs cycles de reconnaissance. La division d'une reconnaissance complète en plusieurs cycles de reconnaissance permet à la reconnaissance de s'achever au moment opportun.

«Cycles de reconnaissance», à la page 348
Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

Tâches associées:

«Surveillance de l'avancement de la reconnaissance», à la page 173
Vous pouvez utiliser l'onglet **Surveillance** pour surveiller la progression de la reconnaissance au cours de chacune des phases de reconnaissance.

Etape de traitement des données

La déduction de la topologie a lieu lors de l'étape de traitement des données, alors que les informations provenant de la collecte des données sont analysées, interprétées et traitées par les programmes stitcher. L'étape de traitement des données atteint son paroxysme avec la génération du modèle de confinement.

L'étape de traitement des données correspond à la création de la topologie. C'est la dernière étape conceptuelle du cycle de reconnaissance.

Les étapes de traitement et de collecte des données se chevauchent généralement car vous pouvez configurer les programmes stitcher pour qu'ils commencent à traiter les informations de connectivité de différents agents de reconnaissance avant que l'opération principale d'assemblage ne commence.

Concepts associés:

«Minutage de la reconnaissance», à la page 340
Chaque reconnaissance complète consiste en un ou plusieurs cycles de reconnaissance. La division d'une reconnaissance complète en plusieurs cycles de reconnaissance permet à la reconnaissance de s'achever au moment opportun.

«Création de la topologie», à la page 355
La création de la topologie s'effectue en plusieurs étapes.

Etape de collecte des données

L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

Phase une

Lors de la phase une de la collecte de données, les outils de recherche identifient tous les périphériques existant sur le réseau. Généralement, une phase peut être terminée lorsque tous les processus lancés ont fini de fonctionner. Toutefois, même si vous vouliez attendre la fin de la reconnaissance de tous les périphériques par les outils de recherche avant de passer à la phase deux, il est inefficace d'entraver le processus de reconnaissance en attendant indéfiniment. La phase une s'achève par conséquent lorsque le *taux de recherche* descend sous un niveau donné, déterminé par l'absence de périphériques reconnus pour la durée indiquée dans `disco.config.m_NothingFndPeriod`.

Les étapes conceptuelles du cycle reconnaissance, indiquées ci-dessous, ont lieu lors de la phase une de la collecte de données :

- Reconnaissance de l'existence des périphériques
- Reconnaissance des détails des périphériques (standard)
- Reconnaissance d'adresses de périphériques associées
- Reconnaissance de la connectivité des périphériques

Agents appartenant à la phase une

Certains agents renvoient des données pouvant être utilisées pour rechercher d'autres périphériques, par exemple l'adresse IP de voisins distants ou le sous-réseau dans lequel existe un voisin local. Ce mécanisme est connu en tant que *retour d'informations*.

Le programme stitcher Feedback gère le retour d'informations en transmettant les informations renvoyées par les agents aux outils de recherche de commandes PING afin qu'elles soient inclues à la reconnaissance. Toutefois, l'état inactif permet d'assurer qu'aucun agent impliqué dans le processus de retour d'informations doive être exécuté lors de la phase une pour les périphériques devant être reconnus durant le cycle de reconnaissance en cours.

La phase une implique généralement que les agents de reconnaissance de commutateurs téléchargent toutes les informations sur le réseau local virtuel et l'interface.

Etat d'inactivité

A l'issue de la phase une, la reconnaissance entre en *état inactif*. Les outils de recherche ont reconnu l'existence d'une majorité de périphériques pré-déterminée sur le réseau. Toute nouvelle adresse de périphérique reconnue à l'état inactif, soit par les outils de recherche, soit par un agent de reconnaissance, est placée dans la table de base de données finders.pending.

Les périphériques figurant dans la table de base de données finders.pending seront traités lors de la prochaine reconnaissance. S'il existe des périphériques dans la table de base de données finders.pending, la prochaine reconnaissance débute dès que celle en cours est achevée.

Phase deux

Une fois le critère d'achèvement de la phase une rempli, la phase deux débute. Afin de mapper les couches deux et trois du modèle OSI, l'agent de reconnaissance de cache ARP remplit le serveur auxiliaire à l'aide de données ARP, c'est-à-dire une liste de résolution d'adresses IP de périphériques sur des adresses MAC.

Avant que la reconnaissance puisse passer de la phase deux à la phase trois, les processus de la phase deux doivent arrêter de fonctionner. Un agent est considéré comme ayant terminé de fonctionner lorsque toutes les entités de sa table .despatch se trouvent également dans la table .returns.

Les agents sont multitâches et les enregistrements des périphériques reconnus transmis aux agents sont référencés avec une phase donnée. Par conséquent, un agent peut traiter des périphériques en deux phases séparées, à n'importe quel moment. Si aucune action devant avoir eu lieu lors de la phase deux n'est détectée après le début de la phase trois, celle-ci se poursuit alors que l'agent s'exécute en phase deux.

Phase trois

Au moment de la phase trois, le processus de reconnaissance connaît parfaitement les périphériques existant au sein du réseau (acquis de la phase une) et a accès aux mappages complets des adresses IP sur des adresses MAC pour tous les périphériques du serveur auxiliaire (acquis de la phase deux). Les agents de commutateur peuvent maintenant effectuer le téléchargement de toutes les informations concernant les tables de base de données de réacheminement des commutateurs réseau tout en émettant une commande PING à l'attention de tous les périphériques pour confirmer la précision des contenus des tables.

Lorsque la phase trois est terminée, c'est-à-dire lorsque l'exécution de tous les processus planifiés pour la phase est terminée, la reconnaissance est prête à passer

de l'étape de collecte des données à l'étape de traitement de ces dernières, durant laquelle toutes les informations de connectivité sont associées pour générer une topologie de réseau.

Impact de l'approche par étapes et par phases sur les processus DISCO

La division de l'étape de collecte des données en plusieurs phases affecte tous les processus impliquée dans la reconnaissance et la déduction de la topologie du réseau car les phases sont traitées dans l'ordre. Une phase donnée ne peut pas commencer avant que les critères d'achèvement de la phase précédente soient remplis.

Tous les processus de DISCO doivent par conséquent disposer d'une ou plusieurs phases associées durant lesquelles ils sont autorisés à fonctionner. Alors que les outils de recherche sont généralement configurés pour s'exécuter durant toutes les phases, il se peut que vous vouliez configurer certains agents de reconnaissance pour qu'ils ne fonctionnent que durant une ou plusieurs phases spécifiques. La flexibilité de DISCO vous permet d'avoir des processus suffisamment intelligents pour se comporter différemment lorsqu'ils fonctionnent sur plusieurs phases et qui peuvent transmettre le contrôle aux autres processus ou arrêter de fonctionner jusqu'au début de leur prochaine phase opérationnelle.

Concepts associés:

«Minutage de la reconnaissance», à la page 340
Chaque reconnaissance complète consiste en un ou plusieurs cycles de reconnaissance. La division d'une reconnaissance complète en plusieurs cycles de reconnaissance permet à la reconnaissance de s'achever au moment opportun.

«Reconnaissance de l'existence des périphériques», à la page 348
La reconnaissance de l'existence du périphérique s'effectue en plusieurs étapes.

«Reconnaissance des détails du périphérique (standard)», à la page 350
La reconnaissance standard des détails du périphérique s'effectue en plusieurs étapes.

«Reconnaissance d'adresses de périphériques associées», à la page 352
Il existe plusieurs étapes dans le flux de processus lors de la reconnaissance d'adresses de périphériques associées.

«Reconnaissance de la connectivité des périphériques», à la page 354
La reconnaissance de la connectivité des périphériques s'effectue en plusieurs étapes.

Avantages de la reconnaissance par étapes

Plusieurs raisons expliquent pourquoi il est avantageux d'appliquer une approche par étapes et par phases à la reconnaissance.

Connectivité du commutateur

Pour déterminer la connectivité de certains périphériques, l'agent de reconnaissance doit parfois connaître tous les périphériques existants avant de rechercher des variables Management Information Base (MIB) spécifiques, en particulier si les informations recherchées sont transitoires.

Exemple : lorsque les agents de couche 2 reconnaissent la connectivité entre les commutateurs Ethernet. Ces derniers ont transmis les tables de base de données qui expirent dans le temps. Par conséquent, pour vous assurer qu'un commutateur

dispose d'une table de base de données complètement remplie au moment de l'interrogation, vous pouvez émettre une commande PING à destination de tous les périphériques associés au commutateur.

Vous devez alors configurer les agents de reconnaissance de commutateurs afin qu'ils exécutent d'autres tâches de traitement lors de la phase une de la collecte de données. Une fois que les agents ont reçu le signal marquant la fin de la phase une (ce qui signifie que tous les périphériques ont été détectés), ils peuvent démarrer les opérations de phase deux. Par exemple, ils peuvent émettre une commande PING à l'attention de tous les périphériques situés dans le domaine de reconnaissance en même temps qu'ils téléchargent les tables de base de données de tous les commutateurs Ethernet.

Mappage des limites de sous-réseau

Une limite de la configuration d'agents de reconnaissance individuels afin qu'ils effectuent directement les requêtes ARP à partir du serveur auxiliaire est que l'auxiliaire ARP ne peut pas s'exécuter simultanément sur plusieurs sous-réseaux sauf s'il est configuré de telle sorte. Afin de résoudre ce problème, utilisez un agent de reconnaissance spécifique au cache ARP imitant un agent de reconnaissance générique (dans le sens où des entités peuvent lui être envoyées) mais pouvant également mapper des limites ou différentes couches du modèle OSI.

L'agent de reconnaissance de cache ARP peut rechercher des caches ARP existant sur les routeurs. Il utilise ces informations pour remplir la base de données de l'auxiliaire ARP se trouvant sur le serveur auxiliaire et pour créer un mappage complet d'une adresse IP sur une adresse MAC pour le périphérique, sans devoir se baser sur l'auxiliaire ARP.

Cette approche peut être appliquée lors de l'utilisation des agents de reconnaissance de commutateurs devant effectuer une résolution d'une adresse IP sur une adresse MAC avant de pouvoir commencer à fonctionner. En suivant l'exemple ci-dessus, vous pouvez configurer votre étape de collecte de données de reconnaissance afin qu'elle soit subdivisée en trois phases :

- Phase une : rechercher tous les périphériques existant sur le réseau.
- Phase deux : utiliser l'agent de reconnaissance de cache ARP pour remplir le serveur auxiliaire avec des mappages d'adresses IP sur des adresses MAC.
- Phase trois : émettre une commande PING à l'attention de tous les périphériques et appeler les agents de reconnaissance de commutateurs en téléchargeant les tables de bases de données de réacheminement pour tous les commutateurs se trouvant sur le réseau à l'aide de mappages d'adresses IP sur des adresses MAC déterminés lors de la phase deux.

Agents de reconnaissance à phases multiples

La division de l'étape de collecte de données en deux phases peut également avoir pour conséquence la possibilité de configurer les agents de reconnaissance afin qu'ils effectuent diverses opérations durant les différentes phases.

Même si un agent de reconnaissance est programmé pour commencer à fonctionner lors de la phase deux, il peut aussi effectuer certaines opérations lors de la phase une. Cette manoeuvre est possible car la fin de la phase une signifie uniquement que tous les périphériques ont été reconnus. L'agent peut être configuré pour effectuer d'autres actions comme le téléchargement d'interfaces, l'émission de requêtes Telnet ou le téléchargement d'autres variables MIB lors de la

phase une. Ce n'est qu'après le début de la phase deux que l'agent commence à traiter les instructions spécifiques à la phase deux.

Conseil : Il est d'usage de configurer la reconnaissance afin qu'elle se produise en plusieurs phases, assurant ainsi une précision maximale de la topologie déduite.

Impact de la division de la reconnaissance en plusieurs phases sur le trafic du réseau

L'un des principaux avantages de la division en phases est la réduction du trafic sur le réseau.

Comme les types similaires de requêtes de réseau sont regroupées en phases, les données peuvent être placées dans la mémoire cache sur le serveur auxiliaire afin de réduire la charge du réseau. Le serveur auxiliaire est l'intermédiaire entre les agents de reconnaissance et le réseau et peut fusionner plusieurs commandes PING du même périphérique en un seul bloc de sorte qu'elles soient résolues en une seule commande PING.

Le serveur auxiliaire dispose également d'un pool de requête qui vérifie que celui-ci ne surcharge pas le réseau. Le pool de requête exécute cette tâche en limitant le nombre de requêtes simultanées auxquelles le réseau doit faire face.

Critères de multiphasage

Le critère principal lors de la configuration d'une reconnaissance à phases multiples est d'évaluer les exigences des différentes opérations devant être effectuées lors du processus de reconnaissance. Les agents de reconnaissance basés sur le système Ethernet nécessitent, par exemple, au moins deux phases. Il est possible d'avoir des agents de reconnaissance pouvant fonctionner lors de n'importe quelle phase.

Gestion des phases

Les différentes phases de la collecte des données de reconnaissance sont gérées par un *gestionnaire de phases* interne.

Le gestionnaire de phases :

- Lit le nombre de phases maximal total et calcule la somme des phases lorsque tous les fichiers de définitions d'agent de reconnaissance et de programme stitcher sont chargés.
- Calcule les dépendances de phase et de processus, c'est-à-dire les agents de reconnaissance dont l'exécution est planifiée, et ce pour chaque phase.
- Surveille les processus en cours d'exécution durant les phases.

Lorsque le gestionnaire de phases détecte que tous les processus de la phase en cours son terminés, il envoie un signal indiquant la fin de la phase pour tous les processus qui attendent d'être lancés durant la prochaine phase.

Cycles de reconnaissance

Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

Le flot de données de reconnaissance peut être catégorisé en étapes contextuelles :

- Reconnaissance de l'existence du périphérique
- Reconnaissance des détails du périphérique (standard)
- Reconnaissance des détails des périphériques (contextuels)
- Reconnaissance d'adresses de périphériques associées
- Reconnaissance de la connectivité du périphérique
- Création de la topologie

Ces étapes suivent le flot de données de reconnaissance dans l'ordre, du début à la fin, à l'exception de la reconnaissance des détails des périphériques (contextuelle), qui remplace la reconnaissance des détails des périphériques (standard) s'il s'agit d'une reconnaissance contextuelle.

Concepts associés:

«Minutage de la reconnaissance», à la page 340
Chaque reconnaissance complète consiste en un ou plusieurs cycles de reconnaissance. La division d'une reconnaissance complète en plusieurs cycles de reconnaissance permet à la reconnaissance de s'achever au moment opportun.

«Etapes et phases de reconnaissance», à la page 342
Le processus de reconnaissance peut être séparé en deux étapes : collecte et traitement des données. Les étapes se divisent en deux phases.

«Processus de reconnaissance avec intégration EMS», à la page 358
Network Manager collecte les données topologiques d'un système de gestion d'éléments à l'aide de collecteurs.

Reconnaissance de l'existence des périphériques

La reconnaissance de l'existence du périphérique s'effectue en plusieurs étapes.

La figure 2, à la page 349 montre comment l'existence initiale de périphériques est reconnue.

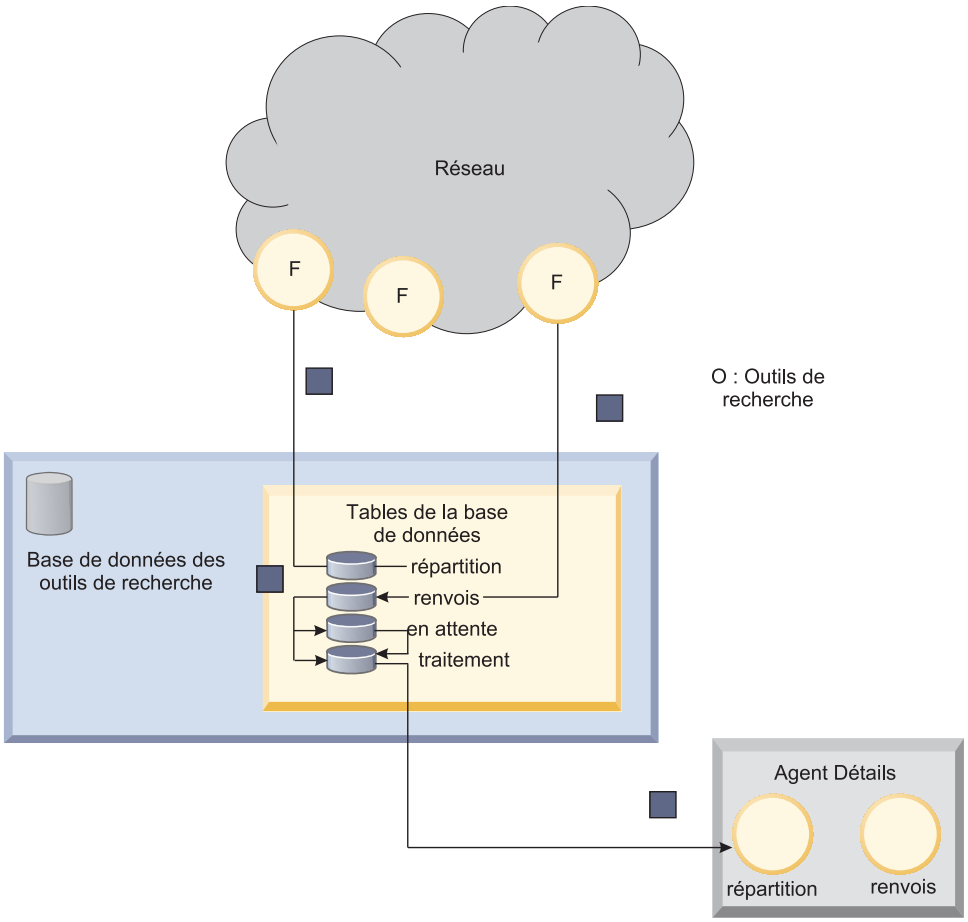

Figure 2. Flux de processus de reconnaissance : existence du périphérique

Le flux de processus affiché dans la figure 2 est décrit ci-après.

1 : les outils de recherche reçoivent leurs instructions de leurs fichiers de configuration et des insertions faites dans la table finders.despatch, puis recherchent des périphériques sur le réseau.

2 : les outils de recherche renvoient les informations sur l'existence du périphérique à la table finders.returns.

3 : une fois que les informations sur l'existence du périphérique sont placées dans la table finders.returns de la mémoire cache, un programme stitcher les déplace dans la table finders.processing. Cela signifie que l'entité réseau est en cours de traitement par DISCO. Si la reconnaissance est à l'état inactif, les informations sont placées dans la table finders.pending.

4 : un programme stitcher déplace les informations concernant l'existence du périphérique de la table finders.processing vers la table Details.despatch, les préparant ainsi au traitement par l'agent Details.

Concepts associés:

«Etape de collecte des données», à la page 343
L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

Reconnaissance des détails du périphérique (standard)

La reconnaissance standard des détails du périphérique s'effectue en plusieurs étapes.

La figure 3 montre comment les détails du périphérique sont reconnus lors d'une reconnaissance standard.

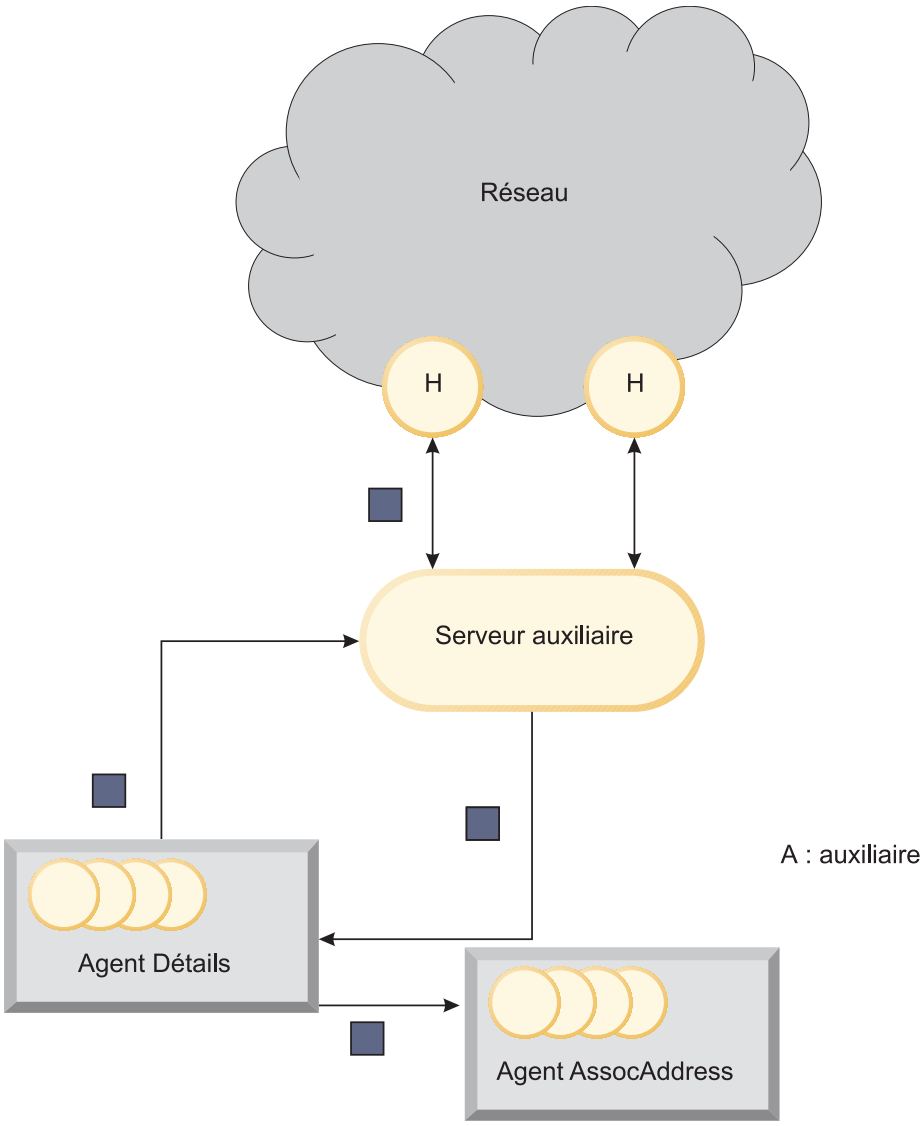

Figure 3. Flux de processus de reconnaissance : détails du périphérique (standard)

Le flux de processus affiché dans la figure 3 est décrit ci-après.

1 : toutes les tables Agent.despatch sont actives de sorte qu'une insertion dans la table Details.despatch pousse l'agent Détails à reconnaître automatiquement les informations de base du périphérique et à déterminer si l'accès SNMP au périphérique est disponible ou non.

2 : l'agent Details interroge le réseau via le serveur auxiliaire. Les requêtes sont placées dans la mémoire cache afin de réduire la fréquence à laquelle les auxiliaires (représentés par la lettre H dans figure 3) doivent interroger directement le réseau.

3 : les informations extraites du réseau sont renvoyées à la table Details.returns.

4 : les informations figurant dans la table Details.returns sont transmises à la table .despatch de l'agent Associated Address (AssocAddress) pour traitement.

Concepts associés:

«Etape de collecte des données», à la page 343
L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

Reconnaissance des détails des périphériques (contextuels)

La reconnaissance des détails contextuels des périphériques s'effectue en plusieurs étapes.

La figure 4 montre comment les détails des périphériques sont reconnus lors d'une reconnaissance contextuelle.

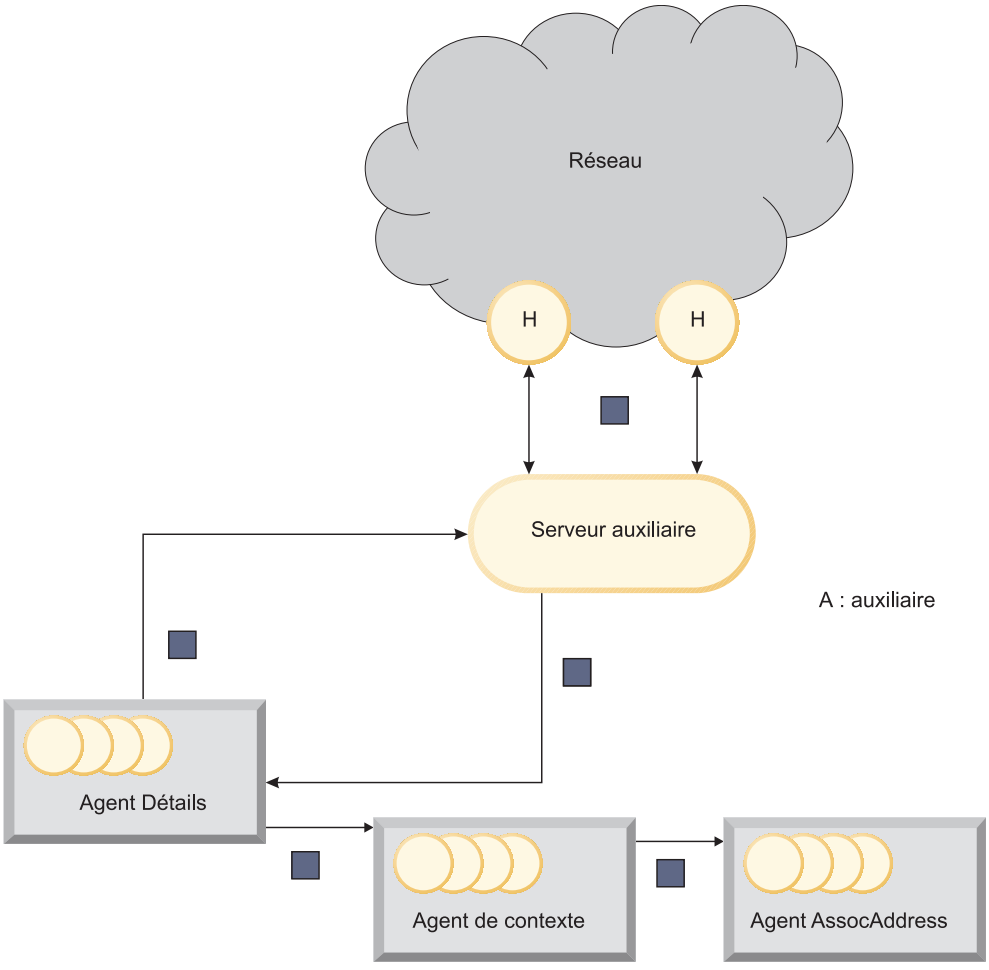

Figure 4. Flux de processus de reconnaissance : détails des périphériques (contextuels)

Le flux de processus affiché dans la figure 4 est décrit ci-après.

1 : toutes les tables Agent.despatch sont actives de sorte qu'une insertion dans la table Details.despatch pousse l'agent Details à reconnaître

automatiquement les informations de base du périphérique et à déterminer si l'accès SNMP au périphérique est disponible ou non.

2 : l'agent Details interroge le réseau via le serveur auxiliaire. Les requêtes sont placées dans la mémoire cache afin de réduire la fréquence à laquelle les auxiliaires doivent interroger directement le réseau.

3 : les informations extraites du réseau sont renvoyées à la table Details.returns.

4 : les informations figurant dans la table Details.returns sont transmises à la table .despatch de l'agent Context approprié, qui ajoute à son tour des balises contextuelles.

5 : lorsque l'agent Context a terminé leur traitement, les informations sont transmises à la table .despatch de l'agent Associated Address (AssocAddress) pour traitement.

Concepts associés:

«Reconnaissance contextuelle», à la page 9
Si vous devez reconnaître des périphériques comme des périphériques SMS, MPLS Edge ou autres à l'aide de routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. Ce type de reconnaissance permet une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type particulier de périphériques est pris en charge par la reconnaissance.

Tâches associées:

«Configuration d'une reconnaissance contextuelle», à la page 139
Si vous disposez d'unités que vous devez reconnaître, comme des unités périphériques SMS, MPLS ou d'autres unités comportant des routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. La reconnaissance contextuelle garantit une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type d'unité est pris en charge par la reconnaissance.

Référence associée:

«Fichier de configuration DiscoConfig.cfg», à la page 74
Le fichier de configuration DiscoConfig.cfg permet à l'outil de recherche Ping de vérifier automatiquement les unités découvertes par l'outil de recherche de fichiers et de permettre une reconnaissance contextuelle.

Reconnaissance d'adresses de périphériques associées

Il existe plusieurs étapes dans le flux de processus lors de la reconnaissance d'adresses de périphériques associées.

La figure ci-après montre comment les adresses de périphériques associées sont reconnues.

