Tivoli Application Dependency Discovery Manager
Version 7.3

Guide des détecteurs

Tivoli Application Dependency Discovery Manager
Version 7.3

Guide des détecteurs

Remarque

Avant d'utiliser la présente documentation et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 467.

Notice d'édition

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

La présente édition s'applique à la version 7.3 d'IBM Tivoli Application Dependency Discovery Manager (numéro de produit 5724-N55) et à toutes les éditions et modifications ultérieures jusqu'à indication contraire dans les nouvelles éditions.

Table des matières

Figures

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 la présente documentation

Ce document PDF est la version imprimable des informations fournies par le centre de documentation.

Conventions utilisées dans ce centre de documentation

Certaines conventions sont utilisées dans la documentation d'IBM® Tivoli Application Dependency Discovery Manager (TADDM). Elles permettent de se référer à des variables et des chemins d'accès dépendants du système d'exploitation, au répertoire `COLLATION_HOME` et à l'emplacement du fichier `collation.properties` dont il fait référence tout au long de la documentation de TADDM, y compris dans les messages.

Variables et chemins dépendant du système d'exploitation

Dans ce centre de documentation, les conventions UNIX sont utilisées pour spécifier des variables d'environnement et pour la notation des répertoires.

Si vous utilisez une ligne de commande Windows, remplacez $*variable* par %*variable*% pour les variables d'environnement, et remplacez toutes les barres obliques (/) par des barres obliques inverses (\) dans les chemins d'accès des répertoires.

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

Répertoire `COLLATION_HOME`

Le répertoire racine de TADDM est également nommé répertoire `COLLATION_HOME`.

Sur les systèmes d'exploitation tels que AIX ou Linux, l'emplacement par défaut pour l'installation de TADDM est le répertoire `/opt/IBM/taddm`. Par conséquent, l'emplacement du répertoire `$COLLATION_HOME` est `/opt/IBM/taddm/dist`.

Sur les systèmes d'exploitation Windows, l'emplacement d'installation par défaut de TADDM est le répertoire `c:\IBM\taddm`. Dans ce cas, l'emplacement du répertoire `%COLLATION_HOME%` est `c:\IBM\taddm\dist`.

Emplacement du fichier `collation.properties`

Le fichier `collation.properties` renferme les propriétés du serveur TADDM et inclut des commentaires sur chacune d'elles. Il se trouve dans le répertoire `$COLLATION_HOME/etc`.

Termes et définitions

Reportez-vous à la liste des termes et définitions pour vous informer sur des concepts importants dans IBM Tivoli Application Dependency Discovery Manager (TADDM).

application métier
Une collection de composants qui fournit une fonctionnalité métier que vous pouvez utiliser au niveau interne, externe ou avec d'autres applications métier.

base de données TADDM
Dans TADDM, la base de données dans laquelle les données de configuration, les dépendances et l'historique des changements sont enregistrés.

Chaque serveur TADDM, à l'exception des serveurs de reconnaissance et des serveurs de stockage secondaires, possède sa propre base de données. Les serveurs de reconnaissance ne comportent aucune base de données. Les serveurs de stockage partagent la base de données du serveur de stockage principal.

collection
Dans TADDM, groupe d'éléments de configuration.

collection d'accès
Une collection utilisée pour contrôler l'accès aux éléments de configuration et les droits de modification des éléments de configuration. Vous ne pouvez créer des collections d'accès que si la sécurité du niveau de données est activée.

Console de gestion de reconnaissance
L'interface utilisateur client TADDM permettant de gérer les reconnaissances. Cette console est également appelée console produit. Elle s'applique au déploiement d'un serveur de domaine et au déploiement de serveurs de reconnaissance dans un déploiement de serveurs de diffusion en continu. La fonction de la console est la même dans ces deux déploiements.

console produit
Voir *console de gestion de reconnaissance*.

déploiement de serveur de domaine
Un déploiement TADDM possédant un serveur de domaine. Un déploiement de serveur de domaine peut faire partie d'un déploiement de serveur de synchronisation.

Dans un déploiement de serveur de domaine, la propriété suivante du serveur TADDM doit être définie sur la valeur suivante :

```
com.collation.cmdbmode=domain
```

déploiement de serveur de synchronisation
Un déploiement TADDM avec un serveur de synchronisation et deux ou plusieurs déploiements de serveur de domaine comportant chacun sa propre base de données locale.

Dans ce type de déploiement, le serveur de synchronisation copie les données de reconnaissance de plusieurs serveurs de domaine, un domaine à la fois, au cours d'un processus de synchronisation par lots.

Dans un déploiement de serveur de synchronisation, la propriété suivante du serveur TADDM doit être définie sur l'une des valeurs suivantes :

```
com.collation.cmdbmode=enterprise
```

Ce type de déploiement est obsolète. Par conséquent, dans un nouveau déploiement TADDM, dans lequel plusieurs serveurs sont requis, utilisez le déploiement de serveurs de diffusion en continu. Vous pouvez convertir

un serveur de synchronisation en serveur de stockage principal d'un déploiement de serveurs de diffusion en continu.

déploiement de serveurs de diffusion en continu
Un déploiement TADDM avec un serveur de stockage principal et au moins un serveur de reconnaissance. Ce type de déploiement peut également inclure un ou plusieurs serveurs de stockage secondaires en option. Le serveur de stockage principal et les serveurs de stockage secondaires partagent une même base de données. Les serveurs de reconnaissance ne comportent aucune base de données.

Dans ce type de déploiement, les données de reconnaissance affluent en parallèle de plusieurs serveurs de reconnaissance pour converger vers la base de données TADDM.

Dans un déploiement de serveurs de diffusion en continu, la propriété du serveur TADDM doit être définie sur l'une des valeurs suivantes :

- `com.collation.taddm.mode=DiscoveryServer`
- `com.collation.taddm.mode=StorageServer`

Pour tous les serveurs, à l'exception du serveur de stockage principal, les propriétés suivantes (pour le nom d'hôte et le numéro de port du serveur de stockage principal) doivent également être définies :

- `com.collation.PrimaryStorageServer.host`
- `com.collation.PrimaryStorageServer.port`

Si la propriété com.collation.taddm.mode est définie, la propriété com.collation.cmdbmode ne doit pas être définie ou elle doit être placée en commentaire.

domaine
Dans TADDM, un sous-ensemble logique de l'infrastructure d'une société ou d'une autre organisation. Les domaines peuvent représenter des limites organisationnelles, fonctionnelles ou géographiques.

EC Voir *élément de configuration*.

élément de configuration (EC)
Un composant de l'infrastructure informatique sous le contrôle de la gestion des configurations et donc soumis à un contrôle formel des modifications. Chaque EC dans la base de données TADDM possède un objet persistant et un historique des changements qui lui sont associés. Exemples d'EC : système d'exploitation, interface L2, taille du pool de mémoire tampon de base de données.

équivalent serveur (ES)
Une unité représentative de l'infrastructure informatique, définie comme un système informatique (avec des configurations standard, des systèmes d'exploitation, des interfaces réseau et des interfaces de stockage) avec un logiciel serveur installé (base de données, serveur Web ou serveur d'applications, par exemple). Le concept d'équivalent serveur inclut aussi le réseau, l'archivage et les autres sous-systèmes fournissant des services pour le fonctionnement optimal du serveur. Un serveur équivalent dépend du système d'exploitation :

Système d'exploitation	Nombre approximatif d'EC
Windows	500
AIX	1000

Système d'exploitation	Nombre approximatif d'EC
Linux	1000
HP-UX	500
Périphériques réseau	1000

ES Voir *équivalent serveur*.

lancement en contexte
Concept consistant à passer de façon homogène d'une interface utilisateur de produit Tivoli à une autre interface utilisateur de produit Tivoli (soit sur une console différente, soit sur la même console ou interface de portail) avec une identification unique et avec l'interface utilisateur cible en position sur l'emplacement correct pour que les utilisateurs poursuivent leur tâche.

location multiple
Dans TADDM, l'utilisation par un fournisseur de services ou un vendeur informatique d'une installation TADDM pour découvrir plusieurs environnements clients. De plus, le fournisseur de services ou le vendeur informatique peut voir les données provenant de tous les environnements clients, mais au sein de chaque environnement client, seules les données spécifiques à un client peuvent être affichées dans l'interface utilisateur ou consultées dans les rapports inhérents à cet environnement client.

Portail de gestion de données
L'interface utilisateur Web de TADDM permettant d'afficher et de manipuler les données d'une base de données TADDM. Elle s'applique à un déploiement de serveur de domaine, à un déploiement de serveur de synchronisation et à chaque serveur de stockage dans un déploiement de serveur de diffusion en continu. L'interface utilisateur est très similaire dans tous les déploiements bien qu'elle comporte quelques fonctions supplémentaires permettant d'ajouter et de synchroniser des domaines dans le déploiement de serveur de synchronisation.

reconnaissance asynchrone
Dans TADDM, l'exécution d'un script de reconnaissance sur un système cible permettant de reconnaître des systèmes auxquels le serveur TADDM n'a pas directement accès. Cette reconnaissance s'effectuant manuellement et indépendamment d'une reconnaissance authentifiée, elle est dite «asynchrone».

reconnaissance authentifiée
L'analyse du détecteur TADDM permettant de reconnaître des informations détaillées sur les éléments suivants :

- Chaque système d'exploitation dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 2 et requiert les droits d'accès au système d'exploitation.
- L'infrastructure d'application, les composants logiciels déployés, les serveurs physiques, les périphériques réseau, les systèmes virtuels et les données hôtes utilisés dans un environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 3 et requiert les droits d'accès au système d'exploitation et à l'application.

reconnaissance basée sur un script
Dans TADDM, l'utilisation dans une reconnaissance authentifiée de scripts de détecteur identiques à ceux fournis par les détecteurs dans le support de reconnaissance asynchrone.

reconnaissance de niveau 1
L'analyse du détecteur TADDM permet de reconnaître des informations de base sur les systèmes informatiques actifs dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance sans autorisation d'accès car elle ne requiert aucune autorisation d'accès. Elle utilise le détecteur Stack Scan et le détecteur de portée IBM Tivoli Monitoring. La reconnaissance de niveau 1 est très superficielle. Elle collecte uniquement le nom hôte, le nom du système d'exploitation, l'adresse IP, le nom de domaine complet et l'adresse MAC (Media Access Control) de chaque interface reconnue. De plus, la reconnaissance des adresses MAC se limite aux systèmes Linux on System z et Windows. La reconnaissance de niveau 1 ne permet pas de reconnaître les sous-réseaux. Pour chaque interface IP reconnue qui n'appartient pas à un sous-réseau existant reconnu lors d'une reconnaissance de niveau 2 ou 3, de nouveaux sous-réseaux sont créés en fonction de la valeur de la propriété `com.collation.IpNetworkAssignmentAgent.defaultNetmask` du fichier `collation.properties`.

reconnaissance de niveau 2
L'analyse du détecteur TADDM permet de reconnaître des informations détaillées sur chaque système d'exploitation de l'environnement d'exécution. Cette analyse est également appelée reconnaissance avec autorisation d'accès car elle requiert les autorisations d'accès au système d'exploitation. La reconnaissance de niveau 2 collecte les noms des applications, les noms des systèmes d'exploitation et les numéros de port associés à chaque application en cours d'exécution. Si une application a établi une connexion TCP/IP avec une autre application, ces informations sont capturées en tant que dépendance.

reconnaissance de niveau 3
L'analyse du détecteur TADDM reconnaît des informations détaillées sur l'infrastructure de l'application, les composants logiciels déployés, les serveurs physiques, les unités réseau, les systèmes virtuels et les données hôte utilisées dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance avec autorisations d'accès, car elle requiert les autorisations d'accès au système d'exploitation et à l'application.

reconnaissance d'utilisation
L'analyse du détecteur TADDM reconnaît les informations d'utilisation du système hôte. La reconnaissance d'utilisation requiert les autorisations d'accès au système d'exploitation.

reconnaissance non authentifiée
L'analyse du détecteur TADDM permet de reconnaître des informations de base sur les systèmes informatiques actifs dans l'environnement d'exécution. Cette analyse est également appelée reconnaissance de niveau 1 et ne requiert aucun droit d'accès.

serveur de domaine
Un serveur TADDM exécutant des détecteurs dans un déploiement de serveur de domaine et possédant sa propre base de données.

serveur de reconnaissance
Un serveur TADDM qui exécute des détecteurs dans un déploiement de serveurs de diffusion en continu mais qui ne possède pas sa propre base de données.

serveur de stockage
Un serveur TADDM qui traite les données reçues des serveurs de reconnaissance et les enregistre dans la base de données TADDM. Le serveur de stockage principal coordonne les serveurs de reconnaissance ainsi que tous les autres serveurs de stockage et fait office de serveur de stockage. Tous les serveurs de stockage qui ne sont pas des serveurs principaux sont appelés serveurs de stockage secondaires.

serveur de synchronisation
Un serveur TADDM qui synchronise les données de reconnaissance à partir de tous les serveurs de domaine de l'entreprise et qui comporte sa propre base de données. Ce serveur ne reconnaît pas directement les données.

serveur TADDM
Une dénomination générique pouvant représenter l'une des dénominations suivantes :

- Serveur de domaine dans un déploiement de serveur de domaine
- Serveur de synchronisation dans un déploiement de serveur de synchronisation
- Serveur de reconnaissance dans un déploiement de serveur de reconnaissance
- Serveur de stockage (y compris le serveur de stockage principal) dans un déploiement de serveurs de diffusion en continu

système cible
Dans le processus de reconnaissance TADDM, le système devant être reconnu.

unité d'exécution de tâche de reconnaissance
Dans TADDM, unité d'exécution qui exécute des détecteurs.

Référence du détecteur

Présentation

Pour chaque détecteur, cette référence comprend des informations de présentation, et le cas échéant pour chacun des détecteurs, elle inclut des informations de configuration et d'identification et de résolution des incidents. Pour certains détecteurs, les informations relatives aux attributs associés aux objets de modèle sont également incluses. Dans les cas où des attributs seraient inclus, ceux-ci sont disponibles dans IBM Tivoli Common Data Model (CDM), mais n'apparaissent pas nécessairement dans l'interface utilisateur d'IBM Tivoli Application Dependency Discovery Manager (TADDM).

Détecteurs et systèmes cible pris en charge

Pour obtenir la liste des détecteurs TADDM et les versions prises en charge des systèmes cible qu'ils peuvent reconnaître, voir Sensors and supported target systems dans le Wiki TADDM.

Présentation du processus de reconnaissance

Le *Guide d'administration* de TADDM contient une présentation du processus de reconnaissance, y compris des informations sur la façon dont un détecteur reconnaît des éléments de configuration (EC) et dont un détecteur d'application est démarré.

Dernières mises à jour

Pour obtenir les mises à jour les plus récentes sur les problèmes de prise en charge des détecteurs TADDM 7.3.0, voir les *Notes sur l'édition* de la documentation TADDM.

Extensions de détecteur

Si vous souhaitez reconnaître des logiciels supplémentaires non reconnus par TADDM par défaut, vous pouvez créer des modèles de serveur personnalisé. Vous pouvez créer vos propres modèles ou utiliser des modèles prédéfinis. Pour plus d'informations, voir la rubrique *Création et gestion de modèles de serveur personnalisé* dans le *Guide d'utilisation* de TADDM.

Détecteurs activés par défaut

Ces listes indiquent quels détecteurs sont activées par défaut dans chacun des quatre profils de reconnaissance suivants : Niveau 1, niveau 2, niveau 3 et utilisation.

Pour plus d'informations sur les niveaux de reconnaissance, voir la rubrique *Niveaux de reconnaissance* dans le *Guide d'administration* de TADDM.

Profil de reconnaissance de niveau 1

Ces détecteurs sont activés par défaut dans un profil de reconnaissance de niveau 1.

Le tableau 1 répertorie les détecteurs activés par défaut pour une reconnaissance de niveau 1.

Les détecteurs sont répertoriés dans l'ordre dans lequel ils apparaissent dans la fenêtre Profils de reconnaissance dans l'interface utilisateur TADDM.

Tableau 1. Détecteurs activés par défaut pour une reconnaissance de niveau 1

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«détecteur d'ancrage», à la page 228	AnchorSensor
«détecteur SNMP Light», à la page 322	SnmpLightSensor
«détecteur d'analyse de piles», à la page 258	StackScanSensor

Profil de reconnaissance de niveau 2

Ces détecteurs sont activés par défaut dans un profil de reconnaissance de niveau 2.

Le tableau 2 répertorie les détecteurs activés par défaut pour une reconnaissance de niveau 2.

Les détecteurs sont répertoriés dans l'ordre dans lequel ils apparaissent dans la fenêtre Profils de reconnaissance dans l'interface utilisateur TADDM.

Tableau 2. Détecteurs activés par défaut pour une reconnaissance de niveau 2

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«détecteur de port Alteon», à la page 282	AlteonPortSensor
«détecteur Alteon SNMP», à la page 283	AlteonSnmpSensor
«détecteur de réseau local virtuel Alteon», à la page 284	AlteonVlanSensor
«détecteur d'ancrage», à la page 228	AnchorSensor
«Détecteur de reconnaissance asynchrone», à la page 229	ASDSensor
«détecteur de port BIG-IP», à la page 285	BigIPPortSensor
«détecteur BIG-IP SNMP», à la page 286	BigIPSnmpSensor
«détecteurs de réseau local virtuel BIG-IP», à la page 288	BigIPVlanSensor
«détecteur de pont SNMP», à la page 289	BridgeSnmpSensor
«détecteur de pont SNMP 2», à la page 292	BridgeSnmpSensor2
«détecteur SNMP Check Point SNMP», à la page 296	CheckpointSnmpSensor
«détecteur Cisco Discovery Protocol», à la page 298	CdpSensor
«détecteur Cisco IOS», à la page 299	CiscoIOSSensor
«détecteur de port Cisco», à la page 300	CiscoPortSensor
«Détecteur de réseau local virtuel Cisco», à la page 305	CiscoVlanSensor
«Détecteur de serveur d'applications personnalisé», à la page 231	CustomAppServerSensor

Tableau 2. Détecteurs activés par défaut pour une reconnaissance de niveau 2 (suite)

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«Détecteur de système informatique MIB2 personnalisé», à la page 232	CustomMib2ComputerSystemSensor
«détecteur Entity MIB», à la page 308	EntityMIBSensor
«détecteur de réseau local virtuel Extreme», à la page 310	ExtremeVlanSensor
«Détecteur de système informatique FreeBSD», à la page 334	FreeBSDComputerSystemSensor
«Détecteur de système informatique générique», à la page 237	GenericComputerSystemSensor
«Détecteur de serveur générique», à la page 237	GenericServerSensor
«Détecteur de système informatique IBM AIX», à la page 347	AixComputerSystemSensor
«Détecteur IBM BladeCenter SNMP», à la page 311	BladeCenterSnmpSensor
«Détecteur de console IBM HMC (Hardware Management Console)», à la page 353	HmcSensor
«Détecteur de système informatique IBM i», à la page 362	I5OSComputerSystemSensor
«Détecteur IBM Integrated Virtualization Manager», à la page 361	IvmSensor
«Détecteur de ressources hôte», à la page 429	HostResourcesSensor
«Détecteur SNMP HP BladeSystem», à la page 338	HPBladeSystemSnmpSensor
«Détecteur de système informatique HP NonStop», à la page 340	HPNonStopComputerSystemSensor
«Détecteur de système informatique HP-UX» , à la page 341	HpUxComputerSystemSensor
«périphérique IP, détecteur», à la page 248	IpDeviceSensor
«système informatique IPSO, détecteur», à la page 364	IPSOComputerSystemSensor
«détecteur LAN Manager SNMP», à la page 314	LanManagerSnmpSensor
«Détecteur de système informatique Linux», à la page 365	LinuxComputerSystemSensor
«Détecteur NetApp», à la page 454	NetAppSensor
«détecteur NetScreen SNMP», à la page 318	NetscreenSnmpSensor
«détecteur Nokia SNMP», à la page 320	NokiaSnmpSensor
«détecteur de système informatique OpenVMS», à la page 374	OpenVmsComputerSystemSensor
«Détecteur Ping», à la page 249	PingSensor
«Détecteur de port», à la page 253	PortSensor
«Détecteur de session», à la page 253	SessionSensor
«Détecteur Snap Drive», à la page 455	SnapDriveSensor

Tableau 2. Détecteurs activés par défaut pour une reconnaissance de niveau 2 (suite)

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«détecteur SNMP MIB2», à la page 324	SnmpMib2Sensor
«détecteur de système informatique Solaris», à la page 375	SunSparcComputerSystemSensor
«Détecteur générique de zones Solaris», à la page 257	ZonesGenericSensor
«détecteur Sun Fire SysControl», à la page 384	SysControlSensor
Fix Pack 2 Détecteur Sun Sparc Virtualization	SunSparcVirtualizationSensor
Fix Pack 1 Détecteur SVC Storage	SVCStorageSensor
«détecteur de système informatique Tru64», à la page 387	Tru64ComputerSystemSensor
«Détecteur de système informatique VMware ESX», à la page 389	VmwareComputerSystemSensor
«Détecteur de systèmes informatiques VMware ESXi», à la page 396	VmwareEsxiComputerSystemSensor
«Détecteur de système informatique Windows», à la page 400	WindowsComputerSystemSensor
«Détecteur générique de partition de charge de travail», à la page 267	WparGenericSensor
Fix Pack 1 Détecteur XIV Storage	XIVStorageSensor
«Détecteur zEnterprise», à la page 268	ZEnterpriseSensor

Profil de reconnaissance de niveau 3

Ces détecteurs sont activés par défaut dans un profil de reconnaissance de niveau 3.

Le tableau 3 répertorie les détecteurs activés par défaut pour une reconnaissance de niveau 3.

Les détecteurs sont répertoriés dans l'ordre dans lequel ils apparaissent dans la fenêtre Profils de reconnaissance dans l'interface utilisateur TADDM.

Tableau 3. Détecteurs activés par défaut pour une reconnaissance de niveau 3

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur Active Directory», à la page 17	Détecteur Active Directory
«détecteur de port Alteon», à la page 282	AlteonPortSensor
«détecteur Alteon SNMP», à la page 283	AlteonSnmpSensor
«détecteur de réseau local virtuel Alteon», à la page 284	AlteonVlanSensor
«détecteur d'ancrage», à la page 228	AnchorSensor
«Détecteur Apache», à la page 19	ApacheServerSensor
«Détecteur de reconnaissance asynchrone», à la page 229	ASDSensor

Tableau 3. Détecteurs activés par défaut pour une reconnaissance de niveau 3 (suite)

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«détecteur de port BIG-IP», à la page 285	BigIPPortSensor
«détecteur BIG-IP SNMP», à la page 286	BigIPSnmpSensor
«détecteurs de réseau local virtuel BIG-IP», à la page 288	BigIPVlanSensor
«détecteur de pont SNMP», à la page 289	BridgeSnmpSensor
«détecteur de pont SNMP 2», à la page 292	BridgeSnmpSensor2
«détecteur Check Point», à la page 295	CheckpointSensor
«détecteur SNMP Check Point SNMP», à la page 296	CheckpointSnmpSensor
«Détecteur Cisco Adaptive Security Appliance», à la page 297	• ASASensor • CiscoApplianceVersionSensor
«détecteur Cisco Discovery Protocol», à la page 298	CdpSensor
«détecteur Cisco IOS», à la page 299	CiscoIOSSensor
«détecteur de port Cisco», à la page 300	CiscoPortSensor
Fix Pack 2 «Détecteur SNMP Cisco UCS», à la page 301	CiscoUCSSensor
«Détecteur de réseau local virtuel Cisco», à la page 305	CiscoVlanSensor
«Détecteur CiscoWorks», à la page 306	• CiscoWorks405FileUDS • CiscoWorks405UDS • CiscoWorksFileUDS • CiscoWorksSensor • CiscoWorksUDS
«Détecteur de serveur Citrix», à la page 22	CitrixServerSensor
«Détecteur Citrix XenServer», à la page 329	XenServerSensor
«Détecteur de serveur d'applications personnalisé», à la page 231	CustomAppServerSensor
«Détecteur de système informatique MIB2 personnalisé», à la page 232	CustomMib2ComputerSystemSensor
«Détecteur DNS», à la page 39	DnsSensor
«Détecteur de portée EMC Storage Scope», à la page 421	• EMCStorageScopeSensor • EMCStorageScopeDetailSensor
«détecteur Entity MIB», à la page 308	EntityMIBSensor
«détecteur de réseau local virtuel Extreme», à la page 310	ExtremeVlanSensor
«Détecteur de système informatique FreeBSD», à la page 334	FreeBSDComputerSystemSensor
«Détecteur de système informatique générique», à la page 237	GenericComputerSystemSensor
«Détecteur de serveur générique», à la page 237	GenericServerSensor

Tableau 3. Détecteurs activés par défaut pour une reconnaissance de niveau 3 (suite)

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«Détecteur HIS», à la page 39	HISServerSensor
«Détecteur de ressources hôte», à la page 429	HostResourcesSensor
«Détecteur SNMP HP BladeSystem», à la page 338	HPBladeSystemSnmpSensor
«Détecteur de système informatique HP NonStop», à la page 340	HPNonStopComputerSystemSensor
«Détecteur de système informatique HP-UX» , à la page 341	HpUxComputerSystemSensor
«Détecteur de système informatique IBM AIX», à la page 347	AixComputerSystemSensor
«Détecteur IBM BladeCenter SNMP», à la page 311	BladeCenterSnmpSensor
«Détecteur IBM DB2», à la page 197	• Db2Sensor • Db2WindowsSensor
«Détecteur de console IBM HMC (Hardware Management Console)», à la page 353	HmcSensor
«Détecteur IBM High-Availability Cluster Multi-Processing», à la page 47	HACMPSensor
«Détecteur de système informatique IBM i», à la page 362	I5OSComputerSystemSensor
«Détecteur IBM Informix», à la page 203	Informix
«Détecteur IBM Integrated Virtualization Manager», à la page 361	IvmSensor
«Détecteur de serveur IBM Lotus Domino», à la page 51	• DominoDomainSensor • DominoServerDetailSensor • DominoInitialSensor
«Détecteur IBM Tivoli Storage Productivity Center», à la page 439	TPCStorageSensor
«Détecteur de cache IBM WebSphere eXtreme Scale», à la page 92	WebSphereXSCacheSensor
«Détecteur IBM WebSphere Message Broker» , à la page 94	MBServerSensor
«Détecteur IBM WebSphere MQ Server», à la page 96	MQServerSensor
«Détecteur IBM WebSphere», à la page 70	• WebSphereCellSensor • WebSphereNodeSensor • WebSphereVersionSensor
«périphérique IP, détecteur», à la page 248	IpDeviceSensor
«Détecteur iPlanet serveur», à la page 100	IPlanetServerSensor
«système informatique IPSO, détecteur», à la page 364	IPSOComputerSystemSensor
«Détecteur JBoss Application Server 7», à la page 104	JBoss7Sensor

Tableau 3. Détecteurs activés par défaut pour une reconnaissance de niveau 3 (suite)

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«Détecteur JBoss server», à la page 100	• JBossSensor • JBossVersionSensor
«Détecteur de la machine virtuelle basée sur le noyau», à la page 108	KvmSensor
«détecteur LAN Manager SNMP», à la page 314	LanManagerSnmpSensor
«détecteur LDAP», à la page 315	LdapSensor
«Détecteur de système informatique Linux», à la page 365	LinuxComputerSystemSensor
«Détecteur Microsoft Cluster», à la page 109	MSClusterSensor
«Détecteur Microsoft Exchange 2003», à la page 124	Exchange2003Sensor
«Détecteur Microsoft Exchange», à la page 113	ExchangeSensor
«Détecteur Microsoft HyperV», à la page 128	Détecteur Microsoft HyperV
«Détecteur de serveur Microsoft Web IIS», à la page 130	• IISWebServiceSensor • IISServerSensor
«Détecteur Microsoft SQL Server», à la page 206	SqlServerSensor
«Détecteur NetApp», à la page 454	NetAppSensor
«détecteur NetScreen SNMP», à la page 318	NetscreenSnmpSensor
«détecteur NFS», à la page 136	NFSServerSensor
«détecteur Nokia SNMP», à la page 320	NokiaSnmpSensor
«détecteur de système informatique OpenVMS», à la page 374	OpenVmsComputerSystemSensor
«Détecteur Oracle Application Server», à la page 137	• OracleAppOpmnSensor • OracleAppSensor
«détecteur Oracle», à la page 212	OracleSensor
«Détecteur Ping», à la page 249	PingSensor
«détecteur PIX», à la page 321	PixSensor
«Détecteur de port», à la page 253	PortSensor
«Détecteur de serveur SAP CCMS», à la page 145	CCMSServerSensor
«Détecteur de serveur SAP SLD», à la page 149	SLDServerSensor
«Détecteur de session», à la page 253	SessionSensor
«détecteur de serveur SMB», à la page 154	SMBServerSensor
«Détecteur de serveur SMS», à la page 154	SMSServerSensor
«Détecteur Snap Drive», à la page 455	SnapDriveSensor
«détecteur SNMP MIB2», à la page 324	SnmpMib2Sensor
«détecteur de système informatique Solaris», à la page 375	SunSparcComputerSystemSensor

Tableau 3. Détecteurs activés par défaut pour une reconnaissance de niveau 3 (suite)

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«Détecteur générique de zones Solaris», à la page 257	ZonesGenericSensor
«Détecteur de stockage», à la page 456	StorageSensor
«détecteur Sybase IQ», à la page 227	SybaseIQSensor
«détecteur Sybase», à la page 219	SybaseSensor
«détecteur Sun Fire SysControl», à la page 384	SysControlSensor
Fix Pack 2 Détecteur Sun Sparc Virtualization	SunSparcVirtualizationSensor
Fix Pack 1 Détecteur SVC Storage	SVCStorageSensor
«détecteur de système informatique Tru64», à la page 387	Tru64ComputerSystemSensor
«Détecteur de cluster Veritas», à la page 158	VeritasClusterSensor
«détecteur Veritas Storage Foundation», à la page 461	VeritasStorageSensor
«Détecteur de système informatique VMware ESX», à la page 389	VmwareComputerSystemSensor
«Détecteur de systèmes informatiques VMware ESXi», à la page 396	VmwareEsxiComputerSystemSensor
«Détecteur de serveur VMware VirtualCenter», à la page 161	VirtualCenterSensor
«Détecteur WebLogic SSH», à la page 182	• WeblogicLauncherSensor • WeblogicApplicationSensor • WeblogicDomainSensor • WeblogicServerSensor
«Détecteur de système informatique Windows», à la page 400	WindowsComputerSystemSensor
«Détecteur générique de partition de charge de travail», à la page 267	WparGenericSensor
Fix Pack 1 Détecteur XIV Storage	XIVStorageSensor
«Détecteur zEnterprise», à la page 268	ZEnterpriseSensor

Profil de reconnaissance d'utilisation

Ces détecteurs sont activés par défaut dans un profil de reconnaissance d'utilisation.

Le tableau 4, à la page 9 répertorie les détecteurs qui sont activés par défaut pour une reconnaissance d'utilisation.

Les détecteurs sont répertoriés dans l'ordre dans lequel ils apparaissent dans la fenêtre Profils de reconnaissance dans l'interface utilisateur TADDM.

Tableau 4. Détecteurs activés par défaut pour une reconnaissance d'utilisation

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«détecteur d'ancrage», à la page 228	AnchorSensor
«Détecteur d'utilisation d'IBM Tivoli», à la page 240	OperatingSystemUtilizationSensor
«Détecteur Ping», à la page 249	PingSensor
«Détecteur de port», à la page 253	PortSensor
«Détecteur de session», à la page 253	SessionSensor

Détecteurs prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows

Ces détecteurs prennent en charge une reconnaissance sous le système d'exploitation Windows sans fournir les données d'identification de l'utilisateur doté du rôle de l'administrateur.

Les détecteurs suivants prennent désormais en charge la reconnaissance sous Windows sans qu'il soit nécessaire de fournir les données d'identification de l'utilisateur doté du rôle d'administrateur :

Détecteurs d'application

Tableau 5. Détecteurs d'application prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows.

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur DNS», à la page 39	DnsSensor
«détecteur NFS», à la page 136	NFSServerSensor
«détecteur de serveur SMB», à la page 154	SMBServerSensor

Détecteurs de base de données

Tableau 6. Détecteurs de base de données prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows.

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur Microsoft SQL Server», à la page 206	SqlServerSensor

Détecteurs génériques

Tableau 7. Détecteurs génériques prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows.

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur de serveur d'applications personnalisé», à la page 231 (avec des restrictions)	CustomAppServerSensor
«Détecteur de système informatique générique», à la page 237	GenericComputerSystemSensor

Tableau 7. Détecteurs génériques prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows. (suite)

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur de serveur générique», à la page 237 (avec des restrictions)	GenericServerSensor
«Détecteur Ping», à la page 249	PingSensor
«Détecteur de port», à la page 253	PortSensor
«Détecteur de session», à la page 253 (avec des restrictions)	SessionSensor

Détecteurs de systèmes d'exploitation

Tableau 8. Détecteurs de systèmes d'exploitation prenant en charge une reconnaissance non administrateur sous le système d'exploitation Windows.

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur de système informatique Windows», à la page 400	WindowsComputerSystemSensor

Restrictions:

- Un détecteur de session ne prend pas en charge un déploiement automatique des fichiers du fournisseur Windows Management Instrumentation (WMI) de TADDM. Voir «Copie des fichiers TaddmWmi», à la page 412.
- Un détecteur de serveur générique ne reconnaît pas les arguments de ligne de commande du processus d'exécution. En conséquence, le détecteur de serveur d'application personnalisée ne démarre pas pour les modèles basés sur les conditions de type `Argument`. En outre, tout détecteur d'application qui utilise des modèles pourrait ne pas démarrer.

Vous devez toujours fournir un nom d'utilisateur qui dispose de données d'identification et de droits d'accès valides.

Pour effectuer la reconnaissance correctement, le reste des détecteurs d'applications requiert toujours que l'utilisateur détienne le rôle d'administrateur.

Remarque : Les paramètres UAC (User Access Control) de Windows n'affectent pas la reconnaissance non administrateur parce qu'ils ne peuvent pas être désactivés pour des utilisateurs standard.

Configuration des détecteurs pour exécuter une reconnaissance non administrateur

Pour configurer les détecteurs pour exécuter une reconnaissance non administrateur sous le système d'exploitation Windows, voir la rubrique «Configuration d'une reconnaissance Windows non administrateur», à la page 409.

Détecteurs prenant en charge une reconnaissance asynchrone et basée sur un script

Certains détecteurs peuvent être exécutés en tant que détecteurs basés sur un script. Ces détecteurs sont plus apparents, ce qui signifie que toutes les

commandes que le détecteur utilise sont dans un seul script, que vous pouvez afficher. Les détecteurs basés sur un script prennent également en charge la reconnaissance asynchrone.

Le tableau suivant répertorie tous les détecteurs basés sur un script, ainsi que les systèmes d'exploitation sur lesquels ils sont pris en charge.

Le «Détecteur de reconnaissance asynchrone», à la page 229 est requis pour la reconnaissance asynchrone. Voir également la rubrique *Configuration pour la reconnaissance asynchrone* dans le *Guide d'administration* de TADDM.

Remarques :

- Certains des détecteurs suivants sont basés sur un script par défaut, mais d'autres doivent être configurés pour activer la reconnaissance basée sur un script. Voir la rubrique *Configuration pour la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.
- Si le système informatique cible exécute le système d'exploitation Solaris, une reconnaissance basée sur un script peut échoue en cas d'utilisation de SunSSH 1.0.

Tableau 9. Liste des détecteurs basés sur un script..