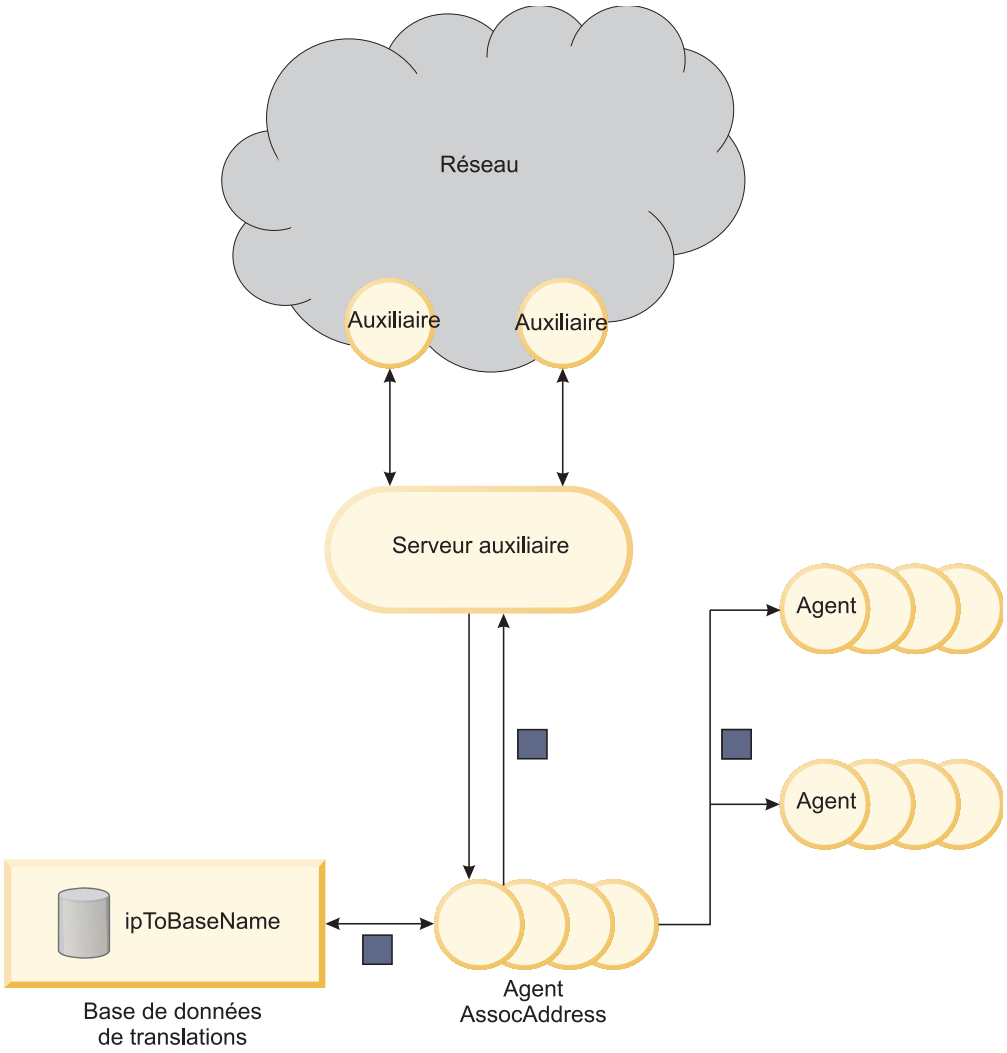

Figure 5. Flux de processus de reconnaissance : adresses de périphériques associées

Le flux de processus ci-après décrit la figure 5 :

1 : l'agent Associated Address utilise le serveur auxiliaire pour télécharger toutes les adresses IP associées aux interfaces du périphérique en cours d'examen.

2 : l'agent Associated Address vérifie les adresses IP sur la base du registre d'adresses, à savoir la table translations.ipToBaseName. Les détails sont également ajoutés à ce registre. Si le périphérique a déjà été reconnu par une autre de ses adresses (c'est-à-dire si la table translations.ipToBaseName contient déjà un enregistrement pour ce périphérique), les détails du périphérique ne sont pas envoyés aux agents de reconnaissance.

3 : Si le périphérique n'a pas encore été reconnu, les programmes stitcher transmettent les détails aux agents de reconnaissance appropriés, comme indiqué dans le fichier de configuration `DiscoAgents.cfg`.

Concepts associés:

«Etape de collecte des données», à la page 343
L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

Reconnaissance de la connectivité des périphériques

La reconnaissance de la connectivité des périphériques s'effectue en plusieurs étapes.

La figure ci-après montre comment la connectivité des périphériques est reconnue et comment les périphériques sont reconnus de manière répétitive.

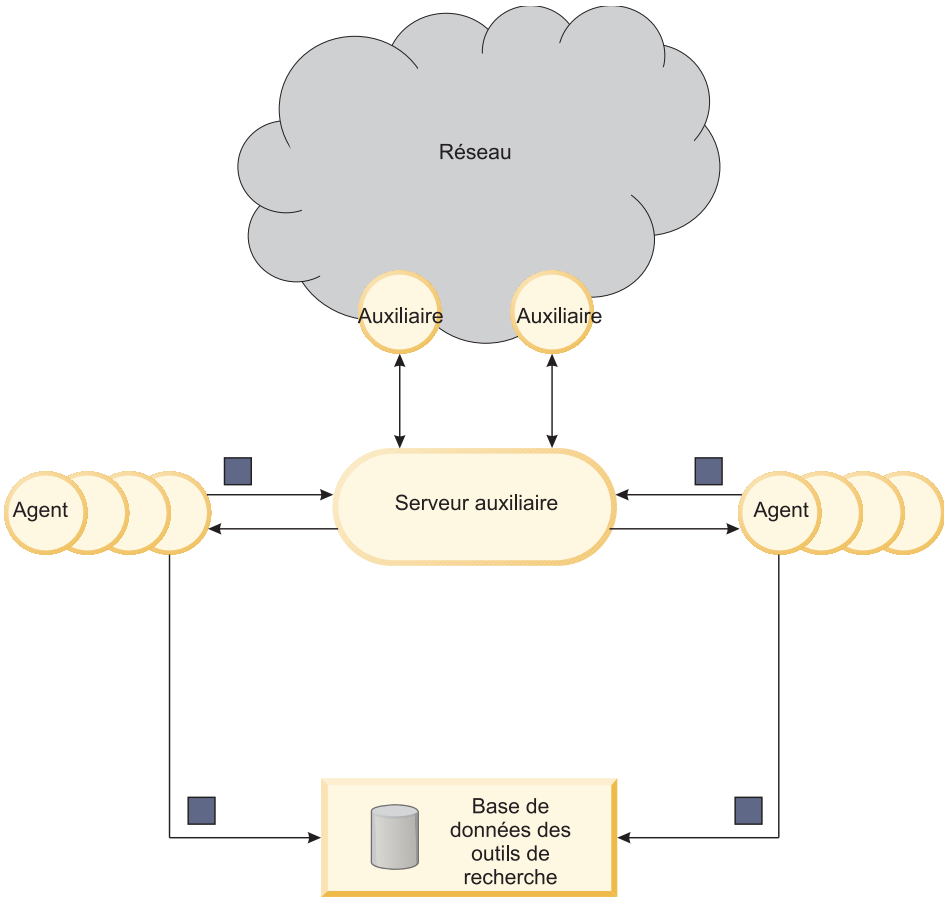

Figure 6. Flux de processus de reconnaissance : connectivité des périphériques

Le flux de processus ci-après décrit la figure 6 :

1 : lorsque les informations sont insérées dans la table `despatch` d'un agent de reconnaissance, l'agent tente de reconnaître les informations de connectivité pour ce périphérique. L'agent définit un lien de données basé sur le socket TCP avec le serveur auxiliaire et demande les informations de connectivité adéquates.

2 : un programme stitcher transmet l'adresse des voisins distants du périphérique et l'adresse du sous-réseau ou les adresses du périphérique à un outil de recherche en vue de la reconnaissance. Il se peut que ces adresses n'existent pas ou qu'elles ne figurent pas dans la portée de reconnaissance indiquée. C'est la raison pour laquelle les adresses doivent s'exécuter via le processus de reconnaissance dès le début.

Concepts associés:

«Etape de collecte des données», à la page 343
L'étape de collecte des données implique l'interrogation du réseau afin d'obtenir des informations sur le périphérique et de générer ainsi une topologie du réseau. DISCO utilise les outils de recherche, les agents et les auxiliaires lors de cette étape. Cette dernière peut être subdivisée en un certain nombre de phases.

Création de la topologie

La création de la topologie s'effectue en plusieurs étapes.

La figure ci-après montre un flot de données simplifié pour la création de la topologie à partir des données brutes renvoyées par les agents de reconnaissance.

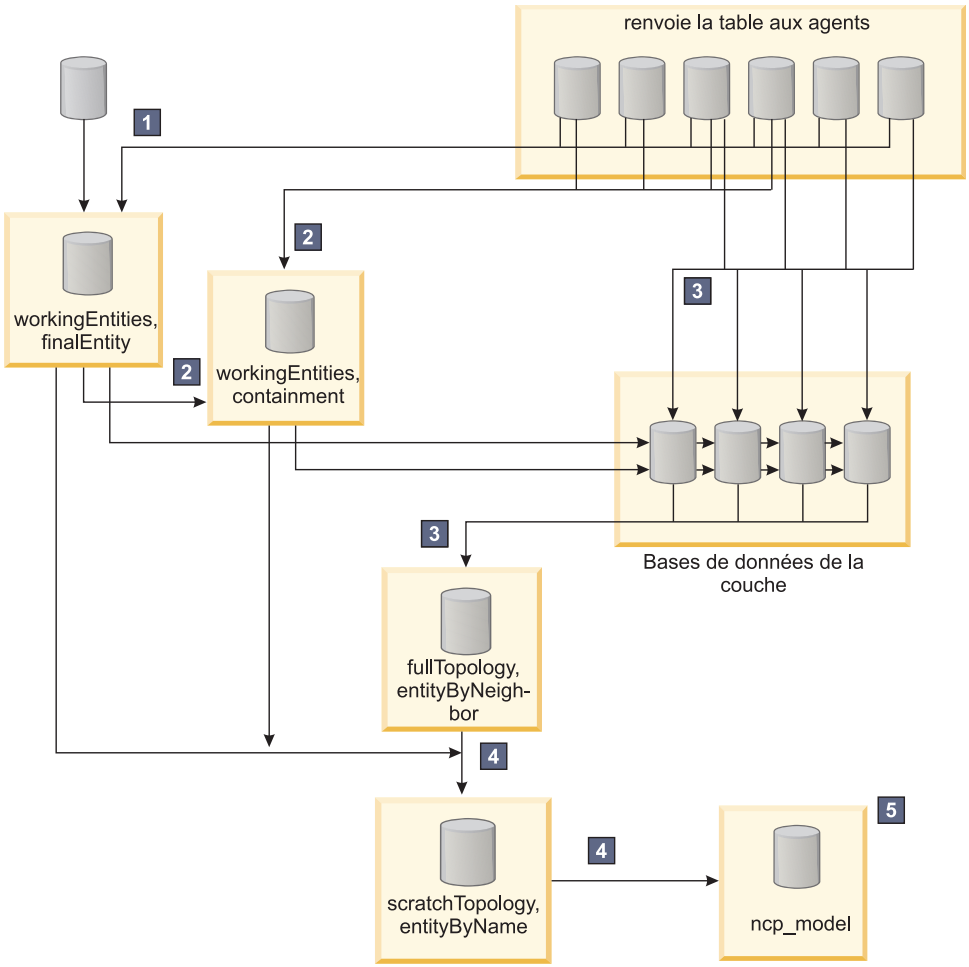

Figure 7. Flux de processus de reconnaissance : création de la topologie

Le flux de processus ci-après décrit le flot de données.

1 : une fois que tous les agents de reconnaissance ont terminé et que la reconnaissance a entré l'état de traitement des données, des programmes stitcher destinés à traiter des données spécifiques interagissent avec les bases de données des agents de reconnaissance pour générer la table workingEntities.finalEntity.

2 : les programmes stitcher utilisent un sous-ensemble de tables contenant les renvois des agents ainsi que la table workingEntities.finalEntity pour déduire et créer le modèle de confinement. Ce modèle est stocké dans la table workingEntities.containment.

3 : les programmes stitcher utilisent un autre sous-ensemble de tables contenant les renvois des agents ainsi que les tables workingEntities.finalEntity et workingEntities.containment pour créer les différentes couches topologiques qui sont stockées dans les tables de bases de données de couches. Le jeu complet des couches est fusionné dans la table fullTopology.entityByNeighbor.

4 : Les programmes stitcher fusionnent les trois tables produites (workingEntities.finalEntity, workingEntities.containment et fullTopology.entityByNeighbor) pour créer le modèle réseau.

5 : Le gestionnaire de topologie, `ncp_model`, instancie chaque élément de réseau (sujet au filtre d'instanciation) et envoie la topologie aux autres composants.

Concepts associés:

«Etape de traitement des données», à la page 343
La déduction de la topologie a lieu lors de l'étape de traitement des données, alors que les informations provenant de la collecte des données sont analysées, interprétées et traitées par les programmes stitcher. L'étape de traitement des données atteint son paroxysme avec la génération du modèle de confinement.

Diffusion de données de reconnaissance

Au terme d'une reconnaissance, le gestionnaire de topologie, ncp_model, utilise le bus de messages pour recevoir des mises à jour de topologie provenant de la reconnaissance et pour transmettre ces mises à jour au bus de messages où d'autres processus tels que la passerelle d'événements peuvent extraire ces mises à jour. En outre, ncp_model utilise également ces mises à jour pour actualiser la base de données topologiques NCIM.

Les données sont stockées dans deux formats :

- Format de cache NCIM
- Format master.entityByName existant

Les objectifs des formats de stockage sont les suivants :

Format de cache NCIM
Les données dans ce format sont utilisées pour insérer des mises à jour sur le bus de messages pour d'autres processus tels que la passerelle d'événements, ncp_g_event

Format master.entityByName existant
Les données dans ce format sont utilisées par ncp_model pour mettre à jour la base de données topologiques NCIM :

Le format de cache NCIM est décrit dans le document *IBM Tivoli Network Manager IP Edition - Guide de référence de la base de données topologiques*.

Options de configuration de reconnaissance avancées

Utilisez ces informations pour comprendre comment configurer le flot de données du processus de reconnaissance et le téléchargement des tables de routage complètes.

Flot de données de reconnaissance configurable

Le flot de données du processus de reconnaissance est configurable par l'utilisateur. Les programmes stitcher contrôlent le déplacement des données entre les bases de données, et vous pouvez personnaliser le processus de reconnaissance en changeant la manière dont les programmes stitcher sont déclenchés et fonctionnent.

Déclencheurs de programmes stitcher et d'agents

Vous pouvez modifier le flot de données en changeant les critères qui déclenchent le déploiement des programmes stitcher et des agents de reconnaissance en modifiant les programmes stitcher et, s'il y a lieu, les définitions des agents. Voici quelques déclencheurs typiques :

- Données insérées dans une table de base de données spécifique
- Un programme stitcher ou un agent de reconnaissance exécutant sa tâche
- La fin d'une phase de reconnaissance

Tous les changements que vous faites sont automatiquement détectés par DISCO lors de son analyse périodique de l'agent et des fichiers des programmes stitcher (la fréquence d'analyse est déterminée par l'entrée dans la base de données disco.config). Lorsqu'il détecte des changements, DISCO modifie ses bases de données de définitions d'agent et de programme stitcher en conséquence et applique ces changements au prochain cycle de reconnaissance.

Pour obtenir plus de détails sur les programmes stitcher et leur langage, consultez le manuel *IBM Tivoli Network Manager IP Edition Language Reference Guide*.

Programmes stitcher sur demande

Les programmes stitcher peuvent être démarrés sur demande. Si vous insérez un programme stitcher dans la base de données stitchers.actions, DISCO exécute automatiquement le programme stitcher. Cela signifie que le cycle de reconnaissance peut être démarré à n'importe quel point et que les actions futures peuvent être configurées pour démarrer lorsque le programme stitcher a terminé sa tâche.

Référence associée:

«Table stitchers.actions», à la page 272
Si un programme stitcher est inséré dans la table stitchers.actions, DISCO l'exécute. Une fois que le programme stitcher s'est terminé, son entrée est supprimée de la table stitchers.actions. Tout programme stitcher déclenché pour être exécuté à partir du programme stitcher inséré, ou à la fin du programme stitcher, est également exécuté.

Correspondance partielle

Par défaut, le processus de reconnaissance utilise la correspondance par défaut, ce qui signifie que les agents de reconnaissance n'ont pas besoin de télécharger les tables complètes de routage lors de la reconnaissance.

Vous ne devez pas modifier les fichiers de définitions de l'agent de reconnaissance pour pouvoir utiliser la correspondance partielle. Toutefois, il est possible d'empêcher les agents de reconnaissance IpForwardingTable et IpRoutingTable d'utiliser la correspondance partielle dans certains cas si vous avez des périphériques sur votre réseau qui ne la prennent pas en charge.

Pour bloquer la correspondance partielle sur certains périphériques, vous devez indiquer les périphériques ne la prenant pas en charge dans la section `DiscoRouterPartialMatchRestrictions();` du fichier de définitions `IpForwardingTable.agnt` (pour les périphériques modernes utilisant RFC2096) ou le fichier de définitions `IpRoutingTable.agnt` (pour les périphériques plus anciens utilisant RFC1213). Si un périphérique reconnu correspond au filtre indiqué dans la section `DiscoRouterPartialMatchRestrictions();`, la correspondance partielle n'est pas tentée sur ce périphérique.

Processus de reconnaissance avec intégration EMS

Network Manager collecte les données topologiques d'un système de gestion d'éléments à l'aide de collecteurs.

Les étapes ci-après montrent comment Network Manager collecte les données topologiques d'un système de gestion d'éléments utilisant des collecteurs.

La reconnaissance basée sur les collecteurs peut être divisée en étapes contextuelles :

- Reconnaissance de l'existence du périphérique
- Reconnaissance des informations de base sur le périphérique
- Reconnaissance des informations détaillées sur le périphérique

Pour savoir comment Network Manager collecte des données topologiques depuis des EMS (Element Management Systems) et intègre ces données à la topologie reconnue, voir *IBM Tivoli Network Manager IP Edition - Présentation du produit*.

Concepts associés:

«Cycles de reconnaissance», à la page 348
Un cycle reconnaissance s'est produit lorsque le flot de données de reconnaissance d'un cycle a débuté puis s'est achevé. Une reconnaissance complète peut nécessiter plusieurs cycles.

Tâches associées:

«Configuration des reconnaissances EMS», à la page 113
Vous pouvez configurer Network Manager pour collecter des données topologiques depuis des EMS (Element Management Systems) et intégrer ces données à la topologie reconnue.

Reconnaissance de l'existence de périphériques à l'aide de collecteurs

Lors d'une reconnaissance de collecteur, la reconnaissance de l'existence de périphériques se déroule en plusieurs étapes.

figure 8 montre comment l'existence initiale de périphériques stockés sur les collecteurs est reconnue.

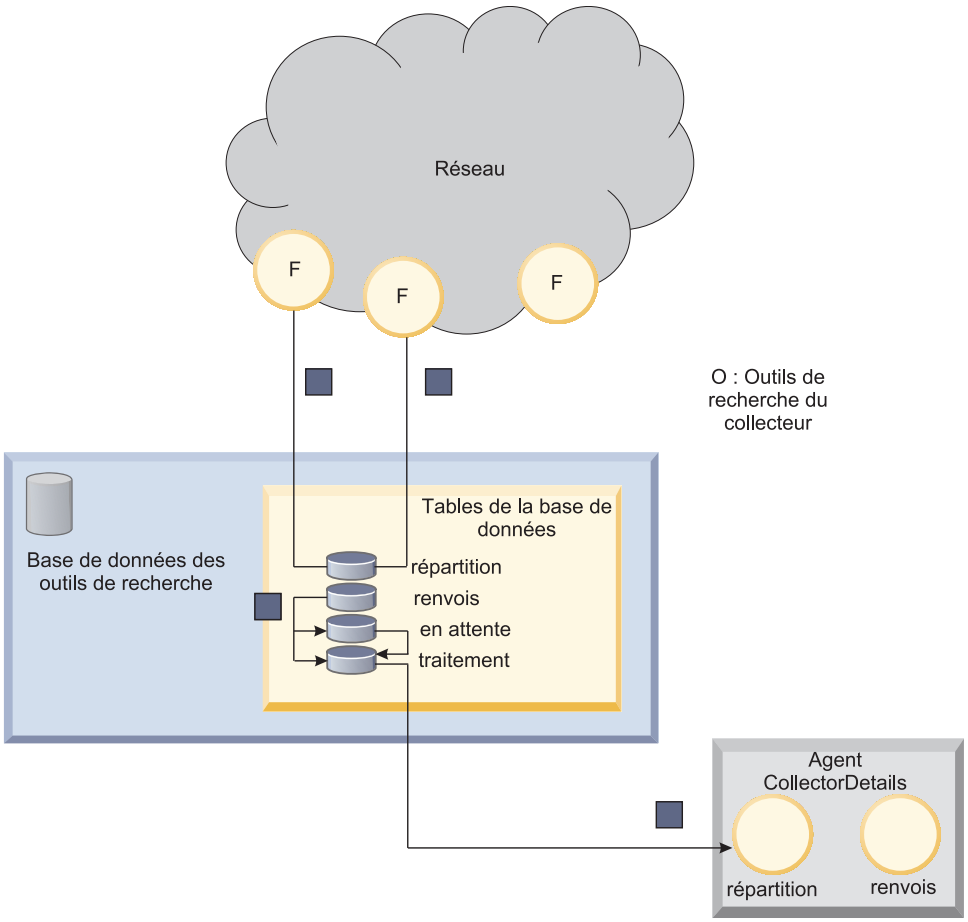

Figure 8. Flux de processus de reconnaissance de collecteur : reconnaissance de l'existence de périphériques

Le flux de processus ci-après décrit la figure 8:

1 : les outils de recherche de collecteurs reçoivent des instructions des fichiers de configuration puis examinent le réseau pour rechercher des collecteurs.

2 : les outils de recherche de collecteurs renvoient la liste des périphériques à la table finders.returns.

3 : immédiatement après que les informations sur l'existence des périphériques ont été placées dans la table finders.returns, le programme stitcher FnderRetProcessing les déplace vers la table finders.processing, pour signifier que l'entité de réseau est en cours de traitement. Si la reconnaissance est à l'état inactif, les informations sont placées dans la table finders.pending.

4 : le programme stitcher FnderProcToDetailsDesp déplace les informations concernant l'existence des périphériques de la table finders.processing vers la table CollectorDetails.despatch de sorte que l'agent CollectorDetails puisse traiter les informations.

Reconnaissance des informations de base sur le périphérique

Lors d'une reconnaissance de collecteur, la reconnaissance des informations de base sur le périphérique se déroule en plusieurs étapes.

La figure ci-après montre comment les détails de base sur le périphérique sont reconnus lors d'une reconnaissance de collecteur.

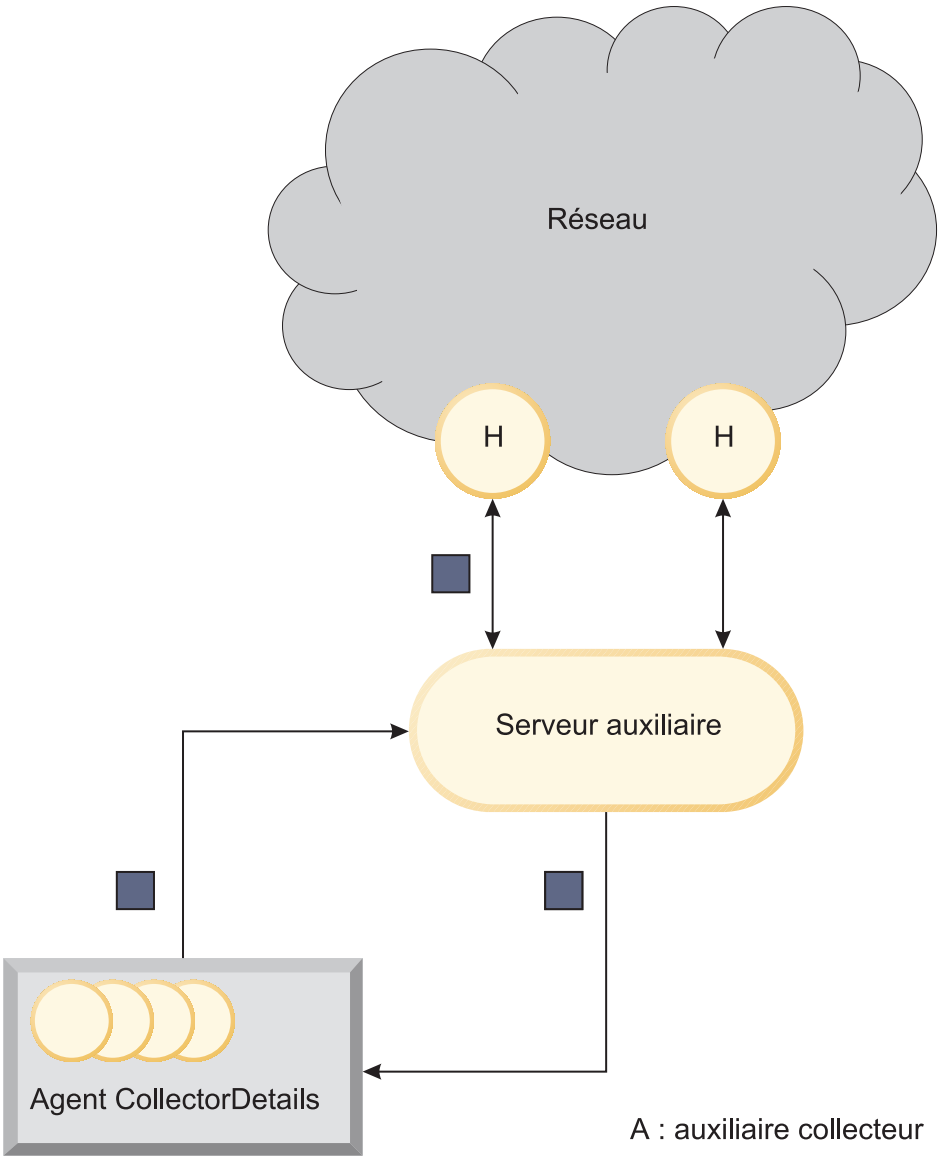

Figure 9. Flux de processus de reconnaissance de collecteur : reconnaissance des informations de base sur le périphérique

Le flux de processus ci-après décrit la figure 9:

1 : toutes les tables .despatch des agents sont actives de sorte qu'une insertion dans la table CollectorDetails.despatch déclenche automatiquement la reconnaissance des informations de base sur le périphérique, par l'agent CollectorDetails, à partir du collecteur.

2 : l'agent CollectorDetails utilise le serveur auxiliaire pour interroger le collecteur auxiliaire.

3 : les informations extraites du réseau sont renvoyées à la table CollectorDetails.returns.

Reconnaissance des informations détaillées sur le périphérique

Lors de la reconnaissance d'un collecteur, la reconnaissance des informations détaillées concernant le périphérique se déroule en plusieurs étapes.

La figure ci-après montre la manière dont les informations détaillées concernant le périphérique sont reconnues lors d'une reconnaissance de collecteur.

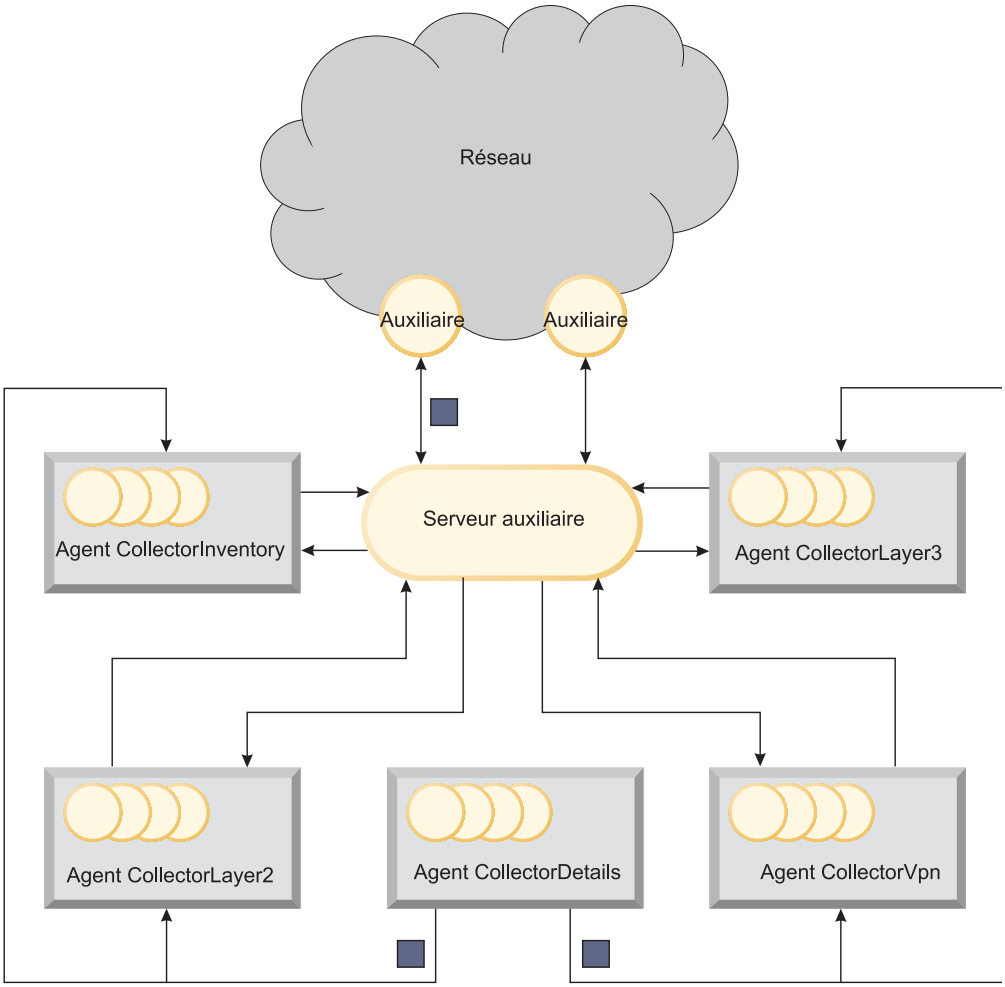

Figure 10. Flux de processus de reconnaissance de collecteur : informations détaillées concernant le périphérique

Le flux de processus ci-après décrit la figure 10:

1 : le programme stitcher CollectorDetailsRetProcessing transmet les informations de la table CollectorDetails.returns à la table .despatch des agents collecteurs suivants pour traitement : les agents CollectorInventory, CollectorLayer2, CollectorLayer3 et CollectorVpn

2 : l'insertion d'informations dans la table .despatch d'un agent déclenche une tentative de reconnaissance des informations concernant le périphérique par ce même agent. Les agents collecteurs interrogent les collecteurs pour reconnaître les informations ci-après pour chaque périphérique. L'agent CollectorInventory

reconnaît l'interface local, les informations de style MIB sur les entités et les adresses IP associées au périphérique. L'agent CollectorLayer2 rassemble les informations pour chaque connexion de couche 2 résolue de tous les périphériques traités. L'agent CollectorLayer3 rassemble les informations pour chaque connexion de couche 3 résolue de tous les périphériques traités. L'agent CollectorVpn rassemble toutes les informations de réseau privé virtuel pour chaque périphérique traité.

Nouvelle reconnaissance

Une fois la reconnaissance terminée, **ncp_disco** entre en mode nouvelle reconnaissance dans lequel la reconnaissance de nouveaux périphériques a pour conséquence des mises à jour du modèle topologique.

Nouvelle reconnaissance complète ou partielle

En modifiant les programmes stitcher, vous pouvez configurer la manière dont DISCO traite les périphériques détecter en mode nouvelle reconnaissance.

Par défaut, lorsque le système est en mode nouvelle reconnaissance et qu'un nouveau périphérique est détecté ou qu'un périphérique existant est modifié, le périphérique est reconnu à nouveau. Les programmes stitcher vérifient que la nouvelle reconnaissance du périphérique n'a lieu qu'une seule fois. Elles peuvent également vérifier que la modification n'a pas entraîné de modification dans la relation entre le périphérique et ses voisins. S'il y a lieu, les voisins du périphérique font l'objet d'une nouvelle reconnaissance. Si le nombre de périphériques devant faire l'objet d'une nouvelle reconnaissance en raison d'une modification dans la relation dépasse une certaine limite, le processus lance une nouvelle reconnaissance complète.

Concepts associés:

«A propos des types de reconnaissance», à la page 1
Différents termes sont utilisés pour décrire la reconnaissance de réseau, en fonction des objets découverts et du type de configuration de la reconnaissance. Vous pouvez exécuter des reconnaissances, de nouvelles reconnaissances, des reconnaissances complètes ou partielles et vous pouvez définir des reconnaissances automatiques.

Flux de processus du programme stitcher FnderRetProcessing

Pour configurer la manière dont DISCO traite les périphériques récemment reconnus, éditez le programme stitcher FnderRetProcessing.stch. Ce programme stitcher traite les entrées qui sont placée dans la table finders.returns.

Le flux de processus par défaut de le programme stitcher FnderRetProcessing.stch est le suivant :

1. Lorsqu'une entrée est placée dans la table finders.returns, le programme stitcher vérifie si le périphérique se trouve dans la portée de reconnaissance. Dans le cas contraire, il est ignoré.
2. Si le périphérique se trouve dans la portée de reconnaissance et si la valeur disco.status.m_DiscoveryMode=0, c'est-à-dire si DISCO est en mode reconnaissance, le programme stitcher déplace les détails sur le périphérique vers la table finders.pending afin qu'il soit traité ultérieurement (si la reconnaissance est à l'état inactif) ou vers la table finders.processing pour être traité immédiatement.
3. Si le périphérique se trouve dans la portée de reconnaissance et si la valeur disco.status.m_DiscoveryMode=1, c'est-à-dire si DISCO est en mode nouvelle

reconnaissance, le programme stitcher détermine si le périphérique doit faire l'objet d'une nouvelle reconnaissance. Par défaut, le programme stitcher effectue une nouvelle reconnaissance des :

- Périphériques pour lesquels la valeur finders.returns.m_Creator='Rediscovery'. Il n'existe aucun outil de recherche Rediscovery, mais cette colonne est définie sur 'Rediscovery' (nouvelle reconnaissance) par les autres programmes stitcher, telles que ProcRemoteConns.stch, pour indiquer que, suite à la nouvelle reconnaissance d'autres périphériques, ce périphérique doit faire l'objet d'une nouvelle reconnaissance.
- Tout périphérique récemment détecté, se trouvant dans la portée de reconnaissance, et n'ayant pas encore été reconnu.

4. S'il y a lieu, vous pouvez modifier la section du programme stitcher FnderRetProcessing.stch qui effectue les vérification ci-dessus afin de configurer le moment où une nouvelle reconnaissance d'un périphérique a lieu, même si cet ajustement de la configuration ne peut être entrepris que par les utilisateurs avancés.
5. Si un périphérique ayant déjà été reconnu doit faire l'objet d'une nouvelle reconnaissance, le programme stitcher actualise les informations stockées dans le serveur auxiliaire, liées à ce périphérique.
6. Pour tous les périphériques devant faire l'objet d'une nouvelle reconnaissance, le programme stitcher supprime les anciennes entrées des tables finders.processing, Details.returns et Details.despatch et copie ces informations dans la table rediscoveryStore.dataLibrary à des fins de comparaison.
7. Le programme stitcher place ensuite les détails du périphérique devant faire l'objet d'une nouvelle reconnaissance dans la table finders.processing et le programme stitcher FnderProcToDetailsDesp.stch déplace les détails concernant le périphérique vers l'agent Details.

Traitement des informations provenant des agents de reconnaissance lors de la nouvelle reconnaissance

Une fois que l'entité en cours de nouvelle reconnaissance a été traitée par l'agent Details et que les détails ont été placés dans la table Details.returns, le programme stitcher DetailsRetProcessing.stch compare les anciennes données se trouvant dans la table rediscoveryStore.dataLibrary avec les nouvelles. Par défaut, la nouvelle reconnaissance se poursuit à partir de ce point.

S'il y a lieu, vous pouvez éditer le programme stitcher DetailsRetProcessing.stch afin que la nouvelle reconnaissance ne se poursuive que lorsque certaines conditions sont en vigueur. Par exemple, lorsque l'accès SNMP est disponible.

Les données de nouvelle reconnaissance sont traitées par l'agent AssocAddress puis par les agents adéquats (en fonction du flux de processus de reconnaissance configuré) et sont renvoyées aux tables de renvoi respectives.

Une reconnaissance complète associe les informations provenant des tables .returns de l'agent de reconnaissance pour générer la topologie. Pourtant, lors d'une nouvelle reconnaissance, les informations doivent être vérifiées afin de déterminer si les relations entre les périphériques ont changé suite à l'obtention de nouvelles informations.

Par exemple, si le périphérique faisant l'objet d'une nouvelle reconnaissance, appelé périphérique A, était connecté au périphérique B avant la nouvelle reconnaissance, mais s'il est maintenant connecté à un troisième périphérique, le périphérique C, alors B et C doivent également faire l'objet d'une nouvelle

reconnaissance car leur relation a changé. Le programme stitcher AgentRetProcessing.stch détermine les relations entre les périphériques et la comparaison est effectuée par le programme stitcher ProcRemoteConns.stch. Contrairement aux routeurs, les commutateurs et les concentrateurs devant faire l'objet d'une nouvelle reconnaissance car les informations de connectivité qu'ils fournissent sont indirectes et non directes. Toute entité devant également faire l'objet d'une nouvelle reconnaissance suite à la nouvelle reconnaissance est réinsérée dans la table finders.returns et le paramètre m_Creator='Rediscovery'.

Nouvelles reconnaissances complètes

Parfois, lorsque vous comparez la relation actuelle entre des périphériques et celle précédente et que vous effectuez une nouvelle reconnaissance de tous les périphériques dont les relations ont changé, vous pouvez être amené à tourner en rond. Pourtant, le processus de reconnaissance inclut une vérification permettant d'éviter cette répétition.

Si le rapport d'entités comparées aux entités devant faire l'objet d'une nouvelle reconnaissance dépasse le pourcentage indiqué dans la colonne disco.config.m_PendingPerCent, DISCO arrête la nouvelle reconnaissance de chaque périphérique et lance une reconnaissance complète du réseau.

De plus, le fait que toutes les entités ayant fait l'objet d'une nouvelle reconnaissance sont enregistrées dans la table rediscoveryStore.rediscoveredEntities signifie qu'une entité donnée ne peut faire l'objet que d'une seule nouvelle reconnaissance.

Achèvement de la nouvelle reconnaissance

Lorsque toutes les entités pour lesquelles une nouvelle reconnaissance doit être effectuée ont été traitées, les couches topologiques sont reformées par le programme stitcher FinalPhase.stch. Celle-ci efface également la base de données rediscoveryStore afin que cette dernière soit prête pour la nouvelle reconnaissance à venir.

Il est important de noter que DISCO peut effectuer plusieurs cycles durant la nouvelle reconnaissance avant que la topologie soit reformée. DISCO reforme la topologie **uniquement** lorsqu'il existe des entités devant faire l'objet d'une nouvelle reconnaissance.

Option permettant de reformer les couches topologiques

Vous pouvez indiquer si vous voulez reformer les couches topologiques à la suite d'une nouvelle reconnaissance partielle. A l'aide de cette option, vous pouvez augmenter la vitesse de la nouvelle reconnaissance partielle.

Les raisons suggérées pour décider s'il est nécessaire, ou non, de reformer les couches topologiques sont :

- Si vous indiquez que les couches topologiques ne doivent *pas* être reformées à la suite d'une nouvelle reconnaissance partielle, les nouveaux périphériques sont ajoutés à la topologie plus rapidement qu'ils ne le seraient si les couches topologiques étaient reformées. Néanmoins, il se peut que la topologie en résultant ne soit pas complète. La connectivité associée au périphérique récemment reconnu n'est pas totalement reflétée dans la topologie. Les couches topologiques sont totalement reformées lorsqu'une nouvelle reconnaissance complète est exécutée.

- Si vous indiquez que les couches topologiques *doivent* être reformées à la suite d'une nouvelle reconnaissance partielle, la topologie est précise et affiche toutes les données de connectivité. Néanmoins, le processus d'ajout de nouveaux périphériques prend plus de temps.

La zone m_RebuildLayers dans la table disco.config vous permet d'indiquer si les couches topologiques doivent, ou non, être reformées à la suite d'une nouvelle reconnaissance partielle. Configurez cette valeur comme suit :

- Si la valeur disco.config.m_RebuildLayers=0, les programmes stitcher de couches topologiques ne sont pas exécutées à la suite d'une nouvelle reconnaissance partielle. La reconnaissance partielle est alors plus rapide. Toutefois, les données de connectivité associées au périphérique récemment reconnu ne sont pas totalement reflétées dans la topologie.
- Si la valeur disco.config.m_RebuildLayers=1, les programmes stitcher de couches topologiques sont exécutées à la suite d'une nouvelle reconnaissance partielle. Cette dernière prend plus de temps mais permet d'obtenir une topologie complète.

Annexe C. Agents de reconnaissance

Ces informations permettent à la sélection d'agents de reconnaissance d'être exécutée comme appartenant à votre reconnaissance.

Les rubriques suivantes fournissent des informations sur les agents de reconnaissance disponibles. Elles contiennent également les agents à sélectionner, en fonction des caractéristiques de votre réseau.

Agents

Les agents de reconnaissance extraient des informations sur les périphériques du réseau. Ils signalent également l'existence de nouveaux périphériques lors de la recherche de connectivité des périphériques. Ils sont utilisés pour des tâches spécialisées. Par exemple, l'agent de reconnaissance du Cache ARP remplit la base de données du serveur auxiliaire à l'aide d'adresses IP en vue du mappage des adresses MAC.

Outre les principaux agents de reconnaissance qui peuvent être activés ou désactivés conformément à vos exigences de reconnaissance, deux agents doivent toujours être exécutés : l'agent Détails et l'agent Associated Address.

Chaque agent de reconnaissance dispose de sa propre base de données résidente dans DISCO. Ces bases de données ont une structure générique et sont basées sur un modèle appelé base de données modèle des agents.

Toutes les bases de données des agents de reconnaissance contiennent les tables suivantes :

- *agentName*.despatch
- *agentName*.returns

Remarque : La configuration par défaut prévoit que la plupart des agents s'exécutent. Ceci s'explique par le fait que plus le nombre d'agents exécutés est élevé, plus la plage de réseaux pouvant être reconnus est large. De plus, les agents sont conçus pour arrêter rapidement l'analyse des périphériques qui ne fournissent pas les données requises. Cela signifie que l'exécution d'un grand nombre d'agents n'augmente que faiblement le trafic sur le réseau.

Remarque : Network Manager tue tous les agents de reconnaissance à la fin de l'étape 3 de la collecte de données. Cette action garantit que la reconnaissance suivante redémarre les agents et les force à relire leurs fichiers de configuration au début d'une reconnaissance, en détectant les modifications apportées aux fichiers de configuration.

Référence associée:

«Bases de données de sous-processus», à la page 272
Les bases de données d'outils de recherche, Details et agent sont utilisées au cours de la reconnaissance par les sous-processus du moteur de reconnaissance pour stocker les informations extraites du réseau. Les bases de données sont définies dans le fichier de configuration DiscoSchema.cfg.

«Fichier de configuration DiscoAgentReturns.filter», à la page 66
Le fichier de configuration DiscoAgentReturns.filter vous permet d'appliquer un filtre de données topologiques aux données renvoyées par tous les agents de reconnaissance.

Agent Détails

Cet agent est déclenché par les entrées dans la table `finders.processing`. Au moins un outil de recherche est donc nécessaire pour l'activer. La configuration auxiliaire SNMP des périphériques associés constitue également un pré-requis pour l'exécution de cet agent.

L'agent Details extrait des informations de base concernant les périphériques reconnus par les outils de recherche et détermine si l'accès SNMP est disponible pour le périphérique. Cet agent obligatoire est déclenché par les entrées dans la table `finders.processing`, au moins un outil de recherche est donc nécessaire pour l'activer.

Il est déclenché lorsque des informations sur le périphérique (généralement transférées par un programme stitcher à partir des outils de recherche) sont placées dans la table `Details.despatch`.

L'agent Details extrait des informations de base du réseau et les dépose dans la table `Details.returns`. Les informations de base extraites comprennent le nom DNS du périphérique, obtenu par l'auxiliaire DNS configuré, et l'ID objet système obtenu par l'auxiliaire SNMP. Les données `IpForwarding` sont téléchargées et insérées dans la zone `ExtraInfo`, utilisée pour identifier les périphériques de routage. Si ce schéma de nommage facultatif est requis, les informations `SysName` sont également téléchargées pour utilisation. L'insertion de données dans la base de données `renvois` déclenche un programme stitcher qui envoie ces informations à l'agent Associated Address.

Concepts associés:

«Reconnaissance des détails du périphérique (standard)», à la page 350
La reconnaissance standard des détails du périphérique s'effectue en plusieurs étapes.

Agent Associated Address (AssocAddress)

Cet agent obligatoire est déclenché par la sortie de l'agent Détails. La configuration auxiliaire SNMP des périphériques associés constitue un pré-requis pour l'exécution de cet agent.

Lorsqu'une interface a été reconnue sur un périphérique et que l'agent Détails a extrait les informations de base sur le périphérique, un programme stitcher transmet les informations sur le périphérique reconnues à l'agent Associated Address. Cet agent télécharge toutes les autres adresses IP associées au périphérique et les ajoute à un répertoire central, conservé dans la table `translations.ipToBaseName`, à condition que les détails du périphérique ne s'y trouvent pas encore. Le téléchargement de toutes les adresses IP associées garantit qu'un périphérique donné n'est interrogé qu'une seule fois par les principaux agents de reconnaissance, réduisant ainsi la charge sur les agents. Toute tentative de reconnaître un périphérique plusieurs fois (à l'aide de plusieurs interfaces) est bloquée par l'agent Associated Address, car les détails du périphérique se trouvent déjà dans la base de données `conversions`.

Si le périphérique vérifié n'a pas encore été reconnu, un programme stitcher envoie les détails de ce périphérique à l'agent de reconnaissance approprié pour l'extraction des informations sur la connectivité du périphérique et de celles spécifiques au protocole.

Concepts associés:

«Reconnaissance d'adresses de périphériques associées», à la page 352
Il existe plusieurs étapes dans le flux de processus lors de la reconnaissance d'adresses de périphériques associées.

Données d'interface extraites par les agents

L'agent Interfaces télécharge les informations d'interface essentiellement à partir des tables d'interfaces de RFC1213.mib. Pour chaque périphérique reconnu, les informations d'interface sont inscrites dans la zone m_LocalNbr de chaque enregistrement dans la table agent.returns adéquate.

Les informations d'interface peuvent contenir plusieurs sous-zones, y compris un numéro d'indice qui identifie l'interface avec ses propriétés ainsi que les valeurs de chaque propriété. Par exemple, la zone m_LocalNbr peut inclure les sous-zones suivantes :

- m_LocalNbr->m_IfIndex : l'indice associé à cette interface
- m_LocalNbr->m_IfType : le type d'interface
- m_LocalNbr->m_SubnetMask : le masque de sous-réseau de l'interface

Référence associée:

«Connectivité de la couche réseau de couche 3», à la page 381
Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

Mots clés du fichier de définition des agents de reconnaissance

Les mots clés contenus dans le fichier de définition des agents de reconnaissance permettent de définir le fonctionnement des agents de reconnaissance.

DiscoAgentClass

Le mot clé `DiscoAgentClass` indique le type de base des agents. Le tableau suivant identifie les valeurs les plus fréquentes :

Valeur	Description
0	Indique un agent de type IP.
1	Indique un agent de type commutateur.
2	Indique un agent de type concentrateur.
3	Indique un agent de type périphérique ATM.
4	Indique un agent de type FDDI.
5	Indique un agent de type PVC.
6	Indique un agent de type relais de trame.
8	Indique un agent de passerelle NAT.

L'exemple ci-dessous illustre le mot clé DiscoAgentClass associé à un agent de type relais de trame. Les agents de type relais de trame reconnaissent les interfaces de relais de trames et les connexions entre deux points sur les réseaux de relais de trames qui comprennent des périphériques réseau spécifiques, tels que des périphériques CISCO.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentClass( 6 );
.
.
.
}
```

DiscoAgentClassEnabledByDefault

Le mot clé DiscoAgentClassEnabledByDefault indique si l'agent est activé par défaut pour les reconnaissances complètes. Spécifiez l'une des valeurs suivantes :

Valeur	Description
0	Indique que l'agent n'est pas activé par défaut pour les reconnaissances complètes.
1	Indique que l'agent est activé par défaut pour les reconnaissances complètes.

L'exemple ci-dessous illustre le mot clé DiscoAgentClassEnabledByDefault configuré pour activer un agent de type relais de trame par défaut pour les reconnaissances complètes.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentClass( 6 );
.
.
.
DiscoAgentEnabledByDefault( 1 );
}
```

DiscoAgentClassEnabledByDefaultOnPartial

Le mot clé DiscoAgentClassEnabledByDefaultOnPartial indique si l'agent est activé par défaut pour les reconnaissances partielles. Spécifiez l'une des valeurs suivantes :

Valeur	Description
0	Indique que l'agent n'est pas activé par défaut pour les reconnaissances partielles.
1	Indique que l'agent est activé par défaut pour les reconnaissances partielles.

L'exemple ci-dessous illustre le mot clé DiscoAgentClassEnabledByDefaultOnPartial configuré pour un agent de type relais de trame par défaut pour les reconnaissances partielles.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentClass( 6 );
.
.
.
DiscoAgentEnabledByDefaultOnPartial( 1 );
DiscoAgentEnabledByDefault( 1 );
}
```

DiscoAgentIsIndirect

Un agent direct renvoie les données de relations sur les objets auxquels il est directement connecté au niveau de la couche active. Un agent indirect renvoie les données de relations sur les objets auxquels il est indirectement connecté. Les agents indirects les plus fréquents sont les agents de commutation. Les enregistrements voisins distants des agents indirects font référence aux périphériques pouvant être atteints à partir d'un port spécifique et non à partir des périphériques auxquels ils sont connectés directement. Les données de relation des agents indirects sont requises pour déterminer les enregistrements voisins distants d'un périphérique devant être reconnus à nouveau lors de l'utilisation d'un nouveau périphérique.

Le mot clé DiscoAgentIsIndirect indique si l'agent est un agent indirect qui renvoie les données de relations sur les objets auxquels il est indirectement connecté. Spécifiez l'une des valeurs suivantes :

Valeur	Description
0	Indique que l'agent est un agent direct.
1	Indique que l'agent est un agent indirect.

L'exemple ci-dessous illustre le mot clé DiscoAgentIsIndirect configuré pour indiquer qu'un agent de type relais de trame est un agent direct.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentGUILocked( 0 );
DiscoAgentClass( 6 );
DiscoAgentIsIndirect( 0 );
.
.
.
DiscoAgentEnabledByDefaultOnPartial( 1 );
DiscoAgentEnabledByDefault( 1 );
}
```

DiscoAgentCompanionAgents

Le mot clé DiscoAgentCompanionAgents permet d'afficher dans l'interface graphique le ou les agents avec lesquels cet agent doit s'exécuter.

L'exemple ci-dessous illustre le mot clé DiscoAgentCompanionAgents permettant d'afficher dans l'interface graphique l'agent (ArpCache.agnt) devant s'exécuter avec l'agent Centillion Networks.

```
DiscoCompiledAgent
{
.
.
.
-- This agent examines all devices originally made by Centillion
-- Networks (enterprise OID 1.3.6.1.4.1.930), to see if it can
-- discover them.
.
.
.

DiscoAgentCompanionAgents( "ArpCache" );
.
.
.
}
```

DiscoAgentCompletionPhase

Le mot clé DiscoAgentCompletionPhase indique la phase de reconnaissance pendant laquelle l'exécution de l'agent spécifié doit se terminer. Spécifiez l'une des valeurs suivantes :

Valeur	Description
1	Indique que l'exécution de l'agent doit se terminer pendant la phase 1 de reconnaissance.
2	Indique que l'exécution de l'agent doit se terminer pendant la phase 2 de reconnaissance.
3	Spécifie que l'agent doit terminer son exécution au cours de la phase 3 de la reconnaissance.

L'exemple ci-dessous illustre le mot clé DiscoAgentCompletionPhase configuré pour activer un agent de type relais de trame pour terminer l'exécution pendant la phase 1 de reconnaissance.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentCompletionPhase( 1 );
.
.
.
DiscoAgentEnabledByDefaultOnPartial( 1 );
DiscoAgentEnabledByDefault( 1 );
}
```

DiscoAgentConflictingAgents

Le mot clé DiscoAgentConflictingAgents permet d'afficher dans l'interface graphique le ou les agents avec lesquels cet agent ne doit pas s'exécuter.

L'exemple ci-dessous illustre le mot clé DiscoAgentConflictingAgents permettant d'afficher dans l'interface graphique les agents (IpRoutingTable.agnt et IpForwardingTable.agnt) avec lesquels l'agent IP routeur de secours ne doit pas s'exécuter.

```
DiscoCompiledAgent
{
.
.
.
-- This agent examines every device with SNMP access to see if it
-- can discover it.
.
.

DiscoAgentConflictingAgents( "IpRoutingTable","IpForwardingTable" );
.
.
.
}
```

DiscoAgentDescription

Le mot clé DiscoAgentDescription fournit une description de l'agent affiché dans l'interface graphique.

L'exemple ci-dessous illustre le mot clé DiscoAgentDescription qui fournit une description à afficher dans l'interface graphique pour un agent de type relais de trame. La description fait appel au codage HTML.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentDescription("
<b>Agent Name :</b>  CiscoFrameRelay<br>
<br>
<b>Agent Type :</b> Layer 3<br>
<br>
<b>Agent Prerequisites :</b>  SNMP helper configuration for associated devices.<br>
<br>
<b>Operation :</b><br>
Discovers Frame Relay interfaces and connections between two points on Frame Relay
networks that incorporate Cisco devices. If you need to add DLCI information to the
interfaces of Frame Relay devices, then run Frame Relay agents in conjunction with
the IP layer agents.<br>
<br>
 ");
.
.
.
}
```

DiscoAgentMinCertifiedDeviceOS

Le mot clé DiscoAgentMinCertifiedDeviceOS indique un filtre spécifique au système d'exploitation du périphérique. Ce filtre peut être configuré pour exécuter l'agent spécifié dans la version du système d'exploitation du périphérique.

L'exemple ci-dessous illustre le mot clé DiscoAgentMinCertifiedDeviceOS qui indique le filtre propre au système d'exploitation du périphérique pour un agent qui effectue des reconnaissances d'informations MPLS VRF, VPN et de

commutation d'étiquette à partir des routeurs CISCO. Ce filtre spécifique configure l'agent pour qu'il s'exécute avec les périphériques CISCO et les versions de système d'exploitation suivantes :

- `m_ObjectId` — Indique les périphériques CISCO (ID objet `1.3.6.1.4.1.9`) que l'agent tente de reconnaître.
- `m_OSVersion` — Indique le système d'exploitation du périphérique CISCO qui configure l'agent pour qu'il s'exécute avec les versions de système d'exploitation suivantes :
  - Versions 12.0 de 12.0(27) ou versions ultérieures non expérimentales
  - Versions 12.2 de 12.2(19) ou versions ultérieures non expérimentales
  - Versions 12.3 de 12.3(18) ou versions ultérieures non expérimentales
  - Versions 12.4

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentMinCertifiedDeviceOS
    (
      "(
          m_ObjectId LIKE '1\.3\.6\.1\.4\.1\.9\.',
          m_OSVersion >= '12.0(27)' AND m_OSVersion < '12.1' AND m_OSVersion
                        NOT LIKE '.*Experimental.*',
          m_MibVar = 'sysDescr.0'
        ),
        (
          m_ObjectId LIKE '1\.3\.6\.1\.4\.1\.9\.',
          m_OSVersion >= '12.2(19)' AND m_OSVersion < '12.3' AND m_OSVersion
                        NOT LIKE '.*Experimental.*',
          m_MibVar = 'sysDescr.0'
        ),
      (
          m_ObjectId LIKE '1\.3\.6\.1\.4\.1\.9\.',
          m_OSVersion >= '12.3(18)' AND m_OSVersion < '12.4' AND m_OSVersion
                        NOT LIKE '.*Experimental.*',
          m_MibVar = 'sysDescr.0'
       ),
      (
          m_ObjectId LIKE '1\.3\.6\.1\.4\.1\.9\.',
          m_OSVersion >= '12.4',
          m_MibVar = 'sysDescr.0'
        )"
    );
.
.
.
}
```

DiscoAgentPrecedence

Le mot clé `DiscoAgentPrecedence` indique l'agent prioritaire en cas de conflit de données provenant de deux agents. Indiquez une valeur supérieure ou égale à 0 (zéro). La plage de valeurs conseillée est comprise entre 1 et 100, dans laquelle le chiffre le plus grand est prioritaire. Plus le chiffre est élevé et plus les données d'agent sont correctes. Par exemple, si un conflit de données existe entre un agent de priorité 2 et un agent de priorité 3, les données de l'agent de niveau 3 sont utilisées.

L'exemple ci-dessous illustre le mot clé `DiscoAgentPrecedence` pour un agent de type relais de trame configuré avec une priorité de niveau 2.

```
DiscoCompiledAgent
{
.
.
.
DiscoAgentGUILocked( 0 );
DiscoAgentClass( 6 );
DiscoAgentIsIndirect( 0 );
DiscoAgentPrecedence( 2 );
.
.
.
DiscoAgentEnabledByDefaultOnPartial( 1 );
DiscoAgentEnabledByDefault( 1 );
}
```

DiscoPerlAgent

Le mot clé `DiscoPerlAgent` indique si le fichier `.agnt` fait référence à un agent Perl.

L'exemple ci-dessous illustre le mot clé `DiscoPerlAgent` défini pour un agent en langage Perl qui extrait des informations sur le système d'exploitation en cours sur le périphérique.