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur	Systèmes d'exploitation sur lesquels le détecteur est pris en charge	Basé sur un script par défaut
«Détecteur Apache», à la page 19	ApacheServerSensor	• AIX • Linux • Solaris	Non
«Détecteur de reconnaissance asynchrone», à la page 229	ASDSensor	• AIX • FreeBSD • Linux • HP NonStop • Solaris • Windows	Oui
«Détecteur Citrix XenServer», à la page 329	XenServerSensor	• Linux	Oui
«Détecteur de système informatique FreeBSD», à la page 334	FreeBSDComputer SystemSensor	• FreeBSD	Non
«Détecteur de serveur générique», à la page 237	GenericServerSensor	• AIX • Linux • Solaris • Windows	Non
«Détecteur de système informatique HP NonStop», à la page 340	HpNonStopComputer SystemSensor	• HP NonStop	Oui
«Détecteur de système informatique IBM AIX», à la page 347	AixComputerSystem Détecteur	• AIX	Non

Tableau 9. Liste des détecteurs basés sur un script. (suite).

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur	Systèmes d'exploitation sur lesquels le détecteur est pris en charge	Basé sur un script par défaut
«Détecteur IBM DB2», à la page 197	Db2Sensor	• AIX • Linux • Solaris	Non
«Détecteur de serveur IBM Lotus Domino», à la page 51	DominoInitialSensor	• AIX • Linux • Solaris	Non
«Détecteur d'utilisation d'IBM Tivoli», à la page 240	OperatingSystem UtilizationSensor	• AIX • FreeBSD • Linux • Solaris	Non
«Détecteur IBM WebSphere MQ Server», à la page 96	MQServerSensor	• AIX • Linux • Solaris • Windows	Oui
«Détecteur IBM WebSphere», à la page 70	WebSphereScript Détecteur	• AIX • Linux • Solaris • Fix Pack 2 Windows	Oui
«Détecteur JBoss Application Server 7», à la page 104	JBoss7Sensor	• AIX • Linux • Solaris • Windows	Oui
«Détecteur de la machine virtuelle basée sur le noyau», à la page 108	KVMSensor	• Linux	Oui
«Détecteur de système informatique Linux», à la page 365	LinuxComputer SystemSensor	• Linux	Non
«Détecteur Microsoft Exchange», à la page 113	ExchangeSensor	• Windows	Oui
«Détecteur de serveur Microsoft Web IIS», à la page 130	IISServerSensor	• Windows	Oui
Fix Pack 2 «Détecteur Microsoft SQL Server», à la page 206 (avec des restrictions)	SqlServerSensor	• Windows	Non
«détecteur Oracle», à la page 212	OracleSensor	• AIX • Linux • Solaris	Non

Tableau 9. Liste des détecteurs basés sur un script. (suite).

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur	Systèmes d'exploitation sur lesquels le détecteur est pris en charge	Basé sur un script par défaut
«détecteur de système informatique Solaris», à la page 375	SunSparcComputer SystemSensor	• Solaris	Non
Fix Pack 2 «Détecteur Sun Sparc Virtualization» , à la page 382	SunSparc VirtualizationSensor	• Solaris	Oui
«Détecteur WebLogic SSH», à la page 182	WeblogicLauncher Détecteur	• AIX • Linux • Solaris	Non
«Détecteur de système informatique Windows», à la page 400	WindowsComputer SystemSensor	• Windows	Non

Restrictions

- Fix Pack 2 Le mode de reconnaissance basée sur un script du détecteur Microsoft SQL Server repose sur le module sqlps, qui est disponible dans Microsoft SQL Server 2008 et versions ultérieures. Par conséquent, si vous souhaitez reconnaître Microsoft SQL Server 2005, vous devez également disposer d'autres instances telles que Microsoft SQL Server 2008, 2008 R2 ou 2012.

Détecteurs prenant en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring (ancienne méthode)

Ces détecteurs prennent en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring.

Nouvelle méthode d'intégration

Important : A partir de TADDM 7.3.0, il est recommandé d'effectuer l'intégration avec IBM Tivoli Monitoring 6.3 via une automatisation OSLC. L'ancienne méthode d'intégration consistant à utiliser un détecteur IBM Tivoli Monitoring Scope est obsolète et sera retirée des prochaines éditions.

Pour plus d'informations sur l'intégration de TADDM avec ITM à l'aide de l'automatisation OSLC, consultez la rubrique *Intégration de TADDM à IBM Tivoli Monitoring via OSLC Automation* du *Guide d'administration* de TADDM et sur les détecteurs qui prennent en charge la reconnaissance à l'aide de l'automatisation OSLC, voir «Détecteurs prenant en charge une reconnaissance via un automatisation OSLC», à la page 15.

Le «Détecteur de portée IBM Tivoli Monitoring», à la page 54 est requis pour une reconnaissance à l'aide d'IBM Tivoli Monitoring. Ce détecteur doit être exécuté au moins une fois pour créer les ensembles de portées nécessaires.

Le détecteur IBM Tivoli Monitoring Scope crée des ensembles de portée pour tous les systèmes informatiques actifs dans un environnement Tivoli Monitoring. Une fois ces ensembles de portées créés, vous pouvez exécuter une reconnaissance de

niveau 2 et 3 de ces systèmes informatiques à l'aide d'une session Tivoli Monitoring, et ce sans inclure le détecteur IBM Tivoli Monitoring Scope dans les profils de reconnaissance de niveau 2 et 3.

Remarque : Si vos systèmes informatiques gérés sur IBM Tivoli Monitoring se cachent derrière un pare-feu (c'est-à-dire ne sont pas accessibles via le serveur de reconnaissance TADDM), vous pouvez intégrer le détecteur IBM Tivoli Monitoring Scope à votre profil avec l'option startSessionOnly activée. Pour plus d'informations, voir la section Configuring the discovery profile de la documentation du détecteur IBM Tivoli Monitoring Scope.

Pour une reconnaissance de niveau 2 et 3 de systèmes surveillés par IBM Tivoli Monitoring, les fonctions suivantes doivent être installées sur le système cible :

- Sur des systèmes cible Windows, Microsoft .NET Framework doit être installé. Pour plus d'informations, voir la rubrique *Configuration pour la reconnaissance des systèmes Windows* dans le *Guide d'administration* de TADDM.
- Sur des systèmes cible Linux et UNIX, les commandes **uuencode** et **uudecode** compatibles avec l'interface POSIX (Portable Operating System Interface) doivent être installées.

  Sur les systèmes d'exploitation Linux, ces commandes sont généralement incluses dans le package **sharutils**.

  Sous les systèmes d'exploitation AIX, Solaris et HP-UX, ces commande sont installées par défaut.

Tous les détecteurs d'un profil de reconnaissance de niveau 2 et 3 ne prennent pas en charge la reconnaissance à l'aide de Tivoli Monitoring. Le tableau 10 répertorie les détecteurs prenant en charge la reconnaissance avec Tivoli Monitoring. Quand un détecteur s'exécute dans la session Tivoli Monitoring, il se sert des données d'identification d'accès de Tivoli Monitoring au lieu des données d'accès configurées pour le détecteur. Le compte utilisateur Tivoli Monitoring doit disposer de l'autorisation nécessaire pour accéder à l'application en cours de reconnaissance. Par exemple, pour reconnaître des serveurs IBM DB2 Universal Database (UDB), le compte utilisateur Tivoli Monitoring sur le serveur DB2 cible doit être membre du groupe d'administration DB2.

Tableau 10. Détecteurs prenant en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring

Détecteur	**Nom du détecteur utilisé dans les journaux et l'interface utilisateur**
«Détecteur Apache», à la page 19	ApacheServerSensor
«Détecteur de serveur générique», à la page 237	GenericServerSensor
«Détecteur de système informatique IBM AIX», à la page 347	AixComputerSystemSensor
«Détecteur IBM DB2», à la page 197	Db2Sensor
«Détecteur IBM WebSphere MQ Server», à la page 96	MQServerSensor
«Détecteur IBM WebSphere», à la page 70	WebSphereScriptSensor
«Détecteur de système informatique Linux», à la page 365	LinuxComputerSystemSensor
«détecteur Oracle», à la page 212	OracleSensor
«détecteur de système informatique Solaris», à la page 375	SunSparcComputerSystemSensor

Tableau 10. Détecteurs prenant en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring (suite)

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
Fix Pack 2 «Détecteur Sun Sparc Virtualization», à la page 382	SunSparcVirtualizationSensor
«Détecteur de stockage», à la page 456	StorageSensor
«Détecteur WebLogic SSH», à la page 182	WeblogicLauncherSensor
«Détecteur de système informatique Windows», à la page 400	WindowsComputerSystemSensor

Détecteurs prenant en charge une reconnaissance via un automatisation OSLC

Ces détecteurs prennent en charge la reconnaissance à l'aide d'IBM Tivoli Monitoring.

Pour exécuter une reconnaissance via une automatisation OSLC, l'agent OSLCAutomationAgent doit créer les ensembles de portées nécessaires. Une fois ces ensembles de portées créés, vous pouvez exécuter une reconnaissance de niveau 2 et de niveau 3 des systèmes informatiques qui utilisent la session d'automatisation OSLC.

Pour plus d'informations sur la configuration de la reconnaissance, voir la rubrique *Configuration pour reconnaissance sur une session d'automatisation OSLC* dans le *Guide d'administration* de TADDM.

Pour une reconnaissance de niveau 2 et 3 de systèmes surveillés par IBM Tivoli Monitoring, Microsoft .NET Framework doit être installé sur les systèmes cible Windows.

Pour plus d'informations sur les versions prises en charge de .NET Framework, voir la rubrique *Configuration pour la reconnaissance des systèmes Windows* dans le *Guide d'administration* de TADDM.

Les détecteurs qui prennent en charge une reconnaissance via une automatisation OSLC sont les mêmes que ceux qui prennent en charge une reconnaissance à l'aide de IBM Tivoli Monitoring.

Tableau 11. Détecteurs prenant en charge une reconnaissance via une automatisation OSLC

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur Apache», à la page 19	ApacheServerSensor
«Détecteur de serveur générique», à la page 237	GenericServerSensor
«Détecteur de système informatique IBM AIX», à la page 347	AixComputerSystemSensor
«Détecteur IBM DB2», à la page 197	Db2Sensor
«Détecteur IBM WebSphere MQ Server», à la page 96	MQServerSensor

Tableau 11. Détecteurs prenant en charge une reconnaissance via une automatisation OSLC (suite)

Détecteur	Nom du détecteur utilisé dans les journaux et l'interface utilisateur
«Détecteur IBM WebSphere», à la page 70	WebSphereScriptSensor
«Détecteur de système informatique Linux», à la page 365	LinuxComputerSystemSensor
«détecteur Oracle», à la page 212	OracleSensor
«détecteur de système informatique Solaris», à la page 375	SunSparcComputerSystemSensor
«Détecteur Sun Sparc Virtualization», à la page 382	SunSparcVirtualizationSensor
«Détecteur de stockage», à la page 456	StorageSensor
«Détecteur WebLogic SSH», à la page 182	WeblogicLauncherSensor
«Détecteur de système informatique Windows», à la page 400	WindowsComputerSystemSensor

Problèmes de configuration des détecteurs

Cette rubrique décrit les problèmes courants qui peuvent survenir avec l'installation du détecteur dans TADDM.

Aucun système d'exploitation Linux, Solaris, AIX ou Linux on System z n'a été reconnu

Problème

Aucun système d'exploitation Linux, Solaris, AIX ou Linux on System z n'a pu être reconnu.

Solution

Assurez-vous que les prérequis de la reconnaissance des systèmes d'exploitation Linux, Solaris, AIX et Linux sur System z ont été satisfaits :

- Créez un compte de service. Configurez le compte pour qu'il soit membre du groupe sys et utilisez `/bin/sh` comme shell pour ce compte.
- Installez et testez le protocole SSH (Secure Shell) dans le serveur TADDM. Si vous utilisez une authentification par clé, installez des clés publiques sur tous les hôtes. Pour vérifier que le nom d'utilisateur et le mot de passe ou la clé et la phrase passe fonctionnent correctement, entrez la commande **ssh** dans l'invite de commande de l'ordinateur où le serveur TADDM est installé.
- Installez le programme LiSt Open Files (lsof) sur tous les ordinateurs hôtes, selon les *exigences lsof* dans le Wiki TADDM à l'adresse https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Application%20Dependency%20Discovery%20Manager/page/TADDM%20lsof%20requirements.

Sur les systèmes d'exploitation Linux, AIX, et Linux on System z, la reconnaissance ne se termine jamais

Problème

Sur un système d'exploitation Linux, AIX, ou Linux on System z, la reconnaissance ne se termine jamais. L'exécution de la commande `ps -ef` montre des instances du processus `stop-local-anchor.sh` qui durent plus de 5 minutes.

Solution

L'accès à la commande **sudo** doit être configuré pour que l'utilisateur TADDM, c'est à dire l'utilisateur qui démarre le serveur TADDM, puisse exécuter les commandes **sudo** sans l'affichage de l'invite d'entrée du mot de passe. Pour configurer ainsi l'accès à la commande **sudo**, procédez comme suit :

1. Connectez-vous au serveur TADDM en tant que superutilisateur.
2. Entrez la commande **visudo**.
3. Entrez la ligne suivante dans le fichier /etc/sudoers, où *TADDM_USER* est l'utilisateur qui démarre le serveur TADDM :

   ```
   <TADDM_USER> ALL=NOPASSWD:ALL
   ```

Pour vérifier que l'accès à la commande **sudo** est correctement configuré, entrez les commandes suivantes :

```
cd $COLLATION_HOME/bin
sh ./stop-local-anchors.sh
```

Si une invite de mot de passe s'ouvre, l'accès NOPASSWD n'a pas été correctement configuré pour cet utilisateur TADDM.

Une reconnaissance des serveurs d'applications en cours d'exécution sur le système d'exploitation Solaris 10 renvoie des numéros de port incorrects

Problème

Des numéros de port incorrects sont renvoyés lorsque vous effectuez une reconnaissance des serveurs d'applications en cours d'exécution sur le système d'exploitation Solaris 10.

Solution

Assurez-vous que lsof 4.77, ou version ultérieure, est installé sur chaque système en cours d'exécution sur le système d'exploitation Solaris 10. Les versions d'lsof antérieures à 4.77 ne prennent pas en charge Solaris 10 6/06 ou version ultérieure. De plus, il existe deux versions d'lsof 4.77. Une version est destinée à la pré-édition 6/06 Solaris 10 et l'autre pour 6/06 Solaris 10 et les versions ultérieures. Assurez-vous que vous installez la version d'lsof 4.77 qui correspond à la version du système d'exploitation Solaris 10 installé.

Détecteurs d'application

Les détecteurs d'application reconnaissant les applications qui s'exécutent dans l'environnement.

Détecteur Active Directory

Le détecteur Active Directory reconnaît les serveurs Microsoft Active Directory.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Détecteur Active Directory

Problèmes de sécurité

Le détecteur utilise la commande **ntdsutil.exe** au cours de la reconnaissance et cette commande requiert des privilèges de sécurité élevés. Pour vérifier que le compte de reconnaissance dispose des privilèges appropriés, entrez la commande suivante sur une seule ligne :

Sous Windows 2000 et Windows Server 2003 :

```
ntdsutil "domain management" connections "connect to server localhost"
q "list" q q
```

Sous Windows Server 2008 :

```
ntdsutil "partition management" connections "connect to server localhost"
 q "list" q q
```

Objets de modèle avec attributs associés

Le détecteur Active Directory crée des objets de modèle avec les attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les serveurs Microsoft Active Directory de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

sys.ActiveDirectory

- Host
- InitRecvTimeout
- MaxConnIdleTime
- MaxConnections
- MaxDatagramRecv
- MaxNotificationPerConn
- MaxPageSize
- MaxPoolThreads
- MaxQueryDuration
- MaxReceiveBuffer
- MaxResultSetSize
- MaxTempTableSize
- MaxValRange
- NamingContexts
- Name
- RootDomain
- SchemaVersion
- ServiceXML
- WorkingDirectory

sys.ServiceAccessPoint

- ContextIp
- BindAddress
- Name
- ProductName
- ProductVersion
- VendorName

sys.NamingContext

- Index
- Valeur

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la portée

Le serveur Active Directory doit être inclus dans la portée de la reconnaissance.

Configuration de la liste d'accès

Vous devez ajouter le système informatique (par exemple, Windows) à la liste d'accès, et l'ID utilisateur pour accéder au système doit appartenir au groupe d'administrateurs.

Configuration du profil de reconnaissance

Le détecteur est activé par défaut dans un profil de reconnaissance de niveau 3. Vous pouvez également créer un profil personnalisé et activer le détecteur Active Directory et le détecteur de système informatique Windows depuis le nouveau profil.

Détecteur Apache

Le détecteur Apache reconnaît les serveurs Web Apache.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ApacheServerSensor

Prérequis

Le compte de service TADDM requiert ce qui suit :

- L'autorisation d'exécution sur le fichier binaire `httpd`
- L'accès en lecture au fichier `httpd.conf`
- L'utilisateur de la reconnaissance dispose d'autorisations de lecture et d'exécution sur l'ensemble des bibliothèques/modules/fichiers/dossiers Apache nécessaires pour exécuter correctement la commande `httpd` (par exemple, /oracle/product/iasgrm/librarypath et /oracle/product/iasgrm/Apache, etc.).

Limitations

Le détecteur Apache ne peut pas reconnaître le serveur Apache si l'instance du serveur Apache est configurée ou démarrée de sorte qu'elle réécrit sa ligne de commande (par exemple, la réécriture du tableau argv), obligeant ainsi l'instance du serveur Apache à se présenter dans une liste de processus comme `httpd`, sans chemin ni options de ligne de commande.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.CertificateFile

- app.ConfigFile
- app.PrivateKeyFile
- app.web.ServerAlias
- app.web.apache.ApacheGlobalSSLSettings
- app.web.apache.ApacheModule
- app.web.apache.ApacheSSLSettings
- app.web.apache.ApacheServer
- app.web.apache.ApacheVirtualHost
- app.web.apache.ApacheWebContainer
- app.web.ibm.IBMHTTPServer
- app.web.oracleapp.OracleAppHTTPServer
- app.web.WebConnection
- app.web.WebVirtualHostConfigDirective

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur Apache prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Certaines fonctions fournies par le détecteur Apache durant une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

La reconnaissance de descripteur d'application n'est pas pris en charge.

Les attributs suivants ne sont pas pris en charge pour un fichier de configuration :

- Dernière modification
- Owner
- Group
- Permissions

Seules les applications sont reconnues.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Ce détecteur peut être exécuté à l'aide des droits d'accès de ComputerSystem utilisés pour reconnaître le client.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.discover.agent.ApacheServerAgent.UseListenningIp=false
Le détecteur reconnaît les serveurs Web Apache et affecte le même nom au lieu d'en signaler un pour chaque nom d'hôte de serveur Web. Lorsque cette propriété est définie sur true, le nom affiché de l'objetApacheServer est défini sur :

HOSTNAME:LISTENINGIP:PORT

La valeur par défaut de cette propriété est false.

Vous devez supprimer manuellement les instances HOSTNAME:PORT.

com.collation.discover.agent.ApacheServerAgent.CmdPrefix
Ajoute une commande ou un script qui doit être exécutée avant la commande **httpd-v** . Cette propriété peut être configurée pour le nom du système d'exploitation, l'adresse IP ou les deux.

Le détecteur Apache tente d'utiliser cette propriété en cas d'échec de la première commande (standard). Par exemple :

com.collation.discover.agent.ApacheServerAgent.CmdPrefix.
AIX.9.156.47.172=LIBPATH=/usr/local/apache2/build:/usr/local/
apache2/lib:/usr/lib:/lib/;export LIBPATH

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Apache et propose des solutions à ces problèmes.

Erreur de reconnaissance avec «Impossible d'exécuter httpd»

Problème
Une erreur de reconnaissance indique `Impossible d'exécuter httpd`, mais le compte de service TADDM peut exécuter le processus httpd manuellement.

Le détecteur de session essaie chaque droit d'accès de la liste d'accès applicable jusqu'à ce que l'un d'entre eux fonctionne. Lorsqu'un droit de la liste fonctionne, le détecteur de session cesse toute tentative. Par conséquent, le premier droit d'accès de la liste d'accès qui fonctionne doit pouvoir exécuter le processus httpd.

Solution

Essayez d'utiliser les restrictions de portée avec une liste d'accès réorganisée pour forcer l'utilisation du compte adéquat afin d'effectuer la reconnaissance du serveur Apache.

Echec du détecteur Apache avec l'erreur CTJTD0072E

Problème

Le détecteur Apache utilise la commande **httpd -V** pour obtenir le répertoire principal, le fichier de configuration et d'autres informations relatives au serveur Apache. Si la commande **httpd -V** échoue, le détecteur échoue également.

Solution

Utilisez la propriété com.collation.discover.agent.ApacheServerAgent.CmdPrefix pour indiquer une commande à exécuter après la commande **httpd -V**.

De nombreuses zones du panneau Détails sont vides

Problème

Plusieurs zones du panneau Détails sont vides.

Solution

Le compte de service ne peut pas lire le fichier `http.conf`. Faites en sorte que le fichier `http.conf` puisse être lu publiquement ou ajoutez ce compte à un groupe doté d'un accès en lecture pour le fichier `http.conf`.

Détecteur de serveur Citrix

Fix Pack 4

Le détecteur de serveur Citrix détecte un serveur de présentation Citrix (Citrix Presentation Server Enterprise 3 et 4) ou un serveur XenApp (Citrix XenApp Enterprise version 5 et version 6).

Nom du détecteur utilisé dans l'interface graphique et les journaux

CitrixServerSensor

Problèmes de sécurité

L'utilisateur de la reconnaissance doit disposer d'autorisations de lecture (définies dans la console de produit Citrix) pour la configuration de Citrix. Pour reconnaître la configuration du serveur de présentation Citrix, vous devez disposer de l'autorisation d'interroger le fournisseur WMI Citrix. Pour pouvoir être reconnu, ce fournisseur doit être en cours de fonctionnement.

Le fournisseur WMI Citrix se trouve sur le système reconnu où le serveur de présentation Citrix est installé. Il fait partie du produit Citrix.

Pour accorder ces droits d'accès, procédez comme suit :

1. Connectez-vous à la console de gestion du serveur de présentation Metaframe.
2. Dans le menu, sélectionnez **Actions** > **Autorisations**.
3. Modifiez les droits d'utilisateur et de groupe.

4. Assurez-vous que l'autorisation **Afficher la gestion de la ferme** a été accordée. Cette autorisation est l'autorisation minimale qui doit être accordée pour interroger le fournisseur WMI Citrix.
   a. Sélectionnez un utilisateur ou un groupe.
   b. Cliquez sur **Editer**
   c. Sélectionnez l'autorisation appropriée :
      - **Visualisation uniquement :** fonctionne pour le détecteur Citrix
      - **Administration complète :** fonctionne pour le détecteur Citrix
      - **Personnalisée :** l'administrateur peut définir son propre niveau d'accès

Objets de modèle avec attributs associés

Le détecteur de serveur Citrix crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur à propos des serveurs Citrix Presentation Server et XenApp dans votre environnement informatique.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur Citrix et propose les solutions à ces problèmes.

Reconnaissance Citrix XenApp 7.6

Cette rubrique présente les détails de la reconnaissance du logiciel Citrix XenApp 7.6.

Objets de modèle avec attributs associés

Le détecteur de serveur Citrix crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur à propos des serveurs Citrix Presentation Server et XenApp dans votre environnement informatique.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

CitrixAccountAuthority

- AuthorityName
- AuthorityType
- Group

CitrixAppFolder

- Applications
- Farm

CitrixApplication

- AppFolder
- ApplicationID
- CitrixFarm
- CitrixGroups
- Servers
- Users

CitrixFarm

- AppFolders
- DSDriver
- DSODBC
- FarmName
- LicensePool
- LocalIp
- SNMPDisconnectTrap
- SNMPLogoffTrap
- SNMPLogonTrap
- SNMPThresholdExceededTrap
- SNMPThresholdValue
- ServerFolders
- Zones

CitrixFolder

- FolderDN
- FolderName
- Folders
- Parent

CitrixGroup

- AccountAuthority
- CitrixApplications

CitrixLicense

- Pool
- SerialNumber

CitrixLicensePool

- DupGroup
- Farm
- FloatOk
- HostBased
- HostID
- Licenses
- PLD
- Platforms
- SubscriptionDate
- UserBased
- VendorString

CitrixServer

- Applications
- Folder
- IsFarmServer
- LocalPrimarySAP
- Processes
- Zone

CitrixServerFolder

- Farm
- Servers

CitrixUser

- AccountAuthority
- Applications

CitrixZone

- DataCollector
- Farm
- Servers
- ZoneName

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur Citrix et propose les solutions à ces problèmes.

L'exécution du détecteur Citrix est lente.

Problème

Le détecteur Citrix s'exécute lentement sur des systèmes qui sont surchargés de nombreuses applications Citrix publiées (les requêtes WMI peuvent durer longtemps).

Solution

Augmentez la valeur du délai d'attente du détecteur en définissant les propriétés suivantes dans le fichier `collation.properties` :

- `com.collation.discover.agent.CitrixServerAgent.sessiontimeout=600000`
- `com.collation.discover.agent.CitrixServerAgent.timeout=600000`

Ces propriétés doivent être définies à une valeur qui est au moins égale à la valeur de la propriété `com.collation.discover.DefaultAgentTimeout`.

Détecteur de serveur Citrix 7

Fix Pack 4

Le détecteur de serveur Citrix 7 découvre un serveur XenApp (Citrix XenApp Enterprise version 7.6) et utilise une interface SDK Citrix powershell à des fins de reconnaissance.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Citrix7Sensor

Eléments reconnus par le détecteur

Le détecteur reconnaît les éléments suivants qui sont associés à l'environnement du logiciel de virtualisation d'application Citrix XenApp :

Site(s) de distribution - Elément de niveau avec la priorité la plus élevée. Les sites offrent des applications au groupe d'utilisateurs.

Catalogues de machines – Peuvent être utilisés pour gérer des machines qui hébergent des applications.

Machine(s) – Machines Citrix qui hébergent Citrix XenApp 7.6

Utilisateurs Citrix – Ensemble d'utilisateurs autorisés à accéder aux applications virtuelles spécifiées.

Applications Citrix – Applications virtualisées accessibles à un groupe d'utilisateurs donné.

Informations sur la licence – Pools de licences Citrix et détails des licences individuelles.

Prérequis

Les prérequis suivants sont obligatoires :

- Ce capteur basé sur des scripts utilise le même utilisateur de la reconnaissance que celui utilisé pour la connexion Windows.
- L'utilisateur de la reconnaissance Windows doit disposer des autorisations “administrateur en lecture seule” (définies dans la console Citrix) pour la configuration Citrix sur n'importe quel contrôleur de livraison pour chaque site. Citrix exige que l'utilisateur de la reconnaissance soit un compte Active Directory et non un compte local.
- Les composants logiciels enfichables Citrix Powershell doivent être installés et disponibles sur le contrôleur de livraison.

Objets de modèle avec attributs associés

Citrix 7 introduit un changement d'architecture issu de Citrix 6, mais le modèle de données TADDM est basé sur l'architecture de Citrix 6. Afin de préserver la compatibilité avec les versions antérieures pour le mappage des applications métier, les composants d'architecture de Citrix 7 sont stockés en tant que composants de modèle de données Citrix 6. Le tableau ci-dessous montre les anciens et les nouveaux concepts ainsi que leur correspondance avec le modèle de données TADDM.

Tableau 12. Correspondance entre Citrix 7 et Citrix 6

Citrix 7	**Citrix 6**	**Commentaires**
Site	CitrixFarm/CitrixZone	Pour chaque site Citrix, il y aura une combinaison Farm/Zone de même nom.
Dossier admin	CitrixAppFolder	Organise les composants CitrixApplication.
Catalogue bureau	CitrixServerFolder	N/A
Groupe bureau	N/A	Les groupes bureau sont utilisés pour affecter les composants CitrixApplications aux CitrixServers.

Le détecteur de serveur Citrix 7 crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur à propos des serveurs Citrix Presentation Server et XenApp dans un environnement informatique.

Certains attributs des objets de modèle Citrix ne sont pas pertinents ou ne sont pas utilisés dans l'architecture Citrix XenApp 7.6. Ils ne seront donc pas remplis et pourront donc être affichés sans aucune valeur (“Blank") dans TADDM Data Management Portal, puisque le modèle de données TADDM est basé sur l'architecture de Citrix 6.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

CitrixAccountAuthority
- AuthorityName
- Group

CitrixAppFolder
- Applications
- Farm

CitrixApplication
- AppFolder
- ApplicationID
- CitrixFarm
- CitrixGroups
- Serveurs
- Users

CitrixFarm
- AppFolders
- FarmName
- LicensePool
- LocalIp
- ServerFolders
- Zones

CitrixFolder
- FolderDN
- FolderName
- Folders
- Parent

CitrixGroup
- AccountAuthority
- CitrixApplications

CitrixLicense
- Pool
- SerialNumber

CitrixLicensePool
- DupGroup

- Farm
- FloatOk
- HostBased
- HostID
- Licenses
- PLD
- Platforms
- SubscriptionDate
- UserBased
- VendorString

CitrixServer
- Applications
- Folder
- LocalPrimarySAP
- Processes
- Zone

CitrixServerFolder
- Farm
- Servers

CitrixUser
- AccountAuthority
- Applications

CitrixZone
- DataCollector
- Farm
- Servers
- ZoneName

Limitations
- Les noms de sites sont supposés être globaux. Il est impossible d'avoir deux sites ayant exactement le même nom ou cela provoquera une sur-fusion.
- Le mode de reconnaissance asynchrone n'est pas pris en charge.

Remarque : Pour la reconnaissance basées sur Anchor de Citrix XenApp 7.6, la reconnaissance de script doit être activée dans le fichier collation.properties :

```
com.ibm.cdb.discover.PreferScriptDiscovery=true
```

Détecteur d'hôte Docker

Fix Pack 4

Le détecteur d'hôte Docker reconnaît les hôtes Docker, les attributs de l'hôte, les conteneurs, les informations liées à la mise en réseau, à l'image et au stockage.

Nom du détecteur utilisé dans l'interface graphique et les journaux

DockerHostSensor

Eléments reconnus par le détecteur

Le détecteur reconnaît les éléments suivants :

- Hôtes Docker
- Conteneurs Docker
- Volumes Docker
- Réseaux Docker
- Images Docker

Dans la console de gestion de la reconnaissance et le portail de gestion des données, un hôte Docker est représenté par une icône en forme de baleine Docker bleue et un conteneur Docker est représenté par des conteneurs d'expédition carrés sur quatre niveaux.

Le détecteur d'hôte Docker utilise des API REST pour extraire les informations de reconnaissance du système hôte Docker qui exécute le processus démon ou l'application 'dockerd'. Les données extraites se composent principalement des données d'attribut nécessaires pour établir une correspondance avec des règles de dénomination et créer des objets de modèle valides.

Prérequis

- Le démon ou l'application Docker est en cours d'exécution sur le système Linux cible.
- Pour permettre la reconnaissance de l'hôte Docker, le support REST doit être activé sur le système cible.
- Vous devez définir des ports pour les communications de services Web. Par défaut, la valeur du port provenant du traitement GenericServerSensor est utilisée. Si l'hôte Docker utilise le mappage de ports ou un port non standard, modifiez la valeur de la propriété *portList* dans le profil de reconnaissance. Pour plus de détails, voir 'Configuration du profil de reconnaissance'.
- Un ensemble unique de certificats TLS est applicable à tous les hôtes Docker pour les communications TADDM.
- L'activation ou la désactivation de la reconnaissance TLS entraîne un comportement uniforme sur TOUS les hôtes Docker définis dans la portée
  - Est applicable à TOUS les hôtes ou n'est applicable à AUCUN des hôtes Docker.

Dans la console de gestion de la reconnaissance et le portail de gestion des données, un hôte Docker est représenté par une icône en forme de baleine Docker bleue et un conteneur Docker est représenté par des conteneurs d'expédition carrés sur quatre niveaux.

Le détecteur d'hôte Docker utilise des API REST pour extraire les informations de reconnaissance du système hôte Docker qui exécute le processus démon ou l'application 'dockerd'. Les données extraites se composent principalement des données d'attribut nécessaires pour établir une correspondance avec des règles de dénomination et créer des objets de modèle valides.

Problèmes de sécurité

Aucune entrée de liste d'accès spécifique n'est requise. Pour plus d'informations sur la sécurité TLS, voir **Connexion à l'hôte Docker** ci-dessous :

Connexion à l'hôte Docker

Le détecteur d'hôte Docker peut reconnaître des données de l'hôte Docker via deux modes : le mode non TLS et le mode TLS.

Mode non TLS

Le mode non TLS est le mode par défaut. Il extrait les données via des services Web et ne requiert pas d'authentification. Ce mode est recommandé dans les déploiements de réseau privé ou de cloud privé sur les sites des clients.

Mode TLS

Le mode TLS est un mode sécurisé de communication avec l'hôte Docker. Il vérifie les certificats TLS installés dans TADDM et l'hôte Docker cible. Pour utiliser ce mode, vous devez affecter la valeur true à la propriété enableTLS et configurer les chemins des certificats définis dans le profil de reconnaissance. Pour plus de détails, voir **Configuration du profil de reconnaissance**. Pour générer manuellement les certificats TLS pour TADDM et l'hôte Docker, voir **Génération manuelle des certificats TLS**.

Objets de modèle avec attributs associés

Le détecteur d'hôte Docker crée des objets de modèle avec les attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les ressources de l'hôte Docker dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

app.docker.dockerhost.DockerHost

- Name
- VersionString
- DockerContainers
- DockerImages
- DockerNetworks
- DockerVolumes
- Host
- XA
  - Architecture
  - KernelVersion
  - OperatingSystem
  - OSType
  - RunningContainers
  - StoppedContainers
  - TotalContainers

app.docker.dockerhost.DockerContainer
- Name
- Parent
- RuntimeProcesses
- DockerContainerStatus
- DockerImages
- DockerNetworks
- DockerVolumes

app.docker.dockerhost.DockerImage
- DockerHost
- ImageName
- DockerContainer

app.docker.dockerhost.DockerNetwork
- Name
- SubnetAddress
- DockerHost
- DockerContainer

app.docker.dockerhost.DockerVolume
- Name
- DockerHost
- DockerContainer

sys.RuntimeProcess (applicable aux processus au sein d'un conteneur)
- PID
- Command
- PPID
- User
- CmdLine (désigne la commande complète)

Configuration du détecteur

Avant d'utiliser le détecteur d'hôte Docker, vous devez le configurer.

Configuration du profil de reconnaissance :

Par défaut, le détecteur d'hôte Docker est activé pour une reconnaissance de niveau 3. Une fois activé, il s'exécute par défaut en mode non TLS. Le détecteur reconnaît tous les conteneurs Hôte Docker, y compris ceux qui ne sont pas en cours d'exécution. Pour reconnaître uniquement les conteneurs qui sont en cours d'exécution ou passer en mode TLS, créez un profil de reconnaissance pour le détecteur d'hôte Docker et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

Exemple :

1. Dans le tiroir Reconnaissance de la console de gestion de la reconnaissance, cliquez sur **Profils de reconnaissance**.

2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre de création de profil, entrez le nom et la description du profil. Dans la liste **Cloner le profil existant**, sélectionnez **Reconnaissance de niveau 3** et cliquez sur **OK**.
4. Dans l'onglet Configuration du détecteur, sélectionnez le détecteur **DockerHostSensor** et cliquez sur **Nouveau**.
5. Dans la fenêtre Création de configuration, entrez le nom et la description de votre configuration du détecteur et cochez la case **Activer la configuration**.
6. Dans la section Configuration de la fenêtre Créer une configuration, cliquez sur **discoverNonRunningContainers**. Cliquez ensuite deux fois sur la zone Valeur dans la ligne et entrez *false*.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Propriétés

Vous pouvez modifier les propriétés et les attributs ci-dessous :

portList

Désigne le(s) port(s) à utiliser pour les communications de services Web sur l'hôte Docker. Par défaut, la valeur du port renvoyée par le traitement GenericServerSensor est utilisée. Si l'hôte Docker utilise le mappage de ports ou un port non standard (ou une liste de ports séparés par des virgules), indiquez la valeur correspondante.

enableTLS

Désigne le mode de connexion entre TADDM et l'hôte Docker.