```
DiscoPerlAgent
{
.
.
.
DiscoAgentGUILocked( 0 );
 DiscoAgentClass( 0 );
 DiscoAgentIsIndirect( 0 );
 DiscoAgentPrecedence( 2 );
 DiscoAgentEnabledByDefaultOnPartial( 0 );
 DiscoAgentEnabledByDefault( 0 );
}
```

Types d'agents

Les agents fournis avec Network Manager peuvent être divisés en catégories en fonction du type de données qu'ils extraient ou de la technologie qu'ils découvrent.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

Reconnaissance de la connectivité pour les commutateurs Ethernet

Les agents de reconnaissance qui reconnaissent les informations de connectivité entre les commutateurs Ethernet disposent de trois étapes opérationnelles principales : accéder au commutateur et télécharger les interfaces de commutateurs ; reconnaître les informations VLAN du commutateur ; télécharger la table de base de données de réacheminement du commutateur.

Une liste d'agents de reconnaissance gérant les commutateurs Ethernet est présentée dans le tableau 138.

Remarque : Avant d'activer ces agents de couche 2, il est nécessaire d'activer l'accès SNMP. Certains agents requièrent également une configuration de l'accès et de l'auxiliaire Telnet. S'il y a lieu, cela est indiqué.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet

Nom de l'agent	Fonction
Agent AccelarSwitch	L'agent AccelarSwitch contient les méthodes d'extraction spécialisées des informations de connectivité des commutateurs de routage Accelar. Ces périphériques sont désormais appelés Nortel Passport 86xx series. Cet agent reconnaît également les périphériques BayStack 450 et BayStack 470. Il télécharge la table de base de données FDB du commutateur et les informations VLAN du périphérique. Le programme stitcher du routeur utilise ces informations pour résoudre la connectivité Ethernet couche 2.
Agent BayEthernetHub	L'agent BayEthernetHub reconnaît les cartes concentrateur fabriquées par Bay. Les informations sur la connectivité sont téléchargées à partir du concentrateur et la connectivité est résolue par le programme stitcher HubFdbToConnections. Avant d'activer cet agent, il est nécessaire de configurer l'auxiliaire SNMP.
Agent CentillionSwitch	L'agent CentillionSwitch contient les méthodes nécessaires à l'extraction et à la résolution d'informations des périphériques de commutation Centillion, en particulier les informations VLAN spécifiques à l'entreprise.
Agent ChipcomDistributedMM	L'agent ChipcomDistributedMM reconnaît la connectivité des commutateurs Ethernet pour les périphériques 3Com CoreBuilder 5000 contenant des modules de gestion répartis.
Agent ChipcomEthernetMM	L'agent ChipcomEthernetMM est approprié pour les concentrateurs en ligne Chipcom contenant des modules de gestion Ethernet (EEM) et reconnaît la connectivité Ethernet des modules de gestion Ethernet Chipcom.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet (suite)

Nom de l'agent	Fonction
Agent CiscoSRP	L'agent CiscoSRP reconnaît la connectivité des réseaux utilisant le protocole SRP (Spatial Reuse Protocol), c'est-à-dire les topologies en anneau DPT. Le protocole SRP est un protocole de couche 2 développé par Cisco qui utilise des informations 'secondaires' pour identifier les voisins adjacents dans ses topologies en anneau. L'agent CiscoSRP reconnaît la connectivité de tout périphérique qui prend en charge CISCO-SRP-MIB. Le fichier de définitions de l'agent est configuré par défaut pour n'accepter que les périphériques Cisco avec toutes les versions d'IOS, sauf celles prises en charge par l'agent CiscoSRPTelnet. L'agent n'accepte que les périphériques qui prennent en charge la variable de base d'informations de gestion srpMacAddress. IOS version 12.2(14)S7 et 12.2(18)S, utilisées avec les cartes NPE-G1, est connu pour endommager les données SNMP. IOS version 12.2(15)BC1 est connu pour ne pas être pris en charge par CISCO-SRP_MIB.
Agent CiscoSRPTelnet	L'agent CiscoSRPTelnet reconnaît la connectivité des réseaux utilisant le protocole SRP (Spatial Reuse Protocol), c'est-à-dire les topologies en anneau DPT. SRP est un protocole de couche 2 développé par Cisco qui utilise les informations 'secondaires' pour identifier les voisins dans sa topologie en anneau. L'agent CiscoSRPTelnet reconnaît la connectivité de tout périphérique qui prend en charge la commande **show controllers srp**. Le fichier de définitions de l'agent est configuré pour n'accepter que les périphériques Cisco qui disposent d'un IOS connu pour ne pas prendre en charge CISCO-SRP-MIB et les versions d'IOS ayant des problèmes connus avec la reconnaissance SNMP. IOS version 12.2(14)S7 et 12.2(18)S, utilisés avec des cartes NPE-G1, est connu pour endommager les données SNMP. IOS version 12.2(15)BC1 est connu pour ne pas être pris en charge par CISCO-SRP_MIB. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire Telnet.
Agent CiscoSwitchSnmp	L'agent CiscoSwitchSnmp contient les méthodes d'extraction spécialisées des informations provenant des commutateurs Cisco utilisant le protocole SNMP. Il utilise plusieurs méthodes de recherche des VLAN et des mappages carte/port sur ifIndex car divers commutateurs Cisco stockent ces informations dans différentes variables de base d'informations de gestion. Lors de la reconnaissance de périphériques utilisant SNMPv3, le contexte de réseau local virtuel (VLAN) doit être ajouté aux commutateurs Cisco du groupe de vues de chaque réseau local virtuel.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet (suite)

Nom de l'agent	Fonction
Agent CiscoSwitchTelnet	L'agent CiscoSwitchTelnet contient des méthodes d'extraction spécialisées des informations de connectivité provenant des commutateurs Cisco utilisant le protocole Telnet. Il utilise plusieurs méthodes pour rechercher les VLAN et les mappages carte/port sur ifIndex car divers commutateurs Cisco stockent ces informations dans différents variables de base d'informations de gestion. Seules les tables FDB sont téléchargées à l'aide de Telnet. Toutes les autres informations sont téléchargées à l'aide du protocole SNMP. Les commandes Telnet utilisées pour obtenir la table FDB sont **show cam dynamic** et **show mac-address table**. Certains périphériques peuvent nécessiter le mode actif afin d'exécuter la commande **show mac-address table**. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer les accès SNMP et Telnet ainsi que les auxiliaires respectifs.
CiscoVSS	L'agent Cisco VSS découvre les informations Virtual Switching System provenant des commutateurs Cisco.
Agent Corebuilder3ComSwitch	L'agent Corebuilder3ComSwitch reconnaît les liens pour les commutateurs de couche 3 CoreBuilder 9000 fabriqués par 3Com.
Agent DasanSwitchTelnet	L'agent DasanSwitchTelnet est responsable de la reconnaissance de la connectivité de couche 2 stockée dans la table FDB/MAC des commutateurs Dasan. Il a été développé par rapport aux périphériques suivants : V5208 (OS 9.07)V5224 (OS 9.10). Il est capable de reconnaître la connectivité de couche 2, les VLAN et les ports d'agrégation des liens. Il est configuré pour ne s'exécuter que sur les périphériques ayant un ID objet système de 1.3.6.1.4.1.6296.* et prenant en charge la commande **show vlan**. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire Telnet.
Agent DefaultEthernetHub	Cet agent dispose d'une classe spécialisée pour gérer les concentrateurs semi-intelligents.
EnterasysSwitch	L'agent EnterasysSwitch fournit une reconnaissance de connectivité de couche 2 en extrayant la table FDB et les informations VLAN du périphérique. L'agent reconnaît la connectivité de couche 2 pour les périphériques qui prennent en charge les normes IEEE 802.1q ou IEEE 802.1d, comme respectivement modélisé dans les bases d'informations de gestion SNMP Q-BRIDGE-MIB et BRIDGE-MIB. **Remarque :** Cet agent est utilisé pour les périphériques Enterasys sur lesquels SecureFast n'est pas activé.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet (suite)

Nom de l'agent	Fonction
Agent ExtremeSwitch	L'agent ExtremeSwitch obtient des commutateurs les informations de connectivité de couche 2, les voisins EDP et les détails VLAN. Afin d'effectuer une reconnaissance de couche 2 détaillée, les périphériques Extreme doivent être configurés pour autoriser l'accès SNMP et le remplissage de la table dot1dFdbTable. Emettez les commandes suivantes à l'attention de chaque périphérique Extreme : • **enable snmp access** • **enable dot1dFdbTable** Cette modification de configuration n'est requise que pour les commutateurs exécutant une version d'ExtremeWare® antérieure à 6.1.8.
Fix Pack 5 F5Switch	Cet agent reconnaît la configuration des commutateurs F5. L'agent extrait les informations de la variable `sysChassisSlotSlotId` dans les bases d'informations de gestion F5-BIGIP-COMMON-MIB et F5-BIGIP-SYSTEM-MIB. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer les accès SNMP et Telnet ainsi que les auxiliaires respectifs.
Agent FoundrySwitch	L'agent FoundrySwitch reconnaît la connectivité de commutateur de tout périphérique Foundry qui prend en charge les normes IEEE 802.1q ou IEEE 802.1d, comme modélisé respectivement dans les bases d'informations de gestion SNMP Q-BRIDGE-MIB et BRIDGE-MIB. Le fichier de définitions de l'agent est configuré pour accepter par défaut tous les périphériques Foundry activés pour SNMP. L'agent ne va reconnaître que les périphériques qui prennent en charge la variable de base d'informations de gestion Q-BRIDGE-MIB dot1qVlanVersionNumber ou BRIDGE-MIB. L'agent FoundrySwitch obtient également les informations d'agrégation des liens pour les ports à plusieurs intervalles de temps, mais il ne reconnaît pas celles pour les ports n'ayant qu'un seul intervalle de temps. Certains périphériques Foundry ne prennent en charge que IEEE 802.1d et, par conséquent, aucune information VLAN n'est reconnue pour ces périphériques.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet (suite)

Nom de l'agent	Fonction
Agent HuaweiSwitchTelnet	L'agent HuaweiSwitchTelnet reconnaît la connectivité des commutateurs Ethernet Huawei Quidway. L'agent est basé sur le protocole Telnet, mais il nécessite également un accès SNMP pour reconnaître certaines informations. Il nécessite l'achèvement des sections Mode privilégié (mode super 3) du fichier de configuration TelnetStackPasswords.cfg. Dans le cas contraire, l'agent échouera. Certaines commandes Telnet ont un effet secondaire qui entraîne la modification de l'invite de commande d'un périphérique Huawei. Par exemple, l'invite de commande `<nom_périphérique>` devient `[nom_périphérique]` ou `[nom_périphérique-diag]` lorsque certaines commandes sont émises. Il est essentiel que les paramètres m_ConPrompt et m_PrivConPrompt dans le fichier TelnetStackPasswords.cfg soient configurés pour faire face à ces variations. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire Telnet.
Agent HPSwitch	L'agent HPSwitch contient les méthodes d'extraction spécialisées des informations de connectivité pour les commutateurs HP ProCurve, y compris le téléchargement d'informations VLAN spécifiques à l'entreprise.
Agent Marconi3810	L'agent spécialisé Marconi3810 reconnaît la connectivité Ethernet des commutateurs Marconi ES-3810 qui exécutent le système d'exploitation versions 4.x.x et 5.x.x. Cet agent supprime également la connectivité des interfaces d'émulation réseau local par défaut - peut être configuré en utilisant l'indicateur GetElanData dans le fichier .agnt.
NortelSwitch	L'agent NortelSwitch extrait les informations sur la connectivité de la couche 2, y compris des informations SMLT (Split Level Multi-Trunking), à partir des commutateurs Nortel.
Agent SecureFast	L'agent SecureFast contient les méthodes d'extraction spécialisées desi informations de connectivité des commutateurs de routage VLAN Enterasys/Cabletron SecureFast. Ces périphériques utilisent le protocole Cabletron Discovery Protocol pour reconnaître leurs voisins et activer le mode de fonctionnement SecureFast. Cet agent est envoyé à tous les périphériques Cabletron et Enterasys, indiqués par 1.3.6.1.4.1.52.* et 1.3.6.1.4.1.5624.* dans le fichier .agnt, et détermine si un périphérique est activé pour SecureFast en téléchargeant la variable MIB sfpsCommonNeighborSwitchMAC. Les périphériques en mode SecureFast ne prennent pas en charge les bases d'informations de gestion dot1dBridge.

Tableau 138. Agents de reconnaissance de commutateurs Ethernet (suite)

Nom de l'agent	Fonction
Agent StandardSwitch	L'agent générique StandardSwitch fournit la reconnaissance de connectivité de couche 2 pour tous les commutateurs pour lesquels il n'existe aucun agent spécialisé. L'agent reconnaît la connectivité de couche 2 pour les périphériques qui prennent en charge les normes IEEE 802.1q ou IEEE 802.1d, comme respectivement modélisé dans les bases d'informations de gestion SNMP Q-BRIDGE-MIB et BRIDGE-MIB. Les périphériques en mode SecureFast ne prennent pas en charge les bases d'informations de gestion dot1dBridge.
Agent SuperStack3ComSwitch	L'agent SuperStack3ComSwitch recherche les connexions dans les commutateurs empilés fabriqués par 3Com.
Agent XyplexEthernetHub	L'agent XyplexEthernetHub reconnaît la connectivité de couche 2 des concentrateurs intelligents fabriqués par Xyplex.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

«Fichier de configuration DiscoTelnetHelperSchema.cfg», à la page 85
Le fichier de configuration DiscoTelnetHelperSchema.cfg définit le fonctionnement de l'auxiliaire Telnet, qui retourne les résultats d'une opération Telnet dans un périphérique indiqué.

Connectivité de la couche réseau de couche 3

Il existe plusieurs agents de reconnaissance qui extraient des informations de connectivité de la couche 3 du modèle OSI (la *couche réseau*). Cette couche est responsable du routage, du contrôle de l'encombrement du trafic et de l'envoi de messages entre les réseaux.

Tableau 139. Agents de couche réseau de couche 3

Nom de l'agent	Fonction
Agent AlteonVRRP	VRRP n'est pas modélisé pour l'analyse d'origine du problème. Il définit uniquement les balises sur les interfaces VRRP qui affichent l'état des routeurs Alteon au moment de la reconnaissance. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.

Tableau 139. Agents de couche réseau de couche 3 (suite)

Nom de l'agent	Fonction
Agent CiscoBGPTelnet	L'agent CiscoBGPTelnet télécharge les données BGP ci-après à partir des routeurs Cisco : • Données homologues : l'agent extrait les données iBGP et eBGP des routeurs homologues. • Données de routage : l'agent extrait les informations de routage des tables de routage BGP des routeurs homologues. Cette option est désactivée par défaut car elle impliquerait l'extraction d'une grande quantité de données d'un réseau fournisseur de services typique. Cet agent propose également une option pour configurer un filtre permettant d'indiquer les données de routage à extraire. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire Telnet.
Agent CiscoFrameRelay	L'agent CiscoFrameRelay reconnaît les interfaces de relais de trames et les connexions entre deux points sur les réseaux de relais de trames qui comprennent des périphériques Cisco. Ce type d'agents doit être exécuté en association avec les agents de couche IP si vous voulez ajouter des informations DLCI aux interfaces de périphériques de relais de trames. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent CiscoOSPFTelnet	L'agent CiscoOSPFTelnet est responsable de la reconnaissance des périphériques Cisco exécutant le protocole OSPF (Open Shortest Path First). Il fournit des informations complémentaires à celles de l'agent StandardOSPF, comme les processus OSPF en cours d'exécution et les informations de lien virtuel. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire Telnet.
Agent ExtremeESRP	L'agent ExtremeESRP reconnaît les informations ESRP (Extreme Standby Routing Protocol) provenant des commutateurs de routage Extreme. ESRP est une fonction d'ExtremeWare qui permet à plusieurs commutateurs de fournir des services de routage redondants aux utilisateurs. L'agent dépend du remplissage correct des tables `extremeEsrpTable` et `extremeEsrpNeighborTable` de EXTREME-ESRP-MIB. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent FoundryVRRP	VRRP n'est pas modélisé pour l'analyse d'origine du problème. L'agent FoundryVRRP définit uniquement les balises sur les interfaces VRRP qui affichent l'état des routeurs Foundry au moment de la reconnaissance. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent HSRPSnmp	L'agent HSRPSnmp utilise SNMP pour extraire les informations des périphériques de routage qui utilisent le protocole d'IP virtuelle HSRP (Hot Stand-by Routing Protocol). Il extrait les données sur les adresses IP principales et secondaires HSRP. Ces informations sont utilisées pour la reconnaissance et la visualisation de l'interface. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent InetRouting	L'agent InetRouting reconnaît la connectivité des périphériques.
Interfaces	Cet agent est déclenché par les renvois de l'agent AssocAddress. L'agent Interfaces télécharge les informations d'interface essentiellement à partir des tables d'interfaces de RFC1213.mib. Les informations sont ensuite inscrites dans la zone m_LocalNbr des entités renvoyées. Vous pouvez augmenter ou réduire le nombre de variables renvoyées en modifiant Interfaces.agnt. Toute variable MIB de base (sysDescr, sysName, etc.) ou indexée par ifIndex peut être ajoutée aux ID objet à télécharger dans le fichier .agnt. L'agent Interfaces extrait également les informations d'interface IPv6. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.

Tableau 139. Agents de couche réseau de couche 3 (suite)

Nom de l'agent	Fonction
IpBackupRoutes	Il recherche des liens en parcourant la table de base d'informations de gestion IpNetToMedia, qui fournit les adresses physiques et IP des périphériques connectés au routeur. Cet agent n'est pas activé par défaut car il extrait une quantité importante d'informations qui ne sont pas essentielles pour déterminer les connexions de couche 3. Par ailleurs, ces informations peuvent être obsolètes car elles sont téléchargées à partir d'une table qui n'est pas dynamique et qui exige une actualisation manuelle. Si vous effectuez une reconnaissance de couche 2, la connectivité du serveur que cet agent reconnaît est souvent obsolète car elle peut avoir été remplacée par les informations sur la connectivité du routeur. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent IpForwardingTable	Il recherche des liens dans la version la plus récente des tables de routage, c'est-à-dire la table Transfert IP, comme indiqué dans la norme RFC 2096. Il exploite également les informations du protocole OSFP (Open Shortest Path First) pour améliorer la reconnaissance des périphériques Juniper. Cet agent télécharge des éléments de la table de routage en se basant sur la portée de reconnaissance. Le paramètre par défaut suppose que l'agent SNMP d'un périphérique spécifique prend en charge la correspondance partielle. Si ce n'est pas le cas, il convient de le spécifier dans la section DiscoRouterPartialMatchRestrictions du fichier .agnt. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
IpRoutingTable	Extrait les informations sur la connectivité générique en parcourant la table de routage du routeur, comme spécifié dans la norme RFC1213. L'agent télécharge des éléments de la table de routage en se basant sur la portée de reconnaissance. Le paramètre par défaut de l'agent suppose que les agents SNMP d'un périphérique donné prennent en charge la correspondance partielle. Si ce n'est pas le cas, il convient de le spécifier dans la section DiscoRouterPartialMatchRestrictions du fichier .agnt. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent ISISExperimental	Il reconnaît la connectivité entre les routeurs qui prennent en charge les base d'informations de gestion ISIS expérimentales. Il devrait être utilisé lorsque certains de vos routeurs sont configurés avec des masques de réseau de 255.255.255.255, ce qui les rend inadaptés à la reconnaissance standard. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent LinkStateAdvOSPF	Il extrait des publicités d'état de liaison des routeurs OSPF. Ces publicités sont utilisées par le programme stitcher CreateOSPFNetworkLSAPseudoNodes pour créer des pseudo-noeuds OSPF. Ces pseudo-noeuds surmontent le problème de de maillage complet lors de la représentation de la zone OSPF dans les vues de réseau Topoviz et permettent la visualisation claire et épurée des connexions au sein des zones OSPF.
Agent JuniperBGPTelnet	Il télécharge les informations BGP à partir des routeurs Juniper. Il n'est pas autorisé par défaut car il ne rassemble qu'une information très spécifique, c'est-à-dire si les périphériques sont des réflecteurs de routes. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire Telnet.
JuniperMXGroupTelnet	L'agent JuniperMXGroupTelnet utilise Telnet pour reconnaître les informations de collections logiques concernant les groupes de moteurs de routage sur les périphériques Juniper MX.
NetScreenInterface	L'agent NetScreenInterface extrait les informations sur toutes les interfaces configurées dans les périphériques Juniper Netscreen. L'agent extrait des informations sur les interfaces logiques et d'autres interfaces, informations qui ne sont pas disponibles dans la base IF-MIB standard et requièrent les fichiers NETSCREEN-INTERFACE-MIB.mib et NS-VPN-MON.mib. Cet agent extrait également des informations sur la connectivité du réseau VPN et du tunnel VPN configurée dans les périphériques Juniper NetScreen. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.

Tableau 139. Agents de couche réseau de couche 3 (suite)

Nom de l'agent	Fonction
NetScreenIpRoutingTable	L'agent NetScreenIpRoutingTable extrait des informations sur les tables de routage IP configurées sur les périphériques Netscreen. L'agent détermine les interfaces et les sous-interfaces à partir de l'index d'interfaces du périphérique Netscreen. Cet agent exécute la même fonction que l'agent IpRoutingTable mais uniquement pour les périphériques Netscreen, afin de tenir compte des sous-interfaces qui ne seraient pas découvertes correctement par l'agent IpRoutingTable. L'agent NetScreenIpRoutingTable utilise la base MIB standard IP-FORWARD-MIB et la base NETSCREEN-INTERFACE-MIB. **Remarque :** L'agent IpRoutingTable ne traite pas les périphériques Netscreen traités par l'agent NetScreenIpRoutingTable.
Agent NokiaVRRP	Il télécharge les informations VRRP à partir des routeurs qui prennent en charge l'interprétation de Nokia de la base d'informations de gestion VRRP. Les informations extraites incluent l'état VRRP, l'ID, l'IP principal et les adresses associées. Ces informations sont extraites des variables de la base d'informations de gestion répertoriées ci-dessous : • vrrpOperState • vrrpOperMasterIpAddr • vrrpAssoIpAddrRowStatus **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
NortelPassport	L'agent NortelPassport extrait les informations de connectivité de couche 3 et les informations de confinement depuis les commutateurs Nortel Passport.
Agent RFC2787VRRP	L'agent RFC2787VRRP télécharge les informations VRRP (Virtual Router Redundancy Protocol) depuis les routeurs exécutant un protocole VRRP compatible RFC2787 et prenant en charge la MIB VRRP RFC2787. Certains pare-feux Nokia prennent en charge cette base d'informations de gestion. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP. VRRP n'est pas modélisé pour l'analyse d'origine du problème. Cet agent définit des balises sur les interfaces VRRP qui affichent l'état des interfaces lors de la reconnaissance. Il télécharge également les adresses IP associées, lesquelles sont utilisées pour construire des collections VRRP. **Conseil :** Il existe deux versions légèrement différentes de la base d'informations de gestion VRRP. Elles contiennent les même noms mais avec des ID objet différents. Si cet agent ne fonctionne pas, utilisez l'autre version de la MIB VRRP.

Tableau 139. Agents de couche réseau de couche 3 (suite)

Nom de l'agent	Fonction
Agent StandardBgp	Il est responsable de la reconnaissance des réseaux exécutant le protocole BGP (Border Gateway Protocol). Il prend en charge tous les périphériques conformes à la norme RFC1657 (BGP4-MIB) de base d'informations de gestion et reconnaît les informations suivantes : • ID système autonome • Connexions homologues BGP aux homologues externes (EBGP) • Connexions homologues BGP aux homologues internes (IBGP) • Données de routage acquises via le protocole BGP (déconseillé) Le fichier de définitions de l'agent est configuré pour accepter par défaut tous les périphériques activés pour SNMP mais l'agent ne va accepter que les périphériques prenant en charge BGP44-MIB, la variable bgpIdentifier de la base d'informations de gestion. L'agent dispose des paramètres de configuration additionnels suivants dans la section DiscoAgentDiscoveryScopingde son fichier .agnt : • GetPeerData – détermine si l'agent doit acquérir les données homologues BGP (activé par défaut). • GetRouteData – détermine si l'agent doit acquérir les routes BGP (désactivé par défaut). L'activation de ce paramètre peut entraîner la reconnaissance d'une quantité importante de données. L'agent StandardBgp ne prend pas actuellement pas en charge les groupes homologues, les confédérations via les processus VRF BGP ou les reflets de routes. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP. Il est également nécessaire de configurer l'auxiliaire Ping.
Agent StandardOSPF	Il est responsable de la reconnaissance des réseaux exécutant le protocole OSPF (Open Shortest Path First). Il prend en charge tout périphérique conforme à la norme RFC1850. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.
Agent TraceRoute	Il recherche des liens en traçant la route prise par un paquet de commandes PING ICMP ayant une durée de vie pré-déterminée. Si vous utilisez cet agent, vous devez augmenter la valeur de m_Timeout dans le fichier de configuration DiscoPingHelperSchema.cfg puisque la fonction traceroute prend plus de temps que l'ICMP standard. Cet agent n'est pas activé par défaut car elle ne fonctionne pas sur les périphériques activés pour SNMP. Par conséquent, si cet agent était activé par défaut, il tracerait la route vers chaque périphérique du réseau. Cela pourrait entraîner une connectivité incomplète dans un environnement maillé ou imprécise dans un environnement à charge équilibrée. **Remarque :** Avant d'activer cet agent, configurez l'accès et l'auxiliaire SNMP.

Tâches associées:

«Configuration de l'accès aux unités», à la page 30
Indiquez les noms de communauté SNMP et les informations d'accès Telnet pour permettre aux auxiliaires et à l'interrogation Network Manager d'accéder aux unités sur votre réseau.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

«Fichier de configuration DiscoPingHelperSchema.cfg», à la page 74
Le fichier de configuration DiscoPingHelperSchema.cfg définit la manière dont les commandes PING doivent être lancées sur les périphériques.

Données topologiques stockées dans un système de gestion d'éléments

Il existe plusieurs agents de reconnaissance qui extraient des informations sur les périphériques gérés par un système de gestion d'éléments.

Les agents de reconnaissance des protocoles de routage interrogent un collecteur de système de gestion d'éléments pour obtenir des informations de base et détaillées sur les périphériques gérés par le système de gestion d'éléments. Ces agents sont répertoriés dans le tableau 140.

Tableau 140. Agents de reconnaissance des protocoles de routage

Nom de l'agent	Fonction
Agent CollectorDetails	Extrait des informations de base sur les périphériques situés sur le collecteur, y compris les données sysObjectId, sysDescr ainsi que les données de désignation.
Agent CollectorInventory	Extrait le voisin local, l'entité et les données d'adresse associées pour chaque périphérique situé sur le collecteur.
Agent CollectorLayer2	Extrait les informations de connectivité de couche 2 pour les périphériques situés sur le collecteur.
Agent CollectorLayer3	Extrait les informations de connectivité de couche 3 pour les périphériques situés sur le collecteur.
Agent CollectorVpn	Extrait les données du réseau privé virtuel de couches 2 et 3 pour les périphériques situés sur le collecteur.

Concepts associés:

«Composants de l'intégration EMS», à la page 116
L'intégration EMS est composée de plusieurs composants qui fournissent une aide lors de la collecte de données topologiques.

Reconnaissance de connectivité pour les périphériques ATM

Le mode de transfert asynchrone (ATM) est un protocole de commutation alternatif pour les données dont le format est mixte (comme les données pures, les voix et les vidéos). Plusieurs types d'agents de reconnaissance peuvent être utilisés pour reconnaître les périphériques ATM sur un réseau.

Remarque : Avant d'activer ces agents, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.

Tableau 141. Agents de reconnaissance ATM

Nom de l'agent	Fonction
AtmForumPnni	L'agent AtmForumPnni extrait les informations de connectivité des périphériques ATM qui utilisent le protocole de routage dynamique de l'interface PNNI (Private Network-to-Network Interface) et la base d'information de gestion PNNI du forum ATM. Le protocole PNNI est généralement utilisé sur des réseaux importants, puisqu'il fournit une mappe détaillée de la topologie de réseau aux commutateurs ATM afin que les périphériques ATM puissent prendre les meilleures décisions de routage.

Tableau 141. Agents de reconnaissance ATM (suite)

Nom de l'agent	Fonction
CellPath90	L'agent CellPath90 permet la reconnaissance de la connexion ATM des multiplexeurs Marconi CellPath 90 WAN (Wide Area Network). Le multiplexeur CellPath 90 WAN ne connaît pas les adresses ATM de ses voisins, donc il ne peut être que reconnu lorsqu'il est connecté à un autre périphérique ATM certifié, plus intelligent. L'agent de reconnaissance CellPath90 est utilisé dans le calcul de la topologie de réseau. Il place les informations relatives à CellPath 90 dans les couches correctes au sein de la base de données de reconnaissance.
CiscoPVC	L'agent CiscoPVC extrait des données PVC des périphériques Cisco.
CiscoSerialInterface Telnet	L'agent CiscoSerialInterfaceTelnet utilise Telnet pour extraire des informations sur la connectivité du mécanisme de transfert asynchrone (ATM) depuis des périphériques Cisco. Utilisez cet agent si vous disposez de routeurs Cisco connectés par des interfaces série configurées en tant que PVC (circuits virtuels privés) ATM. Vous devez exécuter l'agent Interface avec l'agent CiscoSerialInterfaceTelnet.
ILMI	L'agent ILMI extrait des informations de connectivité des périphériques utilisant l'interface ILMI (Interim Local Management Interface), un standard RFC permettant de gérer les réseaux ATM et IP. Il recherche comment les réseaux ATM sont connectés au circuit virtuel de couche 2 et au niveau de port. Il supprime également la connectivité logique des interfaces d'émulation réseau local.
ILMIForeSys	L'agent ILMIForeSys reconnaît les connexions ATM physiques entre les périphériques utilisant les informations de connectivité ILMI fournies par les commutateurs Marconi ASX. Lorsque la connectivité est déduite à l'aide des informations ILMI, elle est généralement identique à celle qui aurait été calculée à l'aide des informations PNNI, comme dans le cas des agents AtmForumPnni standard et ILMI. Toutefois, il existe certaines situations dans lesquelles les informations ILMI contiennent des détails d'une connexion qui ne figure pas dans les informations PNNI ou d'autres situations dans lesquelles les informations PNNI détaillent une connexion ne figurant pas dans les informations ILMI. Les exemples ci-après détaillent de telles situations : • Les connexions entre les commutateurs ASX et les périphériques à accès intégré SE420/SE440 ne sont reconnues qu'à l'aide de ILMI. • Les connexions entre les routeurs ou les commutateurs Cisco contenant des cartes ATM et un noyau ATM ne peuvent être reconnues qu'à l'aide d'ILMI. • Comme pour l'agent PnniForeSys, l'agent ILMIForeSys est conçu pour fonctionner en continu avec l'agent ILMI. Un réseau contenant un mélange de périphériques ASX et de périphériques d'un autre fournisseur (par exemple, des commutateurs Cisco 5509 avec cartes ATM) peut, par conséquent, être reconnu précisément.
MariposaAtm	L'agent MariposaAtm reconnaît la connectivité ATM des périphériques à accès intégré SE420 et SE440 (IAD). **Remarque :** les fonctions de commutation Ethernet et de relai de trame de ces périphériques ne sont actuellement pas certifiées.
PnniForeSys	L'agent PnniForeSys reconnaît les connexions ATM physiques entre les périphériques à l'aide des informations de connectivité PNNI fournies par les commutateurs Marconi ASX. L'agent PnniForeSys est conçu pour fonctionner avec l'agent AtmForumPnni. Il effectue un traitement supplémentaire sur les périphériques Fore qui ne stockent pas d'ifIndex logique dans leur variable pnniLinkIfIndex. Les informations extraites de ces périphériques exigent un traitement supplémentaire afin d'extraire l'ifIndex actuel contenu dans la variable ifTable. **Remarque :** La configuration de l'auxiliaire SNMP pour les périphériques associés constitue un pré-requis pour cet agent. L'agent AtmForumPnni doit également être actif.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Reconnaissance des périphériques MPLS

Pour reconnaître des données MPLS (Multiprotocol Label Switching), notamment des informations VPLS, activez les agents appropriés.

Les agents qui extraient les données MPLS utilisent le protocole Telnet ou SNMP. Avant d'activer les agents MPLS, configurez l'accès Telnet et SNMP.

- Avant d'activer les agents MPLS qui utilisent le protocole Telnet, vérifiez que vous avez configuré le protocole Telnet afin d'activer l'accès des agents aux périphériques et leur compréhension des sorties de périphériques.
- Avant d'activer les agents MPLS qui utilisent le protocole SNMP, configurez SNMP pour activer l'accès aux unités et spécifier les unités d'exécution, les délais d'attente et le nombre de nouvelles tentatives.

Conseil : Les agents qui extraient des informations VPLS peuvent extraire de grandes quantités de données. L'activation de ces agents peut augmenter considérablement le temps de traitement du processus de reconnaissance. Si vous n'avez pas besoin de redécouvrir les informations VPLS, désactivez ces agents pour une reconnaissance plus rapide.

Tableau 142. Agents de reconnaissance MPLS

Nom de l'agent	Fonction
Agent CiscoMPLSSnmp	L'agent CiscoMPLSSnmp reconnaît les chemins d'accès MPLS sur les unités Cisco utilisant des MIB standard et sur les unités Cisco prenant en charge les MIB MPLS Cisco Experimental.
Agent CiscoMPLSTelnet	L'agent CiscoMPLSTelnet reconnaît les chemins d'accès MPLS et VPLS LDP sur les unités Cisco.
CiscoQinQTelnet	L'agent CiscoQinQTelnet reconnaît la configuration QinQ (IEEE 802.1QinQ) sur les unités Cisco.
Agent HuaweiMPLSTelnet	L'agent HuaweiMPLSTelnet reconnaît les informations liées au protocole MPLS/aux réseaux privés virtuels de couche 2 et 3 sur les périphériques Huawei.
Agent JuniperMPLSTelnet	L'agent JuniperMPLSTelnet reconnaît les chemins d'accès MPLS sur les périphériques Juniper. Cet agent reconnaît également les configurations Juniper MultiHome VPLS et balise VIS (Virtual Switch Instance) en conséquence.
Agent JuniperMPLSSNMP	L'agent JuniperMPLSSNMP reconnaît les données liées aux protocoles MPLS/VPN (reconnaissance VPM basée sur RT) et VPLS (LDP et BGP) sur les unités Juniper.
JuniperQinQTelnet	L'agent JuniperQinQTelnet reconnaît la configuration QinQ (IEEE 802.1QinQ) sur les unités Juniper.

Tableau 142. Agents de reconnaissance MPLS (suite)

Nom de l'agent	Fonction
Agent LaurelMPLSTelnet	L'agent LaurelMPLSTelnet reconnaît les chemins d'accès MPLS sur les périphériques Laurel. Il est uniquement destiné aux reconnaissances basées sur la cible.
StandardMPLSTE	L'agent StandardMPLSTE reconnaît les tunnels MPLS Traffic Engineered (TE) utilisant SNMP.
Agent UnisphereMPLSTelnet	L'agent UnisphereMPLSTelnet reconnaît les chemins d'accès MPLS sur les routeurs Juniper ERX (anciennement Unisphere).

Agents de multidiffusion

Les agents de multidiffusion extraient des données d'unités participant aux groupes et routes de multidiffusion.

Les agents qui extraient des données de multidiffusion ont besoin d'un accès à SNMP et Ping pour pouvoir extraire les données. Avant d'activer les agents de multidiffusion, vérifiez que vous avez configuré le protocole SNMP pour activer les agents afin qu'ils puissent accéder aux unités et pour spécifier les unités d'exécution, les délais d'attente et le nombre de nouvelles tentatives.

Le tableau suivant décrit les agents de multidiffusion.

Tableau 143. Agents de reconnaissance multidiffusion

Nom de l'agent	Fonction
StandardIGMP	Reconnaît les réseaux exécutant le protocole IGMP (Internet Group Management Protocol). Prend en charge toutes les unités conformes à la base d'informations de gestion RFC2933 IGMP. En fonction du niveau de prise en charge de la base d'informations de gestion, les informations suivantes peuvent être reconnues : interfaces IGMP, appartenances au groupe par interface, membres de groupes visibles sur des interfaces IGMP.
StandardIPMRoute	Reconnaît les réseaux de multidiffusion IP. Prend en charge toutes les unités conformes à la base d'informations de gestion RFC2932 IPMRoute. En fonction du niveau de prise en charge de la base d'informations de gestion, les informations suivantes peuvent être reconnues : données de routage de multidiffusion (amont/aval), interfaces impliquées dans le routage multidiffusion, sources et groupes de multidiffusion.
StandardPIM	Reconnaît les réseaux exécutant la gestion des informations produit (PIM) du protocole de multidiffusion. Prend en charge toutes les unités conformes à la base d'informations de gestion RFC2934 PIM. En fonction du niveau de prise en charge de la base d'informations de gestion, les informations suivantes peuvent être reconnues : interfaces PIM, adjacences PIM, Candidat RP/BSR.

Tâches associées:

«Activation des agents de multidiffusion», à la page 42
Pour découvrir des groupes de multidiffusion, vous devez activer les agents appropriés et ajouter les noms de communauté SNMP correspondants.

Reconnaissance des passerelles NAT

Il existe plusieurs agents qui téléchargent les informations de conversion d'adresse réseau (NAT) à partir de passerelles NAT connues.

Aucun des agents répertoriés dans la table ci-dessous n'est activé dans la configuration par défaut. Ces agents requièrent une configuration avancée et il est préférable de ne pas les activer par défaut.

Tableau 144. Agents de passerelle NAT

Nom de l'agent	Fonction
Agent CiscoNATTelnet	L'agent CiscoNATTelnet interroge les routeurs Cisco agissant en tant que passerelle NAT. Il télécharge les conversions d'adresses réseau statiques via le protocole TELNET du périphérique. Les conversions sont ensuite utilisées pour identifier la partie du réseau dans laquelle un périphérique particulier existe. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire Telnet.
NATNetScreen	L'agent NATNetScreen interroge les pare-feux NetScreen® agissant en tant que passerelle NAT. Il télécharge les conversions d'adresses réseau statiques via le protocole TELNET du périphérique. Les conversions sont ensuite utilisées pour identifier la partie du réseau dans laquelle un périphérique particulier existe. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire Telnet.
NATTextFileAgent	L'agent NATTextFileAgent imite la fonction des autres agents de passerelle NAT en lisant les informations de mappage NAT dans un fichier à plat. Les conversions sont ensuite utilisées pour identifier la partie du réseau dans laquelle un périphérique particulier existe. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

«Fichier de configuration DiscoTelnetHelperSchema.cfg», à la page 85
Le fichier de configuration DiscoTelnetHelperSchema.cfg définit le fonctionnement de l'auxiliaire Telnet, qui retourne les résultats d'une opération Telnet dans un périphérique indiqué.

Reconnaissance des informations de confinement

Un principe important utilisé par le modèle de réseau est le confinement. Un conteneur stocke d'autres objets. Vous pouvez placer n'importe quel objet dans un conteneur, voire mélanger plusieurs objets dans le même conteneur.

Parmi les informations de confinement figurent une défaillance physique de tous les composants stockés dans le conteneur ainsi que des informations détaillés sur chacun de ces composants. Les composant pouvant être stockés dans un conteneur sont les suivants :

- Boîtier
- Interface
- Interface logique
- Objet Vlan
- Carte
- PSU
- Collections logiques, comme un réseau privé virtuel
- Module
- Fix Pack 4 Ventilateur

Il existe également une catégorie Inconnu qui couvre les entités pour lesquelles aucun type de composant n'a été défini.

Le tableau suivant décrit les agents de reconnaissance qui reconnaissent les informations de confinement.

Tableau 145. Agents de reconnaissance qui reconnaissent les informations de confinement

Nom de l'agent	Fonction
AvayaPhysicalInventory	L'agent AvayaPhysicalInventory interroge la norme RAPID-CITY MIB pour chaque entité physique et extrait les informations de confinement pour cette dernière. Exécutez cet agent afin de modéliser le confinement physique et d'effectuer la gestion des actifs. Activez cet agent si des périphériques Avaya (ex-Nortel) sont présents dans votre réseau. **Remarque :** Configurez l'accès SNMP et l'auxiliaire SNMP avant d'activer cet agent.
BNTSwitch	L'agent BNTSwitch extrait les informations de connectivité de couche 2 et les informations de confinement VLAN (y compris des balises VLAN, VLAN Trunk, et informations Trunk Group) à l'aide du protocole SNMP.

Tableau 145. Agents de reconnaissance qui reconnaissent les informations de confinement (suite)

Nom de l'agent	Fonction
Entity	L'agent Entity interroge la base d'informations de gestion pour chaque entité et extrait les informations de confinement s'y rapportant. Avant d'activer cet agent, vous devez configurer l'accès et l'auxiliaire SNMP. L'exécution de l'agent Entity lors d'une reconnaissance est facultative. Certaines informations de confinement sont rassemblées lors d'une reconnaissance même si l'agent Entity n'est pas exécuté. Exécutez l'agent afin de modéliser le confinement physique et d'effectuer la gestion des actifs. **Remarque :** Lors d'une reconnaissance, l'agent Entity extrait une grande quantité de données. Cela ralentit la reconnaissance. C'est pourquoi vous ne devez utiliser cet agent que si vous devez effectuer la gestion d'actifs sur les données extraites. Vous pouvez configurer l'agent Entity pour spécifier la quantité de données que l'agent doit extraire. Si vous le désirez, vous pouvez télécharger ces informations supplémentaires à partir des bases d'informations de gestion des entités Asset, ExtraPhysData, Module, Power et Sensor. Pour ce faire, configurez les variables ci-après dans le fichier `Entity.agnt` : • GetAssetData • GetExtraPhysData • GetModuleData • GetPowerData • GetSensorData Dans chaque cas, définissez la valeur `1` pour extraire les données et la valeur `0` si vous ne souhaitez pas le faire. La valeur par défaut est 1. Fix Pack 3 En outre, vous pouvez indiquer la façon dont l'agent Entity extrait les données des périphériques. Les options possibles sont les suivantes : **`0` GetNext** Il s'agit de la valeur par défaut. A l'aide de cette option d'extraction de données, le système demande une seule variable SNMP à la fois au périphérique de la série, c'est-à-dire qu'il extrait une seule colonne dans une table, une seule valeur à la fois pour un périphérique précis. Cette approche est plus lente mais est moins contraignante pour le périphérique. Dans une reconnaissance comprenant plusieurs entités, l'idée est que cette approche ne ralentira pas la reconnaissance, car l'auxiliaire SNMP est encore occupé avec d'autres activités. Cette approche peut nécessiter un très long temps pour les grands périphériques individuels. Cette méthode fonctionne avec SNMP version 1. **`1` GetNext asynchrone** Semblable à la méthode GetNext dans laquelle un seul index est extrait à la fois, à la différence près que toutes les colonnes sont extraites en parallèle. Egalement pris en charge par SNMP version 1 et plus rapide, mais charge davantage le périphérique. **`2` GetBulk** Demande la colonne entière ou plusieurs colonnes et des commandes Get individuelles en une seule fois. Cette méthode nécessite SNMP version 2. Si le périphérique prend uniquement en charge la version 1, la méthode d'extraction est divisée en plusieurs commandes SNMP Get Next et Get. C'est l'extraction la plus rapide et elle ne charge pas plus le périphérique que la méthode Asynchronous GetNext. Cette méthode implique aussi des paquets de plus grande taille sur le réseau. **Remarque :** Le fichier `Entity.agnt`, ainsi que tous les autres fichiers de configuration de l'agent, se trouvent dans le répertoire `$NCHOME/precision/disco/agents`.
Agent IfStackTable	L'agent IfStackTable détermine la hiérarchie d'empilement d'interfaces sur les périphériques qui prennent en charge la base d'informations de gestion RFC 2863. **Remarque :** Configurez l'accès SNMP et l'auxiliaire SNMP avant d'activer cet agent.

Tableau 145. Agents de reconnaissance qui reconnaissent les informations de confinement (suite)

Nom de l'agent	Fonction
JuniperBoxAnatomy	L'agent JuniperBoxAnatomy extrait les informations sur les modules et les composants installés sur un périphérique Juniper et leur confinement. L'agent utilise les informations MIB spécifiques du fournisseur telles que celles relatives à Juniper Box Anatomy pour tous les périphériques Juniper. Fix Pack 4 Cet agent est amélioré pour utiliser la base d'informations de gestion Juniper Fabric Anatomy pour les périphériques Juniper QFabric.
Agent JuniperERXIfStackTable	L'agent JuniperERXIfStackTable détermine la hiérarchie d'empilement d'interfaces sur les périphériques Juniper ERX. Il détermine les informations d'empilement contextuelles de routeur virtuel et VRF pour les périphériques Juniper ERX. Lorsqu'une reconnaissance contextuelle est activée, cet agent peut être désactivé puisque l'agent IfStackTable détermine également ces informations. Cela va améliorer les performances de la reconnaissance. **Remarque :** Configurez l'accès SNMP et l'auxiliaire SNMP avant d'activer cet agent.
JuniperLAGStack	L'agent JuniperLAGStack extrait les informations LAG (Link Aggregation Group) des périphériques Juniper. Ces informations permettent de représenter avec précision la hiérarchie d'empilement de l'interface.
Fix Pack 4 ZTEPPhysicalInventory	Fix Pack 4 L'agent ZTEPhysicalInventory interroge les normes ZXR10-MIB, ZXR10-RACK-MIB et ZXR-SYSTEM-HARDWARE-MIB pour chaque entité physique et extrait les informations de confinement pour chacune d'entre elles. Fix Pack 4 Cet agent modélise le confinement physique et effectue la gestion des actifs pour les périphériques ZTE T1200, T600 et M6000. Parmi les informations de confinement figurent une défaillance physique de tous les composants stockés dans le conteneur ainsi que des informations détaillés sur chacun de ces composants.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Agents de reconnaissance utilisant d'autres protocoles

Network Manager propose des agents reconnaissant des périphériques qui utilisent d'autres protocoles que ceux décrits précédemment

Remarque : Avant d'activer ces agents, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.

Tableau 146. Agents de reconnaissance utilisant d'autres protocoles

Nom de l'agent	Fonction
Agent AlteonStp	Il s'agit d'un agent de reconnaissance STP (Spanning Tree Protocol) pour les commutateurs Alteon qui prennent en charge la section dot1dStp de BRIDGE-MIB.

Tableau 146. Agents de reconnaissance utilisant d'autres protocoles (suite)

Nom de l'agent	Fonction
Agent CDP	L'agent CDP comprend le protocole utilisé parmi les périphériques de communication Cisco. A l'aide de l'agent CDP, les périphériques Cisco peuvent reconnaître leur voisins immédiats et stocker des informations minimales les concernant. Cet agent commence par l'adresse d'un périphérique Cisco connu et utilise le protocole CDP pour rechercher des informations plus complètes sur les emplacements d'autres périphériques Cisco connectés ou voisins.
DefaultLLDP	L'agent DefaultLLDP reconnaît la connectivité de couche 2 entre les périphériques qui prennent en charge les normes LLDP MIB et ont activé le protocole LLDP (Link Layer Discovery Protocol). Les agents LLDP et DefaultLLDP utilisent les données de la norme LLDP MIB qui sont indexées par lldpRemLocalPortNum. Cette variable indique sur quel ifIndex ou port se trouve une connexion LLDP particulière. L'agent LLDP prend en charge des périphériques où lldpRemLocalPortNum désigne l'ifIndex sur le périphérique : des périphériques Cisco, en général. L'agent DefaultLLDP prend en charge les périphériques où lldpRemLocalPortNum désigne le port ou un autre index affecté de manière arbitraire ; en général, des périphériques non-Cisco tels que Juniper ou BNT. L'agent DefaultLLDP vérifie si le périphérique prend en charge la norme Extended-LLDP-MIB. Si ce n'est pas le cas, il est admis que lldpRemLocalPortNum est un port de commutation. L'agent utilise alors la variable dot1dBasePortIfIndex de la norme BRIDGE-MIB pour déterminer l'ifIndex de cet enregistrement. Activez les agents LLDP et DefaultLLDP afin que Network Manager puisse trouver la connectivité LLDP sur les périphériques qui comportent des implémentations différentes de lldpRemLocalPortNum.
Agent FddiDefault	L'agent FddiDefault reconnaît tout périphérique qui prend en charge la base d'informations de gestion FDDI standard. Lorsqu'un périphérique FDDI est interrogé, les informations liées à ses interfaces ainsi qu'à ses voisins en amont et en aval sont renvoyées. Le programme stitcher FddiLayer utilise cet agent ainsi que tous les autres agents FDDI pour déterminer la topologie en anneau FDDI.
Agent FddiCiscoConc	L'agent FddiCiscoConc reconnaît les périphériques Cisco Concentrator FDDI. Les concentrateurs Cisco connaissant la connectivité complète de chaque anneau FDDI qui les traversent, et non leurs voisins en aval et en amont uniquement. Par conséquent, le programme stitcher FddiLayer donne la priorité aux informations topologiques renvoyées par cet agent, par rapport à celles trouvées par FddiDefault.

Tableau 146. Agents de reconnaissance utilisant d'autres protocoles (suite)

Nom de l'agent	Fonction
LLDP	L'agent LLDP reconnaît la connectivité de couche 2 entre les périphériques qui prennent en charge les normes LLDP MIB et ont activé le protocole LLDP (Link Layer Discovery Protocol). Les agents LLDP et DefaultLLDP utilisent les données de la norme LLDP MIB qui sont indexées par lldpRemLocalPortNum. Cette variable indique sur quel ifIndex ou port se trouve une connexion LLDP particulière. L'agent LLDP prend en charge des périphériques où lldpRemLocalPortNum désigne l'ifIndex sur le périphérique : des périphériques Cisco, en général. L'agent DefaultLLDP prend en charge les périphériques où lldpRemLocalPortNum désigne le port ou un autre index affecté de manière arbitraire ; en général, des périphériques non-Cisco tels que Juniper ou BNT. L'agent LLDP vérifie si le périphérique prend en charge la norme Extended-LLDP-MIB. Si c'est le cas, il extrait le mappage entre lldpRemLocalPortNum et ifIndex. Dans le cas contraire, il est admis que lldpRemLocalPortNum est l'ifIndex. Activez les agents LLDP et DefaultLLDP afin que Network Manager puisse trouver la connectivité LLDP sur les périphériques qui comportent des implémentations différentes de lldpRemLocalPortNum.
SONMP	L'agent SONMP utilise SynOptics Network Management Protocol, protocole utilisé entre les périphériques de communications Nortel. L'agent SONMP commence avec l'adresse d'un périphérique Nortel connu et utilise SONMP pour reconnaître les informations d'emplacement, de confinement, d'adresse et de connexion à partir des périphériques Nortel de voisinage ou connectés.
Agent StandardSTP	L'agent StandardSTP reconnaît les données de connectivité STP sur tout commutateur activé pour STP qui prend en charge la section dot1dSTP de BRIDGE-MIB. Vous devriez exécuter cet agent en plus de tout autre agent de commutateur nécessaire afin de reconnaître les connexions STP de secours (blocantes). La méthode de reconnaissance de commutateur STP offre les avantages suivants par rapport à d'autres méthodes de reconnaissance basées sur commutateur : • Liens cachés : les connexions STP de secours (blocantes) sont reconnues. • Vitesse : l'agent se termine dans la phase 1 et aucune émission de commande PING n'est nécessaire. **Remarque** : l'agent STP n'affiche que les connexions entre les commutateurs activés pour STP, c'est-à-dire qu'il ignore les connexions aux noeuds, aux périphériques autres que des commutateurs et aux commutateurs non activés pour STP. Cet agent ne va pas reconnaître plusieurs instances STP, VLAN ou routeurs virtuels.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables

MIB des unités.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Agents de reconnaissance contextuelle

Il existe plusieurs agents qui prennent part à la reconnaissance contextuelle.

Avertissement : Lorsqu'une reconnaissance contextuelle est activée, le processus de reconnaissance choisit automatiquement l'agent Context correct pour un périphérique particulier. Pour cette raison, vous ne devriez pas activer ou désactiver manuellement les agents Context à l'aide des fichiers de configuration ou de l'interface graphique de configuration de la reconnaissance.

Remarque : Ces agents requièrent un accès et un auxiliaire Telnet.

Tableau 147. Agents de reconnaissance contextuelle

Nom de l'agent	Fonction
RedbackContext	L'agent RedbackContext reconnaît les informations contextuelles du routeur virtuel pour les périphériques Redback®.
UnisphereERXContext	L'agent UnisphereERXContext reconnaît le routeur virtuel et les informations contextuelles VRF pour les périphériques Juniper ERX. Vous pouvez limiter la portée des contextes VRF reconnus en configurant la section facultative DiscoAgentDiscoveryScoping dans le fichier .agnt. Les options configurables sont les suivantes : • IncludeVRF – autorise la reconnaissance du VRF indiqué. • ExcludeVRF – ne reconnaît pas le VRF indiqué. Les noms de VRF font la distinction entre les majuscules et les minuscules. Le caractère générique " * " peut être utilisé à la place du nom de VRF pour appliquer le filtre à tous les VRF. Si aucun filtre n'est spécifié, tous les VRF sont reconnus par défaut.

Concepts associés:

«Reconnaissance contextuelle», à la page 9
Si vous devez reconnaître des périphériques comme des périphériques SMS, MPLS Edge ou autres à l'aide de routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. Ce type de reconnaissance permet une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type particulier de périphériques est pris en charge par la reconnaissance.

Tâches associées:

«Configuration d'une reconnaissance contextuelle», à la page 139
Si vous disposez d'unités que vous devez reconnaître, comme des unités périphériques SMS, MPLS ou d'autres unités comportant des routeurs virtuels, vous devez exécuter une reconnaissance contextuelle. La reconnaissance contextuelle garantit une représentation correcte des routeurs virtuels. Vérifiez toujours que votre type d'unité est pris en charge par la reconnaissance.

Référence associée:

«Fichier de configuration DiscoConfig.cfg», à la page 74
Le fichier de configuration DiscoConfig.cfg permet à l'outil de recherche Ping de vérifier automatiquement les unités découvertes par l'outil de recherche de fichiers

et de permettre une reconnaissance contextuelle.

«Fichier de configuration TelnetStackPasswords.cfg», à la page 92
Le fichier de configuration TelnetStackPasswords.cfg définit les droits d'accès aux unités Telnet.

«Fichier de configuration DiscoTelnetHelperSchema.cfg», à la page 85
Le fichier de configuration DiscoTelnetHelperSchema.cfg définit le fonctionnement de l'auxiliaire Telnet, qui retourne les résultats d'une opération Telnet dans un périphérique indiqué.

Agents de reconnaissance spécifiques à une tâche

Il existe un groupe d'agents spécifiques à une tâche.

Tableau 148. Agents de reconnaissance spécifiques à une tâche

Nom de l'agent	Fonction
Agent AlliedTelesynATSwitch	L'agent AlliedTelesynATSwitch reconnaît les commutateurs Ethernet fabriqués par Allied Telesyn. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent AlteonSwitch	L'agent AlteonSwitch extrait les informations sur la connectivité de couche 2 des équilibreurs de charge Alteon et des modules de commutation Ethernet. **Remarque :** Configurez l'accès SNMP et l'auxiliaire SNMP avant d'activer cet agent.
Agent ARPCache	Il aide à remplir le serveur auxiliaire avec les mappages d'adresses IP sur MAC pour préparer les agents de reconnaissance Ethernet. Vous devez exécuter cet agent si vous exécutez une reconnaissance de couche 2. Il est facultatif si vous exécutez une reconnaissance de couche 3. Toutefois, il peut être plus efficace d'utiliser l'agent de reconnaissance ARP Cache car, dans la plupart des environnements de réseau, l'auxiliaire ARP ne peut s'exécuter que sur un sous-réseau à la fois. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.

Tableau 148. Agents de reconnaissance spécifiques à une tâche (suite)

Nom de l'agent	Fonction
Agent ASM	Détermine si les ASM du serveur commercial et les produits de base de données sont en cours d'exécution sur un périphérique : • Oracle • Apache • Microsoft SQL Server • Microsoft Exchange • Microsoft Internet Information Server (IIS) • Microsoft Active Directory • IBM WebSphere • BEA WebLogic • SAP • Sybase ASE • IBM Lotus Notes/Domino Server L'agent ASM détermine si une application est en cours d'exécution en interrogeant les bases d'informations des gestion du périphérique, spécifiques aux ASM. Ces bases d'informations de gestion sont installées par défaut lorsque vous installez Network Manager. L'agent ASM ne peut extraire ces informations qu'à partir des périphériques réseau sur lesquels l'agent ASM est déployé. Généralement, vous déployez un sous-agent ASM sur chaque serveur commercial et sur chaque produit de base de données s'exécutant sur un périphérique et dont vous souhaitez surveiller les performances.