La valeur par défaut est false.

pathStore

Chemin local du serveur de reconnaissance TADDM où tous les certificats de sécurité/TLS sont placés.

caFileName

Nom du fichier de l'autorité de certification.

cerFileName

Nom du fichier du certificat client.

keyFileName

Nom du fichier de clés du client.

Activation du support REST sur l'hôte Docker

Sur un hôte Docker, vous devez apporter les modifications suivantes à la configuration :

1. Activez les API REST sur l'hôte Docker.
   - Connectez-vous au système hôte Docker à l'aide de données d'identification 'root'.
   - Créez/mettez à jour le fichier suivant sur l'hôte Docker :

     vim /etc/systemd/system/docker.service.d/remote-api.conf

     avec le contenu :

     [Service]

     ExecStart=

     ExecStart=/usr/bin/dockerd -H tcp://<DockerHost-IP>:2376 -H unix:///var/run/docker.sock
2. Redémarrez le démon 'dockerd' et vérifiez le statut à l'aide de la commande suivante :

   service docker restart

   ps -aef | grep -i dockerd

Génération manuelle de certificats TLS

Lorsque le mode TLS est activé et qu'il n'y a pas de certificats disponibles, vous pouvez générer manuellement les certificats sur un système Linux en suivant la procédure ci-dessous.

A. Hôte Docker :

Sur un système hôte Docker, générez des clés privées et publiques d'une autorité de certification en suivant les étapes de la procédure ci-dessous. Notez que l'exemple de clé ci-dessous est fourni à titre d'exemple ; il vous revient d'effectuer la procédure conformément à vos règles de sécurité.

1. Connectez-vous au système hôte Docker à l'aide d'un compte doté de droit 'root' ou de tout autre droit superutilisateur.
2. Créez un répertoire local à l'aide des commandes suivantes :

   mkdir docker_certificates

   cd docker_certificates
3. Exécutez la commande suivante :

   a. *openssl genrsa -aes256 -out ca-key.pem 4096*
   - 1. Entrez une phrase passe pour générer le fichier ca-key.pem et stockez-le en lieu sûr.

   b. *openssl req -new -x509 -days 365 -key ca-key.pem -sha256 -out ca.pem*
   - 1. Entrez le mot de passe indiqué à l'étape (3.a.1).
   - 2. Entrez les valeurs demandées.
   - 3. Entrez l'hôte Docker 'domain.com' dans Nom de domaine complet.
4. A l'aide d'une autorité de certification, créez une clé de serveur et une demande de signature de certificat (CSR) en exécutant les commandes suivantes :

   a. *openssl genrsa -out server-key.pem 4096*

   b. *openssl req -subj '/CN=$HOST' -sha256 -new -key server-key.pem -out server.csr*
   - 1. Où $HOST est le nom d'hôte de l'hôte Docker.
5. Des connexions TLS peuvent être créées à l'aide de l'adresse IP ou du nom DNS. Les adresses IP doivent être indiquées lors de la création du certificat à l'aide de la commande suivante :

   a. *echo subjectAltName = DNS:$HOST,IP:<DockerHost-IP> > extfile.cnf*

- 1. Où $HOST est le nom d'hôte de l'hôte Docker.

a. *echo extendedKeyUsage = serverAuth >> extfile.cnf*

6. Générez maintenant la clé à l'aide de la commande suivante :

   a. *openssl x509 -req -days 365 -sha256 -in server.csr -CA ca.pem -CAkey ca-key.pem *

   -CAcreateserial -out server-cert.pem -extfile extfile.cnf

   - 1. Entrez le mot de passe indiqué à l'étape (3.a.1).

7. Supprimez les fichiers inutiles et définissez correctement les droits :

   rm -v server.csr

   chmod -v 0400 ca-key.pem server-key.pem

   chmod -v 0444 ca.pem server-cert.pem

8. Démarrez le démon Docker en effectuant une vérification de TLS :

   a. *dockerd --tlsverify --tlscacert=ca.pem --tlscert=server-cert.pem --tlskey=server-key.pem -H=0.0.0.0:2376*

   Remarque : Si le support TLS est activé pour plusieurs hôtes Docker, suivez les étapes 1-3 UNE SEULE fois et suivez les étapes 4-8 séparément pour chaque hôte afin de générer les certificats TLS nécessaires à l'hôte.

B. Système TADDM :

Vous pouvez générer manuellement les certificats client TLS du système TADDM (correspondant à ceux générés pour l'hôte Docker). Sur le système hôte TADDM, générez des clés privées et publiques de l'autorité de certification en suivant les étapes de la procédure ci-dessous :

1. Connectez-vous au système TADDM à l'aide de données d'identification utilisateur 'root'.
2. Créez un répertoire local à l'aide des commandes suivantes :

   a. *mkdir taddm_certificates*

   b. *cd taddm_certificates*

3. A l'aide de l'autorité de certification, créez une clé de serveur et une demande de signature de certificat (CSR) en exécutant les commandes suivantes :

   a. *openssl genrsa -out key.pem 4096*

   b. *openssl req -subj '/CN=client' -new -key key.pem -out client.csr*

   c. *echo extendedKeyUsage = clientAuth >> extfile.cnf*

4. Signez la clé privée en exécutant la commande suivante :

   a. *openssl x509 -req -days 365 -sha256 -in client.csr -CA ca.pem -CAkey ca-key.pem -CAcreateserial -out cert.pem -extfile extfile.cnf*

   - 1. Fournissez les fichiers ca.pem et ca-key.pem générés à la section A, étape (3.a, 3.b)
   - 2. Entrez le mot de passe indiqué à la section A, étape (3.a.1)

5. Supprimez les fichiers inutiles et définissez correctement les droits :

   a. *rm -v client.csr*

   b. *chmod -v 0400 ca-key.pem key.pem*

   c. *chmod -v 0444 ca.pem cert.pem*

   d. *cd ../*

   e. *chown -R taddmusr:taddmusr taddm_certificates*

   f. *chown -R taddmusr:taddmusr taddm_certificates*

6. Validez la connexion TLS avec le système hôte Docker à l'aide des commandes suivantes :

```
curl https://<Dockerhost-IP>:<Docker-Port>/_ping --cert ./cert.pem
--key key.pem --cacert ca.pem
e.g. curl https://<Dockerhost-IP>:<2376>/_ping --cert ./cert.pem
--key key.pem --cacert ca.pem
```

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes courants qui peuvent se produire avec le détecteur d'hôte Docker et propose des solutions à ces problèmes.

Le détecteur échoue en générant le message ` CTJTD1585E Erreur – L'hôte Docker est inaccessible sur les ports suivants :`

Problème : L'API Web distante n'est peut-être pas activée sur l'hôte Docker.

SolutionVérifiez les données à l'aide de la commande *'ps - eaf | grep dockerd'* pour déterminer quel port est utilisé par le processus démon 'dockerd'. La sortie doit se présenter de la manière suivante :

```
/usr/bin/dockerd -H tcp://9.158.143.51:2376 -H unix:///var/run/docker.sock
```

Pour activer le support d'API distante, voir la rubrique relative à l'activation du support REST sur l'hôte Docker.

Le détecteur échoue en générant le message `CTJTD1587E/ CTJTD1590E Erreur – Non-concordance de la configuration TLS entre le détecteur d'hôte Docker et le noeud distant :'

Problème : Ce problème se produit en raison de la non-concordance de la configuration du détecteur d'hôte Docker et du noeud distant de l'hôte Docker. TLS est peut-être activé sur l'un et désactivé sur l'autre.

Solution : Vérifiez et configurez correctement la propriété *enableTLS* pour le détecteur d'hôte Docker.

Le détecteur échoue en générant le message CTJTD1589E Erreur – Problème avec le répertoire Pathstore TLS

Problème : Le répertoire pathstore défini dans la configuration du détecteur d'hôte Docker n'est pas valide ou ne dispose pas des droits appropriés.

Solution : Vérifiez que le répertoire pathstore configuré existe sur le serveur de reconnaissance TADDM. Si le répertoire existe, vérifiez qu'il dispose des droits appropriés.

```
drwxr-xr-x.  2 taddmusr taddmusr 4096 Nov 24 08:28 taddm_certificates
```

Le détecteur échoue en générant la description ` Echec : Code d'erreur HTTP : 503`

Problème : Si TADDM ne parvient pas à se connecter via REST au démon ou à l'application Docker sur le noeud cible, le détecteur peut échouer en générant un message d'erreur.

Solution : Si le processus ou l'application *dockerd* est en cours d'exécution, vérifiez le port spécifique où le processus/démon écoute en exécutant la commande *ps -Aef | grep dockerd*. Le port indiqué dans la sortie doit correspondre à celui auquel TADDM tente de se connecter.

Le détecteur échoue en générant le message `CTJTD3520E Error – A storage error has occurred. Server id:`

Problème : S'il y a des dépendances manquantes de fichiers JAR Java pour la conversion de jeu de caractères, le détecteur peut échouer en générant le message d'erreur lié au stockage ci-dessus.

Solution : Recherchez les fichiers JAR Java manquants et placez les fichiers correspondants dans le répertoire suivant :
/opt/IBM/taddm/dist/lib/jdbc

Réexécutez la procédure de reconnaissance.

Détecteur de cluster Docker Swarm

Fix Pack 4

Détecteur de cluster Docker Swarm

Le détecteur de cluster Docker Swarm reconnaît les informations relatives aux attributs Docker Swarm, ainsi qu'aux noeuds, au réseau et aux services Swarm.

Nom du détecteur utilisé dans l'interface graphique et les journaux

DockerSwarmClusterSensor

Eléments reconnus par le détecteur

Le détecteur reconnaît les éléments suivants :

- Docker Swarm
- Noeuds Docker (appelés Hôte Docker)
- Services Docker
- Réseau Docker

Dans la console de gestion de la reconnaissance et le portail de gestion des données, un cluster Docker Swarm est représenté par une icône en forme de baleine Docker bleue.

Le détecteur de cluster Docker Swarm utilise des API REST pour extraire les informations de reconnaissance du noeud ‘Responsable’ de l'hôte Docker qui exécute le processus démon ou l'application 'dockerd' dans le rôle 'Responsable'. Les données extraites se composent principalement des données d'attribut nécessaires pour établir une correspondance avec des règles de dénomination et créer des objets de modèle valides.

Prérequis

- Le démon ou l'application Docker est en cours d'exécution sur le système Linux cible.
- Pour permettre la reconnaissance de Docker Swarm, le support REST doit être activé sur l'hôte Docker cible.
- Pour déclencher le détecteur de cluster Docker Swarm, au moins UN hôte Docker associé au rôle 'Responsable' doit être inclus dans la portée de reconnaissance.

- Un hôte Docker ne peut appartenir qu'à un SEUL cluster Swarm ; il ne peut pas faire partie de plusieurs clusters Docker Swarm à fois.
- Le détecteur de cluster Docker Swarm dépend de la reconnaissance effectuée par le détecteur d'hôte Docker. La configuration du détecteur de cluster Docker Swarm est implicitement dérivée du détecteur d'hôte Docker. Pour plus de détails, voir la rubrique décrivant l'hôte Docker.
- Un ensemble unique de certificats TLS est applicable à tous les hôtes Docker pour les communications TADDM.
- L'activation ou la désactivation de TLS pour la reconnaissance entraîne un comportement uniforme sur TOUS les hôtes Docker définis dans la portée

  o Est applicable à TOUS les hôtes ou n'est applicable à AUCUN des hôtes Docker.

Problèmes de sécurité

- Aucune entrée de liste d'accès spécifique n'est requise. Pour plus d'informations sur la sécurité TLS, reportez-vous à la rubrique 'Connexion à Docker Swarm' ci-dessous :

Connexion à Docker Swarm

Le détecteur de cluster Docker Swarm reconnaît les données de l'hôte Docker (doté du rôle 'Responsable') via deux modes : le mode non TLS et le mode TLS.

Mode non TLS

Le mode non TLS est le mode par défaut. Il extrait les données via des services Web et ne requiert pas d'authentification. Ce mode est recommandé dans les déploiements de réseau privé ou de cloud privé sur les sites des clients.

Mode TLS

Le mode TLS est un mode sécurisé de communication avec l'hôte Docker. Il vérifie les certificats TLS installés dans TADDM et l'hôte Docker cible. Pour utiliser ce mode, vous devez affecter la valeur true à la propriété enableTLS et configurer les chemins des certificats définis dans le profil de reconnaissance. Pour plus de détails, voir 'Détecteur d'hôte Docker : Configuration du profil de reconnaissance'. Pour générer manuellement les certificats TLS pour TADDM et l'hôte Docker, voir «Détecteur d'hôte Docker», à la page 28 'Configuration du profil de reconnaissance'. Pour générer manuellement les certificats TLS de TADDM et l'hôte Docker, voir «Détecteur d'hôte Docker», à la page 28'Génération manuelle de certificats TLS'.

Objets de modèle avec attributs associés

Le détecteur de cluster Swarm Docker crée des objets de modèle avec les attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les ressources Docker Swarm dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont affichés sous le nom de l'objet de modèle.

app.docker.dockerswarm.DockerSwarm

- app.docker.dockerswarm.DockerSwarm
- Servers

- SwarmServices
- IP
- Port
- DockerNetwork

app.docker.dockerswarm.SwarmService
- Name
- DockerSwarm

app.docker.dockerhost.DockerContainer
- Task
- SwarmService

app.docker.dockerhost.DockerNetwork
- Name
- SubnetAddress
- DockerHost
- DockerContainer

Remarque : Tous les objets de modèle du détecteur d'hôte Docker sont également applicables ici car Docker Swarm est un cluster de noeuds hôte Docker.

Configuration du détecteur

Avant d'utiliser le détecteur de cluster Docker Swarm, vous devez le configurer.

Configuration du profil de reconnaissance :

Le détecteur de cluster Docker Swarm dépend de la reconnaissance effectuée par le détecteur d'hôte Docker. La configuration du détecteur de cluster Docker Swarm est implicitement dérivée du détecteur d'hôte Docker. Pour plus d'informations, voir la rubrique «Détecteur d'hôte Docker», à la page 28 : 'Configuration du profil du détecteur'.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit les problèmes courants qui peuvent se produire avec le détecteur de cluster Docker Swarm et propose des solutions à ces problèmes.

Le détecteur de cluster Docker Swarm n'est pas appelé sur un noeud hôte Docker

Problème : Le détecteur de cluster Docker Swarm ne peut pas être appelé sur un noeud hôte Docker si ce noeud ne dispose pas du rôle 'Responsable' pour ce cluster.

Solution : Vérifiez dans le fichier journal (DiscoverManager.log) que les traces suivantes ont été consignées :

"Either swarm mode is not enabled, or, the Docker host is not currently having manager role".

Pour déclencher le détecteur de cluster Docker Swarm, au moins UN hôte Docker associé au rôle 'Responsable' doit être inclus dans la portée de reconnaissance.

Détecteur DNS

Le détecteur DNS reconnaît les serveurs de système d'adressage par domaines (DNS).

Nom du détecteur utilisé dans l'interface graphique et les journaux

DnsSensor

Objets de modèle créés

Le détecteur crée l'objet de modèle suivant :

- Sys.DNSSAP

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur DNS et propose des solutions à ces problèmes.

Le détecteur ne parvient pas à reconnaître un serveur DNS.

Problème

Le détecteur ne parvient pas à reconnaître un serveur DNS en cours d'exécution.

Solution

Si le détecteur ne parvient pas à reconnaître un serveur DNS, vérifiez que le serveur DNS peut résoudre l'adresse IP 127.0.0.1. Le détecteur DNS requiert le serveur DNS pour résoudre 127.0.0.1 et, si le serveur DNS ne renvoie pas de valeur, le détecteur ne parvient pas à reconnaître le serveur DNS particulier.

Détecteur HIS

Le détecteur HIS reconnaît un serveur Microsoft Host Integration Server.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HISServerSensor

Prérequis

Avant d'exécuter ce détecteur, veillez à ce que les conditions prérequises suivantes soient satisfaites :

- La reconnaissance du système informatique Windows doit être effectuée correctement.
- Le service SNABase doit être en cours d'exécution.
- Grâce au fournisseur TADDM Windows Management Instrumentation (WMI), l'accès en lecture WMI à l'espace de nom `root/microsoftHis` doit être accordé. Si la reconnaissance du système informatique Windows s'est effectuée correctement, cet accès en lecture WMI est accordé par défaut. L'accès de niveau administratif est préférable.

Objets de modèle avec attributs associés

Le détecteur HIS crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources Microsoft Host Integration Server de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

app.his.HISDomain

- APPCModes
- AuditLevel
- BroadcastMeanTime
- BroadcastProtocolIpxSpx
- BroadcastProtocolNamedPipes
- BroadcastProtocolTcpIp
- ClientBackupDomainNames
- ClientBackupSponsorNames
- ClientDomainBackupType
- ConfigServer
- DisplayName
- DisplayVerbConnection
- DomainName
- EventLogServerName
- NetViewConnection
- PopupServerName
- RTMEndOfSession
- RTMOverflow
- RTMThreshold
- RTMTimerUntil
- Security3270
- SecurityAPPC
- SecurityLUA
- Servers
- Status

app.his.HostIntegrationServer

- DisplayName
- Domain
- LinkServices
- Name
- ProductName
- ProductVersion
- ServerRole
- Services
- TransportString
- VendorName

app.his.IPDLCService

- BackupNetworkNameServers
- CMDMaxRetry
- CPName
- DeviceDriver
- DisplayName
- DllName
- IsRemotable
- LENNode
- LocalAddressAdapter
- LocalAddressIP
- MaxActivationAttempts
- MaxBTUReceive
- MaxBTUSend
- Name
- Network
- NodeID
- Parent
- PrimaryNetworkNameServer
- ReceiveAckTimeout
- ResolvedIP
- UseDynamicPUDefinition

app.his.APPCMode

- AllowLZandRLE
- AutoActivate
- DisplayName
- EndPointOnly
- IsPriority
- MaxReceiveCompression
- MaxSendCompression
- MinimumContentionWinnerLimit
- Name
- Parent
- PartnerMinimumContentionWinnerLimit
- ReceivePacing
- ReceiveRuSize
- SessionLimit
- TransmitPacing
- TransmitRuSize

app.his.HISConnection

- Activation
- AllowIncoming
- BlockId
- CompressionLevel
- DisplayName

- DynamicLuDef
- LUs
- LinkService
- Name
- NodeId
- Parent
- PartnerConnectionName
- PeerRole
- RemoteBlockId
- RemoteControlPoint
- RemoteEnd
- RemoteNetName
- RemoteNodeId
- RetryDelay
- RetryLimit
- XIDFormat

app.his.HISLUA

- Compression
- DisplayName
- HighPriorityMode
- Name
- Number
- Parent
- Protocol
- UserWksSecure

app.his.HISLUDisplay

- AssociatedLU
- Compression
- DisplayModel
- DisplayModelOverride
- DisplayName
- HISService
- Name
- Number
- Parent
- Protocol
- UserWksSecure

app.his.HISLUPrint

- AssociatedLU
- Compression
- HISService
- Name
- Number
- Parent

- Protocol
- UserWksSecure

app.his.PrintService

- Account
- ActivationRetryInterval
- ActivationRetryLimit
- AlwaysDoNL
- CanBePaused
- CanBeStopped
- DelayPrintStart
- Description
- DesktopInteract
- DisplayName
- DoAllFF
- ErrorControl
- ExitCode
- FlushFinalFF
- IgnoreCharsUnder3F
- Name
- NoEventLogOnSkippingTransparentSection
- NoSpaceAfterFF
- OperatingState
- Parent
- PathName
- Serveur
- ServiceName
- ServiceSpecificCode
- ServiceType
- SoftwareVersion
- StartMode
- Started
- UseFixedTabs
- UseProportionalFontChange

app.his.SNAService

- ControlPoint
- HISConnections
- Name
- NetworkName
- Parent
- Server

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Il n'existe aucune condition d'accès pour ce détecteur. Ce détecteur peut être exécuté à l'aide des droits d'accès du système informatique utilisés pour reconnaître le client.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur HIS et propose des solutions à ces problèmes.

Le service WMI échoue sur une cible durant la reconnaissance.

Problème

Le service Windows Management Instrumentation (WMI) échoue sur un système cible durant la reconnaissance.

Solution

Vérifiez que tous les correctifs associés à WMI, y compris le correctif KB933061, ont été appliqués sur le système cible. Si le problème persiste, exécutez les outils de diagnostic de Microsoft.

Détecteur IBM Cluster Systems Management

Le détecteur IBM Cluster Systems Management reconnaît les clusters IBM Cluster Systems Management (CSM) High Performance Computing (HPC).

Nom du détecteur utilisé dans l'interface graphique et les journaux

CSMServerSensor et CSMNodeSensor

Prérequis

GenericComputerSystemSensor, ainsi que les détecteurs prérequis, doivent être activés sur le profil de reconnaissance utilisé pour la reconnaissance du cluster CSM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.hpc.cm.ConfigurationManagementCluster
- sys.hpc.cm.ConfigurationManagementNode
- sys.hpc.cm.ConfigurationMangementNodeGroup
- sys.hpc.cm.ConfigurationManagementClusterConfigFile
- sys.hpc.CSMNode

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Pour configurer le détecteur CSMServerSensor, procédez comme suit :

1. Créez un profil de reconnaissance et sélectionnez une configuration de l'agent du type CSMServerAgentConfiguration.
2. Définissez les attributs requis suivants :

masterServerNames
Les adresses IP ou noms d'hôte des noeuds maîtres CSM. Cette propriété doit être définie pour démarrer le détecteur de serveur CSM.

3. Selon les besoins, définissez les paramètres suivants ou acceptez les valeurs par défaut.

lsNodeCommand
Commande permettant de déterminer les noeuds CSM. La valeur par défaut est **lsnode**.

nodeGrpCommand
Commande permettant de déterminer des noeuds CSM dans le groupe. La valeur par défaut est **nodegrp**.

nodeGrpCommandDelimiter
Délimiteur placé entre les noeuds dans la commande nodeGrpCommand. La valeur par défaut est ",".

CFMDirectoryLocation
Emplacement du répertoire principal de CFM. La valeur par défaut est `/cfmroot`.

CFMDiscoveryMode
Profondeur de la capture des fichiers et des scripts dans les répertoires de configuration de CSM. Les valeurs valides sont les suivantes :

- `0` : aucune information de fichier n'est capturée.
- `1` : seuls le nom de fichier et les informations relatives au fichier sont capturés.
- `2` : l'intégralité du contenu de fichier et toutes les informations relatives au fichier sont capturées.

La valeur par défaut est 1.

CFMDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire principal de CFM. La valeur par défaut est "*".

preRebootScriptsLocation
Emplacement des scripts exécutés avant la réinitialisation. La valeur par défaut est `/csminstall/csm/scripts/installprereboot/`.

preRebootScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire `/csminstall/csm/scripts/installprereboot/`.

La valeur par défaut est "*".

postRebootScriptsLocation
Emplacement des scripts exécutés avant la réinitialisation. La valeur par défaut est `/csminstall/csm/scripts/installpostreboot/`.

postRebootScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire `/csminstall/csm/scripts/installpostreboot/`.

La valeur par défaut est "*".

osUpgradePreRebootScriptsLocation
Emplacement des scripts exécutés après la mise à niveau du système d'exploitation, mais avant la réinitialisation. La valeur par défaut est `/csminstall/csm/scripts/osupgradeprerboot/`.

osUpgradePreRebootScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire/csminstall/csm/scripts/osupgradeprereboot/.

La valeur par défaut est "*".

osUpgradePostRebootScriptsLocation
Emplacement des scripts qui sont exécutés après la mise à niveau du système d'exploitation, et après la réinitialisation. La valeur par défaut est /csminstall/csm/scripts/osupgreadepostreboot/.

osUpgradePostRebootScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire/csminstall/csm/scripts/osupgradepostreboot/.

La valeur par défaut est "*".

disklessBootScriptsLocation
Emplacement des scripts d'amorçage pour les noeuds sans disque. La valeur par défaut est /csminstall/csm/scripts/disklessboot/.

disklessBootScriptsDiscoveryPattern
Mode de nom pour les fichiers situés sous le répertoire /csminstall/csm/scripts/disklessboot/.

La valeur par défaut est "*".

disklessPreBuildScriptsLocation
Emplacement des scripts de pré-génération exécutés pour les noeuds sans disque.

La valeur par défaut est /csminstall/csm/scripts/disklessprebuild/.

disklessPreBuildScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire /csminstall/csm/scripts/disklessprebuild/.

La valeur par défaut est "*".

dataScriptsLocation
Emplacement des scripts ou des fichiers de données supplémentaires référencés par les scripts.

La valeur par défaut est /csminstall/csm/scripts/data/.

dataScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire /csminstall/csm/scripts/data/.

La valeur par défaut est "*".

updateScriptsLocation
Emplacement des scripts exécutés après l'exécution de toutes les mises à jour de CSM.

La valeur par défaut est /csminstall/csm/scripts/update/.

updateScriptsDiscoveryPattern
Modèle de nom pour les fichiers situés sous le répertoire /csminstall/csm/scripts/update/.

La valeur par défaut est "*".

nodesScope
Etendue des adresses IP auxquelles les détecteurs de noeud CSM sont limités.

doPingNodes
Indique si les détecteurs de ping sont exécutés sur les noeuds CSM reconnus.

Il n'existe aucune exigence de configuration de détecteur spécifique associée à CSMNodeSensor.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Le détecteur CSMServerSensor utilise l'entrée d'accès CSM Server. Si cette entrée d'accès n'est pas accessible, le détecteur utilise l'entrée d'accès ComputerSystem pour accéder au serveur CSM.

Le détecteur CSMNodeSensor utilise l'entrée d'accès ComputerSystem aux noeuds d'accès CSM.

Détecteur IBM High-Availability Cluster Multi-Processing

Le détecteur IBM High-Availability Cluster Multi-Processing (HACMP) reconnaît les clusters et composants associés HACMP. Le détecteur reconnaît les informations relatives au cluster, aux noeuds, aux groupes de ressources, aux groupes de ressources locales, aux ressources d'application, aux gestionnaire de clusters, au libellé IP de service, au système de fichiers partagé, aux adresses réseau des noeuds et aux informations du site.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HACMPSensor

Prérequis

Le service HACMP et le démon gestionnaire de clusters doit être en cours d'exécution sur les ordinateurs cible.

Problèmes de sécurité

Les privilèges d'exécution des commandes suivantes sur les systèmes reconnus sont requis :**lssrc, clstat, cltopinfo,clRGinfo, cllsserv, cllsif, cllsfs, clshowres, cllsgrp, get_local_nodename, cllssite**.

Limitations

Les limitations suivantes s'appliquent :

- TADDM prend en charge uniquement les serveurs Apache qui s'exécutent sur le cluster HACMP.
- Un seul serveur d'applications peut être exécuté sur le groupe de ressources HACMP.
- En cas d'échec de la commande **clstat**, qui est utilisée par TADDM pour contrôler l'état du cluster HACMP, le détecteur exécute la commande **odmget**. La portée des données reconnues par la commande **odmget** est toutefois limitée, car elle n'inclut pas les attributs state et substate de l'objet du cluster HACMP.

Objets de modèle avec attributs associés

Le détecteur IBM HACMP crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les éléments de configuration dans l'environnement IBM HACMP.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet modèle.

HACMPAppResource

- AppServer
- LocalAppResources
- Name
- Parent

HACMPCluster

- ClusterID
- ComputerSystems
- ConnAuthMode
- HeartbeatNetworks
- MessageAuthMode
- MessageEncryption
- Nodes
- ResourceGroups
- State
- Substate
- UsePersistentLabel

HACMPClusterHeartbeatNetwork

- Name
- Netmask
- NetworkElements
- Parent
- PrefixLength
- Type

HACMPClusterHeartbeatNetworkElement

- L2Interface
- Name
- NetworkAddress
- Parent
- StorageVolume
- Type

HACMPClusterManager

- CurrentState
- HacmpNode

HACMPLocalAppResource

- Node
- Parent
- StartScript

- StopScript

HACMPLocalResourceGroup

- LocalState
- Node
- Parent

HACMPNode

- ClusterManager
- LocalAppResources
- LocalResourceGroups
- Name
- NetworkElements
- Parent
- SiteInfo
- State
- Système

HACMPResourceGroup

- AppResources
- FallbackPolicy
- FalloverPolicy
- FileSystems
- GlobalState
- LocalResourceGroups
- Nodes
- Parent
- PrimaryNode
- ServiceIpLabels
- SitePolicy
- StartupPolicy
- StorageVolumes

ServiceIPLabel

- IpAddress
- Name
- Parent

SiteInfo

- Name

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès dont vous avez besoin.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.

2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour l'authentification auprès du système informatique cible.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur IBM HACMP.

Le détecteur utilise l'entrée suivante du fichier `collation.properties` :

com.collation.platform.os.UnixOs.forcedServerList=clstrmgr
Vous devez ajouter l'attribut `clstrmgr` à cette entrée pour garantir le démarrage du détecteur. Par exemple,

```
com.collation.platform.os.UnixOs.forcedServerList=vxconfigd;clstrmgr
```

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM HACMP et propose des solutions à ces problèmes.

Cluster HACMP en double

Problème
Un cluster HACMP en double risque d'être créé dans les cas suivants :

1. Un cluster HACMP est reconnu.
2. Le nom du cluster HACMP est modifié dans la configuration du cluster.
3. Le cluster HACMP est reconnu de nouveau.

Solution
Pour résoudre une situation où un cluster HACMP a été dupliqué, à l'aide du portail de gestion de données, copiez le cluster qui possède le nom de l'ancien cluster.

Version HACMP incorrecte renvoyée

Problème
Lors de la reconnaissance d'un cluster HACMP à l'aide du détecteur IBM HACMP, la version de produit du cluster HACMP peut être reconnue à tord comme étant "0".

Solution
En raison d'un problème dans HACMP, la version incorrecte du cluster est parfois renvoyée.

Pour vérifier manuellement la version du cluster, exécutez la commande suivante sur l'un des noeuds du cluster HACMP :

```
ssrc -ls clstrmgrES
```

Dans les résultats de la commande, vérifiez la version du cluster HACMP. Par exemple :

```
local node vrmf is 0
```

Si la version correcte du cluster s'affiche, reconnaissez de nouveau HACMP.

Les commandes clstat et cldump ne fonctionnent pas sur des noeuds directement installés sous AIX 6.1

Problème

Lorsqu'un cluster HACMP est installé sur des noeuds qui sont directement installés sous AIX 6.1, les commandes **clstat** et **cldump** ne fonctionnent pas.

Solution

Téléchargez le correctif pour ce problème à l'adresse suivante : http://www-01.ibm.com/support/docview.wss?uid=isg1IZ45540.

Détecteur de serveur IBM Lotus Domino

Le détecteur de serveur IBM Lotus Domino reconnaît les serveurs Lotus Domino.

Nom du détecteur utilisé dans l'interface graphique et les journaux

DominoDomainSensor, DominoServerDetailSensor et DominoInitialSensor

Prérequis

Sous le système Lotus Domino, un compte utilisateur doit être configuré avec un accès approprié aux ressources en cours de reconnaissance. Vérifiez que les conditions suivantes sont remplies :

- Le serveur IIOP (Internet Inter-ORB Protocol) doit être exécuté sur au moins un serveur Domino pour chacun des domaines Domino.
- Ajoutez l'adresse IP ou le nom de domaine complet (FQDN) des serveurs IIOP au fichier `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.lotus.dominoserverinitial_7.5.0/plugin.xml`. Vous pouvez ajouter au nom du serveur le numéro de port du serveur Domino IIOP. L'ajout du numéro de port est facultatif. D'une manière générale, le numéro de port par défaut est 63148 pour DIIOP (Domino Internet Inter-ORB Protocol). Si un accès anonyme est requis, le numéro de port est 80 pour HTTP.

  L'exemple suivant illustre comment ajouter un nom de serveur IIOP :

```
<IIOPServers>
    <item>
        <name>example1-server.ibm.com[:Port_number]</name>
        <SSL>false</SSL>
    </item>
    <item>
        <name>example2-server.ibm.com[:Port_number]</name>
        <SSL>false</SSL>
    </item>
</IIOPServers>
```

- Pour chaque serveur IIOP, vous devez avoir un ID utilisateur et un mot de passe valides.
- L'ID utilisateur sur le serveur IIOP doit disposer des droits de lecture sur le fichier `names.nsf`.
- Vous devez indiquer une portée de reconnaissance contenant tous les noeuds de serveur afin d'obtenir des informations complètes sur les clusters Domino.
- Vérifiez le document serveur dans le répertoire Domino, en vous assurant que l'ID utilisateur dispose d'un accès activé aux paramètres de sécurité :
  - Accès au serveur
  - Exécution d'agents LotusScript/Java restreints

Sous le système Lotus Domino, un compte utilisateur doit être configuré avec l'accès approprié aux ressources en cours de reconnaissance, comme des fichiers et des bases de données.

- Pour permettre à TADDM de se connecter à un serveur Domino IIOP à l'aide de SSL, vous devez définir le fichier `osgi/plugins/com.ibm.cdb.discover.sensor.app.lotus.dominoserverinitial_7.5.0/plugin.xml` à true. Puis, vous devez copier le fichier `TrustedCerts.class` dans le répertoire `$COLLATION_HOME/etc/domino_trusted` du serveur TADDM. Le fichier `TrustedCerts.class` est situé dans le dossier `dossier de données domino/domino/java`.
- Lancer la commande **`show task`** dans la console Domino pour déterminer si la tâche DIIOP est en cours d'exécution.
- Si la tâche DIIOP n'est pas exécutée, lancez la commande **`load diiop`** à l'aide de la console Domino pour charger la tâche DIIOP.
- Lancez la commande **`tell diiop show config`** pour vérifier la configuration.

Si vous mettez à jour le fichier `plugin.xml`, vous devez redémarrer le serveur TADDM pour que les modifications prennent effet.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.lotus.AgentManager
- app.lotus.AdminProcess
- app.lotus.DirectoryAssistance
- app.lotus.DirectoryCataloger
- app.lotus.DomainCatalog
- app.lotus.DominoCluster
- app.lotus.DominoConnection
- app.lotus.DominoDatabase
- app.lotus.DominoDomain
- app.lotus.DominoNamingContext
- app.lotus.DominoReplicas
- app.lotus.DominoSecurity
- app.lotus.DominoServer
- app.lotus.DominoTransactionLogging
- app.lotus.HTTPFilterSpecialtyServer
- app.lotus.IIOPConfig
- app.lotus.IMAPConfig
- app.lotus.InternetClusterManager
- app.lotus.LDAPConfig
- app.lotus.OtherDatabase
- app.lotus.POPConfig
- app.lotus.RemoteDebugManager
- app.lotus.SMTPConfig
- app.lotus.SpecialityServer
- app.lotus.WebConfig
- app.lotus.WebRetriever

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de serveur IBM Lotus Domino prend en charge les reconnaissances asynchrones et basées sur un script. En outre, dans une reconnaissance non basée sur un script, le détecteur de serveur Lotus Domino n'est pas pris en charge par le système d'exploitation Solaris ; il l'est en revanche dans une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, l'entrée de liste d'accès du système informatique est utilisée pour lire le fichier de configuration de Lotus Domino. Une entrée de liste d'accès d'applications pour le serveur Lotus Domino n'est pas nécessaire.