BGPPeerNextHop Interface	Toutes les interfaces PE vers CE sont ajoutées à une liste de membres et un événement sur l'une des interfaces de cette liste de membres entraîne la génération par le système d'un SAE VPN MPLS synthétique. Cet agent, qui est désactivé par défaut, permet la génération d'événements affectés par un service (SAE) VPN MPLS, en fonction des dépendances d'interfaces plus profondément dans le réseau principal. Cet agent appelle le programme stitcher AddLayer3VPNInterfaceDependency.stch. Ce programme stitcher détermine toutes les interfaces PE à routeur de fournisseur principal et les interfaces P à PE, impliquées dans un réseau privé virtuel. Ces interfaces PE -> P et P ->PE sont ajoutées à une liste de dépendances. Un événement sur l'une des interfaces dans cette liste de dépendances entraîne la génération par le système d'un SAE de réseau privé virtuel MPLS. Si un SAE VPN MPLS a déjà été généré en fonction d'un événement sur l'une des interfaces de la liste des membres, tous les événements des interfaces de la liste de dépendances sont ajoutés en tant qu'événements associés à ce SAE VPN MPLS déjà généré.

Tableau 148. Agents de reconnaissance spécifiques à une tâche (suite)

Nom de l'agent	Fonction
Agent CM	Extrait les données des modems câble connectés à un périphérique système de terminaison de modem câble. **Remarque** : s'il est activé, cet agent extrait une grande quantité d'informations. L'activation de cet agent peut de ce fait exercer une forte charge sur la mémoire. Vous ne devriez activer cet agent que si des informations spécifiques au modem câblé sont requises en plus de celles fournies par les autres agents.
Agent CMTS	Reconnaît les périphériques système de terminaison de modem câble. Cet agent reconnaît également la connectivité du modem câblé. **Remarque** : s'il est activé, cet agent extrait une grande quantité d'informations. L'activation de cet agent peut de ce fait exercer une forte charge sur la mémoire. Vous ne devriez activer cet agent que si des informations spécifiques au modem câblé sont requises en plus de celles fournies par les autres agents.
Agent ExtraDetails	L'agent ExtraDetails est un agent basé sur texte reposant sur les informations SNMP de base déjà extraites par l'agent Details. Il extrait les informations suivantes : • sysDescr • sysLocation • sysUpTime • sysServices • ifNumber **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent HPNetworkTeaming	L'agent HPNetworkTeaming reconnaît la carte d'interface réseau secondaire sur les cartes réseau HP Proliant reliées. Si l'agent n'est pas activé, seule la carte d'interface réseau principale d'un périphérique HP Proliant sera reconnue (comme voisin local sur le serveur) car c'est la seule carte d'interface réseau qui se trouve dans la table `ifTable`. Cet agent va créer toutes les cartes d'interface réseau en tant que voisins locaux sur le serveur. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent LoopbackDetails	L'agent LoopbackDetails est utilisé pour vérifier que l'interface de gestion d'un périphérique est utilisée dans la topologie et dans la surveillance ultérieure comme combinaison IP/nom principale. L'agent extrait les informations nécessaires pour identifier les interfaces de gestion. Ces données sont ensuite utilisées dans le programme stitcher NamingFromLoopbackDetails. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent MACFromArpCache	L'agent ArpCache doit être activé pour que cet agent s'exécute. L'agent MACFromArpCache est activé en option durant la phase 3 de la reconnaissance. Il utilise les informations ArpCache extraites par l'agent ArpCache afin d'extraire l'adresse MAC du périphérique. Il est utile puisqu'il ne nécessite pas d'accès SNMP au périphérique pour obtenir l'adresse MAC.

Tableau 148. Agents de reconnaissance spécifiques à une tâche (suite)

Nom de l'agent	Fonction
NetScreenArpCache	L'agent NetScreenArpCache extrait des informations des tables ARP configurées dans les périphériques Netscreen et traite les tables pour obtenir la conversion IP vers MAC. L'agent envoie ensuite les informations ARP à l'auxiliaire ARP. Après traitement, l'auxiliaire ARP envoie le mappage d'adresse IP et MAC à la table ARPHelperTable. L'agent NetScreenArpCache utilise la base d'informations de gestion standard SNMPv2-SMI. **Remarque :** L'agent ArpCache ne traite pas les périphériques Netscreen traités par l'agent NetScreenArpCache. Cela évite les conflits dans la valeur ipForwarding car Netscreen est reconnu comme un périphérique de non routage par l'agent ArpCache.
NMAPScan	L'agent NMAPScan est un agent Perl qui exécute le scanner NMAP sur les périphériques reconnus par Network Manager. Par défaut, l'agent s'exécute sur des périphériques qui n'ont pas d'accès SNMP ou qui ont un accès SNMP mais renvoient des sysObjectIds de périphériques Apple, Compaq, IBM, Microsoft, Sun, Network Harmoni, UC David, Net-SNMP et HP. L'agent extrait les données suivantes : • Détails de l'empreinte digitale du système d'exploitation • Port TCP/UDP et informations sur les applications, y compris le numéro de port, le nom, l'état, le type et le service Vous devez installer NMAP version 4.85 ou ultérieure sur le serveur où sont installés les composants centraux de Network Manager. Vous devez ensuite éditer le fichier `NMAPScan.pl` et spécifier le chemin d'accès vers le fichier binaire NMAP dans la ligne **`my $nmapBinary`** et supprimer le commentaire au début de la ligne. NMAP est disponible sur http://nmap.org. **Avertissement :** L'activation de l'agent NMAPScan peut prolonger la durée de la reconnaissance. NMAP comporte un grand nombre d'options d'analyse, consultez la documentation NMAP pour plus d'informations. Les options suivantes sont définies par défaut pour NMAP : • -sS : Exécuter une analyse TCP SYN • -sV : Activer l'identification de la version du service • -PN : Ne pas effectuer de PING sur chaque cible (Network Manager utilise déjà l'outil de recherche PING ou FILE ou les deux) • -O : Activer l'empreinte digitale du système d'exploitation • -oX : Activer la sortie XML **Important :** Ne modifiez pas cette valeur.
OSInfo	Extrait des informations sur le système d'exploitation s'exécutant sur les périphériques reconnus. Cet agent s'exécute uniquement sur les périphériques Cisco et Juniper. L'agent extrait les informations suivantes : • OSType • OSVersion • OSImage

Tableau 148. Agents de reconnaissance spécifiques à une tâche (suite)

Nom de l'agent	Fonction
Agent SSM	L'agent SSM extrait les informations de base d'informations de gestion des périphériques exécutant les agents SSM, via le protocole SNMP. Il extrait par exemple des informations telles que le logiciel installé sur le périphérique, les processus en cours d'exécution, l'utilisation de l'unité centrale, les périphériques de stockage de cette entité, l'espace disque libre, etc. L'agent SSM peut uniquement extraire ces informations des périphériques réseau sur lesquels l'agent SSM est déployé. Généralement, vous déployez un agent SSM sur des périphériques dont vous souhaitez surveiller les performances. Pour obtenir plus d'informations sur l'agent SSM, consultez le guide *SSM Application Guide*. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent SSMOracle	L'application SSM et le module de surveillance Oracle doivent également être en cours d'exécution. L'agent SSMOracle extrait les informations sur les bases d'informations de données via le protocole SNMP des périphériques exécutant les agents SSM. Il extrait des informations comme les noms de base de données, les zones et les tailles de bases de données Oracle. L'agent SSMOracle peut uniquement extraire ces informations des périphériques réseau sur lesquels l'agent SSM est déployé. Généralement, vous déployez un agent SSM sur des périphériques dont vous souhaitez surveiller les performances. Pour obtenir plus d'informations sur l'agent SSM, consultez le guide *SSM Application Guide*. **Remarque :** Avant d'activer cet agent, il est nécessaire de configurer l'accès et l'auxiliaire SNMP.
Agent Tunnel	Modèle destiné à un agent Perl afin d'extraire des informations sur tous les tunnels, y compris les tunnels IPv6 et IPv4, présents dans le réseau. Cet agent fonctionne en association avec l'agent IPv6Interface.

Référence associée:

«Fichier de configuration SnmpStackSecurityInfo.cfg», à la page 89
Le fichier de configuration SnmpStackSecurityInfo.cfg définit les noms de communauté, la gestion des versions et d'autres propriétés utilisées par tout processus ayant besoin d'interroger des unités qui utilisent SNMP, l'auxiliaire SNMP par exemple. Les noms de communauté peuvent être configurés par unité ou par sous-réseau, afin de permettre à l'auxiliaire SNMP d'extraire les variables MIB des unités.

«Fichier de configuration DiscoSnmpHelperSchema.cfg», à la page 84
Le fichier de configuration DiscoSnmpHelperSchema.cfg définit le fonctionnement de l'auxiliaire SNMP, qui indique les règles générales de récupération des informations SNMP.

Agents de reconnaissance pour IPv6

Network Manager fournit un modèle d'agent Perl que vous pouvez utiliser comme base pour développer vos propres agents Perl afin d'extraire les données de l'interface IPv6.

Le tableau 149 décrit les modèles d'agent Perl.

Remarque : Au lieu d'avoir des agents possédant des compétences IPv6 spécifiques, vous pouvez utiliser des agents de reconnaissance ayant des compétences IPv6 globales. par exemple, l'agent InetRouting prend en charge les entrées de routage IPv6 et permet également de télécharger des interfaces IPv4 et des informations de routage.

Tableau 149. Modèle d'agent IPv6

Nom de l'agent	Fonction
Interface IPv6	Modèle destiné à un agent Perl afin d'extraire les informations d'interface d'un périphérique IPv6. Cet agent est conçu pour fonctionner de la même manière que l'agent Interface. Ce modèle est situé dans le répertoire des agents Perl, à l'emplacement suivant : `$NCHOME/precision/disco/agents/perlAgents`.

Conseils relatifs à la sélection des agents

Pour reconnaître des technologies de périphériques (c'est-à-dire, utilisant d'autres protocoles qu'IP) sur votre réseau, vous devez vous assurer que les agents appropriés sont actifs.

La liste ci-dessous indique les protocoles de périphériques non IP pris en charge par Network Manager. Vous pouvez sélectionner les agents appropriés pour ces protocoles.

- Relais de trame
- Private Network-Network Interface (PNNI)
- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)
- Hot Standby Routing Protocol (HSRP)
- Fibre Distributed Data Interface (FDDI)
- Asynchronous Transfer Mode (ATM)
- Integrated Local Management Interface (ILMI)
- Multiprotocol Label Switching (MPLS)

Agents de couche IP à utiliser

Les agents de couche IP que vous devez utiliser dépendent des périphériques de votre réseau :

- Si vous ne voulez pas d'accès à vos tables de routage IP, vous devez uniquement utiliser l'agent IpBackupRoutes.

  Par défaut, cet agent n'est pas utilisé car il présente les inconvénients suivants :

  – Il extrait des données d'une table non dynamique. Si le routeur n'a pas été régénéré, les données extraites par cet agent peuvent être erronées.

  – La table est de grande taille et, par conséquent, son téléchargement dure longtemps.

- Si votre réseau comprend des périphériques modernes, vous devez utiliser les agents IpRoutingTable et IpForwardingTable.

  Ils fournissent une image réelle de la connectivité de couche IP et sont donc utilisés par défaut.

Agents standard à utiliser

Les agents standard que vous devez utiliser dépendent des informations requises et des périphériques de votre réseau.

- L'agent TraceRoute peut être utilisé si un pare-feu se trouve sur le réseau, car les appels SNMP ne peuvent pas toujours être effectués à travers les pare-feux. Si vous utilisez l'agent TraceRoute, vous devez spécifier, en tant qu'emplacement de départ de la reconnaissance, le noeud de sous-réseau de l'autre côté du pare-feu.
- L'agent ArpCache extrait l'adresse physique d'un périphérique, il est donc uniquement requis (avec les agents Switch) lors de l'exécution de reconnaissances de couche 2.
- Les agents de relais de trame doivent être exécutés conjointement aux agents de couche IP si vous devez ajouter des informations DLCI aux interfaces de périphériques de relais de trame.
- Les agents Switch doivent être exécutés pour une reconnaissance de couche 2.
- Les agents spécifiques au périphérique et au protocole sont uniquement requis pour reconnaître les périphériques ou protocoles auxquels ils font référence.

Agents spécialisés à exécuter

Plusieurs agents ne doivent être exécutés que si vous devez reconnaître certains types de périphériques ou de technologies de réseau.

Les agents spécialisés que vous devez exécuter dépendent des périphériques et protocoles de votre réseau :

- L'agent Extreme peut être utilisé pour extraire les informations de connectivité de couche 2, les voisins EDP et les détails VLAN de commutateurs Extreme.
- L'agent ExtremeESRP reconnaît les informations de la table de routage Extreme Standby Routing Table des commutateurs de routage Extreme.
- L'agent PnniForeSys reconnaît les connexions ATM physiques entre les périphériques en utilisant les informations de connectivité PNNI (Private Network-to-Network Interface) fournies par les commutateurs Marconi ASX.
- L'agent ILMIForeSys reconnaît les connexions ATM physiques entre les périphériques en utilisant les informations de connectivité ILMI (Interim Local Management Interface) fournies par les commutateurs Marconi ASX.
- L'agent CellPath90 reconnaît la connexion ATM d'un multiplexeur WAN (Wide Area Network) CellPath 90.
- L'agent Marconi3810 reconnaît la connectivité Ethernet des commutateurs ES-3810 qui exécutent le système d'exploitation de version 4.x.x.
- L'agent MariposaAtm reconnaît la connectivité ATM des IAD SE420 SE440.

  Remarque : Les fonctions de commutation Ethernet et de relais de trame de ces périphériques ne sont actuellement pas certifiées.
- L'agent ILMI reconnaît la connectivité entre les périphériques ATM exécutant ILMI qui prennent en charge le MIB ATM du forum ATM. L'agent CiscoPVC extrait les données de circuit virtuel permanent des périphériques Cisco.

- L'agent AtmForumPnni reconnaît la connectivité entre les périphériques exécutant le PNNI du forum ATM, qui prennent correctement en charge le PNNI MIB du forum ATM.
- Pour les périphériques Cisco, exécutez l'agent CiscoMPLSSnmp si les MIB MPLS sont activés sur un périphérique, sinon utilisez l'agent CiscoMPLSTelnet.
- Pour les périphériques Juniper, exécutez l'agent JuniperMPLSTelnet si vous souhaitez reconnaître les chemins MPLS.
- Pour les périphériques Juniper ERX (précédemment Unisphere), l'agent UnisphereMPLSTelnet doit être utilisé pour reconnaître les chemins MPLS, car ces périphériques sont suffisamment différents des routeurs Juniper de série "M", qu'un agent différent est requis.
- L'agent StandardMPLSTE reconnaît les tunnels MPLS Traffic Engineered (TE).
- L'agent StandardIGMP reconnaît les réseaux exécutant le protocole IGMP (Internet Group Management Protocol).
- L'agent StandardIPMRoute reconnaît les réseaux de multidiffusion IP.
- L'agent StandardPIM reconnaît les groupes PIM (Protocol Independent Multicast).

Référence associée:

«Types d'agents», à la page 375
Les agents fournis avec Network Manager peuvent être divisés en catégories en fonction du type de données qu'ils extraient ou de la technologie qu'ils découvrent.

Agents suggérés pour une reconnaissance de couche 3

Les agents recommandés pour une reconnaissance de couche 3 dépendent de votre réseau.

Lorsque vous exécutez une reconnaissance de couche 3, les agents suivants doivent être exécutés :

- Details et AssocAddress
- Une combinaison des agents de couche IP suivants :
  - IpRoutingTable
  - IpBackupRoutes
  - IpRoutingTable et IpForwardingTable
- HSRP
- VRRP
- TraceRoute (si des pare-feux sont présents)
- IPv4/6 InetRouting. Si vous avez IPv6 dans votre réseau, considérez l'exécution de cet agent pour reconnaître la connectivité, en particulier la connectivité IPv6.

Conseil : Certains routeurs prennent en charge les technologies de couche 2. Par exemple, lorsqu'une carte ATM se trouve dans un boîtier de routeur, les agents de reconnaissance de couche 3, tels que IpRoutingTable reconnaissent uniquement les interfaces disposant d'une adresse IP. Par conséquent, pour reconnaître complètement toutes les interfaces sur les routeurs qui prennent en charge les technologies de couche 2, vous devez exécuter les agents appropriés.

Référence associée:

«Agents suggérés pour une reconnaissance de couche 2», à la page 405
Les agents recommandés pour une reconnaissance de couche 2 dépendent de votre réseau.

Agents suggérés pour une reconnaissance de couche 2

Les agents recommandés pour une reconnaissance de couche 2 dépendent de votre réseau.

Lorsque vous exécutez une reconnaissance de couche 2, les agents suivants doivent être exécutés :

- Details et AssocAddress
- Une combinaison des agents de couche IP suivants :
  - IpRoutingTable
  - IpBackupRoutes
  - IpRoutingTable et IpForwardingTable
- Switch
- FrameRelay
- ArpCache
- ATM
- FDDI
- HSRP
- VRRP
- MPLS

Référence associée:

«Agents suggérés pour une reconnaissance de couche 3», à la page 404
Les agents recommandés pour une reconnaissance de couche 3 dépendent de votre réseau.

Annexe D. Système auxiliaire

Les auxiliaires sont des applications spécialisées qui extraient des informations du réseau, sur demande.

Remarque : Si les auxiliaires et le serveur auxiliaire sont en cours d'exécution sur un hôte différent de celui du processus DISCO, et si ces hôtes se trouvent derrière un pare-feu, une configuration spécialisée est requise pour vérifier que le système auxiliaire peut communiquer avec DISCO. Pour obtenir plus d'informations, consultez le guide *IBM Tivoli Network Manager IP Edition - Guide d'administration*.

Auxiliaires

Les auxiliaires extraient des informations des périphériques et les consignent dans le serveur auxiliaire pour extraction par les agents.

Par défaut, il existe six auxiliaires qui sont décrits dans le tableau 150.

Tableau 150. Auxiliaires disponibles avec Network Manager.
Remarque : $NCHOME est la variable d'environnement qui contient le chemin d'accès au répertoire netcool.

Auxiliaire	Exécutable	Fichier de configuration	Description
Protocole de résolution d'adresse	ncp_dh_arp	$NCHOME/etc/precision/DiscoARPHelperSchema.cfg	Effectue la résolution d'une adresse IP sur une adresse MAC.
DNS	ncp_dh_dns	$NCHOME/etc/precision/DiscoDNSHelperSchema.cfg	Effectue la résolution d'une adresse IP sur un nom de périphérique.
Commande PING	ncp_dh_ping	$NCHOME/etc/precision/DiscoPingHelperSchema.cfg	Emet une commande PING à l'attention de chaque périphérique dans un sous-réseau, une adresse IP individuelle, une diffusion ou une adresse de multidiffusion. Le résultat de la commande PING peut être utilisé pour remplir la base d'informations de gestion du périphérique.
SNMP	ncp_dh_snmp	$NCHOME/etc/precision/DiscoSnmpHelperSchema.cfg $NCHOME/etc/precision/SnmpStackSchema.cfg $NCHOME/etc/precision/SnmpStackSecurityInfo.cfg	Renvoie les résultats d'une requête SNMP telle que Get, GetNext et GetBulk.

Tableau 150. Auxiliaires disponibles avec Network Manager (suite).
Remarque : $NCHOME est la variable d'environnement qui contient le chemin d'accès au répertoire netcool.

Auxiliaire	Exécutable	Fichier de configuration	Description

TELNET	ncp_dh_telnet	`$NCHOME/etc/precision/DiscoTelnetHelperSchema.cfg`
		`$NCHOME/etc/precision/TelnetStackPasswords.cfg`
		`$NCHOME/etc/precision/TelnetStackSchema.cfg`
			Renvoie les résultats d'une commande du système d'exploitation pour un périphérique spécifique à l'aide du protocole Telnet ou SSH.

XMLRPC	ncp_dh_xmlrpc	$NCHOME/etc/precision/DiscoXmlRpcHelperSchema.cfg	Permet à Network Manager de communiquer avec les collecteurs du système de gestion d'éléments à l'aide de l'interface XML-RPC.

Opération du système auxiliaire

Au démarrage, le serveur auxiliaire charge son schéma à partir du fichier de configuration DiscoHelperServerSchema.cfg et crée les bases de données auxiliaires appropriées. Il crée également un gestionnaire auxiliaire pour chaque base de données auxiliaire.

Le gestionnaire auxiliaire gère la manière selon laquelle l'auxiliaire traite les requêtes du serveur auxiliaire pour extraire les données sur les périphériques réseau. Il indique :

- Le délai d'attente pour la requête
- La durée de vie des variables renvoyées
- Si plusieurs requêtes doivent être traitées en série ou parallèlement

Lorsque le gestionnaire d'auxiliaires détecte une requête pour des données réseau, provenant du serveur auxiliaire,il donne l'ordre à l'auxiliaire associé d'extraire les données du réseau.

Délais d'attente dynamiques

Le système auxiliaire utilise les délais d'attente dynamiques pour gérer les requêtes du réseau.

Exemple de l'avantage des délais d'attente dynamiques : si le système demande à l'auxiliaire SNMP d'effectuer plusieurs requêtes SNMP Get, il se peut que l'auxiliaire se mette à ralentir et dépasse ainsi le délai d'attente. Un délai d'attente statique pourrait causer l'extraction des données se terminant par leur perte, même si le périphérique répond toujours avec les données.

Afin d'éviter cette situation, les auxiliaires intègrent un système de délai d'attente dynamique dans lequel ils notent les requêtes SNMP Get, recalculent et mettent à jour le délai d'attente lorsque les démons SNMP du périphérique commencent à ralentir.

Annexe E. Programmes stitcher de reconnaissance

Les programmes stitcher sont des processus qui transfèrent, manipulent et distribuent des données entre des bases de données. Les programmes stitcher de reconnaissance traitent également les informations collectées par les agents et les utilisent pour créer la topologie réseau.

Les programmes stitcher de reconnaissance livrés avec Network Manager sont stockés dans les répertoires suivants.

- Programmes stitcher de reconnaissance textuels (fichiers texte ayant l'extension .stch) : `$NCHOME/precision/disco/stitchers/`
- Programmes stitcher de reconnaissance précompilés : `$NCHOME/precision/platform/`*`platform`*`/lib/`, où *platform* est le système d'exploitation sur lequel s'exécute Network Manager. Par exemple : `linux2x86`, `win32`, `solaris2`, `aix5`, `hpux11` ou `linux2s390`.

Pour plus d'informations sur le langage utilisé dans les programmes stitcher, voir *IBM Tivoli Network Manager IP Edition - Guide de référence des langages*.

Principaux programmes stitcher de reconnaissance

Cette rubrique répertorie tous les programmes stitcher de reconnaissance.

Le tableau suivant décrit les programmes stitcher de reconnaissance inclus à Network Manager.

Remarque : Cette liste est susceptible d'être modifiée.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager

Programme stitcher	Fonction
AddAEPhysicalIFContainment	Ajout des interfaces physiques au châssis dans la structure de confinement LAG (Link Aggregation Group) des périphériques Juniper. Ce programme stitcher est appelé par BuildContainment.stch.
AddBaseNATTags	Met à jour toutes les adresses NAT privées qui ont une adresse privée avec leur adresse publique et ajoute une balise qui indique l'adresse privée.
AddBasicContainment	Partie du mécanisme de piquage de confinement. Ce programme stitcher insère des informations de confinement dans le boîtier simple.
AddCardContainment	Ajoute des objets carte dans la table `workingEntities.containment`.
AddContainedByAttribute	Ajoute un attribut ExtraInfo appelé m_PhysicallyContainedBy. Analogue à l'attribut RFC2737, PhysicalContainedIn, et identifie l'enregistrement contenant un enregistrement particulier. Ces données sont utilisées par Netcool pour la gestion des actifs et l'intégration à Cramer et ne doivent pas être en commentaire dans le programme stitcher PostScratchProcessing lors de l'utilisation de ces applications.
AddEntityContainment	Ajoute des informations générales sur l'entité dans la table `workingEntities.containment`.
AddGlobalVlans	Crée des objets VLAN (Virtual Local Area Network) globaux à l'aide de la table `translations.vlans`.
AddIfStackContainment	Ajoute des objets interface stack à la table `workingEntities.containment`.
AddJuniperEntityContainment	Ajoute aux enregistrements de périphérique des périphériques Juniper les informations de confinement relatives aux entités de port d'interface.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction

AddLayer3VPNInterfaceDependency	Ce programme stitcher détermine toutes les interfaces PE à routeur de fournisseur principal et les interfaces P à PE, impliquées dans un réseau privé virtuel. Ces interfaces PE -> P et P ->PE sont ajoutées à une liste de dépendances. Un événement sur l'une des interfaces dans cette liste de dépendances entraîne la génération par le système d'un SAE de réseau privé virtuel MPLS. Si un SAE VPN MPLS a déjà été généré en fonction d'un événement sur l'une des interfaces de la liste des membres, tous les événements des interfaces de la liste de dépendances sont ajoutés en tant qu'événements associés à ce SAE VPN MPLS déjà généré.
	
	Les sessions BGP définies entre les haut-parleurs PE et les réseaux privés virtuels (VPN), dépendent des interfaces PE -> P et P -> PE pour une paire VPN et PE donnée. L'avantage d'ajouter ces interfaces à la liste de dépendances de VPN est que cela permet aux liens P->PE et PE->P d'être pris en compte dans les calculs SAE (Service Affected Event) et fournit ainsi une notification lorsqu'un ensemble de VPN sur une interface PE est affecté par un problème de lien entre des routeurs PE et P.
	
	Le diagramme ci-dessous marque par un astérisque les interfaces ajoutées par le programme stitcher AddLayer3VPNInterfaceDependency à une dépendance SAE VPN MPLS. Dans ce diagramme, les conventions suivantes sont utilisées :
	• [ce] est un routeur client (customer-edge)
	• [PE est un routeur fournisseur (provider-edge)
	• [P] est un routeur principal (core)
	`[ce]---[PE]*---*[P]---[P]---[P]*---*[PE]---[ce]`
	`|*`
	`|`
	`|*`
	`[PE]---[ce]`
	
	Les résultats du programme stitcher apparaissent dans la liste m_DependsOn dans l'exemple d'enregistrement suivant, qui montre qu'un exemple de VPN, VPN_CONTAINER_ACME, est constitué d'un certain nombre d'interfaces dans le VPN (la liste m_Members contient les interfaces face à face PE->CE) et dépend ensuite des interfaces face à face PE->P/P->PE dans la liste m_DependsOn.
	`{`
	`m_Name='VPN_CONTAINER_ACME';`
	`m_Creator='STITCHER CREATED';`
	`m_Description='Logical object for VPN ACME';`
	`m_EntityType=7;`
	`m_ObjectId='VIRTUAL_PRIVATE_NETWORK';`
	`m_HaveAccess=0;`
	`m_IsActive=0;`
	`m_ExtraInfo={`
	`m_VPNName='ACME';`
	`m_MPLSVPNType='MPLS IP VPN MESH';`
	`m_Members=['pe7-cr38.core.eu.test.lab[Vl2]',`
	`'pe7-cr38.core.eu.test.lab[Fa0/3/1]',`
	`'pe8-cr72.core.eu.test.lab[Fa5/0]'];`
	`m_DependsOn=['pe7-cr38.core.eu.test.lab[Se0/0/0:0.202]',`
	`'pe8-cr72.core.eu.test.lab[Fa0/0]',`
	`'p4-cr28.core.eu.test.lab[Se0/0/1:0.202]',`
	`'p4-cr28.core.eu.test.lab[Gi0/0]'];`
	`};`
	`}`

AddLogicalToIpToBaseName	Ajoute des informations logiques à la table `translations.ipToBaseName`.
AddLoopbackTag	Ajoute une balise à la colonne ExtraInfo de la base de données topologiques, indiquant qu'une interface est une interface de bouclage globalement adressable.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
AddNoConnectionsToLayer	La couche de topologie finale est créée en fusionnant les informations topologiques de différentes couches. En cas de mauvaise correspondance des informations de connectivité fournies par les différentes couches, les informations de la couche la plus détaillée prévalent. Par exemple, la couche Réseau (couche 3) fournit des informations indiquant qu'une interface de routeur est connectée à une autre interface de ce type. Les informations de la couche Liaison de données (couche 2), plus détaillée, indiquent cependant qu'il existe un commutateur entre les deux interfaces de routeur. Le programme stitcher AddNoConnectionsToLayer est utilisé lorsqu'il est nécessaire de supprimer une connexion d'une couche mais de la conserver dans une autre.
AddOSPFAreaCollections	Crée une collection logique pour chaque zone OSPF contenant les interfaces dans cette zone.
AddSwitchRoutingLinks	Ajoute des données de routage de commutateur (qui aident le plug-in RCA lors de l'exécution de l'analyse origine du problème) à la base de données topologiques.
AddTechnologyType	Programme stitcher facultatif appelé par le programme stitcher `PostScratchProcessing.stch`. Ce programme stitcher est désactivé par défaut. Si elle est activée, elle crée une variable de type technologie pour chaque objet interface. Cette variable peut ensuite être utilisée pour créer des vues de réseau basées sur la technologie. Pour plus d'informations sur les vues de réseau, voir *IBM Tivoli Network Manager IP Edition - Guide de configuration de la visualisation du réseau*. Le programme stitcher crée la variable de type technologie en ajoutant une zone `m_Technology` à la zone `ExtraInfo` dans la table `scratchTopology.entityByName` pour chaque objet interface. La zone `m_Technology` est une chaîne, telle que `Ethernet`, `ATM`. Le programme stitcher contient un vaste ensemble de types de technologie par défaut et d'autres types de technologie peuvent être ajoutés directement en modifiant le programme stitcher. La charge de traitement faible associée à l'activation de ce programme stitcher peut ralentir légèrement la reconnaissance.
AddUnconnectedContainment	Fournit aux entités non connectées un confinement par défaut. Les entités non connectées n'ont pas de parent, à l'exception de leur noeud ou interface principal.