Limitations

La plupart des fonctions fournies par le détecteur de serveur Lotus Domino lors d'une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

Dans une reconnaissance asynchrone ou basée sur un script, seul l'attribut Version est pris en charge.

La reconnaissance de descripteur d'application n'est pas pris en charge.

Configuration de la liste d'accès

Pour donner l'accès au détecteur de serveur IBM Lotus Domino au serveur Lotus Domino, vous devez configurer la liste d'accès.

Pour configurer la liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, créez un ensemble de portée de reconnaissance qui contient l'adresse IP du serveur Lotus Domino.
2. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.
4. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **Serveurs de messagerie**.
5. Dans la zone **Fournisseur** de la fenêtre Caractéristiques de l'accès, cliquez sur **Domino**.
6. Entrez les droits d'accès au serveur Lotus Domino cible.

Vous devez aussi posséder une liste d'accès et des données d'identification pour les systèmes Windows. Le détecteur de session crée une session entre le serveur

TADDM et les systèmes informatiques cible avant l'exécution de la reconnaissance du détecteur de serveur IBM Lotus Domino.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur IBM Lotus Domino et propose des solutions à ces problèmes.

Le détecteur ne démarre pas

Problème

Si DIIOP (Domino Internet Inter-ORB Protocol) n'est pas actuellement exécuté ou si le fichier `plugin.xml` n'est pas correctement configuré, le détecteur ne démarre pas ou échoue.

Solution

- Vérifiez que le fichier `$COLLATION_HOME/OSGi/plugins/com.ibm.cdb.discover.sensor.app.lotus.dominoserverinitial_7.5.0/plugin.xml` est correctement configuré. Si vous mettez à jour le fichier `plugin.xml`, vous devez redémarrer le serveur TADDM pour que les modifications prennent effet.
- A l'aide de la console Domino, exécutez les commandes suivantes :
  - **`load diiop`**
  - **`show tasks`**

Le détecteur ne démarre pas, s'il n'est pas possible d'accéder au fichier notes.ini

Problème

Pour les systèmes d'exploitation AIX, si le fichier `notes.ini` est introuvable dans l'environnement de traitement, le détecteur ne démarre pas.

Solution

L'ID utilisateur exécutant la reconnaissance n'a pas accès à l'environnement du processus pour des raisons de sécurité. Vérifiez l'entrée suivante dans le fichier `collation.properties` :

```
com.collation.platform.os.command.psEnv.AIX
```

Si nécessaire, ajoutez la commande **`SUDO`** pour définir les droits d'accès au fichier.

Détecteur de portée IBM Tivoli Monitoring

En utilisant les données d'identification pour Tivoli Enterprise Portal Server au lieu de celles pour chaque ordinateur surveillé par le serveur de portail, le détecteur IBM Tivoli Monitoring Scope reconnaît les éléments de configuration dans l'environnement IBM Tivoli Monitoring.

Le détecteur de portée IBM Tivoli Monitoring offre la fonction de reconnaissance suivante :

- Fournit une reconnaissance de base des noeuds finaux Tivoli Monitoring, semblable à une reconnaissance TADDM standard de niveau 1. Le détecteur reconnaît les adresses IP, les adresses MAC et le type de système d'exploitation pour chaque système informatique géré par Tivoli Monitoring.
- Crée des ensembles de portées spéciaux pour tous les noeuds finaux Tivoli Monitoring qu'il reconnaît afin que toutes les reconnaissances TADDM postérieures de niveau 2 (et certaines de niveau 3) puissent être exécutées sans autorisations d'accès pour les noeuds finaux Tivoli Monitoring.

Voir aussi le *Guide d'administration* de TADDM pour des informations sur la configuration de la reconnaissance à l'aide d'IBM Tivoli Monitoring.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ITMScopeSensor et ITMScopeSensor-*x.xx.xxx.xxx*.log, où *x.xx.xxx.xxx* représente l'adresse IP du système reconnu.

Le détecteur IBM Tivoli Monitoring Scope journalise aussi des informations dans `local-anchor.`*`hostname`*`.ITMScopeSensor.log`, où *hostname* correspond au nom d'hôte du serveur TADDM.

Prérequis

Pour un système informatique surveillé à stocker dans la base de données TADDM, IBM Tivoli Monitoring doit fournir les adresses IP et MAC du système en réponse aux requêtes du détecteur.

Limitations

La reconnaissance à l'aide du détecteur de portée Tivoli Monitoring implique les impacts de performance suivants dans l'environnement Tivoli Monitoring :

- Augmentation de l'utilisation de l'unité centrale sur les serveurs Tivoli Enterprise Portal Server et Tivoli Enterprise Monitoring Server
- Augmentation de l'utilisation du réseau
- Si deux ou plusieurs serveurs TADDM exécutent simultanément une reconnaissance sur un serveur Tivoli Monitoring, la reconnaissance Tivoli Monitoring n'aboutit pas.

Ces incidences sur la performance sont observées pendant toute la durée de la reconnaissance et peuvent également concerner les fonctions Tivoli Monitoring, en fonction du matériel Tivoli Monitoring utilisé.

Le détecteur ne reconnaît pas les hôtes sur un réseau privé utilisant la conversion d'adresses réseau (NAT).

Objets de modèle avec attributs associés

Le détecteur de portée IBM Tivoli Monitoring crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les éléments de configuration dans l'environnement IBM Tivoli Monitoring.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

net.IpInterface

- IpAddress

Plusieurs systèmes informatiques, avec les objets de modèle suivants :

sys.aix.AixUnitaryComputerSystem
sys.hpux.HpUxUnitaryComputerSystem
sys.linux.LinuxUnitaryComputerSystem
sys.sun.Solaris
sys.sun.SunSPARCUnitaryComputerSystem

sys.UnitaryComputerSystem
sys.windows.WindowsComputerSystem
sys.zOS.ZSeriesComputerSystem

Les attributs suivants sont associés à ces objets de modèle :

- Fqdn
- Ipinterface
- Name
- OSInstalled
- OSRunning
- Signature
- Type

Plusieurs systèmes d'exploitation, avec les objets de modèle suivants :

sys.aix.Aix
sys.hpux.HpUx
sys.linux.Linux
sys.sun.Solaris
sys.zOS.Sysplex
sys.unix.Unix
sys.windows.WindowsOperatingSystem
sys.zOS.ZOS

Les attributs suivants sont associés à ces objets de modèle :

- Name
- ManagedSystemName
- OSVersion

Configuration du détecteur

Avant d'exécuter une reconnaissance de l'environnement IBM Tivoli Monitoring, vous devez configurer le détecteur de portée IBM Tivoli Monitoring.

Copie des fichiers nécessaires à partir du serveur Tivoli Enterprise Portal Server vers le serveur TADDM :

Vous devez copier certains fichiers à partir du serveur Tivoli Enterprise Portal Server vers le serveur TADDM.

Dans un déploiement de serveur de diffusion, procédez comme suit sur le serveur de reconnaissance si vous configurez le détecteur pour la première fois. Cette procédure est inutile si vous avez déjà copié les fichiers du serveur Tivoli Enterprise Portal Server sur le serveur TADDM dans la version 7.2.1.x et fait une mise à niveau à la version 7.2.2 groupe de correctifs 1 ou ultérieure.

1. Sur le serveur TADDM, vérifiez que le répertoire `$COLLATION_HOME/lib/itm` existe.
2. Copiez les fichiers suivants à partir du serveur Tivoli Enterprise Portal Server dans le répertoire `$COLLATION_HOME/lib/itm` sur le serveur TADDM :
   - `browser.jar`
   - `cnp.jar`
   - `cnp_vbjorball.jar`
   - `kjrall.jar`

- `util.jar`
- `tap_cli.jar`

  Sous les systèmes Windows, copiez les fichiers à partir du répertoire *ITM_INSTALLATION_DIR*\CNB\classes.

  Sous les systèmes Linux et UNIX, copiez les fichiers à partir du répertoire *ITM_INSTALLATION_DIR*/classes.

3.

   Remarque : Ignorez cette étape si vous effectuez une intégration avec ITM 6.3 ou ultérieure.
   Copiez le fichier `cfwk.zip` depuis le serveur Tivoli Enterprise Portal dans le répertoire `$COLLATION_HOME/lib/itm` du serveur TADDM.

   Sur les systèmes Windows, copiez le fichier à partir du répertoire *ITM_INSTALLATION_DIR*\GSK7\classes.

   Sur les systèmes Linux et UNIX, copiez le fichier à partir du répertoire *ITM_INSTALLATION_DIR*/ARCH/gs/classes.

4. Sur les systèmes Linux et UNIX, utilisez les commandes suivantes pour définir l'utilisateur et le groupe des fichiers précédemment copiés sur l'utilisateur et le groupe utilisés pour exécuter le serveur TADDM :

   ```
   chown -R taddmuser:taddmuser $COLLATION_HOME/lib/itm
   ```

5. Redémarrez le serveur TADDM.

Distribution de l'ensemble de support cible de la reconnaissance :

Durant le processus de reconnaissance, TADDM doit copier des données de fichier binaire entre lui-même et la cible de reconnaissance par l'intermédiaire d'IBM Tivoli Monitoring. Pour des cibles de reconnaissance Windows, le support de cible de reconnaissance permet de copier des fichiers binaires depuis TADDM vers la cible de reconnaissance dans le cadre du processus de reconnaissance. L'ensemble de support de cible de reconnaissance fournit également une partie de la passerelle Windows sur la cible, la passerelle est par conséquent disponible durant la reconnaissance. Grâce à cette méthode, il n'est pas nécessaire de déployer une passerelle de reconnaissance Windows distincte dans votre environnement Tivoli Monitoring. L'ensemble de support de cible de reconnaissance n'est pas nécessaire sur les systèmes d'exploitation Linux, AIX, Solaris et HP-UX.

Avant la première reconnaissance à partir de TADDM, l'ensemble de support de cible de reconnaissance doit être déployé sur chaque noeud final du système d'exploitation Tivoli Monitoring Windows. Cet ensemble présente un encombrement réduit. De plus, il est conçu pour être non intrusif et s'utilise uniquement durant une reconnaissance TADDM. Si vous effectuez une reconnaissance de niveau 1, cette tâche n'est pas obligatoire.

Vous devez distribuer l'ensemble de support sur les cibles de reconnaissance Windows par le biais du dépôt Tivoli Enterprise Monitoring Server. L'ensemble de support doit alors être chargé dans tous les dépôts Tivoli Enterprise Monitoring Server distants de votre environnement Tivoli Monitoring.

Non seulement vous devez déployer l'ensemble de support de cible de reconnaissance, vous devez vérifier que chaque noeud final Tivoli Monitoring est configuré pour la reconnaissance. Par exemple, le programme LiSt Open Files (lsof) doit être installé sur chaque noeud final UNIX. Pour plus d'informations, voir le *Guide d'administration* de TADDM.

Sur le DVD de TADDM, l'ensemble de support se trouve dans le fichier `KD7.zip` ou `KD7_621.zip`, à l'intérieur du répertoire `/itm-discovery-support`. En fonction de la version de Tivoli Enterprise Monitoring Server, distribuez l'ensemble de support approprié. Pour IBM Tivoli Monitoring version 6.2.1-TIV-ITM-FP0001 ou ultérieure, distribuez l'ensemble de support dans `KD7_621.zip`. Pour IBM Tivoli Monitoring Version 6.2.2-TIV-ITM-FP0002 ou une version ultérieure, distribuez l'ensemble de support dans le fichier `KD7.zip`.

Pour distribuer l'ensemble de support aux cibles de reconnaissance, procédez comme suit :

1. Extrayez le fichier d'ensemble de support approprié `KD7.zip` ou `KD7_621.zip` dans un répertoire sur Tivoli Enterprise Monitoring Server. Par exemple, dans le répertoire `C:\TEMP` sous Windows et `/tmp` sur un système Linux ou UNIX.
2. Pour ajouter l'ensemble de support au dépôt Tivoli Enterprise Monitoring Server, exécutez la commande **tacmd** comme illustré dans l'exemple suivant. Pour supprimer la confirmation, utilisez l'option `-f` suivante.

   Sous le système d'exploitation Windows :

   ```
   C:\IBM\ITM\bin>tacmd login -u sysadmin -p mypassword -s localhost

   Validating user...

   KUIC00007I: User sysadmin logged into server on https://localhost:3102.
   C:\IBM\ITM\bin>tacmd addBundles -i C:\TEMP\KD7\072200000

   KUICAB023I: Are you sure you want to add the following bundles
   to the C:\IBM\ITM\CMS\depot\ depot?

   Type         : Component
   Product Code : d7
   Deployable   : true
   Version      : 072200000
   Description  : TADDM Discovery through ITM enablement
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:

   KUICAB024I: Enter Y for yes or N for no: y

   KUICAB020I: Adding bundles to the C:\IBM\ITM\CMS\depot\ depot.
   The time required to complete this operation depends
   on the number and size of the added bundles.

   KUICAB022I: The following bundles were successfully added to the C:\IBM\ITM\CMS
   ```

   Sous le système d'exploitation Linux ou UNIX :

   ```
   [root@localhost bin]# /opt/IBM/ITM/bin/tacmd login -s localhost -u sysadmin -p "mypassword"

   Validating user...

   KUIC00007I: User sysadmin logged into server on https://localhost:3661.
   [root@localhost bin]# /opt/IBM/ITM/bin/tacmd addBundles -i /tmp/KD7/072200000/

   KUICAB023I: Are you sure you want to add the following bundles
   to the /opt/IBM/ITM/tables/TEMS/depot depot?

   Type         : Component
   Product Code : d7
   Deployable   : true
   Version      : 072200000
   Description  : TADDM Discovery through ITM enablement
   Host Type    : WINNT
   Host Version : WINNT
   Prerequisites:

   KUICAB024I: Enter Y for yes or N for no: y

   KUICAB020I: Adding bundles to the /opt/IBM/ITM/tables/TEMS/depot depot. The time required to complete this operation
   depends on the number and size of the added bundles.

   KUICAB022I: The following bundles were successfully added to the
   /opt/IBM/ITM/tables/TEMS/depot depot:
   ```

3. Pour obtenir les noms de systèmes gérés pour les systèmes d'exploitation Windows, utilisez le commande **tacmd listSystems-t NT** Commande. Pour plus d'informations sur la commande **tacmd listSystems -t NT**, voir les commandes CLI tacmd à l'adresse : http://www-01.ibm.com/support/knowledgecenter/SSTFXA_6.2.2.2/com.ibm.itm.doc_6.2.2fp2/tacmd.htm.

4. Pour distribuer l'ensemble de support à partir du serveur Tivoli Enterprise Monitoring Server aux cibles de reconnaissance, connectez-vous au serveur Tivoli Enterprise Monitoring Server, et exécutez la commande **tacmd** suivante, comme indiqué dans l'exemple ci-dessous :

   Sous le système d'exploitation Windows :

   ```
   C:\IBM\ITM\bin>tacmd login -u sysadmin -p mypassword -s localhost
   Validating user...
   KUIC00007I: User sysadmin logged into server on https://localhost:3102.
   C:\IBM\ITM\bin>tacmd addsystem -t d7 -n Primary:OMPDEV2:NT
   KUICAR010I: The agent type d7 is being deployed.
   KUICAR028I: The operation has been successfully queued for deployment, the transaction
   id is 12196916778130000018467, use the getDeployStatus CLI to view the status.
   ```

   Sous le système d'exploitation Linux ou UNIX :

   ```
   [root@localhost bin]# /opt/IBM/ITM/bin/tacmd login -s localhost -u sysadmin -p "mypassword"

   Validating user...

   KUIC00007I: User sysadmin logged into server on https://localhost:3661.
   [root@blueronin bin]# /opt/IBM/ITM/bin/tacmd addsystem -t d7 -n Primary:OMPDEV2:NT

   KUICAR010I: The agent type d7 is being deployed.

   KUICAR028I: The operation has been successfully queued for deployment,
   the transaction id is 125536065846146000035468707 4,
   use the getDeployStatus CLI to view the status.
   ```

5. Vérifiez le statut du déploiement en entrant la commande **tacmd getDeployStatus**. Par exemple :

   ```
   C:\IBM\ITM\bin>tacmd getdeploystatus -g 12196916778130000018467

    Transaction ID : 12196916778130000018467
    Command        : INSTALL
    Status         : SUCCESS
    Retries        : 0
    TEMS Name      : HUB_TEMS
    Target Hostname: Primary:OMPDEV2:NT
    Platform       : WINNT
    Product        : D7
    Version      : 072200000
    Error Message  : KDY0028I: Request completed successfully. Deployment
     request was processed successfully and is now completed.
   ```

Installation des requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server :

Pour une reconnaissance de niveau 1 et de niveau 2 par le biais d' IBM Tivoli Monitoring, vous devez installer des requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server pour la prise en charge la recherche des adresses MAC et versions d'agents des systèmes gérés par le détecteur de portée IBM Tivoli Monitoring.

Sur le DVD de TADDM, les requêtes personnalisées sont situées dans le fichier`TEPS_Query.zip` du répertoire `/itm-discovery-support`. Les requêtes personnalisées sont définies dans le fichier `install_zkd7.sql`.

Ces requêtes renvoient les informations suivantes :

- Numéro de version de l'agent sur chaque noeud final
- Adresse MAC de chaque noeud final Linux
- Nom et version du système d'exploitation de chaque noeud final

Pour installer des requêtes personnalisées sur le serveur Tivoli Enterprise Monitoring Server, procédez comme suit :

Installation sous le système d'exploitation Linux :

1. Connectez-vous au serveur Tivoli Enterprise Portal Server et copiez le fichier `TEPS_Query.zip` dans un répertoire local.

Dans ces instructions, le fichier TEPS_Query.zip est copié dans le répertoire /tmp/teps et extrait. Les fichiers install_zkd7.sql et uninstall_zkd7.sql sont ensuite localisés dans le répertoire /tmp/teps.

2. Installez les requêtes personnalisées :

```
/opt/IBM/ITM/bin/itmcmd execute cq
"/opt/IBM/ITM/li6263/cq/bin/KfwSQLClient -d KFW_DSN
–f /tmp/teps/install_zkd7.sql"
```

3. Arrêtez le serveur Tivoli Enterprise Portal Server :

```
/opt/IBM/ITM/bin/itmcmd agent stop cq
```

4. Démarrez le serveur Tivoli Enterprise Portal Server :

```
/opt/IBM/ITM/bin/itmcmd agent start cq
```

Installation sous un système d'exploitation Windows :

1. Connectez-vous au serveur Tivoli Enterprise Portal Server et copiez le fichier TEPS_Query.zip dans un répertoire local.

   Dans ces instructions, le fichier TEPS_Query.zip est copié dans le répertoire c:\TEMP\TEPS et extrait. Les fichiers install_zkd7.sql et uninstall_zkd7.sql sont ensuite localisés dans le répertoire c:\TEMP\TEPS.

2. Accédez au répertoire dans lequel le serveur Tivoli Enterprise Portal Server est installé :

```
cd c:\IBM\ITM\CNPS
```

3. Installez les requêtes personnalisées :

```
.\kfwsqlclient.exe /d KFW_DSN /f c:\TEMP\TEPS\install_zkd7.sql
```

4. A partir de la fenêtre Tivoli Monitoring Services, redémarrez le serveur Tivoli Enterprise Portal Server.

Configuration du profil de reconnaissance :

Par défaut, le détecteur de portée IBM Tivoli Monitoring n'est pas activé. Après que vous l'ayez activé, TADDM reconnaît les noeuds finaux Tivoli Monitoring et crée un ensemble de portées. L'ensemble de portées contient les noeuds finaux reconnus et utilise les ports 1920 et 15001 par défaut deTivoli Enterprise Portal Server. Toutefois, par défaut, les objets du système informatique ne sont pas créés pour les noeuds finaux de Tivoli Monitoring. Pour créer des objets de système informatique pour chaque noeud final reconnu ou pour utiliser des ports de Tivoli Enterprise Portal Server autres que les ports par défaut, créez un profil de reconnaissance de niveau 1 ou de niveau 2 pour le détecteur de portées IBM Tivoli Monitoring et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

1. Dans la console de gestion de reconnaissance, cliquez sur l'icône **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre de création de profil, entrez le nom et la description du profil. Dans la zone **Cloner le profil existant**, cliquez sur **Reconnaissance de niveau 1** ou **Reconnaissance de niveau 2**, et cliquez sur **OK**.
4. Dans la liste des détecteurs, cliquez sur **ITMScopeSensor**, puis cliquez sur **Nouveau**.
5. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration du détecteur ITMScopeSensor, puis sélectionnez la case à cocher **Activer la configuration**.

6. Dans la section **Configuration** de la fenêtre de création de la configuration, pour définir un ensemble de ports à rechercher pour le serveur Tivoli Enterprise Portal Server, cliquez sur **portList**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne et entrez la valeur numérique de chaque port, en séparant chaque valeur par une virgule.
7. Pour configurer le détecteur de sorte qu'il n'utilise pas le port 1920, cliquez sur **useDefaultPortList**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne, et entrez `false`.

   La valeur par défaut de **useDefaultPortList** est `true`. Si une liste de ports est fournies et **useDefaultPortList** est définie sur `true`, le port 1920 est ajouté à la liste de ports à rechercher pour le serveur Tivoli Enterprise Portal Server.
8. Pour créer des objets de système informatique qui s'affichent dans l'arborescence des composants reconnus durant une reconnaissance, cliquez sur **discoverITMEndpoints**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne et entrez `true`.

   Si vous ne souhaitez pas créer d'objets de système informatique durant une reconnaissance, n'entrez rien dans cette zone ou uniquement `false`.
9. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
10. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Reconnaissance des noeuds finaux derrière des pare-feux :

Le détecteur IBM Tivoli Monitoring Scope prend en charge les noeuds finaux Tivoli Monitoring qui se trouvent derrière un pare-feu.

Procédure

1. Exécutez une reconnaissance de niveau 1 de votre environnement ITM pour créer le fichier `itmserver.properties`.
2. Insérez le détecteur dans votre profil et définissez le paramètre startSessionOnly sur *true* dans les options de configuration.

Résultats

Le détecteur vérifie si l'adresse IP de la portée d'origine est gérée par ITM et exécute un détecteur de session. Le détecteur utilise la session ITM uniquement s'il est autorisé et prioritaire pour l'hôte.

Restriction : Le paramètre startSessionOnly est prioritaire par rapport à toutes les autres options de configuration. S'il est activé, le détecteur ne lance aucune autre opération.

Configuration de la liste d'accès :

Pour permettre l'accès du détecteur de portée IBM Tivoli Monitoring à l'application Tivoli Enterprise Portal Server, vous devez configurer la liste d'accès.

Pour configurer la liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, créez un ensemble de portées de reconnaissance contenant votre serveur Tivoli Enterprise Portal Server ou utilisez une portée existante contenant votre serveur Tivoli Enterprise Portal Server.
2. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.

4. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **Intégration**.
5. Dans la zone **Fournisseur** de la fenêtre Caractéristiques de l'accès, cliquez sur **IBM Tivoli Monitoring**.
6. Saisissez les autorisations d'accès pour le serveur Tivoli Enterprise Portal Server. Utilisez les autorisations d'accès requises pour la connexion au serveur Tivoli Enterprise Portal Server au lieu des autorisations d'accès de chaque ordinateur sur lequel réside le serveur Tivoli Enterprise Portal Server.

Désinstallation du détecteur

Pour désinstaller les composants de configuration du détecteur de portée IBM Tivoli Monitoring, vous devez exécuter plusieurs étapes.

Suppression des entrées de la liste d'accès :

Dans la console de gestion de reconnaissance, supprimez chaque entrée de liste d'accès IBM Tivoli Monitoring.

Pour supprimer une entrée de la liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, supprimez tous les ensembles de portées de reconnaissance qui contiennent votre serveur Tivoli Enterprise Portal Server.
2. Pour supprimer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, sélectionnez chaque liste d'accès IBM Tivoli Monitoring, et cliquez sur **Supprimer** pour chacune.

Suppression des profils de reconnaissance :

Dans la console de gestion de reconnaissance, supprimez chaque profil de reconnaissance IBM Tivoli Monitoring.

Pour supprimer un profil de reconnaissance, procédez comme suit :

1. Dans la console de gestion de reconnaissance, cliquez sur l'icône **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, sélectionnez chacun des profils de reconnaissance pour IBM Tivoli Monitoring, puis cliquez sur **Supprimer**.

Désinstallation des requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server :

Pour désinstaller la configuration du détecteur de portée IBM Tivoli Monitoring, vous devez désinstaller les requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server.

Les requêtes personnalisées peuvent être supprimées par l'exécution de la requête de désinstallation, `uninstall_zkd7.sql`. Sur le DVD de TADDM, cette requête est située dans le fichier `TEPS_Query.zip` du répertoire `/itm-discovery-support`.

Pour désinstaller les requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server, procédez comme suit :

Désinstallation sous le système d'exploitation Linux :

1. Connectez-vous au serveur Tivoli Enterprise Portal Server et copiez le fichier `TEPS_Query.zip` dans un répertoire local.

Dans ces instructions, le fichier TEPS_Query.zip est copié dans le répertoire /tmp/teps et extrait. Le fichier uninstall_zkd7.sql est ensuite placé dans le répertoire /tmp/teps.

2. Exécutez la requête de désinstallation :

```
/opt/IBM/ITM/bin/itmcmd execute cq
"/opt/IBM/ITM/li6263/cq/bin/KfwSQLClient -d KFW_DSN
–f /tmp/teps/uninstall_zkd7.sql"
```

3. Arrêtez le serveur Tivoli Enterprise Portal Server :

```
/opt/IBM/ITM/bin/itmcmd agent stop cq
```

4. Démarrez le serveur Tivoli Enterprise Portal Server :

```
/opt/IBM/ITM/bin/itmcmd agent start cq
```

Désinstallation sous le système d'exploitation Windows :

1. Connectez-vous au serveur Tivoli Enterprise Portal Server et copiez le fichier TEPS_Query.zip dans un répertoire local.

   Dans ces instructions, le fichier TEPS_Query.zip est copié dans le répertoire c:\TEMP\TEPS et extrait. Le fichier uninstall_zkd7.sql est ensuite placé dans le répertoire c:\TEMP\TEPS.

2. Accédez au répertoire dans lequel le serveur Tivoli Enterprise Portal Server est installé :

```
cd c:\IBM\ITM\CNPS
```

3. Exécutez la requête de désinstallation (prend en charge toutes les plateformes) :

```
.\kfwsqlclient.exe /d KFW_DSN /f c:\TEMP\TEPS\uninstall_zkd7.sql
```

4. A partir de la fenêtre Tivoli Monitoring Services, redémarrez le serveur Tivoli Enterprise Portal Server.

Suppression de l'ensemble de support de cible de reconnaissance :

Pour désinstaller la configuration du détecteur de portée IBM Tivoli Monitoring, vous devez supprimer l'ensemble de support de cible sur les dépôts Tivoli Enterprise Monitoring Server.

Sur le DVD de TADDM, l'ensemble de support est situé dans le fichier KD7.zip du répertoire /itm-discovery-support.

Pour supprimer l'ensemble de support du dépôt de l'agent, procédez comme suit :

1. Extrayez le fichier KD7.zip dans un répertoire du serveur Tivoli Enterprise Monitoring Server (par exemple, le répertoire C:\TEMP).
2. Pour supprimer l'ensemble de support des cibles de reconnaissance, connectez-vous au serveur Tivoli Enterprise Monitoring Server. Exécutez la commande **tacmd**,comme illustré dans l'exemple suivant. Indiquez le code produit (D7) à l'aide de l'option -t et le système géré dans lequel les ensembles doivent être supprimés à l'aide de l'option -n.

```
tacmd removesystem -t D7 -n Primary:Sirius:NT
```

3. Pour supprimer l'ensemble de support du dépôt Tivoli Enterprise Monitoring Server, exécutez la commande **tacmd**, comme indiqué dans l'exemple suivant. Utilisez l'option -i pour indiquer le chemin d'accès au répertoire contenant les ensembles installables.

```
tacmd removeBundles -i C:\TEMP\KD7\072200000
```

Suppression des fichiers Tivoli Enterprise Portal Server à partir du serveur TADDM :

Pour désinstaller la configuration du détecteur de portée IBM Tivoli Monitoring, vous devez supprimer les fichiers que ont été copiés du serveur Tivoli Enterprise Portal Server vers le serveur TADDM.

Pour supprimer les fichiers copiés à partir du serveur Tivoli Enterprise Portal Server, procédez comme suit :

1. Sur le serveur TADDM, supprimez le répertoire `$COLLATION_HOME/lib/itm`.
2. Redémarrez le serveur TADDM.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de portée IBM Tivoli Monitoring et propose des solutions à ces problèmes.

Systèmes informatiques créés en dehors de la portée définie

Problème

Durant une reconnaissance, certains systèmes informatique qui sont en dehors de la portée définie sont créés.

Solution

Si l'attribut discoverITMEndpoints contenu dans le profil de reconnaissance pour ce détecteur est défini à `true`, durant une reconnaissance, le détecteur crée un système informatique pour chaque noeud final Tivoli Monitoring connu du serveur Tivoli Enterprise Portal Server. Cette création se produit même si un noeud final se situe en dehors de la portée de reconnaissance initiale qui incluait le serveur de portail.

Les mises à jour apportées à la portée Tivoli Monitoring générée à l'aide de la console de gestion de reconnaissance sont remplacées

Problème

Les mises à jour qui ont été effectuées sur la portée Tivoli Monitoring générée dans la reconnaissance précédente à l'aide de la console de gestion de reconnaissance ont été remplacées.

Solution

Durant une reconnaissance de Niveau 1, une nouvelle portée est créée d'après le nom du serveur Tivoli Enterprise Portal Server. Cette portée est remplacée lors de la reconnaissance suivante, de Niveau 1 ou Niveau 2, du serveur de portail.

Pour modifier la portée Tivoli Monitoring, créez une portée d'un nom différent contenant les éléments de la portée générée.

Dans un environnement Tivoli Monitoring étendu, le détecteur échoue avec une erreur de dépassement de délai

Problème

Dans un environnement Tivoli Monitoring étendu, le détecteur de portée Tivoli Monitoring échoue avec une erreur de dépassement de délai.

Solution

Dans le fichier `etc/collation.properties`, modifiez la propriété suivante, où *valeur* indique, en millièmes de seconde, le délai d'exécution du détecteur (par exemple, 60000 correspond à 1 minute) :

```
com.collation.discover.agent.ITMScopeSensor.timeout=valeur
```

Le détecteur échoue avec une erreur de dépassement de délai en cas de liaisons de réseau lentes ou d'un nombre élevé de sauts de routeur entre les systèmes cibles et le serveur Tivoli Enterprise Portal Server ou TADDM

Problème

Le détecteur de portée Tivoli Monitoring échoue avec une erreur de dépassement de délai. Des liaisons de réseau lentes ou un nombre élevé de sauts de routeur sont observés entre les systèmes cibles et le serveur Tivoli Enterprise Portal Server ou TADDM. Cet environnement inclut les systèmes Windows, Linux et UNIX.

Solution

Ce problème est lié aux paramètres de mémoire tampon TCP. En raison des tailles de mémoire tampon parfois trop petites, les performances peuvent être médiocres avec les détecteurs TADDM et le serveur Tivoli Enterprise Portal Server.

Pour résoudre ce problème, procédez comme suit selon le système d'exploitation :

Sous les systèmes AIX :

1. Exécutez les commandes suivantes :

   ```
   /usr/sbin/no -o tcp_sendspace=32768
   /usr/sbin/no -o tcp_recvspace=32768
   ```

2. Redémarrez le serveur TADDM.

Sous les systèmes Linux :

1. Editez le fichier `/etc/sysctl.conf` avec les paramètres suivants :

   ```
   # increase TCP maximum buffer size
     net.core.rmem_max = 16777216
     net.core.wmem_max = 16777216

   # increase Linux autotuning TCP buffer limits

   # min, default, and maximum number of bytes to use
     net.ipv4.tcp_rmem = 4096 87380 16777216
     net.ipv4.tcp_wmem = 4096 65536 16777216
   ```

2. Exécutez `sysctl -p` pour lire et définir les nouvelles valeurs.
3. Redémarrez le serveur TADDM.

Sur les systèmes Solaris :

1. Exécutez les commandes suivantes :

   ```
   /usr/sbin/ndd -set /dev/tcp tcp_xmit_hiwat 32768
   /usr/sbin/ndd -set /dev/tcp tcp_recv_hiwat 32768
   ```

2. Redémarrez le serveur TADDM.

Des messages d'erreur s'affichent suite à l'exécution de la commande `tacmd getDeployStatus` après le déploiement de l'ensemble de support de la cible de reconnaissance

Problème

Un ou plusieurs des messages suivants apparaissent lors de l'exécution de la commande **`tacmd getDeployStatus`** suite au déploiement de l'ensemble de support de cible de reconnaissance :

- Error Message: KDY1024E: The command /opt/IBM/ITM/bin/CandleAgent -h /opt/IBM/ITM start d7 did not start or stop agent. The command returned a return code.
- Error Message: KDY1008E: The agent action INSTALL failed with a return code of for product code d7. The command /opt/IBM/ITM/tmaitm6/aix526/bin/kdy_xa -setCMS d7 produced the following error text: <Variable formatSpec="{4}">stdErr Text</Variable>. The specified return code was received from the two-way translator.
- Error Message: KDY1024E: The agent failed to respond to the command C:\itmagent\installITM\Batch\kincli -startagent -akd7 did not start or stop agent. The command returned a failure return code.

Solution

Ces messages n'indiquent pas d'erreurs réelles, car l'ensemble de support de cible de reconnaissance n'est pas conçu pour répondre à la commande **start** ou **stop** de l'agent. La commande Tivoli Monitoring **cinfo** ne répertorie pas l'ensemble de support, car celui-ci vient s'ajouter à l'agent de système d'exploitation existant.

Vérifiez que l'ensemble de support de cible de reconnaissance est correctement installé sur la cible de reconnaissance. Dans le répertoire Tivoli Monitoring de l'ordinateur cible, exécutez la commande **directory**, comme indiqué dans l'exemple suivant :

```
C:\Documents and Settings\Administrator>cd %CANDLEHOME%

C:\IBM\ITM>dir taddm
 Volume in drive C has no label.
 Volume Serial Number is B81D-9114

 Directory of C:\IBM\ITM\taddm

09/24/2010  06:38 PM    <DIR>          .
09/24/2010  06:38 PM    <DIR>          ..
09/24/2010  06:38 PM             6,656 Base64.exe
09/24/2010  06:38 PM             1,960 KD7WINNT.dsc
09/24/2010  06:38 PM             1,363 post.bat
09/24/2010  06:38 PM             4,280 pre.bat
09/24/2010  06:38 PM           249,856 TaddmTool.exe
09/24/2010  06:38 PM           474,624 TaddmTool.pdb
09/24/2010  06:38 PM           569,344 TaddmWmi.dll
09/24/2010  06:38 PM           106,496 TaddmWmi.exe
09/24/2010  06:38 PM             1,424 TaddmWmi.mof
09/24/2010  06:38 PM         2,968,576 TaddmWmi.pdb
              10 File(s)      4,384,579 bytes
               2 Dir(s)  10,931,712,000 bytes free
```

Les fichiers d'ensemble de support de reconnaissance doivent être présents dans le répertoire %CANDLE_HOME%\taddm .

Lorsque le détecteur est utilisé pour une reconnaissance de Niveau 2 sur des systèmes cibles Windows, plusieurs fenêtres de commande s'ouvrent sur l'ordinateur sur lequel s'exécute le serveur Tivoli Enterprise Portal Server

Problème

Lorsque vous exécutez le détecteur de portée IBM Tivoli Monitoring pour une reconnaissance de Niveau 2 sur des systèmes cibles Windows, plusieurs fenêtres de commande s'ouvrent sur l'ordinateur sur lequel s'exécute le serveur Tivoli Enterprise Portal Server.