AddVlanContainers	Utilise les informations des tables `workingEntities.finalEntity` et `translations.vlans` pour ajouter des objets VLAN à la table `workingEntities.containment`.
AddVTPCollections	Augmente les entités de domaine VTP avec des ports qui sont connectés à des domaines VTP.
AddVTPEdges	Augmente les entités de domaine VTP avec des ports qui sont connectés à des domaines VTP.
AdjustedIPLayer	Ajuste la couche IP pour déplacer la connectivité de la couche IP sur les interfaces logiques et sur l'interface physique pour certains routeurs.
AgentRetProcessing	Traite les données de la table `returns` de chaque table.
AgentRetToInstrumentationCiscoFrameRelay	Remplit la table `instrumentation.ciscoFrameRelay` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationFddi	Remplit la table `instrumentation.fddi` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationFrameRelay	Remplit la table `instrumentation.frameRelay` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationHSRP	Remplit la table `instrumentation.hsrp` avec des informations de la table `returns` de l'agent approprié.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
AgentRetToInstrumentationIp	Remplit la table `instrumentation.ip` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationName	Remplit la table `instrumentation.name` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationPnniPgi	Remplit la table `instrumentation.pnniPeerGroup` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationSubnet	Remplit la table `instrumentation.subNet` avec des informations de la table `returns` de l'agent approprié.
AgentRetToInstrumentationVlan	Remplit la table `instrumentation.vlan` avec des informations de la table `returns` de l'agent approprié.
AgentStatus	Ce programme stitcher envoie des événements à la table `disco.events` sur le statut des agents de reconnaissance. Ces événements indiquent les modifications de l'état de l'agent ; par exemple, s'il a démarré, s'il est terminé ou s'il est en panne. Voir aussi les programmes stitcher FinderStatus, CreateStchTimeEvent et DiscoEventProcessing.
AnalyseTopology	Analyse une base de données de connectivité pour déterminer le nombre de connexions sur chaque interface.
AnalyseTopologySummary	Ce programme stitcher utilise les informations de récapitulatif d'analyse produites par le programme stitcher AnalyseTopology pour fournir une analyse de topologie plus détaillée, facultative. Cette fonctionnalité est distincte de l'analyse de topologie de base car elle peut affecter les performances ou créer des problèmes de topologie sur certains réseaux.
AnalyseTopology	Analyse une base de données de connectivité pour déterminer le nombre de connexions sur chaque interface.
AnalyseTopologySummary	Ce programme stitcher utilise les informations de récapitulatif d'analyse produites par le programme stitcher AnalyseTopology pour fournir une analyse de topologie plus détaillée, facultative. Cette fonctionnalité est distincte de l'analyse de topologie de base car elle peut affecter les performances ou créer des problèmes de topologie sur certains réseaux.
ApplyMainDisplayLabel	Définit le libellé affiché pour les périphériques dans l'interface graphique en fonction du paramètre de m_DisplayMode dans le fichier de configuration disco.config. Modifie les entités dans la table de base de données workingEntities.finalEntity. Appelé par les programmes stitcher BuildFinalEntityTable.stch et RebuildFinalEntityTable.stch.
ASMAgentRetProcessing	Ce programme stitcher génère une liste de sous-agents ASM exécutés sur un périphérique donné, en se basant sur les données de variable MIB récupérées par le programme stitcher ASM. Chaque sous-agent ASM exécuté sur un périphérique correspond à un produit de serveur commercial ou de base de données exécuté sur ce périphérique. La liste des ASM permet le partitionnement automatique des périphériques dans un réseau basé sur un serveur commercial ou des produits de base de données s'exécutant sur ces périphériques.
ASAMIfStringLayer	Utilise le format ASAM ifDescr pour déduire la connectivité.
ASMProcessing	Met à jour des entités en fonction des services qui s'exécutent sur ces entités.
ASRetProcessing	Utilisée dans les reconnaissances MPLS où les périphériques dans différents VPN clients ont des adresses IP identiques. Ce programme stitcher effectue le traitement nécessaire pour différencier ces périphériques et résoudre correctement la connectivité du périphérique. Ce programme stitcher est appelé par l'agent AsAgent et fonctionne conjointement au fichier `ASMap.txt` du répertoire `NCHOME/precision/etc`.
AssocAddressRetProcessing	Traite les données de la table `AssocAddress.returns` et envoie les détails du périphérique à l'agent de reconnaissance approprié si le périphérique n'a pas encore été reconnu.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
BGPLayer	Génère la couche BGP créée par l'agent BGP. Avec d'autres programmes stitcher de couche, ce programme stitcher reçoit des entrées des agents appropriés. Cette entrée est constituée d'enregistrements d'entité contenant des zones de données de voisins locaux et distants. Le programme stitcher utilise ces enregistrements pour établir les connexions locales et distantes pour chaque entité.
BuildBaseSubnetRegex	A partir d'un sous-réseau et d'un masque donnés, produit une expression régulière pour trouver des adresses IP dans ce sous-réseau.
BuildContainment	Appelle les programmes stitcher suivants pour ajouter différents types d'objets à la table `workingEntities.finalEntity` : • Programme stitcher `AddBasicContainment` qui ajoute des informations de confinement du périphérique. • Programme stitcher `AddCardContainment` qui ajoute des informations de confinement de la carte. • Programme stitcher `AddIfStackContainment` qui ajoute des informations de confinement de la pile d'interfaces. • Programme stitcher `AddEntityContainment` qui ajoute des informations de confinement générales. • Programme stitcher `NATAddressSpaceContainment`, qui ajoute des informations de confinement associées à l'espace adresse NAT. • Programme stitcher `AddVlanContainers` qui ajoute des informations de confinement VLAN. Vous pouvez désactiver des lignes dans ce programme stitcher selon vos besoins, afin d'exclure les types d'objets inutiles. **Remarque :** Ce programme stitcher gère également les périphériques reconnus par collecteur en acceptant les données de l'agent CollectorInventory.
BuildFinalEntity	Génère les enregistrements pour un seul boîtier. Le programme stitcher BuildFinalEntity fusionne les données de plusieurs agents pour créer la déefinition complète d'une entité. Ce programme stitcher est appelé par le programme stitcher `BuildFinalEntityTable`.
BuildFinalEntityTable	Utilise les entrées de la table `translations.ipToBaseName` pour remplir la table `workingEntities.finalEntity`.

BuildInterfaceName	Utilisée pour contrôler la désignation des interfaces. Par défaut, ce programme stitcher est appelé par le programme stitcher `BuildFinalEntity`.
	
	La stratégie de désignation par défaut pour toute interface de périphérique est la suivante :
	`baseName[<card>[<port>]]`
	
	Network Manager utilise également la convention de désignation par défaut suivante si la carte et le port ne sont pas valides :
	`baseName[0[<ifIndex>]]`
	
	Vous pouvez utiliser le programme stitcher `BuildInterfaceName` pour modifier la convention de désignation d'une interface de l'une des manières suivantes :
	• Spécifiez que vous souhaitez utiliser `ifName` ou `ifDescr` pour nommer les interfaces au lieu de leurs informations `ifIndex`, de carte ou de port. A l'aide de cette option, les interfaces ont des noms du type :
	`baseName[eth0/0]`
	Dans cet exemple `eth0` est le `ifName` d'une interface.
	Pour modifier la convention de désignation de cette manière, modifiez la valeur de `m_UseIfName` dans la table `disco.config`.
	• Modifiez directement le programme stitcher `BuildInterfaceName` pour spécifier toute convention de désignation d'interface.

BuildLayers	Activée dans la phase finale pour implémenter les programmes stitcher qui génèrent les bases de données de couche.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
BuildMPLSContainers	Ce programme stitcher appelle les programmes stitcher BuildVPNContainers et BuildVRAndVRFContainer. Elle génère les conteneurs VPN, VR et VRF.
BuildNATTranslation	Génère une table de conversion globale pour tous les périphériques de conversion NAT.
BuildVPNContainers	Crée des objets pour représenter les réseaux VPN MPLS dans le système.
BuildVRAndVRFContainers	Crée des objets VR (virtual router) et table VRF (virtual routing and forwarding) dans le système. Ces objets sont utilisés pour afficher des informations MPLS.
BuildVSIContainers	Crée des entités VSI (Virtual Switch Instance) et VFI (Virtual Forwarding Instance). Ce programme stitcher crée également un confinement logique de périphériques associés à des VSI, des VFI et des liens CE-PE.
CabletronLayer	Détermine les informations de connectivité basées sur les données Cabletron renvoyées par les agents de reconnaissance.
CDPLayer	Détermine les informations de connectivité basées sur les données renvoyées par l'agent CDP.
CheckAndSendNATGatewaysToArpCache	Envoie les passerelles NAT à l'agent ArpCache.
CheckForMasterLink	Recherche les connexions inférieures de la pile d'interfaces qui prévalent sur les connexions de niveau plus élevé.
CheckIfMgmtAddress	Détermine si une adresse IP donnée est une adresse de gestion définie.
CheckIndirectResponse	Gère les réponses ICMP indirectes dues à la conversion NAT.
CheckInterfaceStatus	Vérifie les données `ifOperStatus` et met à jour l'état des interfaces pour lesquelles `ifOperStatus` est différent de 1.
CheckManagedProcesses	Vérifie si les processus dans disco.managedProcesses ont été démarrés et, si tel n'est pas le cas, tente de les démarrer.
CheckMultipleIPNoAccess	Vérifie les périphériques sans accès mais avec plusieurs adresses IP. Crée des objets d'interface pour ces adresses IP et met à jour l'entité de manière appropriée.
CheckValidVirtual	Détermine si l'adresse IP donnée est une adresse IP virtuelle valide.
CiscoSerialInterfaceLayer	Crée une nouvelle couche intitulée CiscoSerialInterfaceLayer et connectant les commutateurs Cisco reliés par des interfaces série. Par défaut, le programme stitcher supprime toutes les connexions de la couche CiscoSerialInterfaceLayer dupliquées dans la base de données IPLayer, afin d'empêcher une connectivité incorrecte. La fonction de suppression des liaisons peut être activée ou désactivée en modifiant un indicateur dans le programme stitcher.
CiscoVSSContainment	CiscoVSSContainment ajoute de nouvelles entités de confinement, représentant les deux boîtiers physiques et leurs interfaces et objets respectifs, dans la table workingEntities.finalEntity.
CMTSLayer	Utilise les données téléchargées par l'agent CMTS pour générer les informations de connexion entre les systèmes CMTS (cable modem termination system) et les périphériques modem connectés.
ContextAgentRetProcessing	Ce programme stitcher est utilisé pour le flux de données de la reconnaissance contextuelle. Elle fusionne les sorties de tous les agents Context pour chaque entité. Elle insère ensuite les résultats de cette fusion dans la table `AssocAddress.despatch`, à l'aide du programme stitcher DetailsOrContextRetProcToAgent.
CollectorAddressTranslation	Ce programme stitcher traite les périphériques reconnus à l'aide d'un collecteur EMS. Elle effectue les tâches suivantes : • Garantit que tous les périphériques reconnus par un collecteur sont identifiés comme étant identiques aux périphériques équivalents reconnus par SNMP. • Stocke les données sur le collecteur associé à chaque périphérique. • Effectue d'autres tâches administratives associées à une reconnaissance par collecteur.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
CollectorDetailsRetProcessing	Ce programme stitcher traite les périphériques reconnus à l'aide d'un collecteur EMS. Ce programme stitcher traite les entrées de la table returns de l'agent CollectorDetails et les envoie à d'autres agents de reconnaissance collecteur. Les agents de reconnaissance collecteurs extraient les données de périphérique détaillées des collecteurs EMS.
CollectorIPLayer	Ce programme stitcher génère la connectivité de couche 2 pour les périphériques reconnus à l'aide d'un collecteur EMS, basée sur les données de connexion fournies par l'agent CollectorLayer2.
CollectorLagLayer	Crée une connectivité EMS de couche 2 à partir des informations LAG (Collector Link Aggregation) Alcatel Lucent 5620.
CollectorSwitchLayer	Ce programme stitcher génère la connectivité de couche 3 pour les périphériques reconnus à l'aide d'un collecteur EMS, basée sur les données de connexion fournies par l'agent CollectorLayer3.
CreateAndSendTopology	Active les programmes stitcher qui créent la topologie et envoie la topologie Scratch finale à MODEL.
CreateBGPAutonomousSystems	Crée et nomme un système autonome (AS) BGP. Offre la possibilité de résoudre le numéro du système autonome en nom de système autonome, qui permet d'afficher un nom lié à un client ou à une entreprise lors de la visualisation du système autonome dans une mappe topologique. Récupère également les données qui indiquent si ce système dispose d'une seule interface réseau. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateBGPNetworksCollection	Crée un enregistrement de base de données topologiques, connu sous le nom de réseau BGP, qui regroupe une collection de systèmes autonomes BGP. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateBGPProtocolEndPoints	Crée des noeuds finaux de protocole BGP. Un noeud final de protocole BGP est une interface logique qui peut être utilisée par le service hébergé par BGP sur un périphérique. Un port physique peut implémenter plusieurs noeuds finaux de protocole BGP. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateBGPServices	Crée des entités de service hébergées par BGP. Un service hébergé est un service ou une application exécutée sur un périphérique spécifique. Par exemple, un périphérique peut héberger des services BGP et OSPF. Chaque entité de service hébergée par BGP décrit un processus BGP sur un routeur. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateBGPTopology	Crée des connexions entre les haut-parleurs BGP. Ces connexions sont présentées dans les vues de réseau et correspondent aux connexions BGP fonctionnant au moment de la reconnaissance. Ce programme stitcher peut également induire des routeurs BGP homologues auxquels Network Manager ne peut pas accéder. Ces routeurs induits peuvent correspondre à des systèmes BGP autonomes en-dehors de votre société. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateIGMPGroups	Crée des entités de groupe de multidiffusion et ajoute les points d'extrémité IGMP associés en tant que membres. Les entités de groupe remplissent la table igmpGroup NCIM.
CreateIGMPProtocolEndPoints	Crée des entités de noeud final de protocole IGMP multidiffusion, qui remplissent la table igmpEndPoint NCIM.
CreateIGMPServices	Crée des entités de service IGMP multidiffusion qui remplissent la table igmpService NCIM.
CreateImpactTopology	Programme stitcher facultatif qui peut être utilisé pour effectuer une copie de la topologie Scratch avant de l'envoyer au gestionnaire de topologie, ncp_model.
CreateIPMRouteGroups	Crée les entités MDT, groupe et source qui remplissent les tables ipMRouteMDT, ipMRouteGroup et ipMRouteSource NCIM.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
CreateIPMRouteProtocolEndPoints	Crée les entités de noeud final de protocole de routage multidiffusion qui remplissent la table ipMRouteEndPoint NCIM.
CreateIPMRouteRoutes	Gère la création d'entités de route en amont et en aval pour les routes téléchargées des routeurs de multidiffusion. Permet également la résolution MDT.
CreateIPMRouteTopology	Remplit les zones adjacentes IPMRoute qui remplissent la topologie IPMRoute dans NCIM.
CreateIPMRouteServices	Crée des entités de service de routage de multidiffusion qui remplissent en dernier lieu la table ipMRouteService NCIM.
CreateMPLSTEResources	Crée des entités de ressource TE MPLS.
CreateMPLSTEServices.stch	Crée des entités de service TE (Tunnel Engineering) MPLS et les associe à leurs entités de boîtier hôte.
CreateMPLSTETunnels.stch	Crée des entités TE MPLS et les associe à l'entité de service TE appropriée.
CreateMPLSTEProtocolEndPoints.stch	Crée des noeuds finaux de protocole TE MPLS et les associe à l'entité de service TE appropriée.
CreateMPLSTENetworkPipes.stch	Crée des zones de tunnel réseau dans les entités Tunnel. Les tunnels sont des entités de connexion IP qui représentent le chemin du tunnel.
CreateMPLSTEPipeHop.stch	Crée des entités de connexion IP à utiliser avec des tunnels réseau.
CreateMPLSTETopology.stch	Ajoute des zones de lien TE MPLS aux entités d'interface impliquées dans les chemins de tunnel TE.
CreateMXGroupCollection	Crée des collections basées sur l'adresse IP maître pour un groupe de moteurs de routage. Appelé par le programme stitcher PostScratchProcessing.
CreateNetworkManagementCards	Ce programme stitcher crée des objets NetworkManagementCard.
CreateOSPFAreas	Crée et nomme une zone OSPF. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateOSPFNetworkLSAPseudoNodes	Extrait les données associées à des pseudonoeuds OSPF dont la publicité est effectuée par des routeurs désignés et génère ces pseudonoeuds dans la topologie. Cela permet de résoudre le problème de maillage complet lors de la représentation de la zone OSPF dans les vues de réseau et permet de visualiser les connexions dans les zones OSPF de manière claire et épurée.
CreateOSPFPointToPointAdjacencies	Extrait les données associées à des connexions point-à-point dans une zone OSPF et crée ces connexions dans la topologie. Elles sont affichées dans les vues de réseau. Seules les connexions activées sont affichées.
CreateOSPFProtocolEndPoints	Crée des noeuds finaux de protocole OSPF. Un noeud final de protocole OSPF est une interface logique qui peut être utilisée par le service hébergé par OSPF sur un routeur. Ce programme stitcher rassemble également des données qui indiquent dans quelle zone OSPF se trouve un noeud final. Un port physique peut implémenter plusieurs noeuds finaux de protocole OSPF. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateOSPFRoutingDomains	Crée un enregistrement de base de données topologiques, connu sous le nom de domaine de routage OSPF, qui regroupe un ensemble de zones OSPF. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreateOSPFServices	Crée des entités de service hébergées par OSPF. Un service hébergé est un service ou une application exécutée sur un périphérique spécifique. Par exemple, un périphérique peut héberger des services BGP et OSPF. Chaque entité de service hébergée par OSPF décrit un processus OSPF sur un routeur et indique également si le routeur sur lequel le service OSPF est exécuté est un routeur de bordure de zone ou un routeur de bordure de système autonome. Ce programme stitcher est appelé par le programme stitcher PostScratchProcessing suite à la création de la topologie scratch.
CreatePIMNetworksCollection	Crée une entité de collection pour collecter les routeurs activés pour PIM.
CreatePIMProtocolEndPoints	Crée des noeuds finaux de protocole pour chaque interface PIM.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
CreatePIMServices	Crée un objet de service de niveau périphérique représentant l'état du service de multidiffusion hébergé et un lien à partir du boîtier vers cet objet de service.
CreatePIMTopology	Crée la topologie PIM à l'aide des informations adjacentes PIM plutôt que m_RouterLinks.
CreateScratchTopology	Crée la topologie scratch.
CreateStchTimeEvent	Ce programme stitcher envoie des événements à la table `disco.events` sur la progression dans la phase de traitement des données. Par exemple, le programme stitcher génère des événements pour indiquer que le processus de reconnaissance a commencé à construire la table d'entités de travail et la table de confinement. Voir aussi les programmes stitcher AgentStatus, FinderStatus et DiscoEventProcessing.
CreateTrunkConnections	Modifie le modèle de confinement pour prendre en compte les tronçons VLAN.
CreateVlanEntity	Ce programme stitcher crée un objet d'entité VLAN unique en ajoutant les données VLAN à la topologie Scratch.
CreateVRRPCollection	Crée des collections basées sur l'ID de routeur virtuel VRRP (Virtual Router Redundancy Protocol) et l'adresse IP associée. Appelé par le programme stitcher PostScratchProcessing.
DetailsOrContextRetProcToAgent	Ce programme stitcher est utilisé comme partie du flux de données de la reconnaissance contextuelle. Elle est équivalente au programme stitcher DetailsRetProcessing mais gère la reconnaissance contextuelle. Elle traite les entités de la table `details.returns` et envoie les détails à la table despatch de l'agent Context approprié.
DetailsRetProcessing	Traite les entités de la table `details.returns` et envoie les détails à la table `AssocAddress.despatch`.
DetectionFilter	Détermine si un périphérique donné passe le filtre de détection et doit être reconnu, en fonction du `detectionFilter` défini dans la base de données `scope`. Par défaut, les filtres de reconnaissance ne filtrent pas le serveur de Network Manager car il sert généralement aussi de station d'interrogation pour l'analyse d'origine du problème. Pour que cette analyse puisse fonctionner correctement, la station d'appel, et par conséquent le serveur Network Manager, doit faire partie de la topologie. Si vous devez exclure le serveur Network Manager à l'aide de `detectionFilter`, modifiez le programme stitcher DetectionFilter et supprimez les sections de code indiquées par des commentaires, qui empêchent le filtrage de la machine hôteNetwork Manager.
DiscoEventProcessing	Ce programme stitcher répond à une insertion dans la table `disco.events` et crée et envoie l'événement de reconnaissance approprié à la sonde pour Tivoli Netcool/OMNIbus, processus nco_p_ncpmonitor, qui transmet ensuite l'événement au serveur d'objets. Vous pouvez contrôler si les événements de reconnaissance sont générés en modifiant la valeur de la zone `m_CreateStchrEvents` dans la table `disco.config`. Voir aussi les programmes stitcher AgentStatus, FinderStatus et CreateStchTimeEvent.
DiscoShutdown	Activée lorsque DISCO est arrêté. Appelle le programme stitcher RefreshDiscoveryTables.
ExampleContainment1	Un exemple de programme stitcher qui peut être modifié pour configurer le modèle de confinement.
ExampleContainment2	Un exemple de programme stitcher qui peut être modifié pour configurer le modèle de confinement.
FddiLayer	Déduit la topologie de couche FDDI.
Feedback	Renvoie les détails du périphérique à l'outil de recherche Ping afin de redéfinir l'emplacement de départ de la reconnaissance.
FinalPhase	Activée dans la phase finale pour implémenter les programmes stitcher finals.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
FindAddressSpace	Identifie l'espace adresse d'une adresse IP.
FinderStatus	Ce programme stitcher envoie des événements à la table `disco.events` sur le statut des outils de recherche. Pour chaque outil de recherche, le programme stitcher envoie un événement pour indiquer les modifications de l'état de l'outil de recherche ; par exemple, s'il a démarré, s'il est terminé ou s'il est en panne. Voir aussi les programmes stitcher AgentStatus, CreateStchTimeEvent et DiscoEventProcessing.
FindGatewayInterfaces	Identifie l'interface de passerelle sur les périphériques de conversion NAT.
FindPhysIpForVirtIp	Utilisée dans la résolution des problèmes HSRP. Recherche l'adresse IP physique correspondant à une adresse HSRP virtuelle.
FnderProcToDetailsDesp	Traite les entrées de la table `finders.processing` et envoie les détails à l'un des agents suivants : • L'agent Details, si le périphérique a été reconnu directement dans le réseau. • L'agent CollectorDetails, si l'enregistrement est un périphérique reconnu à l'aide d'un collecteur EMS.
FnderRediscoveryToCollectorFinder	Envoie des adresses IP ou des plages d'adresses de la table `finders.rediscovery` vers les collecteurs. Si l'adresse du serveur collecteur ou de l'une des unités qu'il collecte correspond à l'adresse ou à la plage d'adresses, le collecteur la traite à nouveau.
FnderRediscoveryToPingFinder	Envoie des données de la table `finders.rediscovery` à l'outil de recherche Ping.
FnderRetProcessing	Traite les entités dans la table `finders.returns`. Vérifie si le périphérique se trouve dans la portée et déplace cette entrée dans la table `finders.processing` ou `finders.pending` en fonction de l'état d'activité ou d'inactivité de la reconnaissance.
FullDiscovery	Détermine si une reconnaissance complète doit être exécutée.
GetEntityNameByBase	Pour un nom de base et un index d'interface (ou ID d'interface) donnés, ce programme stitcher résout le nom d'entité associé.
GetEntityNameByIp	Pour une adresse et un espace adresse facultatif donnés, ce programme stitcher résout le nom d'entité associé. Un nom de base facultatif peut également être spécifié pour limiter la recherche.
GetBaseNameByIp	Renvoie le nom de base associé à l'adresse IP fournie ou "" si aucun nom n'est trouvé. En cas de correspondances multiples, la première est utilisée.
HandleIPMRouteDownstream	Traite les données de routage en aval IPMRoute pour le périphérique en cours. Crée des entités de route en aval qui remplissent la table ipMRouteDownstream NCIM. Trace également les noeuds finaux requis par la route, qui sont créés ultérieurement, et le MDT auquel la route doit être associée.
HandleIPMRouteUpstream	Traite les données de routage en amont IPMRoute pour le périphérique en cours. Crée des entités de route en amont qui remplissent la table ipMRouteUpstream NCIM. Trace également les noeuds finaux requis par la route, qui sont créés ultérieurement, et utilisés par le MDT pour être associés à la route.
HubFdbToConnections	Programme stitcher précompilé qui traite toutes les connexions pour les concentrateurs Ethernet. Elle requiert également les informations de connectivité de la reconnaissance de commutateur Ethernet.
IlmiLayer	Crée les connexions de topologie ILMI (Interim Local Management Interface) en fonction des informations ILMI ATM.
InitiateNATGatewayDiscovery	Définit l'emplacement de départ de l'outil de recherche Ping avec les adresses de passerelle NAT.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
InstantiationFilter	Détermine si une entité donnée doit être instanciée (c'est-à-dire envoyée à MODEL), en fonction du `instantiateFilter` défini dans la base de données `scope`. Par défaut, les filtres de reconnaissance n'excluent pas le serveur Network Manager. Cela est dû au fait que ce serveur sert généralement aussi de station d'interrogation pour l'analyse origine du problème. Pour que cette analyse puisse fonctionner correctement, la station d'appel, et par conséquent le serveur Network Manager, doit faire partie de la topologie. Si vous devez exclure le serveur Network Manager à l'aide de `instantiateFilter`, modifiez le programme stitcher InstantiationFilter et supprimez les sections de code indiquées par des commentaires, qui empêchent le filtrage de la machine hôteNetwork Manager.
IPLayer	Crée les connexions de topologie de couche IP.
Fix Pack 4 IPAddressNaming	Indique au système qu'il doit nommer des périphériques en utilisant l'adresse IP dans laquelle les données sont valides. Ce programme stitcher est facultatif et est désactivé par défaut.
IpToBaseName	Remplit la table `translations.ipToBaseName` avec des informations de l'agent AssocAddress.
IsForcedRediscovery	Ce programme stitcher est utilisé pour déterminer si une insertion d'outil de recherche fait partie d'une nouvelle reconnaissance forcée. Une reconnaissance forcée est différente d'une nouvelle reconnaissance réactive, le mode adopté par le moteur de reconnaissance, ncp_disco, à la fin de la reconnaissance. Dans ce mode, un périphérique n'est généralement redécouvert que s'il est nouveau ou si l'insertion de l'outil de recherche référence une interruption, suggérant ainsi que l'entité à été modifiée. Les nouvelles reconnaissances forcées sont démarrées à l'aide de l'interface graphique Configuration de la reconnaissance.
IsInMPLSScope	Détermine si une adresse IP donnée se trouve dans la portée des périphériques considérés comme des périphériques CE valides, connectés à un périphérique PE MPLS tiers inaccessible.
IsInScope	Utilisée par d'autres programmes stitcher pour vérifier qu'une entité se trouve dans la portée de la reconnaissance (c'est-à-dire, dans la portée définie dans la table `scope.zones`).
LLDPLayer	Détermine les informations sur la connectivité des voisins distants en fonction des données renvoyées par l'agent LLDP. **Remarque :** Si la connectivité est affichée incorrectement pour une unité, cela peut signifier que le MIB LLDP sur l'unité réseau n'a pas été alimenté correctement. Dans certains cas, les données MIB appropriées sont renseignées de manière incorrecte avec le numéro de modèle de l'unité au lieu d'un identificateur unique. Dans ce cas, le programme stitcher LLDP ne parvient pas à calculer correctement la connectivité LLDP. Pour vérifier qu'il s'agit bien de ce problème, pour chacun des périphériques qui ne sont pas connectés correctement, vous devez examiner la valeur de la zone LLDPChassisId dans la table `LLDP.returns` de l'agent LLDP. S'il s'avère que les valeurs de la zone LLDPChassisId ne sont pas uniques, modifiez le programme stitcher LLDPLayer afin d'affecter la valeur 2 à la méthode de traitement en modifiant la ligne suivante dans ce programme : `int processingMethod = 2;`