Solution

L'agent IBM Tivoli Monitoring Windows OS est probablement configuré pour s'exécuter en tant que service système et l'option **Autoriser le service à interagir avec le bureau** est activée. Pour remédier à ce problème, procédez comme suit :

1. Cliquez avec le bouton droit sur l'agent dans le programme Manage Tivoli Monitoring Services.
2. Cliquez sur **Change Startup**.
3. Dans le volet «Log on As» de la fenêtre qui s'ouvre, désélectionnez la case à cocher **Autoriser le service à interagir avec le bureau**.
4. Cliquez sur **OK**.
5. Cliquez à nouveau avec le bouton droit de la souris dans la programme Manage Tivoli Monitoring Services.
6. Cliquez sur **Recycle**.

Les fichiers temporaires sont situés dans le répertoire de journalisation du système cible

Problème

Durant une reconnaissance de Niveau 2 par l'intermédiaire de IBM Tivoli Monitoring, certaines commandes échouent sur des noeuds finaux, ce qui entraîne la présence de plusieurs fichiers `KD7*` ou `session_script*.bat` dans le répertoire de journalisation du système cible. Ces fichiers peuvent également être présents pour d'autres raisons, telles que la fin prématurée d'une reconnaissance ou un problème de connexion de l'agent Tivoli Monitoring au serveur Tivoli Enterprise Monitoring Server.

Solution

L'administrateur peut supprimer ces fichiers manuellement à tout moment hors exécution de la reconnaissance. La suppression de ces fichiers durant une reconnaissance peut entraîner l'échec de cette reconnaissance.

Présence possible d'espaces blancs de fin dans la sortie des cibles de reconnaissance

Problème

Si vous créez des modèles de serveur personnalisés qui s'exécutent sous le détecteur de portée IBM Tivoli Monitoring, des espaces blancs de fin (comme des caractères de retour à la ligne ou des caractères de retour chariot) peuvent être présents dans la sortie des cibles de reconnaissance.

Solution

Pour garantir que les modèles de serveur personnalisés fournissent la même sortie avec le détecteur de portée Tivoli Monitoring, supprimez les espaces blancs dans la logique côté serveur du modèle de serveur personnalisé.

Après la mise à niveau de IBM Tivoli Monitoring, des erreurs se produisent durant la reconnaissance

Problème

Après la mise à niveau de IBM Tivoli Monitoring, des erreurs risquent de se produire durant la reconnaissance pour les raisons suivantes :

- résultat de mises à jour apportées aux bibliothèques ou aux tables d'agentsTivoli Monitoring ;

- résultat des mises à jour apportées à la logique de la reconnaissance TADDM.

Solution

Si les erreurs résultent de mises à jour apportées aux bibliothèques ou aux tables d'agents Tivoli Monitoring, réexécutez les tâches suivantes :

- «Copie des fichiers nécessaires à partir du serveur Tivoli Enterprise Portal Server vers le serveur TADDM», à la page 56
- «Installation des requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server», à la page 59

Si les erreurs résultent de mises à jour apportées à la logique de reconnaissance TADDM, réexécutez les tâches suivantes :

- «Copie des fichiers nécessaires à partir du serveur Tivoli Enterprise Portal Server vers le serveur TADDM», à la page 56
- «Distribution de l'ensemble de support cible de la reconnaissance», à la page 57
- «Installation des requêtes personnalisées sur le serveur Tivoli Enterprise Portal Server», à la page 59
- «Configuration du profil de reconnaissance», à la page 60
- «Configuration de la liste d'accès», à la page 61

Si aucune des solutions ci-dessus ne fonctionne, assurez-vous que la propriété `com.ibm.cdb.discover.ITM.https.strictChecking` dans le fichier `collation.properties` est définie sur `false`. Par défaut, cette propriété n'est pas ajoutée au fichier `collation.properties`, ce qui signifie que sa valeur par défaut est `false`. Son utilisation est réservée à la session SSL. Si vous définissez sa valeur sur `true`, le nom d'hôte de connexion doit correspondre au nom d'hôte de certificat. Sinon, la reconnaissance échoue.

Des erreurs se produisent lors de la reconnaissance d'un environnement Tivoli Monitoring 6.2.2

Problème

Au cours de la reconnaissance d'un environnement Tivoli Monitoring version 6.2.2, le serveur Tivoli Enterprise Monitoring Server peut s'arrêter de façon inattendue, ce qui provoque l'affichage des messages d'erreur TADDM suivants :

- `CTJTD0203E L'agent du système informatique ne peut pas extraire les informations hôte et IP pour le système informatique suivant`
- `CTJTD3000E Démarrage - Un erreur s'est produite et le délai du détecteur a expiré`

Solution

Vérifiez que le processus du serveur Tivoli Enterprise Monitoring Server sur le serveurTivoli Monitoring est en cours d'exécution et si nécessaire, redémarrez le serveur Tivoli Enterprise Monitoring Server. Ce processus peut s'arrêter de manière inattendue en raison d'un trop grand nombre de demandes de proxy, ce qui est lié à un problème connu concernant Tivoli Monitoring 6.2.2. Pour plus d'informations, voir l'APAR IZ52960.2 de Tivoli Monitoring.

La portée Tivoli Monitoring n'inclut pas tous les noeuds finaux définis sur le serveur Tivoli Enterprise Portal Server

Problème

La portée de Tivoli Monitoring créée lors d'une reconnaissance n'inclut pas tous les noeuds finaux qui sont définis sur le serveur Tivoli Enterprise Portal Server.

Solution

Des noeuds finaux inactifs et des noeuds finaux pour lesquels des adresses MAC ne peuvent pas être résolues ne sont inclus dans un ensemble de portées créé.

Les cibles sont reconnues lors de la session IBM Tivoli Monitoring et non par SSH ou WMI durant une reconnaissance de niveau 2

Problème

Une fois que le détecteur IBM Tivoli Monitoring Scope a reconnu un noeud final, les reconnaissances ultérieures de niveau 2 se servent par défaut de Tivoli Monitoring. Aucune connexion directe (SSH ou WMI) n'est utilisée. Cette méthode est utilisée même si le détecteur IBM Tivoli Monitoring Scope ne fait pas partie du profil de reconnaissance.

Solution

Pour reconnaître le noeud final via SSH ou WMI, définissez la propriété suivante dans le fichier `collation.properties` : `com.ibm.cdb.session.allow.ITM.`*`endpoint_ip_address`*`=false`.

Voir le *Guide d'administration* de TADDM pour des informations sur la façon de modifier les propriétés de configuration de la reconnaissance des noeuds finaux Tivoli Monitoring via TADDM.

Trop de requêtes de rapport actives sur le serveur Tivoli Enterprise Portal Server

Problème

Le message d'information suivant est généré dans le fichier `SessionSensor.log` :

```
KFWITM460E: Too many active report queries from client IPAddress;
 exceeding limit at number requests.
```

Solution

Augmentez le nombre maximum de requêtes en attente. Editez les paramètres de configuration sur le serveur Tivoli Enterprise Portal Server, sous le système d'exploitation Windows, éditez le fichier `KFWENV` et sous les systèmes d'exploitation Linux ou UNIX, éditez le fichier `cq.ini` avec les paramètres suivants :

```
KFW_REPORT_REQUEST_LIMIT_MAX=100
KFW_REPORT_REQUEST_LIMIT=30
KFW_REPORT_REQUEST_LIMIT_DURATION=300
```

La propriété `KFW_REPORT_REQUEST_LIMIT` indique la limite normale de demandes en attente pour le serveur Tivoli Enterprise Portal Server pour un client unique. `KFW_REPORT_REQUEST_LIMIT_MAX` indique la limite maximale temporaire des demandes en attente qui peut dépasser `KFW_REPORT_REQUEST_LIMIT`, seule autorisée au cours d'une période définie par `KFW_REPORT_REQUEST_LIMIT_DURATION` (en secondes).

Détecteur IBM WebSphere

Le détecteur IBM WebSphere reconnaît les informations du noeud IBM WebSphere Application Server, les informations de cellule ainsi que les informations de version.

TADDM capture tous les fichiers de configuration et les informations de configuration à partir du systèmeWebSphere Network Deployment Manager. Si des modifications sont apportées aux fichiers situés sur le système Deployment Manager, il se peut que ces fichiers soient différents sur le système de noeud distribué actuel. Cette différence peut être due à la durée de la mise à jour de ces modifications sur le système de noeud distribué. En conséquence, une modification de configuration marquée sur un noeud distribué ne reflète peut-être pas ce qui est effectivement sur le noeud distribué.

Le détecteur WebSphere Application Server est exécuté dans sa propre machine virtuelle Java™ (JVM). Le détecteur peut donc personnaliser le chemin d'exécution pour éviter un conflit avec d'autres processus TADDM.

Nom du détecteur utilisé dans l'interface graphique et les journaux

WebSphereCellSensor, WebSphereJDBCDriverSensor, WebSphereNodeSensor, WebSphereVersionSensor, et WebSphereScriptSensor.

Prérequis

Pour les reconnaissances du pilote JDBC IBM WebSphere, assurez-vous que les exigences suivantes sont satisfaites :

- Vous devez disposer d'une autorisation pour exécuter la machine virtuelle Java imbriquée dans l'installation du serveur d'applications WebSphere.
- Vous devez disposer d'une autorisation pour exécuter le script `setupCmdLine` imbriqué dans l'installation du serveur d'applications WebSphere.
- Vous devez disposer d'une autorisation pour lire les fichiers JAR du pilote JDBC.

Limitations

Les limitations suivantes s'appliquent :

- Pour la reconnaissance à l'aide d'IBM Tivoli Monitoring, TADDM prend uniquement en charge la reconnaissance basée sur un script pour le détecteur WebSphere.
- Les connexions JDBC qui utilisent des alias de base de données natifs configurés dans des clients de base de données natifs ne sont pas pris en charge.
- Les serveurs WebSphere distribués ne peuvent pas être reconnus sans assistance. La reconnaissance est effectuée à partir de **dmgr** (gestionnaire de cellule). Pour reconnaître cette machine, elle doit figurer dans la portée de la reconnaissance. Si elle ne figure pas dans la portée de reconnaissance, le journal d'ancrage local affiche les messages suivants :

  ```
  CTJTD1121W verifyStandaloneServer() determined cell to be distributed
  (DISTRIBUTED), terminating discovery
  CTJTD1116W Terminating discovery of managed server/nodeagent <SERVER NAME>
  - discovery will be handled at cell level
  ```

- Les informations sur l'exécution de la machine virtuelle Java, à savoir la version Java et le nom du diffuseur de publications, sont reconnues pour chaque serveur en cours d'exécution. La reconnaissance des informations d'exécution dépend de

la synchronisation de l'agent de noeud et de la cellule. La synchronisation doit être activée pour chaque noeud dans une cellule. L'intervalle de synchronisation détermine dans quel mesure la reconnaissance est à jour. Les informations les plus récentes sont rassemblées à partir de la cellule une fois celles sur la machine virtuelle Java propagées depuis l'agent de noeud.

- La version du pilote JDBC pour les fournisseurs JDBC n'est pas reconnue pour les instances WebSphere Application Servers s'exécutant sur z/OS.
- En raison d'un problème connu avec WebSphere Application Server, des informations sur un correctif temporaire ne sont pas collectées pour certaines version de WebSphere Application Server (telles que WebSphere Application Server 8.0.0.0 et 8.0.0.1).
- Lorsque vous effectuez la reconnaissance des pilotes JDBC de WebSphere Application Server, les données ne sont pas remplies. Ceci se produit car les sources de données JDBC n'utilisent pas les adresses IP mais des noms d'hôte (FQDN), tandis que TADDM repose sur DNS. Lors de la création des dépendances entre WebSphere Application Server et les serveurs de base de données, le fichier `/etc/hosts` n'est pas lu.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.AppServer
- app.ConfigFile
- app.SoftwareContainer
- app.j2ee.J2EEComponent
- app.j2ee.J2EEDeployedObject
- app.j2ee.J2EEModule
- app.j2ee.J2EEResource
- app.j2ee.JDBCDriver
- app.j2ee.websphere.WebSphereAuthMappingModule
- app.j2ee.websphere.WebSphereCell
- app.j2ee.websphere.WebSphereCluster
- app.j2ee.websphere.WebSphereConfiguredConnection
- app.j2ee.websphere.WebSphereConnector
- app.j2ee.websphere.WebSphereConnectorModule
- app.j2ee.websphere.WebSphereCustomUserRegistry
- app.j2ee.websphere.WebSphereDeploymentManager
- app.j2ee.websphere.WebSphereDynamicCache
- app.j2ee.websphere.WebSphereEFixInfo
- app.j2ee.websphere.WebSphereEJB
- app.j2ee.websphere.WebSphereEJBModule
- app.j2ee.websphere.WebSphereGlobalSecuritySettings
- app.j2ee.websphere.WebSphereJ2EEApplication
- app.j2ee.websphere.WebSphereJ2EEResource
- app.j2ee.websphere.WebSphereJ2EEResourceProperty
- app.j2ee.websphere.WebSphereJDBCConnectionPool
- app.j2ee.websphere.WebSphereJDBCDataSource

- app.j2ee.websphere.WebSphereJDBCProvider
- app.j2ee.websphere.WebSphereJMSDestination
- app.j2ee.websphere.WebSphereJMSProvider
- app.j2ee.websphere.WebSphereJMSQueue
- app.j2ee.websphere.WebSphereJMSTopic
- app.j2ee.websphere.WebSphereLDAPUserRegistry
- app.j2ee.websphere.WebSphereLibraryRef
- app.j2ee.websphere.WebSphereMQJMSDestination
- app.j2ee.websphere.WebSphereMQJMSQueue
- app.j2ee.websphere.WebSphereMQJMSTopic
- app.j2ee.websphere.WebSphereNamedEndpoint
- app.j2ee.websphere.WebSphereNode
- app.j2ee.websphere.WebSphereNodeAgent
- app.j2ee.websphere.WebSphereServlet
- app.j2ee.websphere.WebSphereServer
- app.j2ee.websphere.WebSphereSessionTuningParams
- app.j2ee.websphere.WebSphereSharedLibrary
- app.j2ee.websphere.WebSphereSSLSettings
- app.j2ee.websphere.WebSphereUserRegistry
- app.j2ee.websphere.WebSphereVariable
- app.j2ee.websphere.WebSphereVirtualHost
- app.j2ee.websphere.WebSphereWebModule
- Fix Pack 5 app.j2ee.websphere.WebSphereGroup
- Fix Pack 5 app.j2ee.websphere.WebSphereRole
- Fix Pack 5 app.j2ee.websphere.WebSphereUser
- app.JVM

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur IBM WebSphere prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour effectuer une reconnaissance basée sur un script, vous devez créer un profil de reconnaissance avec uniquement WebSphereScriptSensor activé et le reste des détecteurs WebSphere désactivé.

Remarque : WebSphereScriptSensor est exclusivement destiné pour la reconnaissance asynchrone et basée sur un script, et ne collecte aucune données lorsqu'il est utilisé en mode reconnaissance régulière.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, l'entrée de liste d'accès du système informatique est utilisée pour lire des fichier de configuration WebSphere. Une entrée de liste d'accès d'applications pour le serveur WebSphere n'est pas nécessaire.

Exécution de reconnaissances

Lors de la reconnaissance d'une cellule WebSphere distribuée, une grande partie de sa configuration est collectée à partir de son référentiel maître qui est stocké en mode DMGR. Cependant, d'autres hôtes qui appartiennent à la cellule doivent également être reconnus pour créer des relations entre des serveurs WebSphere et ses systèmes informatiques qui sont exécutés dessus.

Important : La reconnaissance de WAS basée sur un script varie selon du mode régulier dans lequel un hôte d'un gestionnaire de déploiement est la seule cible de reconnaissance requise.

Limitations

Certaines fonctions fournies par le détecteur WebSphere durant une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

La reconnaissance de descripteur d'application n'est pas pris en charge.

Les objets de modèle suivants ne sont pas pris en charge :

- app.j2ee.JDBCDriver
- app.j2ee.websphere.WebSphereConnector
- app.j2ee.websphere.WebSphereEFixInfo
- app.j2ee.websphere.WebSphereLibraryRef
- app.j2ee.websphere.WebSphereServlet
- app.j2ee.websphere.WebSphereSessionTuningParams
- app.j2ee.websphere.WebSphereSharedLibrary
- app.JVM

Uniquement les fichiers de configuration suivants sont stockés dans la base de données TADDM :

- Dans `<PROFILE_HOME>/config/cells/<CELL_NAME>/` :
  - `cell.xml`
  - `resources.xml`
  - `virtualhosts.xml`
  - `variables.xml`
  - `security.xml`
  - Fix Pack 5 `fileRegistry.xml`
  - Fix Pack 5 `admin-authz.xml`
  - Fix Pack 5 `audit-authz.xml`
- Dans `<PROFILE_HOME>/config/cells/<CELL_NAME>/nodes/<NODE_NAME>/`:

  - node.xml
  - variables.xml
  - resources.xml
  - serverindex.xml
  - spi.policy
  - app.policy
  - library.policy
- Dans <PROFILE_HOME>/config/cells/<CELL_NAME>/nodes/<NODE_NAME>/servers/<SERVER_NAME>/ :
  - server.xml
  - variables.xml
  - resources.xml

Remarque : La limitation suivante ne s'applique qu'à la version 7.3.0 de TADDM, elle ne s'applique pas aux versions 7.3.0.1 et ultérieures.
Les objets app.ProcessPool sont reconnus uniquement pour les serveurs s'exécutant sur un hôte DMGR.

Configuration du détecteur

Avant d'effectuer une reconnaissance, il se peut que vous deviez configurer le détecteur IBM WebSphere en fonction du type d'environnement.

Activation de la reconnaissance du pilote JDBC :

Pour reconnaître les informations sur le pilote JDBC, vous devez activer le détecteur de pilote JDBC WebSphere.

Pour activer le détecteur de pilote JDBC WebSphere, procédez comme suit :

1. Créez un profil de reconnaissance de niveau 3.
2. Pour le détecteur de cellule WebSphere, activez l'élément de configuration deepDiscoveryLevel.
3. Activez le détecteur de pilote JDBC WebSphere dans le nouveau profil de reconnaissance.
4. Définissez les options de configuration appropriées pour le détecteur de pilote JDBC WebSphere. Les options de configuration sont disponibles :
   - Vous pouvez configurer l'ajout d'un préfixe à chaque commande exécutée par le détecteur de pilote JDBC WebSphere sur l'hôte cible. Vous pouvez configurer un préfixe distinct pour les systèmes UNIX et Windows. Par défaut, aucun préfixe n'est défini.
   - Vous pouvez configurer la suppression par le détecteur de fichier OracleUtility au terme de la reconnaissance. Le fichier OracleUtility est un fichier auxiliaire employé par TADDM sur les hôtes cible pour reconnaître les informations sur le pilote JDBC pour les bases de données Oracle. Par défaut, le fichier OracleUtility n'est pas supprimé.

Configuration du profil de reconnaissance :

Si vous souhaitez modifier le niveau de reconnaissance, mettez à jour le profil de reconnaissance du détecteur IBM WebSphere.

Remarque : Le changement de niveau de reconnaissance ne s'applique pas au mode de reconnaissance dépendant d'un script ou asynchrone parce que WebSphereScriptSensor n'a aucune propriété de configuration.

Pour modifier le niveau de reconnaissance par défaut de ce détecteur, procédez comme suit :

1. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
2. Dans la fenêtre Créer un profil, entrez le nom et la description du profil, puis cliquez sur **OK**.
3. Dans la liste de détecteurs, cliquez sur **WebSphereCellSensor**, puis sur **Nouveau**.
4. Dans la fenêtre Création de configuration, entrez le nom et la description de votre configuration du détecteur WebSphereCellSensor, et cochez la case **Activer la configuration**.
5. Dans la section **Configuration** de la fenêtre Création de configuration, sélectionnez l'une des options suivantes pour modifier la valeur du niveau de reconnaissance :
   - Pour activer la reconnaissance moyenne, cliquez deux fois sur la valeur de **mediumDiscoveryLevel** et remplacez *false* par *true*
   - Pour activer la reconnaissance approfondie, cliquez deux fois sur la valeur de **deepDiscoveryLevel** et remplacez *false* par *true*

   Si **deepDiscoveryLevel** est défini sur *true*, une reconnaissance approfondie est exécutée, quelle que soit la valeur des niveaux de reconnaissance superficielle et moyenne (*true* ou *false*).
6. Facultatif : pour configurer le détecteur afin qu'il reconnaisse uniquement les serveurs en cours d'exécution, cliquez sur **discoverStoppedServers**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne, et entrez `false`.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Assurez-vous que WebSphereVersionSensor et WebSphereNodeSensor sont sélectionnés avec la nouvelle configuration WebSphereCellSensor créée.
9. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.
10. Sélectionnez ce profil de reconnaissance lors de l'exécution d'une reconnaissance.

Pour plus d'informations sur les profils de reconnaissance, voir la rubrique *Utilisation de profils de reconnaissance* dans le *Guide d'utilisation* de TADDM.

Propriétés de détecteurs

shallowDiscoveryLevel, mediumDiscoveryLevel, deepDiscoveryLevel

Le détecteur WebSphere comporte trois niveaux de reconnaissance : superficielle, moyenne et approfondie. Par défaut, le niveau de reconnaissance superficielle est activé. Pour modifier la valeur du niveau de reconnaissance, sélectionnez l'une des options suivantes :

- Pour activer la reconnaissance moyenne, cliquez deux fois sur la valeur de mediumDiscoveryLevel et remplacez false par true.
- Pour activer la reconnaissance approfondie, cliquez deux fois sur la valeur de deepDiscoveryLevel et remplacez false par true.

Si deepDiscoveryLevel est défini sur true, une reconnaissance approfondie est exécutée, quelle que soit la valeur des niveaux de reconnaissance superficielle et moyenne (true ou false).

- La liste suivante répertorie les informations enregistrées à chaque niveau de reconnaissance.
  - La reconnaissance superficielle reconnaît les composants suivants :
    - Fichiers libellés d'application
    - Noms de cellule, de noeud et de serveur
    - Type de cellule, de noeud et de serveur
    - Système hôte
    - Version d'exécution de la machine virtuelle Java pour tous les serveurs en cours d'exécution
    - Nom et version de produit
    - Répertoire principal
  - La reconnaissance moyenne reconnaît les composants suivants :
    - Clusters
    - Fichiers de configuration
    - Connexions
    - Modules connecteurs déployés
    - Modules EJB déployés
    - Applications Java EE déployées
    - Modules Web déployés
    - Correctifs d'urgence
    - Conteneurs d'EJB
    - Noeuds finaux
    - Paramètres de machine virtuelle Java
    - Ports
    - Définition des processus
    - Stratégie de contrôle de processus
    - Pools de processus
    - Sécurité, paramètres SSL et registres d'utilisateurs
    - Hôtes virtuels
    - Conteneurs Web
  - La reconnaissance approfondie reconnaît les composants suivants :
    - Cellule, noeud, serveur, fournisseurs JDBC de cluster, sources de données JDBC et dépendances JDBC
    - Propriétés personnalisées
    - Descripteurs de déploiement pour les modules et les applications Java EE
    - Fournisseurs JMS et destinations JMS
    - Bibliothèques partagées
    - Variables
    - Services Web
    - Paramètres du service de cache dynamique et clusters dynamiques

traceSpecification

Définit la chaîne de spécification de trace pour activer la journalisation de trace du code client WebSphere appelé par le détecteur TADDM WebSphere. sample value - Admin=all=enabled

Attention : La valeur précédente génère une journalisation de trace verbose. Si aucune valeur n'est définie, la journalisation de trace ne peut pas être effectuée.

traceOutputFile

Vous permet de spécifier le nom de chemin complet du fichier de sortie à utiliser pour la journalisation de la sortie de trace. N'attribuez pas de valeur à cette propriété si le traçage n'est pas requis.

L'utilisateur TADDM doit disposer des droits requis pour créer le fichier de sortie.

ffdcLogDirectory

Active les journaux FFDC du code client WebSphere appelé par le détecteur WebSphere à des fins de résolution d'incidents. Les journaux FFDC capturent le chemin de l'échec via le code client WebSphere dans un sous-répertoire appelé `ffdc` dans le répertoire indiqué dans cette propriété.

Une valeur non définie signifie que FFDC n'est pas activé. Le répertoire doit exister et l'utilisateur TADDM doit disposer d'un accès en écriture.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requis en fonction du type de configuration utilisé.

Remarque : La configuration de la liste d'accès ne s'applique pas au mode de reconnaissance asynchrone ou basée sur un script, parce que WebSphereScriptSensor nécessite uniquement un utilisateur de niveau système d'exploitation dans la liste d'accès TADDM.

Pour configurer la liste d'accès, procédez comme suit :

1. Si la sécurité est désactivée, aucun compte utilisateur n'est nécessaire.
2. Si la sécurité est activée, indiquez les détails suivants :
   a. Pour le type de composant, entrez `Serveur d'applications`.
   b. Pour le fournisseur, entrez `WebSphere`.
   c. Indiquez le nom d'utilisateur et le mot de passe de WebSphere Application Server.
   d. Dans les paramètres SSL, téléchargez deux certificats (de confiance et de fichiers de clés) avec leur phrase de passe. La phrase de passe par défaut est `WebAS`.
3. Pour le détecteur de pilote JDBC WebSphere, procédez comme suit :
   a. Pour le type de composant, entrez `Serveur d'applications`.
   b. Pour le fournisseur, entrez `WebSphere SSH`.
   c. Indiquez le nom d'utilisateur et le mot de passe d'un compte système avec les droits appropriés. Si la liste d'accès WebSphere SSH n'est pas précisée, le détecteur de pilote JDBC WebSphere tente de se connecter avec les droits d'accès ComputerSystem.
4. L'utilisateur WebSphere Application Server peut être doté du rôle moniteur, opérateur, configurateur ou administrateur. Ces rôles peuvent reconnaître toutes les informations. Seul le rôle administrateur reconnaît les informations de configuration de la sécurité pour WebSphere Application Server.

5. La désactivation de la sécurité ne signifie pas que vous n'utilisez pas le protocole SSL. Vérifiez si un mot de passe vous est demandé lorsque vous vous connectez à la console d'administration WebSphere Application Server.
   - S'il vous faut uniquement un nom d'utilisateur pour vous connecter à la console d'administration, la sécurité est désactivée.
   - S'il vous faut un nom d'utilisateur et un mot de passe pour vous connecter à la console d'administration, la sécurité est activée.
   - Si la connexion à la console d'administration se fait via https (observez l'URL dans votre navigateur Web), vous avez besoin des certificats.

Accès aux fichiers de configuration

- En règle générale, le détecteur WebSphere Application Server capture les fichiers de configuration suivants :
  – Cellule WebSphere Application Server
  – Noeud WebSphere Application Server
  – Serveur WebSphere Application Server

  Ces informations sont rendues disponibles pour l'historique des modifications sur une période donnée. Elles sont également visibles dans la console de gestion de reconnaissance (onglet Fichiers de configuration du panneau Détails) pour chaque élément de configuration précédent.
- Lorsque le serveur démarre, il utilise également les deux fichiers suivants pour prendre des décisions clé sur la reconnaissance de WebSphere Application Server :
  – `$RACINE_WAS/config/cells/cell_name/cell.xml`

    Ce fichier permet de déterminer si le système est un serveurWebSphere Application Server ND ou autonome. Si l'accès en lecture à ce fichier n'est pas disponible, le détecteur continue et utilise JMX pour déterminer s'il s'agit d'un serveur WebSphere Application Server ND ou autonome.
  – `$RACINE_WAS/config/cells/cell_name/nodes/nom_noeud/serverindex.xml` (pour ND, *nom_noeud* est le noeud de dmgr, il existe un seul noeud pour le serveur autonome)

    Ceci permet de déterminer le port sur lequel le connecteur JMX SOAP est en mode écoute. Si l'accès en lecture à ce fichier n'est pas disponible, le détecteur tente d'établir une connexion JMX en parcourant tous les ports d'écoute du serveur/dmgr WebSphere Application Server faisant l'objet d'une reconnaissance. Les ports sont essayés par ordre croissant puisque cette méthode se traduit par une identification plus rapide du port JMX.

Configuration de certificats :

Si la sécurité est activée quand vous reconnaissez WebSphere Application Server, vous devez définir les certificats SSL dans les entrées de la liste d'accès. TADDM prend en charge les types de magasin de certificats PKCS12 et JKS. Les fichiers de clés certifiées et de clés doivent se trouver sur l'ordinateur exécutant la console TADDM, et non sur le serveur TADDM.

Remarque : La configuration de certificat ne s'applique pas au mode de reconnaissance asynchrone ou basée sur un script, parce que WebSphereScriptSensor nécessite uniquement un utilisateur de niveau système d'exploitation dans la liste d'accès TADDM.

Les fichiers de clés et de clés certifiées se trouvent en général dans le répertoire $PROFILE_HOME/etc, sur le système où est installé WebSphere Application Server. Par défaut, les fichiers suivants sont des magasins de certificats :

- PKCS12
  - $PROFILE_HOME/etc/trust.p12
  - $PROFILE_HOME/etc/key.p12
- JKS
  - $PROFILE_HOME/etc/DummyClientTrustFile.jks
  - $PROFILE_HOME/etc/DummyClientKeyFile.jks

La phrase passe par défaut pour ces fichiers est WebAS. Vous pouvez aussi créer des fichiers de clés et de clés certifiées en téléchargeant des certificats via la console WebSphere Application Server.

TADDM requiert un fichier de clés certifiées avec certificat de signataire uniquement pour la connexion à DMGR, en ce qu'il s'agit de WebSphere Application Server Network Deployment (ND), et server1, pour un serveur autonome.

En raison des restrictions du protocole JMX, qui sert à extraire des données de WebSphere Deployment Manager ou d'un serveur autonome, TADDM peut gérer un seul fichier de clés certifiées pour une seule reconnaissance. Les certificats stockés dans le fichier de clés certifiées sont chargés quand la connexion à WebSphere Application Server est établie. Seuls ces certificats peuvent être utilisés par TADDM lors d'une reconnaissance entière. Si les certificats de plusieurs fichiers de clés certifiées sont requis ; ne les associez pas séparément dans la liste d'accès. Vous devez exporter les fichiers de clés certifiées d'origine vers un même fichier, manuellement ou via un script collectwascerts associé à TADDM. Quand toutes les entrées nécessaires pour chaque serveur WebSphere se trouvent dans la liste d'accès TADDM, les fichiers de clés et de clés certifiés exportés doivent être associés à la première de ces entrées. Il existe toujours une entrée pour chaque combinaison utilisateur/mot de passe pour les serveurs WebSphere reconnus.

Création d'un fichier de clés certifiées avec le script collectwascerts :

TADDM peut utiliser un seul fichier de clés certifiées pour une même reconnaissance. Si vous voulez utiliser des certificats de plusieurs fichiers de clés certifiées, vous devez exporter ces fichiers dans un même fichier. Vous pouvez utiliser le script collectwascerts qui télécharge les certificats pour leur exportation.

Procédure

1. Editez le fichier $COLLATION_HOME/bin/collectwascerts.config.

   Ajoutez une ligne pour chaque serveur WebSphere duquel vous voulez télécharger les certificats. Pour les cellules distribuées, vous n'avez besoin que de certificats du gestionnaire de déploiement (DMGR) afin d'exécuter une reconnaissance. Si vous commencez une ligne par un dièse (#), elle est prise comme un commentaire et n'est pas traitée.

   Chaque ligne doit être au format suivant :

   ```
   <Server IP/HOSTNAME/FQDN><numéro de port SOAP><nom d'utilisateur><mot de passe>
   156.24.24.11 8879 wasadmin waspassword
   ```

   Vous trouverez la valeur du numéro de port SOAP dans la section Ports du panneau de DMGR ou du serveur, dans la console d'administration WAS. Le nom exact est SOAP_CONNECTOR_ADDRESS.

2. Exécutez `$COLLATION_HOME/bin/collectwascerts.sh` (ou `$COLLATION_HOME/bin/collectwascerts.bat`) sur votre hôte TADDM, même si le fichier `collectwascerts.config` n'a pas d'entrées. Le fichier n'a peut-être pas d'entrées car tous les serveurs WAS sont accessibles depuis des serveurs d'ancrage uniquement.

   Tous les certificats extraits sont stockés dans `$COLLATION_HOME/bin/collectedwascerts.jks`. La phrase de passe est écrite par l'outil dans la sortie standard. Vous pouvez aussi la lire dans la propriété `com.collation.sslpassphrase`, dans `$COLLATION_HOME/etc/collation.properties`.

   Suivez uniquement les étapes facultatives si vos environnements WAS ne sont pas directement accessibles depuis votre serveur TADDM.
3. Facultatif : Copiez le fichier `collectedwascerts.jks` de l'hôte TADDM dans votre première ancre.

   Copiez le fichier dans le répertoire bin contenant les fichiers `collectwascerts.config`, `collectwascerts.bat` et `collectwascerts.sh`.
4. Facultatif : Exécutez `collectwascerts.sh` (ou `collectwascerts.bat`) sur l'hôte d'ancrage.
5. Facultatif : Copiez `collectedwascerts.jks` de l'hôte d'ancrage dans l'ancre suivante.

   Copiez le fichier dans le répertoire bin contenant les fichiers `collectwascerts.config`, `collectwascerts.bat` et `collectwascerts.sh`.
6. Facultatif : Exécutez `collectwascerts.sh` (ou `collectwascerts.bat`) sur l'hôte d'ancrage suivant.
7. Facultatif : Répétez les étapes 5 et 6 pour toutes vos ancres.
8. Associez le fichier `collectedwascerts.jks` de la dernière ancre, ou de votre hôte TADDM si vous n'utilisez pas le script sur des ancres, à l'entrée de votre liste d'accès WebSphere en tant que fichier de clés certifiées. Le type SSL de ce fichier est JKS. Utilisez la phrase de passe décrite à l'étape 2.

Création manuelle d'un fichier de clés certifiées :

TADDM peut utiliser un seul fichier de clés certifiées pour une même reconnaissance. Si vous voulez utiliser des certificats de plusieurs fichiers de clés certifiées, vous devez exporter ces fichiers dans un même fichier. Vous pouvez extraire les certificats et les ajouter manuellement aux fichiers de clés et de clés certifiées.

Pourquoi et quand exécuter cette tâche

Procédure

1. Extrayez tous les certificats du fichier de clés ou du fichier de clés certifiées pour chaque serveur en procédant comme suit :
   a. Dans la console d'administration de WebSphere Application Server, cliquez sur **Sécurité** > **Certificat SSL et gestion des clés**.
   b. Cliquez sur **Fichiers de clés et certificats**.
   c. Cliquez sur **NodeDefaultTrustStore**.
   d. Cliquez sur **Certificats de signataire**.
   e. Sélectionnez un certificat de signataire et cliquez sur **Extraire**.
   f. Entrez un chemin et un nom uniques pour le certificat de signataire. Par exemple, entrez `C:\temp\signer1.arm`.
   g. Cliquez sur **OK**.

h. Répétez cette procédure pour chaque certificat de signataire figurant dans le fichier de clés certifiées.

i. Répétez cette procédure pour tous les serveurs à reconnaître.

2. Si vous utilisez des fichiers de clés certifiées JKS, ajoutez les certificats de signataire exportés aux fichiers `.jks`. Pour les ajouter aux fichiers `DummyServerTrustFile.jks` et `DummyClientTrustFile.jks` par défaut, procédez comme ci-après. Si vous utilisez des fichiers de clés certifiées PKCS12, suivez la même procédure pour les fichiers `key.p12` et `trust.p12` :

   a. Pour ouvrir **iKeyman**, dans le répertoire *WebSphere_Root*`/profiles/`*dmgr_profile*`/bin`, exécutez `ikeyman.sh`, ou `ikeyman.bat`.

   b. Cliquez sur **Fichier de clés** > **Ouvrir**.

   c. Sélectionnez le fichier `DummyServerTrustFile.jks` dans l'un des répertoires suivants :

      - *Racine_WebSphere*`/profiles/`*profil_dmgr*`/etc`
      - *Racine_WebSphere*`/profiles/`*profil_serveur_autonome*`/etc`

   d. A l'invite de saisie du mot de passe, entrez `WebAS`.

   e. Cliquez sur **Ajouter** et sélectionnez l'un des certificats de signataire extraits à l'étape 1.

   f. Répétez les étapes précédentes pour chaque certificat de signataire à ajouter.

   g. Répétez cette procédure pour ajouter les certificats de signataire exportés dans le fichier *Racine_WebSphere*`/profiles/`*profil_dmgr*`/etc/DummyClientTrustFile.jks`.

3. Extrayez les certificats SSL côté client de WebSphere Application Server. Si de nouveaux certificats ne sont pas générés, ceux par défaut `DummyClientTrustFile.jks` et`DummyClientKeyFile.jks` (ou `trust.p12` et `key.p12`) se trouvent normalement dans les répertoires suivants :

   - *Racine_WebSphere*`/profiles/`*profil_dmgr*`/etc`
   - *Racine_WebSphere*`/profiles/`*profil_serveur_autonome*`/etc`

   La phrase passe par défaut pour des fichiers factices est `WebAS`.

4. Si vous voulez utiliser des certificats différents, ne tentez pas de les éditer. Supprimez l'ancienne entrée de liste d'accès et créez-en une autre.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur IBM WebSphere.

Remarque : Les propriétés suivantes ne s'appliquent pas au mode de reconnaissance dépendant d'un script ou asynchrone, parce que WebSphereScriptSensor ne les utilise pas.

com.collation.discover.localanchor.timeout=7200000
com.collation.discover.agent.WebSphereNodeSensor.timeout=7200000
com.collation.discover.agent.WebSphereCellSensor.timeout=7200000

La valeur par défaut est `7200000`, ce qui correspond à 7 200 000 millisecondes (ou encore 2 heures).

Ces propriétés définissent le temps alloué pour l'exécution du détecteur WebSphere.

Si vous possédez une environnement WebSphere important et des niveaux de reconnaissance moyens ou profonds, vous devez éventuellement augmenter la valeur afin que le détecteur ait le temps de reconnaître l'environnement.

com.collation.discover.websphere.jmx.timeout=
Ce propriété définit le temps autorisé pour établir une connexion JMX avec WebSphere. Par défaut, la valeur est 600 000 millisecondes (10 minutes).

com.collation.discover.agent.WebSphereVersionAgent.versionscript=sudo
Cette propriété peut être activée pour accéder au fichier WebSphere `versionInfo.sh` si l'utilisateur de la reconnaissance ne dispose pas d'un accès au système WebSphere Application Server cible.

Utilisation du détecteur de valeurs de départ WebSphere pour z/OS

TADDM ne prend pas en charge de détecteur de système d'exploitation pour un système z/OS. Pour reconnaître les ressources WebSphere sur un système z/OS, le détecteur WebSphere est amélioré afin de prendre en charge la reconnaissance initiée depuis des fichiers de départ créés par l'utilisateur.

Du fait de l'absence de détecteur de système z/OS, vous devez vous servir de l'utilitaire de valeur de départ WebSphere Application Server pour l'adaptateur de bibliothèque de reconnaissance z/OS. Cet utilitaire crée un fichier de départ XML à partir d'un manuel IdML z/OS. Ce fichier contient des informations relatives aux ressources WebSphere que vous tentez de reconnaître sur le système z/OS.

Une fois ce fichier de départ créé, lors de la reconnaissance suivante, le détecteur WebsphereIdmlSeedSensor recherche les fichiers de départ z/OS WebSphere sur le serveur TADDM. S'il en existe, il analyse ce fichier de départ et crée un *véritable* fichier de départ de reconnaissance servant à déclencher le détecteur WebSphere. Le détecteur WebSphere procède ensuite à une recherche approfondie de WebSphere sur ce système z/OS.

Pour installer et configurer l'utilitaire de valeur de départ WebSphere Application Server pour l'adaptateur de bibliothèque de reconnaissance z/OS, consultez la section correspondante.

Préparation pour l'exécution sur le détecteur de valeur de départ WebSphere :

Avant d'exécuter le détecteur de valeur de départ WebSphere, vous devez créer un fichier de départ.

Avant d'exécuter le détecteur de valeur de départ WebSphere, procédez comme suit :

1. Choisissez la méthode appropriée pour créer le fichier de départ WebSphere :
   - Pour faire une reconnaissance de WebSphere sur un système z/OS à l'aide de l'adaptateur de bibliothèque de reconnaissance, utilisez l'utilitaire de valeur de départ de WebSphere Application Server qui génère automatiquement les fichiers de départ à partir des manuels IdML créés depuis cet adaptateur de bibliothèque de reconnaissance z/OS. L'utilitaire est fourni dans le package de l'adaptateur de bibliothèque de reconnaissance z/OS.

     Pour plus d'informations sur cet utilitaire, voir la section Reconnaissance de WebSphere Application Server de l'adaptateur de bibliothèque de reconnaissance pour le centre de documentation z/OS.
   - Pour reconnaître WebSphere sur un système secondaire en créant manuellement un fichier de départ, utilisez les conventions de dénomination de fichier suivantes lors de la création du fichier de départ :
     – Si vous voulez que le fichier soit inclus dans le cadre de la reconnaissance, le nom de fichier doit se terminer par une extension `.xml`.

– Le nom de fichier doit respecter le format suivant :

  `<cellname>_<fqdn>_<port>.xml`

  Voici un exemple : `c1_0.0.0.0_2809.xml`.

L'exemple suivant illustre le format du fichier :

```
<IDML_WAS_SEED>
  <WAS_ROOT_DIR>/opt/WebSphere/AppServer</WAS_ROOT_DIR>
  <WAS_VERSION>6.0.2.7</WAS_VERSION>
  <SOAP_CONNECTOR_PORT>8880</SOAP_CONNECTOR_PORT>
  <RMI_CONNECTOR_PORT>2809</RMI_CONNECTOR_PORT>
  <JMX_LISTEN_IP_ADDRESS>0.0.0.0</JMX_LISTEN_IP_ADDRESS>
  <HOST_MAPPINGS>
    <HOST_MAPPING>
      <HOST_NAME>wasserver.company.com</HOST_NAME>
      <PRIMARY_IP_ADDRESS>0.0.0.0</PRIMARY_IP_ADDRESS>
      <IP_ADDRESS>0.0.0.0</IP_ADDRESS>
    </HOST_MAPPING>
  </HOST_MAPPINGS>
</IDML_WAS_SEED>
```

WAS_ROOT_DIR
: Chemin d'accès au répertoire d'installation de WebSphere Application Server.

WAS_VERSION
: Version de WebSphere Application Server, qui se trouve dans le fichier produit, dans le répertoire *<répertoire principal WebSphere>*`/properties/version`.

SOAP_CONNECTOR_PORT
: Le numéro de port est extrait du fichier `serverindex.xml` pour le nom de noeud final *SOAP_CONNECTOR_ADDRESS*. Par exemple *<WebSphere Root Directory>*`/profiles/`*<app server or dmgr>*`/conf/cells/`*<cell name>*`/nodes/`*<node name>*

  Si la ressource est un gestionnaire de déploiement, utilisez le fichier `serverindex.xml`, qui contient la valeur suivante : `serverType="DEPLOYMENT_MANAGER"`.

  Si la ressource est un composant autonome, utilisez le fichier `serverindex.xml` avec la valeur suivante : `serverType="APPLICATION_SERVER"`

RMI_CONNECTOR_PORT
: Le numéro de port est extrait du fichier `serverindex.xml` qui a été utilisé pour trouver le port SOAP, où le nom de noeud final est *BOOTSTRAP_ADDRESS*.

JMX_LISTEN_IP_ADDRESS
: Adresse IP utilisée pour se connecter via JMX. En règle générale, il s'agit de la même adresse IP que celle du serveur WebSphere.

HOST_MAPPINGS
: Liste de mappages entre le nom d'hôte et l'adresse IP de WebSphere Application Server ou du gestionnaire de déploiement et chaque agent de noeud réparti.

HOST_MAPPING
: Mappage d'hôte qui se compose d'un nom d'hôte, d'une adresse IP principale et d'une adresse IP.

HOST_NAME
: Nom de domaine complet.

PRIMARY_IP_ADDRESS
Adresse IP principale de la résolution du nom d'hôte.

IP_ADDRESS
Adresse IP de la résolution du nom d'hôte, si différente de l'adresse IP principale.

2. Placez les fichiers `.xml` dans le répertoire `$COLLATION_HOME/var/dla/zos/was`. Si le répertoire n'existe pas, vous devez le créer. La portée de la reconnaissance est contrôlée par les fichiers de ce répertoire. Si la reconnaissance d'un serveur WebSphere particulier n'est plus souhaitée, le fichier doit être supprimé de ce répertoire ou renommé sans l'extension `.xml`.
3. Créez un nouveau fichier de configuration du détecteur lors de l'exécution du détecteur de valeur de départ WebSphere. Modifiez l'emplacement du fichier de départ XML à l'aide des deux balises suivantes :

   <fileName>
   Définissez cette balise sur le répertoire où se trouvent les fichiers de départ XML WebSphere.

   <scope>
   Définissez cette balise sur l'adresse IP du serveur TADDM sur lequel se trouvent les fichiers de départ XML WebSphere.

Exécution du détecteur de valeur de départ WebSphere :

Cette rubrique décrit comment exécuter le détecteur de valeur de départ WebSphere.

Pour exécuter le détecteur de valeur de départ WebSphere, procédez comme suit :

1. Démarrez le serveur TADDM.
2. Ouvrez la console de gestion de reconnaissance.
3. Ajoutez l'adresse IP du serveur dans lequel le fichier de départ WebSphere se trouve dans une portée.
4. Dans la liste d'accès, ajoutez les droits d'accès du serveur dans lequel se trouve le fichier de départ WebSphere.
5. Si la sécurité est activée pour le serveur WebSphere qui fait l'objet de la reconnaissance, ajoutez l'entrée d'authentification correspondant au serveur WebSphere. Pour utiliser l'entrée avec une restriction de portée, vous devez inclure l'adresse IP de votre serveur WebSphere dans la portée de reconnaissance en plus de l'adresse IP de l'hôte où se trouve le fichier de départ de WebSphere.

   Vous avez également besoin d'un certificat SSL côté client lors de le création de l'entrée de liste d'accès. Ce certificat doit être exporté à partir du produit de sécurité grand système, par exemple RACF (Resource Access Control Facility), et transféré sur un outil pour la maintenance des certificats numériques. Utilisez cet outil, pour exemple IKeyMan, pour générer un fichier JKS ou PKCS12. Ce fichier contient le certificat SSL côté client dans un format utilisable par TADDM. Le fichier JKS ou PKCS12 doit ensuite être utilisé pour les paramètres SSL dans l'entrée de liste d'accès TADDM WebSphere pour des certificats de fichiers de clés et de fichiers de clés certifiées.
6. Procédez comme suit :
   a. Configurer le détecteur IdmlFileUDS à l'aide de la console de gestion de reconnaissance :
      1) Dans la fenêtre **Profils de reconnaissance**, cliquez sur **IdmlFileUDS**.
      2) Cliquez sur **Nouveau**.

3) Entrez le nom de la configuration du détecteur et une description.
4) Sélectionnez **Activer la configuration.**
5) Cliquez deux fois sur */data/latest/dist/var/dla/zos/was* et entrez l'emplacement des fichiers de départ XML de WebSphere. Cet emplacement est le serveur dans lequel se trouve le fichier de départ WebSphere.
6) Cliquez deux fois sur *0.0.0.0* et entrez l'adresse IP de la machine dans laquelle se trouve le fichier de départ.

b. Créez un profil de reconnaissance comprenant les détecteurs suivants :
   - Détecteur d'ancrage
   - Nom du détecteur entré à l'étape a. (Le détecteur IdmlFileUDS modifié créé précédemment.)
   - PortSensor
   - PingSensor
   - SessionSensor
   - GenericServerSensor
   - WebSphereIdmlSeedSensor
   - WebSphereCellSensor
   - WebSphereNodeSensor
   - WebSphereSensor (sélectionnez ce détecteur au lieu de WebSphereCellSensor et WebSphereNodeSensor uniquement si com.collation.websphere.performance.setting=false)

   Les détecteurs peuvent nécessiter l'activation de détecteurs supplémentaires dans le profil par défaut ; activez tous les détecteurs supplémentaires.

c. Sauvegardez le fichier de configuration.

7. Exécutez la reconnaissance puis sélectionnez la portée pour inclure le serveur et le profil de reconnaissance que vous avez créé.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes susceptibles de survenir avec le détecteur IBM WebSphere et propose des solutions à ces problèmes.

Démarrage impossible du détecteur

Problème

Le détecteur WebSphere Application Server ne démarre pas.

Solution

Pour déterminer pourquoi le détecteur WebSphere Application Server ne démarre pas, validez les critères suivants sur votre serveur WebSphere :

- Le processus WebSphere est en cours d'exécution.
- La ligne de commande n'est pas tronquée (le processus en cours d'exécution doit correspondre au modèle pour le serveur WebSphere Application Server).

  Pour les systèmes d'exploitation Windows 2003/2008, Linux, Solaris, AIX et Linux sur System z, la ligne de commande doit contenir le mot WsServer.
- WebSphere Application Server a été démarré en tant que service (sur Windows 2000), ou en tant que service ou à partir de la ligne de commande (Windows 2003 ou Windows 2008).

Si aucun des éléments précédents n'est à l'origine de l'incident, vérifiez le journal du système et les journaux de démarrage de WebSphere Application Server en recherchant les messages d'erreur.

Des noeuds ou des serveurs WebSphere ne peuvent pas être reconnus

Problème

Certains noeuds ou serveurs WebSphere ne peuvent pas être reconnus.

Solution

Quand le noeud ou serveur WebSphere à reconnaître est configuré pour utiliser FQDN à la place d'une adresse IP comme adresse d'amorce, le serveur TADDM doit avoir accès à un serveur DNS capable de résoudre ce FQDN. Sinon, les informations sur ce noeud ou serveur ne peuvent pas être reconnues, même si la portée de la cible est définie à l'aide de l'adresse IP.

La reconnaissance de WebSphere Application Server n'est pas enregistrée

Problème

La reconnaissance de WebSphere Application Server n'est pas enregistrée dans le fichier `DiscoverManager.log`. Etant donné qu'un ancrage local est utilisé pour la reconnaissance, les messages du journal sont placés dans un fichier distinct.

Solution

Les messages du journal sont placés dans les fichiers journaux suivants, où *nom_hôte* est le nom de domaine complet du serveur TADDM :

- `local-anchor*.`*`hostname`*`.WebSphereAgent.log`
- `local-anchor*.`*`hostname`*`.WebSphereNodeSensor.log`

Erreurs lorsque la sécurité est activée sur WebSphere Application Server

Problème

Les types de message d'erreur suivants s'affichent :

- ```
  ERROR cdb.WebSphereAgentDelegate - [WebSphereAgentDelegate.E.1]
  Echec de discover() avec l'exception : java.lang.Exception:
  Impossible de connecter le serveur WebSphere à
  9.48.158.37:8,880 - ADMC0016E:
  Le système ne peut pas créer un connecteur SOAP
  pour se connecter à l'hôte 9.48.158.37 au port 8880...
  ```
- ```
  ERROR cdb.WebSphereJMXUtils - Une erreur est survenue,
  Impossible d'établir une connexion au référentiel.
  Utilisation des droits d'accès raleigh-was60 :
  com.ibm.websphere.management.exception.AdminException:
  javax.management.JMRuntimeException: ADMN0022E:
  Accès refusé pour l'opération getServerConfig sur le
  Mbean FileTransferServer car les droits d'accès sont
  insuffisants ou vides.
  ```

Ces erreurs peuvent survenir pour l'une des raisons suivantes :

- Aucun droit d'accès n'existe dans la liste d'accès pour le WebSphere Application Server.
- Dans les droits d'accès du WebSphere Application Server, les certificats ne sont pas corrects ou n'ont pas été saisis dans la liste d'accès.
- Dans les droits d'accès du WebSphere Application Server, le mot de passe est incorrect.

Solution

Ajoutez les droits d'accès dans la liste d'accès pour le WebSphere Application Server. Corrigez les certificats, entrez les certificats via la liste d'accès, ou fournissez le mot de passe correct.

Echec d'établissement d'une connexion JMX

Problème

Le type d'erreur suivant se produit :

```
Sensor failed in remote server:
Unable to connect to WebSphere server at 10.0.1.69:8880 - ADMC0016E:
Could not create SOAP Connector to connect to host 10.0.1.69 at port 8880
```

Ce type d'erreur indique les incidents suivants :

- Un certificat manquant ou incorrect ou un ID utilisateur et un mot de passe incorrects. L'exemple suivant illustre une cause fondamentale :

  ```
  [SOAPException: faultCode=SOAP-ENV:Client;
  msg=Error opening socket:
  javax.net.ssl.SSLHandshakeException: certificate expired;
  targetException=java.lang.IllegalArgumentException:
  Error opening socket:
  javax.net.ssl.SSLHandshakeException: certificate expired]
  ```

- Un pare-feu qui bloque une connexion au WebSphere Application Server via le port SOAP.
- Le WebSphere Application Server peut ne pas se trouver dans l'état requis, même si le processus s'affiche dans la table de processus ou la liste des services Windows. Pour tester l'état du serveur d'application WebSphere, essayez de vous connecter à ce serveur à l'aide de l'utilitaire administratif wsadmin WebSphere. Si le wsadmin rencontre un échec, c'est que le détecteur a également des problèmes.

Solution

Utilisez l'une des solutions suivantes :

- Exécutez l'un des programmes suivants, qui teste la connexion JMX afin de vérifier les droits d'accès et la connectivité :
  - Pour les systèmes d'exploitation Linux, AIX, et Linux on System z : $*COLLATION_HOME*/bin/testwasconnection.sh. Les instructions d'exécution de ce programme se trouvent dans le fichier testwasconnection.sh.
  - Pour les systèmes Windows : *%COLLATION_HOME%*\bin\ testwasconnection.bat. Les instructions d'exécution de ce programme se trouvent dans le fichier testwasconnection.bat.
- Vérifiez que votre liste d'accès est correctement définie. Si vous reconnaissez WAS on z/OS et voulez utiliser une entrée de liste d'accès avec une restriction de portée, vous devez inclure l'adresse IP de votre serveur WebSphere dans la portée de reconnaissance en plus de l'adresse IP de l'hôte où se trouve le fichier de départ de WebSphere.

Echec du détecteur sur une requête JMX

Problème

Le détecteur échoue sur une requête JMX avec le message suivant :

```
failed on JMX query--check server health and retry
```

Cette erreur indique que l'installation de la configuration pourrait être endommagée.

Solution

Contrôlez les journaux pour identifier les requêtes et déterminer si les valeurs sont lisibles dans la console WebSphere Application Server. Cette erreur se produit généralement parce que la reconnaissance s'effectue durant la nuit et que les serveurs WebSphere Application Server sont désactivés pour des besoins de maintenance. Dans ce cas, redémarrez le serveur et essayez à nouveau d'effectuer une reconnaissance.

Erreur de magasin de données - le stockage des données collectées prend trop de temps

Problème

Le stockage des données collectées suite à une reconnaissance WebSphere prend trop de temps.

Solution

Le script d'optimisation de la base de données n'a pas été exécuté avant la création de schéma TADDM. Avant de créer le schéma TADDM, exécutez le script d'optimisation de base de données suivant :

- Pour les systèmes autres que Windows :

  `$COLLATION_HOME/bin/gen_db_stats.jy`

- Pour les systèmes Windows :

  `%COLLATION_HOME%\bin\gen_db_stats.bat`

WebSphere Application Server est arrêté

Problème

Le WebSphere Application Server est arrêté pour l'une des raisons suivantes :

- TADDM s'exécute lorsque WebSphere Application Server est en cours de maintenance, la reconnaissance ne se terminant pas. Le fichier `local-anchor*.hostname.WebSphereAgent.log` ou le fichier `local-anchor*.hostname.WebSphereNodeSensor.log` affiche peut-être le message d'erreur suivant :

  ```
  INFO cdb.AnchorServer[main] - [AnchorServer.I.0] le serveur n'accepte plus de nouvelles connexions
  ```

- Un message d'erreur indique que la requête ne peut pas être achevée.

Solution

Vérifiez que WebSphere Application Server fonctionne correctement.

Le détecteur n'affiche pas autant de données que dans les éditions précédentes de TADDM

Problème

La fenêtre Caractéristiques des cellules, noeuds et serveurs WebSphere n'affiche pas autant de détails que dans les versions précédentes de TADDM, la plupart des onglets ne comportant aucune donnée.

Solution

TADDM implémente les niveaux de reconnaissance suivants :

- Superficielle
- Moyenne
- Approfondie

Le niveau de reconnaissance par défaut pour le détecteur de WebSphere Application Server est "superficielle".

Pour obtenir davantage de détails sur WebSphere Application Server, créez une configuration de détecteur de reconnaissance pour le détecteur WebSphereCellSensor, et, dans la fenêtre de configuration du détecteur, définissez la valeur de la propriété mediumDiscoveryLevel ou deepDiscoveryLevel sur true.

Le détecteur WebSphere échoue au cours de la reconnaissance WebSphere sur un système d'exploitation AIX en raison de problèmes liés à la commande ps d'AIX

Problème

Sous certains systèmes d'exploitation AIX, l'exécution de la commande UNIX **ps** renvoie des chaînes Java CLASSPATH tronquées. Les chaînes ne sont pas reconnues par le détecteur WebSphere TADDM, ce qui se traduit par l'échec de la reconnaissance.

Solution

Mettez le système à niveau au moins vers la version AIX 5.3. FP5 (5.3.0.50). Cette version et les versions ultérieures d'AIX retournent les chaînes Java CLASSPATH entières.

Le message CTJDT0736W s'affiche

Problème

Les autorisations d'accès qui existent dans la liste d'accès sont insuffisantes pour le protocole Secure Shell (SSH) ou pour Windows Management Instrumentation (WMI) dans le système hôte où s'exécute le noeud distribué.

L'accréditation du système informatique pour ce système hôte est utilisée pour extraire les informations pour renseigner l'hôte sur les éléments de configuration de noeud et de serveur sur ce système.

Solution

Si vous souhaitez que ces informations soient renseignées, vous devez ajouter l'accréditation de système informatique appropriée pour ce système hôte.

Echec du détecteur WebSphere avec affichage du message suivant : CTJTD0692E

Problème

En tentant de reconnaître une cellule WebSphere distribuée, le détecteur WebSphere échoue avec le message suivant :

```
CTJTD0692E The distributed cell deployment manager bind address is not
found for the following cell:etabsap1TCell
```

Solution

Les reconnaissances impliquant les détecteurs liés au Gestionnaire de déploiement WebSphere doivent disposer d'un DNS opérationnel. Pour résoudre ce problème, définissez la valeur de `com.collation.platform.os.disableRemoteHostDNSLookups` sur true, et assurez-vous que le serveur TADDM dispose toujours du chemin d'accès à la recherche DNS correct.

Le détecteur WebSphere échoue et le message suivant s'affiche : CTJTD3021E

Problème

Le détecteur WebSphere échoue et affiche le message suivant :

```
CTJTD3021E Le détecteur a échoué dans un serveur distant :
 CTJTD2120E Une erreur s'est produite dans le processus de reconnaissance. :
CTJTD0775E Une connexion au serveur WebSphere n'est pas
 disponible : << adresse ip d'IBM WebSphere Application Server >>
 - ADMC0016E : Le système ne peut pas créer un connecteur SOAP pour se connecter
    à l'hôte
<< adresse ip d'IBM WebSphere Application Server >> >>
```

Solution

Vérifiez que le problème est avec le support SSL dans le code client WebSphere. Pour vérifier, assurez-vous que l'entrée de liste d'accès WebSphere pour ce serveur WebSphere est la première dans la liste d'accès (avant toute autre autorisation d'accès WebSphere). Si la reconnaissance réussit, importez dans un fichier de clés certifiées tous les certificats de WebSphere à partir des différents serveurs. Des entrées de liste d'accès multiples avec des ID utilisateur et des mots de passe différents sont acceptées. Cependant, toutes les entrées de liste d'accès doivent indiquer le même fichier de clés certifiées, qui contient tous les certificats.

Pour plus d'informations, voir «Configuration de la liste d'accès», à la page 77.

Le détecteur de pilote JDBC WebSphere ne démarre pas

Problème

Le détecteur de pilote JDBC WebSphere ne démarre pas.

Solution

Pour comprendre pourquoi le détecteur de pilote JDBC WebSpherene démarre pas, vérifiez que les conditions suivantes ont été remplies :

- Un profil utilisateur pour la reconnaissance de niveau 3 a été créé et le détecteur de pilote JDBC WebSphere est activé.
- La reconnaissance profonde est activée pour le détecteur de cellule WebSphere.

Le détecteur de pilote JDBC WebSphere ne peut pas se connecter à l'hôte cible et le message suivant apparaît : CTJTD0796E

Problème

Lors de la reconnaissance, le détecteur de pilote JDBC WebSphere ne peut pas établir de connexion à l'hôte cible et le message d'erreur CTJTD0796E s'affiche.

Solution

Les situations suivantes peuvent être à l'origine de cette erreur :

- La connexion SSH n'a pas pu être établie avec l'hôte.
- Une connexion à l'hôte a été établie mais l'utilisateur n'avait pas les droits appropriés pour exécuter le script WebSphere **setupCmdLine**.
- Une connexion avec l'hôte a été établie, mais l'utilisateur ne possède pas les privilèges appropriés pour exécuter la commande **Java**.

Vous devez consulter les fichiers journaux du détecteur pour déterminer quelle situation s'est produite.

Si le détecteur échoue et que l'avertissement CTJTD0798W s'affiche dans les fichiers journaux, vérifiez que l'utilisateur indiqué dans l'entrée de liste d'accès WebSphere SSH possède les droits appropriés pour exécuter le script WebSphere **setupCmdLine**.

Si le détecteur échoue et que l'avertissement CTJTD0799W apparaît dans les fichiers journaux, vérifiez que l'utilisateur indiqué dans l'entrée de liste d'accès WebSphere SSH possède les droits appropriés pour exécuter la commande **Java**.

Certaines dépendances JDBC ne sont pas créées entre un serveur WebSphere et des serveurs de base de données

Problème

TADDM reconnaît le serveur WebSphere et un serveur associé de base de données mais ne crée pas de relation entre eux. Une telle relation est basée sur les propriétés de connexion JDBC qui sont définies sur le serveur d'applications.

Solution

Le problème peut être causé par l'un des cas suivants :

- Les informations sur la connectivité JDBC sont collectées par des reconnaissances profondes uniquement. Assurez-vous que le profil de reconnaissance pour le détecteur WebSphere est configuré pour ce niveau de reconnaissance.
- Les dépendances sont créées par l'agent JDBCDependencyAgent qui s'exécute dans le groupe d'agents de topologie des dépendances. Assurez-vous que l'agent est exécuté après la reconnaissance des serveurs WebSphere.
- JDBCDependencyAgent traite uniquement les serveurs d'applications récemment reconnus. Si certaines dépendances sont toujours manquants une fois que l'agent a été exécuté, relances la reconnaissance des serveurs WebSphere, et attendez que les agents de topologie s'exécutent de nouveau.
- Assurez-vous que le serveur de base de données prend en charge la création de dépendances transactionnelles entre lui et le serveur d'applications WebSphere. Les bases de données suivantes sont prises en charge :
  - Oracle
  - IBM DB2
  - Microsoft SQL Server
  - Sybase

Echec du détecteur WebSphere lorsque le serveur TADDM exécute Red Hat Enterprise Linux 6

Problème

Echec du détecteur WebSphere lorsque le serveur TADDM exécute Red Hat Enterprise Linux 6. Les erreurs suivantes peuvent s'afficher :

```
CTJTD3021E The sensor fails in a remote server
CTJTD2015E There is a local anchor sensor failure
```

Solution

Dans le fichier de configuration `/etc/security/limits.d/90-nproc.conf`, mettez en commentaire la ligne suivante :

```
*          soft    nproc     1024
```

Une fois que vous avez modifié le fichier de configuration, vous devez redémarrer le serveur TADDM.

Seuls les objets marque de réservation sont enregistrés après une reconnaissance basée sur un script

Problème

Après l'exécution d'une reconnaissance WebSphereScriptSensor réussie, tous les objets enregistrés sont marqués en tant que marque de réservation et contiennent peu de détails.

Solution

WebSphereScriptSensor crée des objets marque de réservation lorsqu'une cible de découverte est un noeud WebSphere Application Server dans une cellule distribuée autre que la cellule de gestion (un noeud DMGR). Pour plus d'informations détaillées sur les objets de modèle marque de réservation, exécutez une reconnaissance de l'hôte avec DMGR.

Détecteur de cache IBM WebSphere eXtreme Scale

Le détecteur de cache IBM WebSphere eXtreme Scale reconnaît les caches IBM WebSphere eXtreme Scale et certains de leurs composants.

Le détecteur reconnaît les éléments suivants pour le cache eXtreme Scale :

- le nom du cache,
- une liste de noeuds sur lesquels se trouve le cache.

Le détecteur reconnaît les éléments suivants pour chaque noeud eXtreme Scale :

- le nom du noeud,
- le nom d'hôte du noeud,
- le contenu du fichier de configuration principal,
- le contenu du fichier de configuration `orb.properties` pour la machine virtuelle Java qui exécute ce noeud et la version de cette machine virtuelle Java,
- le contenu des fichiers `.xml`, `.sh`, `.props` et `.properties` qui figurent dans le même répertoire comme fichier de configuration principal.

Nom du détecteur utilisé dans l'interface graphique et les journaux

WebSphereXSCacheSensor

Prérequis

IBM WebSphere eXtreme Scale doit être en cours d'exécution sur les ordinateurs cible.

Le chemin d'accès au fichier de configuration, indiqué par le paramètre `-objectgridfile`, doit être absolu.

Problèmes de sécurité

L'utilisateur doit être autorisé à exécuter les tâches suivantes :

- obtenir la liste complète de processus, dont les processus de la machine virtuelle Java, en cours d'exécution sur le système cible ;
- lire le fichier de configuration indiqué par le paramètre `-objectgridfile`, en général `objectGrid.xml` ;

- lire les fichiers XML, les fichiers scripts ou les fichiers de propriétés dans le même répertoire que le fichier de configuration indiqué par le paramètre `-objectgridfile`, si ces informations doivent être capturées ;
- exécuter la machine virtuelle Java qui exécute le noeud eXtreme Scale avec le paramètre `-version` afin d'obtenir des informations sur la version de l'environnement d'exécution ;
- lire le fichier de configuration `orb.properties` figurant dans le répertoire `lib` de la machine virtuelle Java.

Limitations

Les limitations suivantes s'appliquent :

- Seuls les noeuds eXtreme Scale utilisant des machines virtuelles Java comme conteneurs pour les caches eXtreme Scale sont reconnus. Les caches utilisant des applications Web spéciales comme conteneurs pour les noeuds eXtreme Scale ne sont pas reconnus.
- Les machines virtuelles Java fournissant des services de catalogue pour les noeuds eXtreme Scale ne sont pas reconnues.
- Si plusieurs processus de machine virtuelle Java sont démarrés avec le même nom de noeud et la même copie du fichier de configuration indiqué par le paramètre `-objectgridfile`, le détecteur ne reconnaît pas qu'il s'agit de noeuds distincts et ces derniers sont fusionnés.
- Le détecteur recherche uniquement des fichiers de configuration dans le même répertoire que le fichier de configuration indiqué par le paramètre `-objectgridfile`, ainsi que dans ses sous-répertoires. Seuls les fichiers avec l'une des extensions suivantes sont reconnus :
  - `.xml`
  - `.sh`
  - `.props`
  - `.properties`

  Vous ne pouvez pas configurer l'extension de fichier reconnue.
- Le détecteur n'analyse pas les fichiers de configuration mais capture l'intégralité de leur contenu.
- Lors de la vérification du paramètre `-objectgridfile`, le détecteur ignore la casse.

Objets de modèle avec attributs associés

Le détecteur de cache IBM WebSphere eXtreme Scale crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les éléments de configuration dans l'environnement IBM WebSphere.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous leur nom.

app.JVM

ExecutableName

JVMVersion

Publisher

SoftwareVersion

websphere.WebSphereXSCache

- Name

websphere.WebSphereXSCacheNode

- Name
- Host

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour l'authentification auprès du système informatique cible.

Détecteur IBM WebSphere Message Broker

Le détecteur IBM WebSphere Message Broker reconnaît l'attribution WebSphere Message Broker au niveau de l'instance du courtier, de la configuration et de l'application pour Windows et UNIX.

Nom du détecteur utilisé dans l'interface graphique et les journaux

MBServerSensor

Prérequis

Le serveur TADDM requiert les informations de connexion suivantes :

Connexion système, avec la possibilité de reconnaître l'ordinateur cible.

Vous devez être autorisé à exécuter la commande **mqsiprofile**.

Limitations

Après une reconnaissance à l'aide du détecteur IBM WebSphere Message Broker, certaines valeurs d'attribut du panneau Détails restent vides car le détecteur ne renseigne pas tous les éléments du courtier de messages. Vous trouverez la liste complète des classes et des attributs reconnus dans le dictionnaire de données du détecteur. Pour renseigner les valeurs des attributs manquants, vous pouvez utiliser d'autres fournisseurs de données, tels que Discovery Library Adapters (DLAs), ou des extensions de serveur personnalisées qui étendent les capacités de reconnaissance de TADDM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- messaging.mb.MBBroker
- messaging.mq.MQQueueManager
- messaging.mb.MBExecutionGroup
- messaging.mb.MBHTTPListenerProperties
- messaging.mb.MBHTTPConnectorProperty
- messaging.mb.MBHTTPSConnectorProperty

- messaging.mb.MBHTTPListenerProperty
- messaging.mb.MBBrokerSecurity
- messaging.mb.MBBrokerProfile
- messaging.mb.MBMessageFlow
- messaging.mb.MBMessageFlowNode
- messaging.mb.MBBarFile
- messaging.mb.MBProperty

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Si vous souhaitez modifier le niveau de reconnaissance, mettez à jour le profil de reconnaissance du détecteur IBM WebSphere Message Broker.

Pour modifier le niveau de reconnaissance par défaut de ce détecteur, procédez comme suit :

1. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
2. Dans la fenêtre Créer un profil, entrez le nom et la description du profil, puis cliquez sur **OK**.
3. Dans la liste de détecteurs, cliquez sur **MBServerSensor**, puis sur **Nouveau**.
4. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration du détecteur MBServerSensor.
5. Dans la section **Configuration** de la fenêtre Création de configuration, sélectionnez l'une des options suivantes pour modifier les options de reconnaissance :
   - Pour utiliser les données d'identification du système d'exploitation afin d'activer la reconnaissance, cliquez deux fois sur la valeur de **useHostAuth** et remplacez *false* par *true*
   - Pour reconnaître les attributs de noeud de flux de messages WebSphere, cliquez deux fois sur la valeur de **useNodeLevel** et remplacez *false* par *true*
6. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
7. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.
8. Sélectionnez ce profil de reconnaissance lors de l'exécution d'une reconnaissance.