MergeLayers	Fusionne les topologies de couche.
ModifyIPContainment	Modifie le confinement des interfaces IP sur des périphériques de transfert non-IP afin qu'elles ne soient pas connectées en amont. Cette modification est requise pour tracer l'origine du problème.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
MPLSAddPathnames	Met à jour les enregistrements d'interface MPLS avec des informations sur l'appartenance à un chemin.
MPLSAddVPNNames	Détermine quels chemins appartiennent à quels réseaux VPN et met à jour les enregistrements d'interface MPLS avec les informations sur l'appartenance au réseau VPN/chemin.
MPLSCE	Tente de résoudre la connectivité CE à PE pour les interfaces VRF sur un PE où le CE de connexion n'a pas été identifié. Elle utilise les informations de couche 3 pour essayer de trouver la connectivité correcte.
MPLSPathDiscovery	Identifie les LSP (labels switched paths) entre les routeurs PE (provider edge) à travers un noyau MPLS. Démarre les traces de chemin à partir des périphériques PE. Le programme stitcher de point d'entrée configure la base de données de trace de chemin et démarre une trace de chemin pour chaque chemin possible, appelant d'autres programmes stitcher pour mettre à jour les enregistrements avec des informations de chemin et de VPN.
MPLSProcessing	Détermine le mode de reconnaissance MPLS à effectuer en fonction de la valeur de la zone `m_RTBasedVPNs` dans la table `disco.config`. • Si `m_RTBasedVPNs` est égal à `1`, le traitement post-couche MPLS basé sur la cible de la route est effectué. Le programme stitcher `MPLSProcessing` appelle le programme stitcher `RTBasedVPNDiscovery` pour effectuer ce traitement. La reconnaissance MPLS permet uniquement d'afficher une vue de bordure. • Si `m_RTBasedVPNs` est égal à `0`, le traitement post-couche basé sur LSP (label switched path) est effectué. Le programme stitcher `MPLSProcessing` appelle le programme stitcher `MPLSPathDiscovery` pour effectuer ce traitement. La reconnaissance MPLS permet d'afficher une vue de bordure et une vue du noyau. Ce programme stitcher effectue également le traitement d'arrière-plan requis pour générer des événements affectés par le service.
MPLStackProcessing	Garantit que toutes les interfaces situées sous une interface de support VPN dans la pile d'interfaces sont marquées comme faisant partie des VPN qui transitent par les interfaces supérieures.
NameResolution	Recherche les entités dont le nom n'a pas été résolu et tente de résoudre le nom d'entité en se basant sur les noms résolus des autres interfaces du périphérique.
NamingFromLoopbackDetails	Si un agent LoopBack est exécuté, ce programme stitcher met à jour les noms dans la table `translations.ipToBaseName`. L'adresse IP de gestion du périphérique utilisée par les règles d'interrogation est définie sur un pour les adresses de bouclage si Network Manager ait confirmé qu'il a un accès SNMP.
NamingViaManagementInterface	Recherche les adresses IP de gestion sur translations.ipToBaseName et garantit que l'adresse de base et le nom d'une entité sont ceux du serveur de gestion.
NATAddressSpaceContainers	Programme stitcher facultatif qui génère des objets de conteneur NAT contenant des périphériques au sein d'un espace adresse particulier et crée des insertions dans la table `workingEntities.finalEntity` pour ces objets de conteneur NAT. Génère également les entrées correspondantes dans la table `workingEntities.containment`.
NATAgentRetProcessing	Traite les sorties des agents de passerelle NAT.
NATFnderRetProcessing	Effectue le traitement des périphériques NAT.
NATGatewayRetProcessing	Utilisé dans les reconnaissances impliquant des passerelles NAT où une ou plusieurs interfaces de gestion du périphérique de passerelle NAT se trouvent dans un espace adresse privé. Ce programme stitcher effectue le traitement nécessaire pour déterminer si chaque interface de gestion se trouve dans un espace adresse public ou privé. Elle est appelée par l'agent NATGatewayAgent et fonctionne avec le fichier `NATGateways.txt` du répertoire `NCHOME/precision/etc`.
NATIpCheck	Résout un problème lorsqu'une passerelle NAT ajoute toutes ses adresses IP converties à sa table IP.
NATTimer	Déclenche la nouvelle reconnaissance des passerelles NAT.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
NortelPassportLayer	Résout la connectivité NortelPassport reconnue par l'agent NortelPassport.
OSPFLayer	Crée une topologie du routage OSPF dans le réseau. Ces informations de routage OSPF sont utilisées par le programme stitcher DetermineOSPFDomains afin de baliser les périphériques et interfaces avec des informations de domaine OSPF.
ParseASAMIfString	Analyse les données de description de l'interface ASAM dans ses parties de composant. Appelé à partir du programme stitcher ASAMIfStringLayer.
ParseZyxelIfString	Analyse les données de description de l'interface ZYXEL dans ses parties de composant. Appelé à partir du programme stitcher ZyxelIfStringLayer.
PeerBasedPWDiscovery	Utilisée dans la reconnaissance des VPN de couche 2 améliorés dans un réseau principal MPLS. Ce programme stitcher identifie les connexions de pseudoconnexion MPLS extraites par les agents MPLS Cisco et ajoute des informations sur ces connexions aux entités réseau concernées pour l'affichage dans Topoviz. Les informations sont stockées en tant que VPN de pseudoconnexion et fournissent des informations sur les deux extrémités de routeur PE (provider edge) de la pseudoconnexion.
PIMLayer	Crée une table de topologie PIM basée sur des données de voisins distants, provenant des agents de prise en charge PIM. Les données de topologie permettent de peupler les données m_PIMAdjacency data, qui sont à leur tour utilisées pour alimenter la topologie PIM dans NCIM
PingFinderScopeRefresh	Indique à l'outil de recherche Ping de régénérer sa portée. Ce programme stitcher est activé par l'interface graphique Configuration de la reconnaissance lorsque vous régénérez la portée et garantit par conséquent que l'outil de recherche Ping dispose d'une portée à jour.
PnniLayer	Crée les connexions de topologie PNNI, à condition que des connexions aient été découvertes aux deux extrémités.
PostLayerProcessing	Un conteneur pour toutes les fonctionnalités requises suite à la création des couches. Appelle les programmes stitcher suivants : • AddGlobalVlans • AddSwitchRoutingLinks • AddUnconnectedContainment • BuildMPLSContainers • BuildVRAndVRFContainers • BuildVPNContainers • CreateTrunkConnections • CreateVlanEntity • MPLSAddVPNNames • MPLSPathDiscovery • MPLSInterfaceStackTrace • MPLSFindConnectionInStack • MPLSFindInterfaceInStack • MPLSAddPathNames • PVCPathMemberships • PVCTracePath • PVCProcessingRecord • PVCTraceAway • PVCTraceCrossConnected • PVCNamePath • PVCProcessedRecord • ProcessSwitchModules

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
PostScratchProcessing	Un conteneur pour les fonctionnalités à exécuter suite à la création de la topologie scratch. Appelle les programmes stitcher suivants : • CreateNetworkManagementCards • InstantiationFilter : ce programme stitcher est exécuté autant de fois que nécessaire pour vérifier si une entité donnée doit être envoyée à MODEL. • SendTopologyToModel • AddTechnologyType Ce programme stitcher appelle également les programmes stitcher suivants qui configurent les informations liées à BGP dans la topologie : • CreateBGPServices • CreateBGPProtocolEndPoints • CreateBGPTopology • CreateBGPAutonomousSystems • CreateBGPNetworksCollection Ce programme stitcher appelle également les programmes stitcher suivants qui configurent les informations liées à OSPF dans la topologie : • CreateOSPFServices • SetOSPFServiceDesignatedStatus • CreateOSPFProtocolEndPoints • CreateOSPFNetworkLSAPseudoNodes • CreateOSPFPointToPointAdjacencies • CreateOSPFAreas • CreateOSPFRoutingDomains
PreProcessIGMPEndPointData	Crée et remplit une table temporaire contenant des informations sur les noeuds finaux pour chaque interface activée IGMP et les groupes connus. Trace également les groupes de multidiffusion pour lesquels il existe des données IGMP. Ces données sont utilisées par d'autres programmes stitcher IGMP pour créer des entités de noeud final et de groupe.
PresetLayer	Peut être utilisée pour "prédéfinir" les connexions non reconnaissables, le cas échéant. Ce programme stitcher n'est pas utilisé par défaut. Ce programme stitcher contient des paramètres de configuration avancés. Les modifications doivent uniquement être effectuées par du personnel certifié.
ProcessQinQData	Traite les données QinQ associées à des interfaces et construit le confinement approprié.
ProcessSwitchModules	Identifie les modules de commutation ayant leurs propres adresses IP.
ProcRemoteConns	Prend un enregistrement contenant un voisin distant et traite les connexions distantes si l'agent qui les a reconnues prend en charge les connexions indirectes.
ProfilingEndFinal ProfilingPhase1 ProfilingPhase2 ProfilingPhase3 ProfilingStartFinal	Ces programmes stitcher remplissent la table `disco.profilingData`, fournissant des données sur la durée de la reconnaissance, l'utilisation de mémoire et une présentation générale des résultats de la reconnaissance. Ces informations sont utilisées dans l'estimation de mise à l'échelle et fournissent une présentation des performances de la reconnaissance.
PruneSwitchConnections	Ce programme stitcher peut être utilisé pour améliorer la connectivité des commutateurs dans le cas où les commutateurs ne fournissent pas des informations complètes sur la connectivité. Ce programme stitcher n'est pas activé par défaut et doit être activé uniquement sur recommandation du support IBM.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
PVCNamePath	Ajoute le nom d'un chemin PVC à la table de base de données interne`atmPVCs.memberships`.
PVCPathMemberships	S'exécute automatiquement par `CreateScratchTopology.stch` lors du processus de reconnaissance. Utilise les informations de connectivité de la topologie Scratch et les informations PVC extraites par l'agent CiscoPVC pour tracer les PVC à travers le réseau.
PVCProcessedRecord	Met à jour la base de données `atmPVCs` pour indiquer l'enregistrement en cours de traitement.
PVCProcessingRecord	Met à jour la base de données `atmPVCs` pour indiquer l'enregistrement en cours de traitement.
PVCTraceAway	Exécute la fonction de trace PVC.
PVCTraceCrossConnected	Exécute la fonction de trace PVC.
PVCTracePath	Exécute la fonction de trace PVC pour une interface donnée à l'aide des autres programmes stitcher de trace PVC afin d'effectuer la trace de tous les chemins à travers la section ATM complète du réseau.
PVCTraceTowards	Exécute la fonction de trace PVC.
RebuildFinalEntityTable	Ce programme stitcher est similaire au programme stitcher BuildFinalEntityTable. Elle utilise également les entrées de la table `translations.ipToBaseName` pour remplir la table `workingEntities.finalEntity`. La différence est que ce programme stitcher est utilisé en mode nouvelle reconnaissance et non en mode reconnaissance complète.
RecreateAndSendTopology	Ce programme stitcher est similaire au programme stitcher CreateAndSendTopology.stch. Elle active également les programmes stitcher qui créent la topologie et envoie la topologie Scratch finale à MODEL. La différence est que ce programme stitcher est utilisé en mode nouvelle reconnaissa nce et non en mode reconnaissance complète.
RecreateScratchTopology	Ce programme stitcher est similaire au programme stitcher CreateAndSendTopology.stch. La différence est que ce programme stitcher est utilisé en mode nouvelle reconnaissance et non en mode reconnaissance complète.
ReDoIpToBaseName	Régénère la table `translations.ipToBaseName`.
RefreshDiscoveryTables	Régénère les tables de base de données de reconnaissance.
RefreshLayerDatabase	Régénère une base de données topologiques de couche donnée.
RefreshMPLSTEScope	Régénère la portée de l'agent StandardMPLSTE.
RefreshMulticastScope	Régénère la portée de l'agent StandardPIM.
RefreshSubnets	Régénère une base de données de sous-réseau donnée.
RemoveDeviceFromTopology	Supprime un périphérique de la topologie. Le premier argument de ce programme stitcher doit être le nom de base du périphérique à supprimer.
RemoveInferredCEDuplicates	Lorsque l'existence d'un routeur CE est présumée, ce programme stitcher supprime les périphériques en doublon potentiels dans la topologie.
RemoveOutOfBandConnectivity	Supprime la connectivité pour les périphériques hors bande dans la table fullTopology.entityByNeighbor.
RemoveOutOfBandRouterLinks	Supprime la connectivité de lien de routeur pour les périphériques hors bande dans la table scratchTopology.entityByName.
RemoveWrongConnectionsToTA838	Supprime les connexion erronées des périphériques Cisco 7609 et Cisco 3400 à Adtran TA838.
ResetNATMainNodes	Réinitialise l'adresse IP de périphériques dont les adresses ont été converties par NAT à partir de l'adresse IP privée, utilisée pour résoudre la connectivité vers l'adresse IP publique pour la surveillance. Les périphériques peuvent ainsi être connectés et visualisés correctement et restent également accessibles à des fins de surveillance.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
ResolveHSRPIssues	Recherche les entités découvertes via leur adresse HSRP (Hot Standby Routing Protocol). Dans cette situation, le programme stitcher met à jour les tables `returns` de l'agent de reconnaissance et la table `translations.ipToBaseName` pour afficher l'interface physique correcte.
ResolveVRRPAssocAddresses	Résout les problèmes causés par les adresses VRRP. Dans une telle situation, le programme stitcher met à jour les tables `returns` de l'agent de reconnaissance et la table `translations.ipToBaseName` pour afficher l'interface physique correcte.
Fix Pack 3 RestartDiscoProcess	Appelle le script **`restart_disco_process.pl`** qui arrête le processus de reconnaissance en cours d'exécution et démarre une nouvelle instance de celui-ci. Un seul argument est nécessaire. Une nouvelle reconnaissance complète est initiée par le processus de reconnaissance nouvellement démarré si la valeur est définie à 1. Si elle est définie à 0, une reconnaissance complète n'est pas initiée.
Restitcher	Rassemble la topologie.
RTBasedVPNDiscovery	Reconnaît les VPN MPLS en se basant sur l'utilisation de la cible de route. Le seul résultat de cette opération est une vue de bordure qui montre le réseau MPLS principal avec les routeurs PE (provider edge) pour les VPN et VRF dans la portée de la reconnaissance. Cette vue n'affiche pas les routeurs P (provider) dans le réseau MPLS principal ni les LSP (label switched paths) associés qui lient ces routeurs P. Pour chaque routeur PE reconnu, Network Manager conserve des informations sur les cibles de route importées dans et exportées de ce routeur PE. Vous pouvez ainsi identifier quels VPN utilisent quels routeurs.
RTBasedVPNResolution	Utilise les données VRF prétraitées par le programme stitcher RTBasedVPDiscovery pour résoudre les VPN en fonction de l'importation et l'exportation de la cible de route.
ScopeRefresh	Informe les outils de recherche et les agents qui requièrent des informations sur la portée que la table de portée a été modifiée.
SendToCollectors	Envoie l'emplacement de départ fourni à l'outil de recherche de collecteur pour une nouvelle reconnaissance.
SendTopologyToModel	Envoie la topologie assemblée à MODEL.
SerialLinkLayer	Détermine les connexions à partir des données renvoyées par l'agent SerialLink.
SetOSPFServiceDesignatedStatus	Indique si le routeur exécutant un service OSPF est un routeur désigné ou un routeur de secours.
SONMPLayer	Détermine les connexions à partir des données renvoyées par l'agent SONMP.
SubnetConnections	Crée des entités de sous-réseau et des insertions dans chaque interface appartenant au sous-réseau. Au niveau de la couche 3, les interfaces dans un sous-réseau sont toutes considérées comme étant connectées, de façon à ce que toute connexion non reconnue soit ajoutée à la base de donnée de couche IP.
SubnetToIPLayer	Ajoute un confinement et/ou une connectivité de couche trois par défaut.
SRPLayer	Génère la couche SRP pour contenir les informations de confinement reconnues par l'agent SRP. Avec d'autres programmes stitcher de couche, ce programme stitcher reçoit des entrées des agents appropriés. Cette entrée est constituée d'enregistrements d'entité contenant des zones de données de voisins locaux et distants. Le programme stitcher utilise ces enregistrements pour établir les connexions locales et distantes pour chaque entité.
SwitchFdbToConnections	Copie les entrées des tables `returns` de l'agent Switch dans la table `connections`.
SwitchStpMltProcessing	Ajoute des connexions pour tous les liens dans une liaison multi-liens à une table entityByNeighbor.

Tableau 151. Liste des programmes stitcher de reconnaissance Network Manager (suite)

Programme stitcher	Fonction
SwitchStpToConnections	Génère une nouvelle couche basée sur la connectivité SwitchStp. Traite les données de l'agent STP pour créer des enregistrements de connexion d'entité locales et distantes correctement nommés dans la base de données stpTopology. Avec d'autres programmes stitcher de couche, ce programme stitcher reçoit des entrées des agents appropriés. Cette entrée est constituée d'enregistrements d'entité contenant des zones de données de voisins locaux et distants. Le programme stitcher utilise ces enregistrements pour établir les connexions locales et distantes pour chaque entité.
SysNameNaming	Provoque l'attribution de noms aux périphériques par le système à l'aide du sysName SNMP dans lequel les données sont valides. Il s'agit d'un programme stitcher facultatif désactivé par défaut.
TagManagedEntities	Ajoute une balise à chaque interface d'un noeud principal indiquant si cette interface doit être surveillée ou non. Cette balise se trouve dans la zone `m_ExtraInfo` et s'appelle `m_IsManaged`. Cette balise peut recevoir les valeurs suivantes : • `0` - Indique que l'interface est gérée. Il s'agit de la valeur par défaut. • `1` - Indique que l'interface n'est pas gérée. Ce paramètre peut être modifié depuis l'interface graphique. • `2` - Indique que l'interface n'est pas gérée par le processus **`ncp_disco`**. Ce paramètre ne peut pas être modifié depuis l'interface graphique. • `3` - Indique que l'interface est en dehors de la portée de reconnaissance et ne doit pas être interrogée. Les valeurs `m_IsManaged` de toutes les interfaces dans un noeud principal sont concaténées et stockées dans la zone `m_ExtraInfo` pour le noeud principal, dans `m_UnmanagedInterfaces`, en utilisant le format : `[<ifIndex1>, <IfIndex2>, ..... <IfIndexN>]`, où ifIndices sont les ifIndices des interfaces que vous ne désirez pas que le système surveille. Par défaut, le programme stitcher définit `m_IsManaged` sur `0` pour certains types d'interface prédéfinis, comme les interfaces virtuelles. Vous pouvez spécifier d'autres types d'interface que le système ne doit pas surveiller en ajoutant une clause `where` dans le programme stitcher.
TagManagementInterfaces	Balise l'interface ayant l'adresse IP utilisée comme adresse IP d'accès principale pour une entité donnée. Ce programme stitcher est utilisé dans l'analyse origine du problème.
TraceRouteConnectivity	Met à jour la table `IPLayer.entityByNeighbor` avec les informations de connectivité extraites de données renvoyées par l'agent TraceRoute.
VRFBasedVPNResolution	Utilise les données VRF prétraitées par le programme stitcher RTBasedVPDiscovery pour résoudre les VPN en fonction des noms VRF.
ZyxelIfStringLayer	Utilise le format ZYXEL ifDescr pour déduire la connectivité.

Concepts associés:

«Filtres», à la page 6
Utilisez des filtres de pré-reconnaissance pour augmenter l'efficacité des filtres de reconnaissance et de post-reconnaissance afin d'éviter l'instanciation d'unités.

«Flux de processus pour la création d'événements de reconnaissance», à la page 208
Les événements de reconnaissance sont créés lors du processus de reconnaissance affichant la progression des agents, des programmes stitcher et des outils de recherche. Ces événements sont envoyés et stockés dans Tivoli Netcool/OMNIbus et peuvent être visualisés à l'aide de l'Interface graphique Web.

Tâches associées:

«Définition des filtres de reconnaissance», à la page 36
Les filtres permettent d'exclure des périphériques avant ou après reconnaissance. Vous pouvez exclure des périphériques en fonction de différents critères, tels que l'emplacement, la technologie et le fabricant. Les filtres apportent des restrictions supplémentaires à celles définies dans les zones de portée.

«Définir la portée de la reconnaissance», à la page 23
Pour définir la portée de la reconnaissance, définissez les zones du réseau (c'est-à-dire, les intervalles de sous-réseau) que vous souhaitez inclure dans la reconnaissance, ainsi que les zones que vous souhaitez exclure.

Programmes stitcher interdomaine

Fix Pack 4

Les programmes stitcher interdomaine recherchent les liens entre les périphériques dans différents domaines et créent des connexions entre eux dans la topologie.

Le tableau suivant décrit les programmes stitcher utilisés avec la reconnaissance interdomaine.

Tableau 152. Programmes stitcher interdomaine

Programme stitcher	Fonction
`AggregationDomainCollectionOfCollections.stch`	Crée des collections d'entités de collection dans le domaine agrégé.
`AggregationDomainCollections.stch`	Crée des collections d'entités dans le domaine agrégé.
`AggregationDomainCopyEntity.stch`	Crée l'entité dans le domaine d'agrégation sur la base de l'entité dans le domaine source.
`AggregationDomainCreate.stch`	Crée un domaine d'agrégation.
`AggregationDomainFindEntity.stch`	Recherche des entités dans le domaine d'agrégation.
`AggregationDomainMain.stch`	Met à jour le domaine d'agrégation après la fin d'une reconnaissance. Appelle les autres programmes stitcher de domaine d'agrégation.
`AggregationDomain.stch`	Vérifie que le processus **`ncp_disco`** ne se trouve pas en phase de traitement, puis appelle le programme de stitcher `AggregationDomainMain.stch`.
`AggregationDomainUpdateChangeTime.stch`	Met à jour l'horodatage des entités de collection.
`AggregationDomainUpdateRequired.stch`	Vérifie les horodatages des entités de collection pour déterminer si une mise à jour est requise.
`LinkDomains.stch`	Contrôle la liaison des domaines. Vous pouvez modifier ce programme de stitcher pour configurer la façon dont les domaines sont liés.
`LinkDomainsActOnInstructions.stch`	Traite les instructions contenues dans le tableau linkDomains.instruction et crée des connexions via le programme stitcher `LinkDomainsCreateConnection.stch`.
`LinkDomainsAddInstruction.stch`	Les autres programmes stitcher fournissent des instructions pour ajouter des connexions interdomaine à ce programme stitcher. Ce programme stitcher vérifie si chaque connexion linkDomains.instructions figure déjà dans la table. Les connexions qui ne figurent pas déjà dans le tableau sont ajoutées au tableau.
`LinkDomainsDatabaseSetup.stch`	Crée les bases de données utilisées par les programmes stitcher de liaison de domaine.

Tableau 152. Programmes stitcher interdomaine (suite)

Programme stitcher	Fonction
LinkDomainsGetEntityIdFromNCIMByEntityName AndDomainName.stch	Vérifie si l'entité indiquée est dans NCIM en fonction de EntityName et de domainName.
LinkDomainsGetNumConnectsForEntityName.stch	Récupère les nombre d'éléments réseau apparentés pour une entité.
LinkDomainsInScopeIpAddresses.stch	Interroge la base de données NCIM pour les adresses IP des domaines adjacents. Les adresses IP sont transmises aux agents de commutation afin de pouvoir être interrogées par commande ping au cours de la phase 3 de la reconnaissance. Cela permet de remplir les tables de base de données de réacheminement des commutateurs du domaine sur lequel la reconnaissance est en cours d'exécution.
LinkDomainsLoadInterfaceDescriptionMatches.stch	Vous pouvez configurer les programmes stitcher interdomaine afin que les périphériques soient reliés les uns aux autres sur la base de la zone ifAlias de l'interface. Vous pouvez éditer ce programme stitcher pour définir les correspondances de description d'interface.
LinkDomainsLoadPresetConnections.stch	Vous pouvez éditer ce programme stitcher pour définir les connexions entre des périphériques spécifiques.
LinkDomainsPopulateDomainAdjacencies.stch	Remplit la table de base de données NCIM domainAdjacencies avec les informations sur les domaines qui sont considérés comme adjacents. Les domaines adjacents doivent disposer de liaisons de couche 2.
LinkDomainsPreProcessInterfaceMatches.stch	Traite les périphériques ayant des descriptions d'interface correspondantes.
LinkDomainsProcessConnectivityMatrix.stch	Traite les périphériques ayant des descriptions d'interface correspondantes.
LinkDomainsProcessPresetConnections.stch	Traite les périphériques ayant des connexions prédéfinies.
LinkDomainsResolveInterfaceToLowestPortNCIM.stch	Recherche le port ou l'interface le plus bas pour un nom entityName d'interface NCIM.
LinkDomainsUnMergeCheck.stch	Crée des liaisons de couche 2 induites à partir des liaisons de Couche 3 si aucune liaison de Couche 2 n'est reconnue. Ce programme stitcher vérifie que les programmes stitcher interdomaine ont reconnu une vraie liaison de couche 2 vers ou à partir d'un périphérique dans un domaine différent. Si c'est le cas, le programme stitcher LinkDomainsUnMergeCheck.stch appelle LinkDomainsUnMergeLayers.stch afin de supprimer la liaison de de Couche 2 induite.
LinkDomainsUnMergeLayers.stch	Vérifie si une liaison de Couche 2 a été induite à partir d'une liaison de Couche 3. Si c'est le cas, la liaison de Couche 2 induite est supprimée.
LinkDomainsViaBGPSessions.stch	Crée des connexions entre les domaines via des sessions BGP.
LinkDomainsViaCDP.stch	Crée des connexions entre les domaines via des données CDP.
LinkDomainsViaLayer1NameInterface.stch	Crée des connexions entre les domaines sur la base de la connectivité de couche 1.

Tableau 152. Programmes stitcher interdomaine (suite)

Programme stitcher	Fonction
LinkDomainsViaMPLSTE.stch	Crée des connexions entre les domaines via des données MPLS TE.
LinkDomainsViaOSPF.stch	Crée des connexions entre les domaines via des données OSPF.
LinkDomainsViaOSPFAssist.stch	Activé si le programme stitcher LinkDomainsViaOSPF.stch est activé.
LinkDomainsViaPIM.stch	Crée des connexions entre les domaines via des données PIM.
LinkDomainsViaPseudoWires.stch	Crée des connexions entre les domaines sur la base de la connectivité de pseudo-connexion.
LinkDomainsViaSlash30Subnet.stch	Crée des connexions entre les domaines sur la base de la connectivité de masque de sous-réseau /30.
LinkDomainsViaUnresolvedFDBPorts.stch	Itère sur les ports non résolus et recherche un port correspondant unique dans un domaine adjacent. Lors de l'exécution du programme stitcher du commutateur, les ports non résolus pour lesquels aucune liaison n'a été trouvée dans le domaine sont stockés dans la base de données switchTopology.unresolvePort.

Annexe F. Types d'interruption

Les interruptions sont des messages administratifs envoyés depuis des périphériques réseau, tels que des routeurs, pour indiquer que le périphérique ou ses connexions sont actifs ou inactifs.

L'outil de recherche d'interruption reconnaît les périphériques en écoutant les interruptions SNMP et en extrayant les adresses IP de ces interruptions. Les différents types d'interruption sont décrits dans le tableau 153.

Tableau 153. Types d'interruption

Numéro	Nom	Description
0	Interruption coldStart	Une interruption coldStart signifie que l'entité du protocole d'envoi est en cours de réinitialisation, de sorte que la configuration de l'agent ou l'implémentation de l'entité du protocole risque d'être altérée.
1	Interruption warmStart	Une interruption warmStart signifie que l'entité du protocole d'envoi est en cours de réinitialisation, de sorte que ni la configuration de l'agent ni l'implémentation de l'entité de protocole ne soit altérée.
2	Interruption linkDown	Une interruption linkDown est générée lors de l'échec d'une liaison de communication reconnue.
3	Interruption linkUp	Une interruption linkUp est générée lorsqu'une liaison de communication est rétablie.
4	Interruption authenticationFailure	Une interruption authenticationFailure est générée par un message de protocole qui n'a pas été authentifié par le destinataire, par exemple, un mot de passe incorrect.
5	Interruption egpNeighborloss	Une interruption egpNeighborLoss signifie qu'un voisin EGP, dont le protocole d'envoi était un homologue EGP, a été signalé comme étant arrêté et que la relation homologue n'est plus valide.
6	Interruption enterprise-specific	Une interruption enterprise-specific signifie que l'entité du protocole d'envoi détecte qu'un événement enterprise-specific a eu lieu.

Annexe G. 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 154 sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

Tableau 154. 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

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

Z