Pour plus d'informations sur les profils de reconnaissance, voir la rubrique *Utilisation de profils de reconnaissance* dans le *Guide d'utilisation* de TADDM.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises pour configurer la liste d'accès.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Serveurs de messagerie** comme **Type de composant**.
2. Sélectionnez WebSphere Message Broker comme **fournisseur**.
3. Indiquez les informations requises suivantes :
   - Nom d'utilisateur
   - Mot de passe

Vous devez être autorisé à exécuter la commande **mqsiprofile**.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.platform.os.UnixOs.forcedServerList=bipbroker
Cette propriété oblige le processus bipbroker à démarrer le détecteur sur la plateforme UNIX.

com.collation.platform.os.WindowsOs.forcedServerList=bipservice
Cette propriété oblige le processus bipservice à démarrer le détecteur sur la plateforme Windows.

com.collation.platform.os.AixOs.forcedServerList=bipbroker

Cette propriété oblige le processus bipbroker à démarrer le détecteur sur la plateforme AIX.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM WebSphere Message Broker et propose des solutions à ces problèmes.

Le détecteur ne démarre pas

Problème
Le détecteur WebSphere Message Broker ne démarre pas.

Solution
Assurez-vous que le nom de processus bipbroker est ajouté à la propriété `com.collation.platform.os.UnixOs.forcedServerList` dans le fichier collation.properties.

Détecteur IBM WebSphere MQ Server

Le détecteur IBM WebSphere MQ Server reconnaît IBM WebSphere MQ servers.

Nom du détecteur utilisé dans l'interface graphique et les journaux

MQServerSensor

Problèmes de sécurité

Le serveur TADDM requiert les informations de connexion suivantes :

- Connexion système, avec la possibilité de reconnaître l'ordinateur cible.
- Pour le serveur WebSphere MQ sur un système UNIX, le mot de passe et le nom de l'utilisateur WebSphere MQ permettant d'accéder à la console MQSC.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.messaging.mq.MQChannel
- app.messaging.mq.MQClientConnectionChannel

- app.messaging.mq.MQCluster
- app.messaging.mq.MQClusterReceiverChannel
- app.messaging.mq.MQClusterSenderChannel
- app.messaging.mq.MQInstallation
- app.messaging.mq.MQListener
- app.messaging.mq.MQNameList
- app.messaging.mq.MQQueueManager
- app.messaging.mq.MQRequesterChannel
- app.messaging.mq.MQServerChannel
- app.messaging.mq.MQTCPListener
- app.ProcessPool

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur IBM WebSphere MQ Server ne prend en charge qu'une reconnaissance basée sur un script ou asynchrone. Il n'exécute pas de reconnaissances régulières.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone ou basée sur un script, le détecteur ne nécessite aucune configuration.

Limitations

La reconnaissance de descripteur d'application n'est pas prise en charge.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Décrit les informations d'accès requises pour des installations UNIX et Windows.

Prérequis

Pour les systèmes Windows, l'utilisateur doit appartenir au groupe d'administrateurs Windows pour exécuter la commande **runmqsc**.

Pour les systèmes UNIX, l'utilisateur WebSphere MQ dispose des droits appropriés pour exécuter la **runmqsc**.

Configurez la liste d'accès comme suit :

1. Sélectionnez **Serveurs de messagerie** comme **Type de composant**.
2. Sélectionnez **WebSphere MQ** comme **Fournisseur**.

Les systèmes Windows nécessitent les informations suivantes :

- Nom d'utilisateur
- Mot de passe

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.platform.os.UnixOs.forcedServerList=amqzxma0
Cette propriété oblige le processus aqmzxma0 à démarrer le détecteur.

com.collation.topobuilder.mq.clusterrelations=true
Cette propriété permet de créer des dépendances basées sur l'appartenance à un cluster. Chaque gestionnaire de file d'attente du cluster est doté de deux dépendances (une en tant que source et l'autre en tant que cible) à tous les autres gestionnaires de file d'attente de ce même cluster.

Si aucune valeur n'est définie, la valeur par défaut est false.

com.collation.topobuilder.mq.channelrelations=true
Cette propriété permet de créer des dépendances basées sur les noms de canaux émetteur-récepteur. Si aucune valeur n'est définie, la valeur par défaut est false.

Limitation : Cette fonction est disponible uniquement si les noms de canaux se composent du nom du gestionnaire source et celui du gestionnaire cible. Si tel n'est pas le cas, il n'est pas possible de créer un caractère générique pour la propriété com.collation.topobuilder.mq.channelnaming.

com.collation.topobuilder.mq.checkreceiverchannelname=true
Si cette propriété est définie à true, la dépendance est définie uniquement s'il existe un canal récepteur dont le nom correspond au nom du canal émetteur sur le gestionnaire cible. La valeur par défaut est false.

com.collation.topobuilder.mq.channelnaming=<REGULAR EXPRESSION>
Cette propriété vous permet de spécifier des règles d'affectation de noms de canaux personnalisés pour créer des dépendances de canal. REGULAR_EXPRESSION doit renvoyer deux groupes nommés :

- Le premier correspond au nom du gestionnaire source.
- Le second correspond au nom du gestionnaire de file d'attente cible.

Si l'affectation de nom de canal personnalisé ne comporte pas le nom du gestionnaire de file d'attente source, par exemple TO.TARGET_MANAGER, le premier groupe peut être défini à une valeur vide, telle que ()TO.(.*). Dans ce cas, le nom du gestionnaire de file d'attente source n'est pas comparé au nom du gestionnaire de file d'attente parent du canal émetteur.

Si aucune valeur n'est définie, la valeur par défaut pour <REGULAR_EXPRESSION) est CH\\.(.*?)\\.TO\\.(.*

Les propriétés suivantes sont utilisées pour générer des noms d'affichage pour le gestionnaire de file d'attente.

com.collation.discover.agent.MQQueueManager.Use ListenningIp=true
Définit le nom de l'élément QueueManager ; la valeur par défaut est false.

<FQDN>:<QUEUE_MANAGER_NAME> - Le premier nom de domaine complet ou la première adresse IP non vide du premier MQListener en mode écoute est utilisé(e)

com.collation.discover.agent.MQQueueManager.UseIpFromConnections=true
La valeur par défaut est false.

<FQDN>:<QUEUE_MANAGER_NAME> - Le premier nom de domaine complet non vide (ou la première adresse IP non vide) récupéré(é) de l'attribut LOCLADDR de l'élément ServerConnection est utilisé(e).

com.collation.discover.agent.MQQueueManager.UseEmptyHostName=true
Si le nom de domaine complet n'est pas défini, le premier nom de domaine complet non vide (ou la première adresse IP non vide) récupéré(é) de l'attribut LOCLADDR de l'élément ClientConnection est utilisé(e). La valeur par défaut est false.

<QUEUE_MANAGER_NAME> - Le nom de l'élément QueueManager sans le nom de domaine complet est utilisé.

com.collation.topobuilder.mq.removerelations
Si aucune valeur n'est définie, la valeur par défaut est false. Lorsque la valeur définie est true, les dépendances pour le gestionnaire de file d'attente WebSphere MQ sont supprimées si l'état est autre que en cours d'exécution.

Si aucune propriété mentionnée ci-dessus n'a la valeur true (UseListenningIp ou UseIpFromConnections n'a pas résolu le nom de domaine complet), le nom de domaine complet de l'hôte parent est utilisé.

<HOST_FQDN>:<QUEUE_MANAGER_NAME>

Les propriétés suivantes permettent d'indiquer que le détecteur doit utiliser la commande **sudo** lors de l'exécution de commandes MQ sur le serveur.

com.collation.discover.agent.MqServerAgent.versionCommand=sudo -u *utilisateur*
Indique que le détecteur doit utiliser **sudo** avec le nom d'utilisateur spécifié lors de l'exécution de la commande MQ **version**.

com.collation.discover.agent.MqServerAgent.statusCommand=sudo -u *utilisateur*
Indique que le détecteur doit utiliser **sudo** avec le nom d'utilisateur spécifié lors de l'exécution de la commande MQ **dspmq**.

com.collation.discover.agent.MqServerAgent.mqscCommand=sudo -u *utilisateur*
Indique que le détecteur doit utiliser **sudo** avec le nom d'utilisateur spécifié lors de l'exécution de la commande MQ **runmqsc**.

Chacune des propriétés précédente peut être sectorisée pour un type de système d'exploitation donné, une adresse IP particulière ou les deux, comme dans l'exemple suivant :

```
com.collation.discover.agent.MqServerAgent.mqscCommand.Linux.1.2.3.4=sudo -u mqm
```

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM WebSphere MQ Server et propose des solutions à ces problèmes.

Démarrage impossible du détecteur

Problème
Le détecteur WebSphere MQ Server ne démarre pas.

Solution
Assurez-vous que le nom de processus `amqzxma0` est ajouté à la propriété `com.collation.platform.os.UnixOs.forcedServerList` dans le fichier `collation.properties`.

Le détecteur se lance, mais ne détecte pas toute l'information via la reconnaissance IBM Tivoli Monitoring discovery

Problème

La détection du détecteur WebSphere MQ via IBM Tivoli Monitoring a été effectuée correctement, mais toutes les informations n'ont pas été découvertes.

Solution

Vérifiez sur l'hôte cible que l'utilisateur pour lequel l'agent IBM Tivoli Monitoring s'exécute est ajouté au groupe `mqm`.

Détecteur iPlanet serveur

Le détecteur de serveur iPlanet reconnaît les serveurs Web iPlanet.

Nom du détecteur utilisé dans l'interface graphique et les journaux

IPlanetServerSensor

Prérequis

Le compte de service TADDM doit disposer de ce qui suit :

- Droits d'exécution sur le fichier binaire iPlant, soit **ns-httpd** soit **webserd**.
- Accès en lecture aux fichiers de configuration iPlanet

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.SoftwareContainer
- app.SoftwareModule
- app.StaticContentModule
- app.web.CGIScript
- app.web.iplanet.IPlanetJSP
- app.web.iplanet.IPlanetJVMSettings
- app.web.iplanet.NSAPIPlugin
- app.web.iplanet.IPlanetServer
- app.web.iplanet.IPlanetServlet
- app.web.iplanet.IPlanetSSLSettings
- app.web.iplanet.IPlanetVirtualHost
- app.web.iplanet.IPlanetWebContainer
- app.web.iplanet.WebLogicConnection
- app.web.WebConnection
- sys.DataFile sys.Directory

Détecteur JBoss server

Le détecteur JBoss reconnaît la version d'une installation JBoss et collecte des données pour le serveur. Il permet de reconnaître JBoss AS versions 4, 5 et 6.

Nom du détecteur utilisé dans l'interface graphique et les journaux

JBossVersionSensor, JBossSensor

Prérequis

Les conditions suivantes doivent être remplies :

- La reconnaissance du système informatique doit s'effectuer correctement.
- JMX doit être activé sur le serveur JBoss ;
- Si la console JMX est protégée par mot de passe, les informations d'identification doivent être entrées dans la liste d'accès.

Le détecteur JBoss nécessite des fichiers JAR qui font partie de l'installation JBoss Server. Vous devez copier les fichiers JAR dans les répertoires suivants (`$COLLATION_HOME`) du serveur TADDM.

Pour JBoss AS 4 :

- `lib/jboss/402/jbossall-client.jar, lib/jboss/402/jnpserver.jar`
- `lib/jboss/402/jboss-jmx.jar`

Pour JBoss AS 5 :

- `lib/jboss/5/jboss-client.jar`
- `lib/jboss/5/jnp-client.jar`
- `lib/jboss/5/jboss-logging-spi.jar`
- `lib/jboss/5/jboss-security-spi.jar`
- `lib/jboss/5/jboss-common-core.jar`
- `lib/jboss/5/jboss-javaee.jar`
- `lib/jboss/5/jmx-invoker-adaptor-client.jar`
- `lib/jboss/5/jbosssx-client.jar`
- `lib/jboss/5/jboss-integration.jar`
- `lib/jboss/5/jboss-serialization.jar`
- `lib/jboss/5/jboss-remoting.jar`
- `lib/jboss/5/jboss-jca.jar`

Pour JBoss AS 6 :

- `lib/jboss/6/jboss-client.jar`
- `lib/jboss/6/jnp-client.jar`
- `lib/jboss/6/jboss-logging.jar`
- `lib/jboss/6/jboss-security-spi.jar`
- `lib/jboss/6/jboss-common-core.jar`
- `lib/jboss/6/jmx-invoker-adaptor-client.jar`
- `lib/jboss/6/jbosssx-client.jar`
- `lib/jboss/6/jboss-integration.jar`
- `lib/jboss/6/jboss-serialization.jar`
- `lib/jboss/6/jboss-remoting.jar`
- `lib/jboss/6/jboss-jca.jar`

Limitations

Important : JBoss AS 6 est pris en charge à partie de TADDM 7.2.2 Groupe de correctifs 1.

Si la reconnaissance d'une version de JBoss via une connexion JMX échoue, JBossVersionSensor utilise la session SSH pour la reconnaissance. Le détecteur ne reconnaît pas le contenu de JBoss et les objets de modèle ne sont pas créés.

Pour JBoss ManagedConnectionFactories, le propriétés de la source de données JDBC XA ne sont pas reconnues par le détecteur. Par conséquent, les dépendances transactionnelles entre le serveur JBoss et les serveurs de base de données qui sont dénotés par de telles sources de données ne sont pas créées.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppServer
- app.j2ee.J2EEServer
- app.j2ee.jboss.JBossCluster
- app.j2ee.jboss.JBossDomain
- app.j2ee.jboss.JBossJMSServer
- app.j2ee.jboss.JBossServer

Configuration du détecteur

Vous devez configurer le détecteur JBoss Server avant d'exécuter une reconnaissance de l'installation JBoss.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Vous devez disposer des informations suivantes :

- entrée de la liste d'accès pour le système informatique exécutant le serveur JBoss ;
- entrée de la liste d'accès pour la console JMX du serveur JBoss, en cas de protection par mot de passe.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.ibm.cdb.discover.jbossversion.sockettimeout
: Cette propriété indique une valeur d'expiration de délai d'un socket (en millisecondes) pour JBossVersionSensor.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur JBoss et propose des solutions à ces problèmes.

JBossVersionSensor ne démarre pas

Problème

Le détecteur JBossVersionSensor ne démarre pas.

Solution

- Accédez à `http://`*`adresseIP`*`:`*`portWeb`*`/jmx-console` et faites défiler la console pour vérifier si la console JMX du serveur JBoss est activée.
- Assurez-vous que lsof fonctionne correctement.

Bibliothèques JBoss introuvables

Problème

Lorsque vous exécutez le détecteur, le message `Bibliothèques JBoss non trouvées` s'affiche.

Solution

Assurez-vous que les fichiers JAR JBoss de votre version de serveur JBoss sont présents dans le répertoire `dist`, et que l'accès en lecture est activé pour l'utilisateur.

Certaines dépendances JDBC ne sont pas créées entre un serveur JBoss et des serveurs de base de données

Problème

TADDM reconnaît le serveur JBoss et un serveur associé de base de données mais ne crée pas de relation entre eux. Une telle relation est basée sur les propriétés de connexion JDBC qui sont définies sur le serveur d'applications.

Solution

Le problème peut être causé par l'un des cas suivants :

- Les dépendances sont créées par l'agent JDBCDependencyAgent qui s'exécute dans le groupe d'agents de topologie des dépendances. Assurez-vous que l'agent est exécuté après la reconnaissance des serveurs JBoss.
- JDBCDependencyAgent traite uniquement les serveurs d'applications récemment reconnus. Si certaines dépendances sont toujours manquants une fois que l'agent a été exécuté, relances la reconnaissance des serveurs JBoss, et attendez que les agents de topologie s'exécutent de nouveau.
- Assurez-vous que le serveur de base de données prend en charge la création de dépendances transactionnelles entre lui et le serveur d'applications JBoss. Les bases de données suivantes sont prises en charge :
  - Oracle
  - IBM DB2
  - Microsoft SQL Server
  - Sybase

Echec de JBossVersionSensor avec le message d'erreur "CTJTD0030E Une erreur s'est produite lors de l'exécution de ./run.bat -V".

Problème

JBossVersionSensor échoue et le message d'erreur suivant peut être trouvé dans des journaux :

- Pour JBoss AS sous Windows:

  ```
  ERROR sensor.JBossVersionSensor - CTJTD1573E An error occurred while
  executing ./run.bat -V: com.collation.platform.os.OsException:
  '.' is not recognized as an internal or external command,.
  ```

- Pour JBoss AS sous Linux:

  ```
  ERROR sensor.JBossVersionSensor - CTJTD1573E An error occurred while
  executing ./run.sh -V: com.collation.platform.os.OsException:
  '.' is not recognized as an internal or external command,.
  ```

Solution

JBossVersionSensor n'a pas été en mesure de détecter la version de JBoss AS parce que le chemin d'accès complet du script `run.bat` ou `run.sh` n'a pas été fourni avant le démarrage du serveur d'applications. Copiez les bibliothèques JBoss requises (fichier JAR) dans le répertoire `$COLLATION_HOME/lib/jboss` pour activer une détection de version via JMX. Sans ces bibliothèques, le détecteur de serveur JBoss n'enregistre aucun objet de modèle. Voir la section «Prérequis», à la page 101 pour savoir quelles bibliothèques sont à copier.

Détecteur JBoss Application Server 7

Le détecteur JBoss Application Server 7 reconnaît une configuration JBoss AS pour JBoss AS 7.0 et ultérieur.

Le détecteur reconnaît des serveurs JBoss exécutés à la fois comme des serveurs autonomes et dans un domaine géré. Chaque hôte appartenant à un domaine géré est reconnu indépendamment, en conséquence pour obtenir une image complète d'une topologie JBoss, vous devez exécuter une reconnaissance pour chacun des hôtes. Lorsqu'un environnement est reconnu pour la première fois, il est recommandé de démarrer par la reconnaissance d'un hôte qui agit comme un contrôleur de domaine JBoss, et d'exécuter ensuite une reconnaissance des membres du domaine.

Nom du détecteur utilisé dans l'interface graphique et les journaux

JBoss7Sensor

Prérequis

Un utilisateur du système d'exploitation qui exécute une reconnaissance doit avoir l'accès en lecture aux fichiers de configuration et au contenu de déploiement de JBoss. L'utilisateur doit également être en mesure d'exécuter `java`, sinon les descripteurs de déploiement ne sont pas reconnus.

Limitations

- Les applications et modules qui sont déployés sur un serveur autonome en plaçant le contenu du déploiement dans le dossier des déploiements (déploiement du système de fichiers) ne sont pas reconnus par le détecteur. Seuls les applications et modules déployés à l'aide des API de gestion de JBoss AS (la ligne de commande ou l'interface Web) sont pris en charge.
- La reconnaissance du type de déploiement dépend de la recherche de fichiers descripteur spécifiques dans le contenu du déploiement. Si aucun de ces descripteurs n'est trouvé, un type général J2EEDeployedObject est affecté à un objet de modèle qui est enregistré par le détecteur.

Objets de modèle créés

Le détecteur crée des objets de modèle des types suivants :

- app.j2ee.jboss.JBossDomain
- app.j2ee.jboss.JBossHost (uniquement pour des domaines gérés)
- app.j2ee.jboss.JBossCluster (représentant des groupes de serveurs dans un domaine géré JBoss).
- app.j2ee.jboss.JBossServer
- app.ConfigFile
- app.j2ee.J2EEDeployedObject (et ses sous-types)

Les sources de données JDBC sont enregistrées comme des données étendues de JBossClusters (pour un domaine géré) ou JBossServer (pour un serveur autonome). Les descripteurs de déploiement sont enregistrés comme des données étendues de J2EEDeployedObjects.

Configuration du détecteur

Avant d'exécuter une reconnaissance, vous devez configurer le détecteur JBoss Application Server 7.

Les options de configuration du détecteur JBoss Application Server 7 sont les suivantes. Pour changer ces options, créez une configuration de détecteur personnalisée. Voir la rubrique *Création de profils de reconnaissance* dans le *Guide d'utilisation* de TADDM.

extractAllXmlDescriptors
La valeur par défaut de cette propriété est `true`.

Si cette propriété est définie à `true`, le détecteur reconnaît tous les fichiers dont l'extension est `.xml` dans les répertoires `META-INF` et `WEB-INF` des applications ou modules déployés sous JBoss. Si cette propriété est définie à `false`, la propriété `descriptorsToExtract` est utilisée.

descriptorsToExtract
Cette propriété spécifie une liste séparée par des espaces de fichiers qui sont reconnus pour des déploiements JBoss si la propriété `extractAllXmlDescriptors` est définie à `false`. Par exemple, `META-INF/application.xml WEB-INF/web.xml`. Les caractères génériques ne sont pas autorisés.

extractSubmodules
La valeur par défaut de cette propriété est `false`.

Si cette propriété est définie à `true` et si un déploiement est une application Java Platform Enterprise Edition (JPEE) sous la forme d'un fichier d'archive d'entreprise (EAR), le détecteur reconnaît des descripteurs de ce déploiement et de ses modules, par exemple à partir de fichiers JAR ou WAR. Si cette propriété est définie à `false`, les descripteurs issus des sous-modules du déploiement ne sont pas reconnus.

Remarque : Pour reconnaître des modules d'un fichier d'archive d'entreprise (EAR), vous devez extraire son `META-INF/application.xml`. Cela signifie que la propriété `extractAllXmlDescriptors` doit être définie à `true` ou que la valeur de la propriété `descriptorsToExtract` doit inclure `META-INF/application.xml`.

Fix Pack 1 **tagsToMask**
La valeur par défaut de cette propriété est 'password'.

Cette propriété indique une liste de balises XML séparée par des espaces. Tout contenu textuel de ces balises dans les fichiers découverts est marqué par des astérisques.

Configuration des entrées du fichier `collation.properties` :

Vous pouvez configurer les entrées du fichier `collation.properties` pour ajuster des commandes utilisées par le détecteur de JBoss Application Server 7.

com.ibm.cdb.discover.sensor.app.j2ee.jboss7.java ou com.collation.discover.agent.command.java
est un fichier exécutable `java`. Si cette commande n'est pas définie, le détecteur utilise le `java` par défaut sur un hôte reconnu (celui qui est présent dans système `$PATH`). En cas d'échec, `java` qui exécute le JBoss AS reconnu, est alors utilisé.

com.ibm.cdb.discover.sensor.app.j2ee.jboss7.pwdx ou com.collation.discover.agent.command.pwdx
indique le répertoire de travail en cours d'un processus (pour des systèmes UNIX uniquement).

La valeur par défaut est `pwdx`.

com.ibm.cdb.discover.sensor.app.j2ee.jboss7.ps.full ou com.collation.discover.agent.command.ps.full
répertorie tous les processus d'exécution dans un format complet (pour des systèmes UNIX uniquement).

La valeur par défaut est `ps -ef`, sauf pour le système d'exploitation Solaris pour qui la valeur par défaut est `/usr/ucb/ps auxww`.

Configuration de la reconnaissance asynchrone :

Vous pouvez modifier les paramètres par défaut si vous voulez exécuter le détecteur JBoss Application Server 7 en mode de reconnaissance asynchrone.

Les configurations de détecteur personnalisées ne sont pas lues lorsqu'un package de reconnaissance asynchrone est préparé. Si vous devez utiliser une configuration autre que celle par défaut, modifiez la configuration dans le fichier `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.j2ee.jboss7_<version>/plugin.xml`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur JBoss Application Server 7 et propose des solutions à ces problèmes.

Un domaine géré est dupliqué

Problème
Lorsque plusieurs hôtes qui appartiennent au même domaine géré JBoss sont reconnus simultanément pour la première fois, des doublons pourraient être créés dans la base de données de TADDM.

Solution
Exécutez à nouveau une reconnaissance du domaine JBoss. Les doublons sont fusionnés.

Pour éviter un tel problème à l'avenir, reconnaissez tout d'abord un hôte qui agit comme un contrôleur de domaine JBoss, puis exécutez une reconnaissance des membres du domaine.

Pas de reconnaissance des déploiements ou des sources de données JDBC, ou des deux

Problème

Les déploiements ou les sources de données ou les deux ne sont pas tous présents dans la base de données TADDM après la reconnaissance de certains hôtes qui appartiennent à un domaine JBoss géré.

Solution

Bien que JBoss AS propage automatiquement les déploiements et sources de données JDBC sur un domaine géré, la totalité des informations les concernant ne pourraient être accessible que sur un hôte qui agit comme un contrôleur de domaine JBoss. Pour obtenir une image complète d'un environnement JBoss, tous les hôtes qui constituent le domaine doivent être reconnus, notamment le contrôleur de domaine.

Des modules d'un déploiement EAR ne sont pas reconnus

Problème

Une application JPEE (Java Platform, Enterprise Edition) de la forme d'un fichier d'archive d'entreprise (EAR) est déployé sous JBoss AS, mais le détecteur ne reconnaît pas des modules de l'application.

Solution

Configurez le détecteur pour que le descripteur `META-INF/application.xml` soit collecté. Voir «Configuration du détecteur», à la page 105.

Certaines dépendances JDBC ne sont pas créées entre un serveur ou un groupe de serveurs JBoss et des serveurs de base de données

Problème

TADDM reconnaît le serveur ou un groupe de serveurs JBoss et un serveur et un serveur de base de données associé sans créer de relation entre eux. Une telle relation est basée sur les propriétés de connexion JDBC qui sont définies sur le serveur d'applications.

Solution

Le problème peut être causé par l'un des cas suivants :

- Les dépendances sont créées par l'agent JDBCDependencyAgent qui s'exécute dans le groupe d'agents de topologie des dépendances. Assurez-vous que l'agent est exécuté après la reconnaissance de JBoss AS.
- JDBCDependencyAgent traite uniquement les serveurs d'applications récemment reconnus. Si certaines dépendances sont toujours manquantes une fois que l'agent a été exécuté, reconnaissez à nouveau de l'environnement JBoss, et attendez que les agents de topologie s'exécutent de nouveau.

Le détecteur JBoss Application Server 7 ne démarre pas

Problème

Bien que JBoss AS ait été démarré, le détecteur JBoss 7 Application Server n'est pas déclenché.

Solution

Si un serveur autonome JBoss ou un contrôleur d'hôte écoute uniquement sur une adresse de bouclage et si la propriété `com.collation.platform.os.ignoreLoopbackProcesses=true` est définie dans TADDM, le processus serveur est ignoré et le détecteur ne démarre

pas. Changez la valeur de la propriété pour `false` pour l'hôte JBoss qui n'a pas été reconnu, en procédant comme suit :

```
com.collation.platform.os.ignoreLoopbackProcesses.x.x.x.x=false
```

où *x.x.x.x* est l'adresse IP de la cible reconnue.

Détecteur de la machine virtuelle basée sur le noyau

Le détecteur de la machine virtuelle basée sur le noyau utilise la bibliothèque `libvirt` pour reconnaître l'administrateur système KVM avec la liste de machines virtuelles gérées.

Nom du détecteur utilisé dans l'interface graphique et les journaux

KvmSensor

Prérequis

Le démon `libvirt` doit être en cours d'exécution sur un hôte KVM cible.

Pour éviter des doublons qui sont générés par le détecteur de système informatique Linux et par le détecteur KVM, vous devez installer le décodeur DMI sur chacun des systèmes informatiques invités.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- KVM
- L2Interface
- ComputerSystem
- StoragePool
- StorageVolume
- UC

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

La propriété suivante indique que le détecteur utilise **`sudo`** pour élever les privilèges lors de l'exécution de la commande **`virsh`** KMV :

- `com.collation.discover.agent.kvm.systemcommand.Linux=sudo`

Vous pouvez configurer cette propriété pour une adresse IP spécifique, comme dans l'exemple suivant :

```
com.collation.discover.agent.kvm.systemcommand.Linux.192.168.1.1=sudo
```

Indiquez l'option **`sudo`** pour un système d'exploitation uniquement si elle est requise pour tous les systèmes qui utilisent ce système d'exploitation. Sinon, indiquez l'option uniquement pour les adresses IP spécifiques où la commande **`sudo`** est configurée.

Sur les systèmes cibles nécessitant une escalade des privilèges, configurez la commande **sudo** avec l'option NOPASSWD. Sinon, la reconnaissance se bloque jusqu'au dépassement du délai du serveur TADDM.

Configuration du profil de reconnaissance :

Si vous souhaitez modifier le niveau de reconnaissance, mettez à jour le détecteur KVM. Vous pouvez désactiver la reconnaissance des invités qui ne sont pas en cours d'exécution afin de reconnaître uniquement les serveurs qui sont en cours d'exécution.

Procédure

1. Dans la console de gestion de reconnaissance, cliquez sur l'icône **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil, puis cliquez sur **OK**.
4. Dans la liste des détecteurs, cliquez sur **KVMSensor**, puis cliquez sur **Nouveau**.
5. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration du détecteur KVM, puis sélectionnez la case à cocher **Activer la configuration**.
6. Dans la section **Configuration** de la fenêtre de création de configuration, pour configurer le détecteur pour reconnaître uniquement les serveurs en cours d'exécution, cliquez sur **discoverNonRunningGuests**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne, et entrez `false`.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Détecteur Microsoft Cluster

Le détecteur Microsoft Cluster reconnaît une installation en cluster de serveurs Microsoft Windows Server. Le détecteur reconnaît uniquement des clusters de serveurs (inclut un processus appelé reprise) et non les clusters Network Load Balancing. Le détecteur reconnaît les noeuds, les ressources et les groupes de ressources sur le cluster.

Nom du détecteur utilisé dans l'interface graphique et les journaux

MSClusterSensor

Prérequis

Le détecteur MS Cluster requiert :

- La reconnaissance des systèmes informatiques Windows
- Le service **ClusSvc** de Cluster Server doit être en cours d'exécution
- Si le fournisseur TADDM Windows Management Instrumentation (WMI) est utilisé, un accès en lecteur de WMI à l'espace de nom `root/mscluster` doit être accordé. Si la reconnaissance des systèmes informatiques Windows a abouti, ce droit d'accès en lecture WMI est accordé par défaut. L'accès de niveau administratif est préférable.

Limitations

La portée de la reconnaissance doit contenir l'adresse IP d'au moins un des noeuds MS Cluster ou indiquer l'adresse IP du cluster. Un noeud correspond à un ordinateur inclus dans un cluster.

Objets de modèle avec attributs associés

Le détecteur MS Cluster crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les clusters Microsoft Server Cluster de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

app.MsFailoverCluster.MsCluster

- CrossSubnetDelay
- CrossSubnetThreshold
- DefaultNetworkRole
- Description
- DisableGroupPreferredOwnerRandomization
- Domain
- EnableEventLogReplication
- HangRecoveryAction
- HangTimeout
- InternalNetwork
- LogLevel
- LogSize
- MaintenanceFile
- MaxNumberofNodes
- MaxQuorumArbitrationTime
- MinQuorumArbitrationTime
- Name
- Nodes
- PlumbAllCrossSubnetRoutes
- PublicNetworks
- QuorumLogFileSize
- QuorumPath
- QuorumType
- RegroupOpeningTimeout
- RegroupPruningTimeout
- RegroupStageTimeout
- RegroupTick
- RequestReplyTimeout
- ResourceDllDeadlockPeriod
- ResourceGroups
- Resources
- SameSubnetDelay
- SameSubnetThreshold

- SecurityLevel
- WitnessDatabaseWriteTimeout
- WitnessRestartInterval

app.MsFailoverCluster.MsClusterNode

- Description
- EnableEventLogReplication
- InitialLoadInfo
- LastLoadInfo
- Name
- NodeHighestVersion
- NodeLowestVersion
- Système

app.MsFailoverCluster.MsClusterResource

- AppServers
- CryptoCheckpoints
- DeadlockTimeout
- DebugPrefix
- DeleteRequiresAllNodes
- DependsOnResources
- Description
- HasSeparateMonitor
- IpAddresses
- IsAlivePollInterval
- IsCoreResource
- IsLocalQuorumCapable
- IsPersistentState
- IsQuorumCapable
- LooksAlivePollInterval
- Name
- PendingTimeout
- RegistryCheckpoints
- RestartAction
- RestartDelay
- RestartPeriod
- RestartThreshold
- RetryPeriodOnFailure
- Type

app.MsFailoverCluster.MsClusterResourceGroup

- AntiAffinityClassNames
- AutoFailbackType
- Description
- FailbackWindowEnd
- FailbackWindowStart
- FailoverPeriod

- FailoverThreshold
- IsPersistentState
- Name
- Parent
- Resources

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Un compte de niveau domaine membre du groupe d'administrateurs est requis. Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem (Windows)** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe).

Un compte disposant de privilèges d'administrateur doit être utilisé.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

Fix Pack 2 **com.ibm.cdb.topomgr.topobuilder.agents.MSClusterAgent.setComputerSystemMSClusterRel=false**

Cette propriété indique si l'agent MS Cluster Topology Builder Agent définit la relation entre `ComputerSystem` et `MSCluster`. Si elle est définie sur `true`, la relation est définie.

La valeur par défaut est `false`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit les problèmes classiques susceptibles de survenir avec le détecteur Microsoft cluster et propose des solutions.

Défaillance du service WMI

Problème

Le service WMI ne fonctionne pas sur la cible pendant la reconnaissance.

Solution

Vérifiez que tous les correctifs associés à WMI, y compris le correctif KB933061, ont été appliqués sur le système cible. Si l'incident n'est pas résolu, utilisez les utilitaires Microsoft suivants pour résoudre les incidents liés à WMI :

WMIDiag

L'utilitaire WMIDiag est disponible sur le site Web suivant : http://www.microsoft.com/downloads/details.aspx?familyid=d7ba3cd6-18d1-4d05-b11e-4c64192ae97d&displaylang=en

Suivez les instructions pour installer et exécuter l'utilitaire et vérifiez que WMI fonctionne correctement.

Détecteur Microsoft Exchange

Le détecteur Microsoft Exchange reconnaît les serveurs Microsoft Exchange.

Pour connaître les versions prises en charge des serveurs Microsoft Exchange, voir le document Détecteurs et systèmes cible pris en charge.

Notes :

- Dans les éditions de TADDM antérieures à la version TADDM 7.2.2, ce détecteur s'appelait détecteur *Microsoft Exchange 2007 Server*.
- Le détecteur Microsoft Exchange prend en charge uniquement une reconnaissance asynchrone et basée sur un script. Elle ne prend pas en charge des reconnaissances régulière.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ExchangeSensor

Prérequis

Le détecteur utilise les outils Exchange Management Tools fournis avec Microsoft Exchange Server 2007 etMicrosoft Exchange Server 2010.

Si vous utilisez Microsoft Exchange Server 2007 pour vérifier que les autorisations du compte utilisateur sont correctes, exécutez la commande suivante sur le serveur Exchange Server lorsque vous êtes connectés en tant que compte de reconnaissance TADDM :

```
C:\> powershell Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin;Get-ExchangeServer
```

Si vous utilisez Microsoft Exchange Server 2010 pour vérifier que les autorisations du compte utilisateur sont correctes, exécutez la commande suivante sur le serveur Exchange Server lorsque vous êtes connectés en tant que compte de reconnaissance TADDM :

```
C:\> powershell Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010;Get-ExchangeServer
```

Limitations

Dans l'environnement de clusters du serveur Exchange, le détecteur reconnaît uniquement le serveur de boîte aux lettres actif.

Objets de modèle avec attributs associés

Le détecteur Microsoft Exchange crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources Microsoft Exchange Server de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

app.messaging.exchange.AcceptedDomain

- AcceptedDomainName
- Default
- DistinguishedName
- DomainName
- DomainType

- Parent

app.messaging.exchange.ActiveSyncVirtualDirectory

- BasicAuthenticationEnabled
- ClientAccessServer
- ClientCertEnabled
- DistinguishedName
- ExternalURL
- InternalURL
- Path
- RemoteDocumentsActionForUnknownServers
- VirtualDirectoryName
- WebSiteName
- WebSiteSSLEnabled

app.messaging.exchange.ClientAccess

- ClientAuthenticationMethod
- ExchangeProtocols
- ExternalHostName
- Host
- Name
- OutlookAnywhereEnabled
- PrimarySAP
- ProductName
- ProductVersion
- RoleName
- SSLOffloading
- VersionString

Les attributs ClientAuthenticationMethod, ExternalHostName et SSLOffloading s'appliquent uniquement lorsque la fonction Outlook Anywhere est activée.

app.messaging.exchange.EdgeTransport

- AcceptedDomains
- AntiSpamUpdatesEnabled
- ConnectivityLogEnabled
- ConnectivityLogPath
- DelayNotificationTimeout
- ExternalDNSAdapterEnabled
- Host
- InternalDNSAdapterEnabled
- MaxOutboundConnections
- MaxPerDomainOutboundConnections
- MessageExpirationTimeout
- MessageTrackingLogEnabled
- MessageTrackingLogPath
- ObjectType

- OutboundConnectionFailureRetryInterval
- PrimarySAP
- ProductName
- ProductVersion
- Queues
- ReceiveConnectors
- ReceiveProtocolLogPath
- RoleName
- SendConnectors
- SendProtocolLogPath
- TransientFailureRetryCount
- TransientFailureRetryInterval
- TransportRules
- VersionString

app.messaging.exchange.HubTransport

- AntiSpamUpdatesEnabled
- ConnectivityLogEnabled
- ConnectivityLogPath
- DelayNotificationTimeout
- ExternalDNSAdapterEnabled
- Host
- InternalDNSAdapterEnabled
- Journals
- MaxOutboundConnections
- MaxPerDomainOutboundConnections
- MessageClassifications
- MessageExpirationTimeout
- MessageTrackingLogEnabled
- MessageTrackingLogPath
- ObjectType
- OutboundConnectionFailureRetryInterval
- PrimarySAP
- ProductName
- ProductVersion
- Queues
- ReceiveConnectors
- ReceiveProtocolLogPath
- RoleName
- SendConnectors
- SendProtocolLogPath
- TransientFailureRetryCount
- TransientFailureRetryInterval
- TransportRules
- VersionString

app.messaging.exchange.TransportServer

- AntiSpamUpdatesEnabled
- ConnectivityLogEnabled
- ConnectivityLogPath
- DelayNotificationTimeout
- ExternalDNSAdapterEnabled
- Host
- InternalDNSAdapterEnabled
- MaxOutboundConnections
- MaxPerDomainOutboundConnections
- MessageExpirationTimeout
- MessageTrackingLogEnabled
- MessageTrackingLogPath
- ObjectType
- OutboundConnectionFailureRetryInterval
- PrimarySAP
- ProductName
- ProductVersion
- Queues
- ReceiveConnectors
- ReceiveProtocolLogPath
- RoleName
- SendConnectors
- SendProtocolLogPath
- TransientFailureRetryCount
- TransientFailureRetryInterval
- TransportRules
- VersionString

app.messaging.exchange.ExchangeConnector

- Enabled
- Fqdn
- ProtocolLoggingLevel

Cette classe est étendue par les attributs ReceiveConnector et SendConnector qui sont des sous-classes directes de cette classe.

app.messaging.exchange.ExchangeJournalRule

- EmailAddress
- JournalRuleIdentity
- Parent
- Recipient
- Scope

app.messaging.exchange.ExchangeMailbox

- ActiveDirectoryGUID
- Alias
- Enabled

- LegacyDN
- MailboxDisplayName
- OrganizationalUnit
- Parent
- PrimarySmtpAddress
- RecipientTypeDetails
- UserDistinguishedName

app.messaging.exchange.ExchangeMailboxStore

- AllowFileRestore
- CopyEdbFilePath
- DatabaseName
- DatabasePath
- DeletedItemRetention
- DistinguishedName
- IssueWarningQuota
- JournalRecipient
- LastFullBackup
- LastIncrementalBackup
- MailboxRetention
- MailboxStoreName
- Mailboxes
- MaintenanceSchedules
- MountAtStartup
- ProhibitSendQuota
- ProhibitSendReceiveQuota
- PublicFolderStore
- QuotaNotificationSchedules
- RetainDeletedItemsUntilBackup

app.messaging.exchange.ExchangeProtocol

- AuthenticatedConnectionTimeout
- Banner
- DistinguishedName
- LoginType
- MaxCommandSize
- MaxConnections
- MaxConnectionsFromSingleIP
- MaxConnectionsPerUser
- PreAuthenticatedConnectionTimeout
- ProtocolName
- ProxyTargetPort
- SSLBindings
- UnencryptedOrTLSBindings
- X509CertificateName

app.messaging.exchange.ExchangePublicFolder

- AgeLimit
- Children
- DeletedItemLifetime
- MailEnabled
- MaximumItemSize
- Parent
- Path
- PerUserReadDisabled
- ProhibitPostLimit
- PublicFolderName
- ReplicaAgeLimit
- URL
- UseDatabaseQuotaDefaults
- UseDatabaseReplicationSchedule
- UsePublicStoreAgeLimits
- UsePublicStoreDeletedLifetime
- WarningLimit

app.messaging.exchange.ExchangePublicFolderStore

- AllowFileRestore
- CopyEdbFilePath
- CustomReferralServerList
- DatabaseName
- DatabasePath
- DeletedItemRetention
- DistinguishedName
- IssueWarningQuota
- ItemRetentionPeriod
- LastFullBackup
- LastIncrementalBackup
- MaintenanceSchedules
- MaxItemSize
- MountAtStartup
- ProhibitPostQuota
- PublicFolderHierarchy
- PublicFolderStoreName
- PublicFolders
- QuotaNotificationSchedules
- ReplicationMessageSize
- ReplicationPeriod
- ReplicationSchedules
- RetainDeletedItemsUntilBackup
- StorageGroup
- UseCustomReferralList

app.messaging.exchange.ExchangeServer

- Acceptеddomain
- ActiveDirectoryDomainName
- ActiveDirectoryGUID
- AdministrativeGroup
- CreationTime
- DistinguishedName
- Domain
- Edition
- ErrorReportingEnabled
- ExchangeArchitecture
- ExchangeGroup
- Host
- Journals
- MessageClassifications
- Name
- ObjectType
- PrimarySAP
- ProductID
- ProductName
- ProductVersion
- Protocols
- ServerRoles
- Site
- VendorName
- VersionString
- VirtualDirectories

app.messaging.exchange.ExchangeServerRole

- Name
- ProductName
- ProductVersion
- RoleName
- VersionString

Cette classe est étendue par les attributs ClientAccess, TransportServer (EdgeTransport et HubTransport), et UnifiedMessagingServer qui sont des sous-classes directes de cette classe.

app.messaging.exchange.ExchangeVirtualDirectory

- ClientAccessServer
- DistinguishedName
- ExternalURL
- InternalURL
- Path
- VirtualDirectoryName

Cette classe est étendue par les attributs ActiveSyncVirtualDirectory, OABVirtualDirectory et OwaVirtualDirectory qui sont des sous-classes directes de cette classe.

app.messaging.exchange.MailboxServer

- AutoDatabaseMountDial
- ClusteredStorageType
- ForcedDatabaseMountAfter
- Host
- Name
- PrimarySAP
- ProductName
- ProductVersion
- RedundantMachines
- RoleName
- StorageGroups
- VersionString
- VirtualDirectories

app.messaging.exchange.OABVirtualDirectory

- PollInterval
- VirtualDirectoryName

Cette classe étend la classe ExchangeVirtualDirectory.

app.messaging.exchange.OwaVirtualDirectory

- ActiveSyncIntegrationEnabled
- AllAddressListsEnabled
- BasicAuthentication
- CalendarEnabled
- ChangePasswordEnabled
- ContactsEnabled
- DefaultDomain
- Description
- DigestAuthentication
- FormsAuthentication
- JournalEnabled
- JunkEmailEnabled
- LogonFormat
- MailboxServer
- NotesEnabled
- OwaVersion
- PremiumClientEnabled
- PublicFoldersEnabled
- RecoverDeletedItemsEnabled
- RemindersAndNotificationsEnabled
- RulesEnabled
- SMimeEnabled
- SearchFolderEnabled
- SignatureEnabled
- SpellCheckerEnabled

- TasksEnabled
- ThemeSelectionEnabled
- UMIntegrationEnabled
- VirtualDirectoryName
- WebSiteName
- WindowsAuthentication

app.messaging.exchange.ReceiveConnector

- AnonymousUsersPermission
- BasicAuthRequiresTLS
- BasicAuthentication
- BindAddresses
- ConnectorName
- DistinguishedName
- Enabled
- ExchangeAuthentication
- ExchangeLegacyServersPermission
- ExchangeServersPermission
- ExchangeUsersPermission
- ExternalAuthoritative
- Fqdn
- MaxMessageSize
- MutualAuthTLS
- PartnersPermission
- ProtocolLoggingLevel
- RemoteIPRanges
- TLS
- WindowsAuthentication

app.messaging.exchange.SendConnector

- AddressSpaces
- ConnectorName
- DistinguishedName
- DNSRoutingEnabled
- DomainSecureEnabled
- Enabled
- Fqdn
- IsScoped
- MaxMessageSize
- ProtocolLoggingLevel
- SmartHosts
- UseExternalDNSRoutersEnabled

app.messaging.exchange.TransportRule

- Comments
- Enabled
- Parent

- RulePriority
- TransportRuleName

app.messaging.exchange.UMDialPlan

- DigitsInExtension
- DistinguishedName
- UMDialPlanName

app.messaging.exchange.UnifiedMessagingServer

- Host
- Languages
- MaxCallsAllowed
- MaxFaxCallsAllowed
- ProductName
- ProductVersion
- RoleName
- StorageGroups
- UMDialPlans
- VersionString

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Le détecteur requiert les informations d'identification (nom d'utilisateur et mot de passe) pour le système informatique sur lequel le serveur Exchange Server exécute **ComputerSystem (Windows)**.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem (Windows)** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour accéder au domaine Active Directory sur lequel s'exécute le serveur Exchange Server. L'utilisateur doit appartenir au groupe des administrateurs locaux et doit être affecté des autorisations **Exchange View Only Administrator** sur le serveur Exchange Server 2007.
3. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour accéder au rôle de serveur Edge Transport. Le serveur Edge Transport est hébergé sur un ordinateur dédié et requiert des informations d'accès distinctes.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur Microsoft Exchange.

com.collation.discover.agent.ExchangeServerAgent.capturePublicFolders=true
La valeur par défaut est `true`, ce qui signifie que le détecteur reconnaît les dossiers publics de Microsoft Exchange.

Cette propriété indique si les dossiers publics sont reconnus et stockés dans la base de données TADDM. En fonction de la taille de

l'environnement et du nombre de dossiers devant être reconnus, vous pouvez modifier la valeur par défaut afin d'améliorer les performances. Si vous définissez la valeur sur `false`, une reconnaissance profonde des dossiers public n'est pas effectuée.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Microsoft Exchange et propose des solutions à ces problèmes.

Le détecteur Exchange ne démarre pas

Problème

Le détecteur Exchange Server n'est pas démarré.

Solution

Pour Microsoft Exchange Server 2007, vérifiez que les services suivants sont démarrés :

- Microsoft Exchange Information Store (store.exe)
- Microsoft Exchange Service Host (Microsoft.Exchange.ServiceHost.exe)
- Microsoft Exchange Transport (MSExchangeTransport.exe)
- Microsoft Exchange Unified Messaging (umservice.exe)

Pour vérifier l'état du service, exécutez le programme **services.msc** ou utilisez Windows Task Manager.

La reconnaissance renvoie un message `Stored-0 Exchange Server in the database`

Problème

Le détecteur Exchange s'exécute correctement avec le message suivant : `Stored-0 Exchange Server in the database`.

Solution

Aucun serveur Exchange Server actif n'est exécuté sur le système informatique cible. Les causes possibles sont les suivantes :

- Exchange Server est installé dans un noeud de grappe, mais il est actuellement inactif. Pour Microsoft Exchange Server 2007, démarrez le programme d'administration de grappe sur l'ordinateur sur lequel est installé Exchange Server en tant que noeud de grappe, Vérifiez ensuite que le noeud est actif.
- Le serveur fait fonction de volume d'approvisionnement et n'héberge aucun des rôles de serveur.
- Recherchez dans le fichier journal la cause de l'échec et vérifiez que la passerelle est configurée correctement.

Droits d'accès au domaine utilisés non valides

Problème

Le détecteur s'arrête avec le message d'erreur suivant :

```
CTJTD0835E Invalid domain credentials.
```

Solution

Vérifiez dans la configuration de la liste d'accès que les informations d'accès (nom d'utilisateur et mot de passe) sont correctes. Vérifiez que les autorisations d'accès au domaine Active Directory sur lequel le serveur Exchange Server, et non l'ordinateur local, s'exécute sont accordées.

Détecteur Microsoft Exchange 2003

Le détecteur Microsoft Exchange 2003 reconnaît Microsoft Exchange Server 2003.

Remarque : Dans les éditions de TADDM antérieures à la version TADDM 7.2.2, ce détecteur s'appelait détecteur *Microsoft Exchange Server*.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Exchange2003Sensor

Prérequis

Le compte TADDM utilisé pour accéder à la passerelle Windows doit disposer d'un compte Active Directory et non un compte local sur la passerelle.

Limitations

Prenez connaissance des limitations suivantes :

- Dans un environnement de clusters Exchange Server, ce détecteur reconnaît uniquement le noeud de cluster actif.
- Ce détecteur reconnaît les serveurs virtuels uniquement pour les protocoles SMTP et X400.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.messaging.exchange.ExchangeAdministrativeGroup
- app.messaging.exchange.ExchangeConnector
- app.messaging.exchange.ExchangeDSAccessDomainController
- app.messaging.exchange.ExchangeFolderTree
- app.messaging.exchange.ExchangeLink
- app.messaging.exchange.ExchangeMailbox
- app.messaging.exchange.ExchangeMailboxStore
- app.messaging.exchange.ExchangeProtocolVirtualServer
- app.messaging.exchange.ExchangePublicFolder
- app.messaging.exchange.ExchangePublicFolderStore
- app.messaging.exchange.ExchangeQueue
- app.messaging.exchange.ExchangeRoutingGroup
- app.messaging.exchange.ExchangeScheduleInterval
- app.messaging.exchange.ExchangeServer
- app.messaging.exchange.ExchangeStorageGroup

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Serveurs de messagerie** comme **Type de composant**.
2. Sélectionnez **Microsoft Exchange Server** pour le **Fournisseur**.
3. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

Le détecteur utilise les données d'identification extraites de la liste d'accès dans l'ordre suivant :

1. Le détecteur tente de connecter le serveur Microsoft Exchange Server, à l'aide des informations d'identification d'utilisateur Microsoft Exchange Server de la liste d'accès.
2. En cas d'échec de l'étape 1, le détecteur tente de se connecter au serveur Microsoft Exchange Server à l'aide des informations d'identification d'utilisateur du système informatique (Windows) de la liste d'accès.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

com.collation.discover.agent.exchange.command.timeout=600000

La valeur par défaut est `600000` (en millisecondes), à savoir 10 minutes. La valeur doit être un entier.

Cette propriété indique le délai d'attente (en millisecondes) pour obtenir des informations Exchange Server après un appel WMI.

Si l'appel WMI prend trop longtemps (ce qui peut se produire dans de grands environnements), vous pouvez augmenter cette valeur.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Microsoft Exchange 2003 et propose des solutions à ces problèmes.

Le détecteur ne démarre pas

Problème

Le détecteur Exchange 2003 n'est pas démarré.

Solution

Avec Microsoft Exchange Server 2003, vérifiez que le service de gestion de Microsoft Exchange est démarré sur le système Windows cible. Exécutez le programme **services.msc** pour vérifier l'état du service.

La reconnaissance ne trouve aucun système

Problème

Le détecteur Exchange 2003 s'exécute correctement avec le message suivant : “Il n'y avait rien à reconnaître”.

Solution

Aucun serveur Exchange Server actif n'est exécuté sur le système informatique cible. Une liste de causes possibles est fournie ci-dessous :

- Exchange Management Tool est installé, mais le serveur Exchange ne l'est pas. Avec Microsoft Exchange Server 2003, vérifiez que :
  1. Exchange System Manager est démarré sur l'ordinateur sur lequel est installé Exchange Server.

2. Dans la liste de serveurs, vérifiez que le serveur Exchange Server local s'affiche.
3. Si le serveur Exchange Server local n'apparaît pas, vérifiez que Microsoft Exchange Server est installé et s'exécute correctement.

- Exchange Server est installé dans un noeud de grappe, mais il est actuellement inactif. Pour Microsoft Exchange Server 2003, procédez comme suit :
  1. Démarrez le programme d'administration de grappe sur l'ordinateur sur lequel est installé le serveur Exchange Server en tant que noeud de grappe.
  2. Vérifiez la ressource Exchange affectée au serveur virtuel Exchange.

Le détecteur ne parvient pas à extraire les informations sur le serveur

Problème

Le détecteur Exchange 2003 s'arrête avec le message d'erreur suivant :

```
CTDTD0811E L'agent du serveur Exchange Server ne peut pas extraire les
informations du serveur Microsoft Exchange Server
```

Solution

Ce message d'erreur signifie qu'aucune sortie n'est extraite par l'intermédiaire de Windows Management Instrumentation (WMI). Pour Microsoft Exchange Server 2003, procédez comme suit :

1. Exécutez le programme services.msc sur le système Windows cible.
2. Redémarrez le service Microsoft Exchange Management.
3. Exécutez de nouveau la reconnaissance.
4. Si l'incident persiste, consultez le fichier `sensors/ExchangeServerSensor-*.log` pour déterminer si l'incident est lié à WMI.

Microsoft Exchange Server 2007, 2000 et 5.5 ne sont pas reconnus

Problème

Le détecteur Exchange 2003 s'arrête avec le message d'erreur suivant : CTDTD0812E Aucun serveur Microsoft Exchange Server n'a été trouvé.

Solution

Ce message d'erreur signifie qu'il n'existe aucun objet Exchange Server dans la sortie extraite par l'intermédiaire de Windows Management Instrumentation (WMI). Pour Microsoft Exchange Server 2003, procédez comme suit :

1. Exécutez le programme **services.msc** sur le système Windows cible.
2. Redémarrez le service Microsoft Exchange Management.
3. Exécutez de nouveau la reconnaissance.
4. Si l'incident persiste, consultez le fichier `sensors/ExchangeServerSensor-*.log` pour déterminer si l'incident est lié à WMI.

Le détecteur ne peut pas accéder à l'espace de nom de Windows Management Instrumentation (WMI)

Problème

Le message suivant figure dans le fichier `sensors/ExchangeServerSensor-*.log` :

```
System.UnauthorizedAccessException: Accès refusé
```

Solution

D'une manière générale, ce message signifie que le compte de service TADDM ne dispose pas de l'autorisation appropriée pour accéder à l'espace de nom WMI requis. Pour Microsoft Exchange Server 2003, procédez comme suit :

1. Vérifiez que le compte de service TADDM possède les autorisations pour les espaces de nom WMI suivants :

   ```
   Root\CIMV2
   Root\CIMV2\Applications\Exchange
   Root\MicrosoftExchangeV2
   ```

   Pour configurer les autorisations, procédez comme suit :

   a. Cliquez sur **Démarrer** > **Exécuter** > **Ouvrir wmimgmt.msc**.
   b. Cliquez droit sur **Commande WMI (Local)**, puis cliquez sur **Propriétés**.
   c. Dans la fenêtre de propriétés Commandes WMI (Local), cliquez sur l'onglet **Sécurité**.
   d. Cliquez sur **Espace de nom WMI**, puis cliquez sur **Sécurité**.
   e. Dans la fenêtre Sécurité, sélectionnez les autorisations suivantes pour autoriser l'utilisateur ou groupe :
      - **Exécuter Méthodes**
      - **Ecriture Complète**
      - **Ecriture Partielle**
      - **Ecriture Fournisseur**
      - **Activer compte**
      - **Activation à Distance**
      - **Lire Sécurité**
      - **Editer Sécurité**
2. Vérifiez que le compte de service TADDM dispose des droits suffisants pour les objets Exchange Server et Folder Tree. Pour configurer les autorisations, procédez comme suit :

   a. Cliquez sur **Démarrer** > **Tous les programmes** > **Microsoft Exchange** > **System Manager**
   b. Dans Exchange System Manager, développez l'arborescence **Serveurs**, puis recherchez l'objet de serveur à reconnaître.
   c. Cliquez à l'aide du bouton droit de la souris sur le serveur, puis sélectionnez **Propriétés**.
   d. Dans la fenêtre Propriétés, cliquez sur l'onglet **Sécurité**.
   e. Cliquez sur **Ajouter**, sélectionnez l'utilisateur du compte de service TADDM, puis cliquez sur **OK**.
   f. Dans la zone **Permissions for Administrator**, vérifiez que **Allow check boxes** en regard des autorisations suivantes est activé :
      - **Read**
      - **Execute**
      - **Read permissions**
      - **List contents**
      - **Read properties**
      - **List object**
      - **View information store status**

g. Dans Exchange System Manager, développez l'arborescence des dossiers et recherchez l'objet d'arborescence de dossier à reconnaître.
h. Procédez de la même manière pour le serveur.

La classe WMI n'existe pas

Problème

Le message suivant apparaît dans le fichier `sensors/ExchangeServerSensor-*.log` :

```
System.Management.ManagementException: Invalid class
```

Solution

En général, le message signifie que le détecteur a tenté de faire référence à une classe WMI qui n'existe pas. Les causes possibles sont que Exchange Server n'est pas installé correctement, ou que la version de Exchange Server n'est pas prise en charge.

Seul Microsoft Exchange Server 2003 est pris en charge. Microsoft Exchange Server 2007, 2000 et 5.5 ne sont pas reconnus car ces versions ne sont pas prises en charge.

Résultat de reconnaissance inattendu

Problème

Les serveurs virtuels correspondant aux serveurs suivants ne sont pas reconnus :

- HTTP
- IMAP4
- NNTP
- POP3

Solution

Pour Microsoft Exchange Server 2003, le détecteur prend en charge les serveurs virtuels pour les protocoles SMTP et X400 uniquement.

Détecteur Microsoft HyperV

Le détecteur Microsoft HyperV reconnaît des systèmes informatiques basés sur Microsoft Windows avec le serveur Hyper-V. La reconnaissance inclut l'hôte (également appelé partition parent ou racine) et les systèmes informatiques invité virtuels (également appelés partitions enfant) dans un environnement Hyper-V.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Détecteur Microsoft HyperV

Problèmes de sécurité

Le compte de service TADDM sur le système Hyper-V cible doit pouvoir exécuter la commande **wmic** pour interroger l'interface Windows Management Instrumentation (WMI).

Entrez la commande suivante sur une ligne, à partir de l'interface de ligne de commande du système hôte cible (partition parent) à des fins de vérification :

```
wmic /namespace:'\\root\virtualization' path Msvm_VirtualSystemSettingData
get SystemName, BaseBoardSerialNumber, ElementName
```

Objets de modèle avec attributs associés

Le détecteur Microsoft HyperV crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur des systèmes informatiques basés sur Microsoft Windows avec un serveur Microsoft Hyper-V dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs qui sont associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

sys.ComputerSystem

L'attribut suivant est associé avec l'hôte exécutant le logiciel Hyper-V :

- ChildSystem (host)

sys.ComputerSystem

Les attributs suivants sont associés aux objets reconnus qui sont virtualisés sur l'hôte :

- HostSystem
- IsVMIDanLPAR
- Manufacturer
- MemorySize
- Model
- le nom
- NumCPUs
- SerialNumber
- UUID
- Virtual
- VirtualMachineState

app.AppServer

- Host
- MajorVersion
- ProductName
- ProductVersion
- VendorName
- VersionString

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Le détecteur Microsoft HyperV utilise les mêmes données d'identification d'accès du **Système informatique (Windows)** que celles requises pour reconnaître l'hôte cible (partition parent). Aucune configuration supplémentaire n'est nécessaire.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit les problèmes classique susceptibles de peuvent survenir avec le détecteur Microsoft HyperV et propose des solutions.

Des systèmes informatiques invités n'apparaissent pas

Problème

Le détecteur HyperV a été exécuté, mais où se trouvent les invités situés dans le portail de gestion de données après une reconnaissance ?

Solution

Dans la sous-fenêtre Composants reconnus, accédez à **Récapitulatif de l'inventaire** > **Systèmes informatiques** > **Autres systèmes informatiques** pour rechercher les systèmes invité Hyper-V (partitions enfant).

Détecteur de serveur Microsoft Web IIS

Le détecteur de serveur Microsoft Web IIS reconnaît des serveurs Microsoft Internet Information Services (IIS).

L'attribut IIsWebServiceSensor prend en charge la reconnaissance d'IIS 6.0, tandis que l'attribut IISServerSensor prend en charge la reconnaissance d'IIS 7.0 et versions ultérieures.

Restriction : Le détecteur de serveur Microsoft Web IIS ne définit plus l'attribut IIsParametersRow pour les classes IIsWebServer, IIsWebService et IIsWebVirtualDir. Utilisez plutôt l'attribut IIsParameters.

Fix Pack 2

L'attribut IISServerSensor reconnaît les chaînes de connexion qui sont ensuite stockées au format XML dans l'attribut XD de la classe IISModule. En fonction de ces chaînes de connexion, les agents de topologie créent des dépendances entre le module IIS et les bases de données Oracle utilisées par le module.

Le détecteur de serveur Microsoft Web IIS reconnaît le fichier `tnsnames.ora`, qui est utilisé pour définir les informations relatives aux chaînes de connexion lorsque la base de données Oracle est utilisée. Le détecteur reconnaît le fichier sur le système cible aux emplacements suivants, dans l'ordre spécifié :

1. Le répertoire `<saisie_chemin d'accès>\..\network\admin\` pour chaque saisie de chemin d'accès indiquée dans la variable `%PATH%`.
2. L'emplacement indiqué par la propriété `com.ibm.cdb.tnsNamesLocation`.
3. Le répertoire d'installation du client Oracle indiqué dans la variable `%PATH%`.
4. `%TNSNAMES_PATH%\tnsnames.ora`.
5. `%ORACLE_HOME%\network\admin\tnsnames.ora`.

Fix Pack 4 Dans TADDM 7.3.0.4 et versions ultérieures, TADDM prend en charge la reconnaissance non administrateur des serveurs IIS. Pour plus d'informations, voir «Configuration d'une reconnaissance IIS non administrateur», à la page 132.

Nom du détecteur utilisé dans l'interface graphique et les journaux

IIsWebServiceSensor, IISServerSensor

Prérequis

Vérifiez que les conditions requises ci-dessous sont remplies.

Conditions requises pour la reconnaissance de toutes les versions d'IIS

- La reconnaissance du système informatique doit s'effectuer correctement.

Conditions requises pour la reconnaissance d'IIS 6.0

Remarque : La prise en charge des systèmes d'exploitation sur lesquels des cibles IIS 6.0 sont exécutées n'est plus assurée. Comme le détecteur a été

conçu et mis à jour pour reconnaître les nouvelles éditions des cibles, il est donc possible que la reconnaissance d'IIS 6.0 échoue.

- IIS Manager doit être installé sur la passerelle. Cette méthode garantit l'installation des classes COM. Ces classes sont requises par les commandes TaddmTool **AdsiDump** et **AdsiEnum**.
- Si le Gestionnaire des services Internet n'est pas installé, installez-le via l'option Ajout/Suppression de programmes du Panneau de configuration Windows. Sélectionnez **Composants Windows** > **Serveur d'applications** > **IIS** > **Installer le Gestionnaire des services Internet**.

.

Conditions requises pour la reconnaissance d'IIS 7.0 et versions ultérieures

Pour reconnaître des serveurs IIS 7.0, le composant logiciel enfichable d'IIS PowerShell doit être installé sur le serveur cible. Ce composant est fourni dans les Scripts et outils de gestion d'IIS. Vous pouvez également le télécharger avec le package approprié depuis le Centre de téléchargement Microsoft et l'installer manuellement.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.ProcessPool
- app.web.iis.IIsModule
- app.web.iis.IIsParameter
- app.web.iis.IIsWebServer
- app.web.iis.IIsWebService
- app.web.iis.IIsWebVirtualDir
- sys.RuntimeProcess

Remarque : Les modules reconnus par le détecteur sont de la classe IIsWebVirtualDir. Le détecteur ne reconnaît pas les modules IIS et la classe IIsModule n'est pas utilisée pour les modules IIS.

Configuration du détecteur

Avant d'exécuter une reconnaissance, vous devez configurer le détecteur de serveur Web IIS Microsoft.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Il n'existe aucune condition d'accès spécifique. Ce détecteur peut être exécuté à l'aide des droits d'accès de ComputerSystem utilisés pour reconnaître le client.

Configuration du profil de reconnaissance :

Vous pouvez personnaliser le paramètre du détecteur de serveur Web IIS Microsoft en définissant la configuration du détecteur dans la console de gestion de reconnaissance.

Si vous souhaitez personnaliser IIsWebServiceSensor et IISServerSensor, créez un profil de reconnaissance dans la console de gestion de reconnaissance. Dans ce profil, créez une configuration du détecteur, puis cochez la case **Activer cette configuration et désactiver la configuration sélectionnée**.

Vous pouvez modifier les propriétés du profil de reconnaissance suivantes :

discoverIISParameters
Cette propriété indique si les paramètres IIS sont reconnus. Par défaut, elle est définie sur `true`, ce qui signifie que les paramètres sont reconnus.

Les paramètres IIS peuvent être conséquents et peuvent impliquer une dégradation des performances, ou des erreurs liées à une insuffisance de mémoire. Si vous ne souhaitez pas reconnaître ces paramètres, définissez la propriété sur `false`.

Fix Pack 2 **tagsToMask**
Cette propriété indique une liste séparée par des virgules des propriétés des chaînes de connexion. Le contenu textuel de ces propriétés des chaînes de connexion qui sont reconnues est marqué par des astérisques.

La valeur par défaut de cette propriété est `password,pwd`.

Remarque : Cette propriété est disponible seulement pour IISServerSensor.

Configuration d'une reconnaissance IIS non administrateur : Fix Pack 4

Vous pouvez configurer le détecteur de serveur Web Microsoft IIS pour qu'il exécute la reconnaissance non administrateur des serveurs IIS. Une telle reconnaissance ne nécessite pas un utilisateur avec des droits d'administrateur. Dans ce mode, l'option de contrôle de compte d'utilisateur peut être activée.

Remarque : La reconnaissance non administrateur est uniquement prise en charge avec IISServerSensor, qui accepte IIS version 7.0 et ultérieures.

Avec la reconnaissance non administrateur, l'option Contrôle de compte d'utilisateur peut être activée. Selon que vous utilisez une session WMI ou PowerShell, vous pouvez créer les types d'utilisateurs suivants :

- Pour la session WMI, les utilisateurs qui ne sont pas des administrateurs mais qui appartiennent au groupe d'administrateurs sont pris en charge.
- Pour la session PowerShell, les utilisateurs qui ne sont pas des administrateurs et qui n'appartiennent pas au groupe d'administrateurs sont pris en charge.

Procédure
Pour configurer TADDM pour utiliser la reconnaissance non administrateur des serveurs IIS, procédez comme suit :

1. Copiez les fichiers suivants sur le système cible :
   - A partir du répertoire `$COLLATION_HOME/dist/support/bin`, procédez comme suit :
     - `copyFiles.ps1`
     - `dcomConfiguration.ps1`
     - `iisConfiguration.ps1`
     - `nonadmin.properties`
     - `psSessionConfiguration.ps1`
     - `scriptsRunner.bat`
     - `scriptsRunner.ps1`
     - `wmiConfiguration.ps1`
     - `wrmConfiguration.ps1`
   - A partir du répertoire `$COLLATION_HOME/dist/lib/ms/gateway`, procédez comme suit :

- TaddmWmi.pdb
- TaddmWmi.exe
- TaddmWmi.mof
- TaddmWmi.dll

2. Configurez le fichier nonadmin.properties en mettant à jour les propriétés nonadmin.user et nonadmin.files.path :

```
nonadmin.user=utilisateur
nonadmin.wmi.namespace=root
nonadmin.files.path=chemin
nonadmin.permissions=Enable,MethodExecute,RemoteAccess
nonadmin.components.iis7=yes
```

   La valeur du paramètre *utilisateur* représente l'utilisateur que vous souhaitez utiliser pour la reconnaissance non administrateur. Si vous spécifiez l'utilisateur local, il vous suffit d'ajouter le nom d'utilisateur. Sinon, indiquez également le nom de domaine, par exemple, domaine\utilisateur. La valeur du paramètre *chemin* représente le chemin d'accès au répertoire dans lequel vous avez copié les fichiers à l'étape 1. Ne modifiez pas les valeurs des autres propriétés.

3. Exécutez le fichier scriptsRunner.bat en tant qu'administrateur avec l'une des options suivantes :
   - scriptsRunner.bat set -wmi : définit les autorisations de la session WMI.
   - scriptsRunner.bat set -ps : définit les autorisations de la session PowerShell.
   - scriptsRunner.bat set -wmi -ps : définit les autorisations des sessions WMI et PowerShell.

Si vous décidez de ne plus exécuter de reconnaissances non administrateur, vous pouvez revenir à la configuration initiale. Exécutez le fichier scriptsRunner.bat avec l'une des options suivantes :

- scriptsRunner.bat revert -wmi
- scriptsRunner.bat revert -ps
- scriptsRunner.bat revert -wmi -ps

Tâches associées:

«Configuration d'une reconnaissance Windows non administrateur», à la page 409
Vous pouvez configurer le détecteur pour exécuter des reconnaissances sans fournir des données d'identification de l'utilisateur doté du rôle d'administrateur.

Différences entre IISServerSensor et IisWebServiceSensor

IISServerSensor et IisWebServiceSensor reconnaissent diverses versions d'IIS. Lorsqu'ils sont combinés dans un profil de reconnaissance, toutes les versions d'IIS qui sont prises en charge par TADDM peuvent être reconnues à l'aide de ce profil.

IISServerSensor

IISServerSensor est un détecteur séparé qui prend en charge la reconnaissance de IIS 7 et ultérieur à l'aide des cmdlets du composant logiciel enfichable PowerShell IIS. Ce détecteur ne prend en charge qu'une reconnaissance basée sur un script ou asynchrone. Il utilise une nouvelle désignation des propriétés de métabase IIS et des paramètres de configuration. Les attributs changés sont enregistrés dans le modèle existant.

IIsWebServiceSensor

IIsWebServiceSensor est un détecteur antérieur qui prend en charge la reconnaissance d'IIS 6.0 ou version antérieure. Il exécute une reconnaissance régulière à l'aide des commandes **AdsiDump** et **AdsiEnum** de TaddmTool.

Remarque : Pour tous les profils non par défaut pour lesquels le détecteur IIsWebServiceSensor est activé, IIsWebServiceSensor est également activé après la migration.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur Web Microsoft IIS et propose des solutions à ces problèmes.

Fix Pack 2

Les dépendances de module IIS ne sont pas incluses dans les applications métier

Problème

Même créées, les dépendances de module IIS ne sont pas incluses dans les applications métier.

Solution

Les dépendances de module IIS ne sont pas incluses dans les applications métier parce que la configuration des modèles de regroupement par défaut exclut de telles relations. Pour résoudre le problème, procédez comme suit :

1. Exportez la configuration par défaut en exécutant l'outil `bizappscli` :

   ```
   $COLLATION_HOME/sdk/bin/bizappscli.sh exportDefaultConfiguration -f
   conf.xml
   ```

2. Ouvrez le fichier `conf.xml` et supprimez les lignes suivantes :

   ```
   <exclude relation="{any}" source="app.web.iis.IIsModule"
   target="{any}"/>
   <exclude relation="{any}" source="{any}"
   target="app.web.iis.IIsModule"/>
   ```

3. Importez la configuration modifiée en exécutant l'outil `bizappscli` :

   ```
   $COLLATION_HOME/sdk/bin/bizappscli.sh importDefaultConfiguration -f
   conf.xml
   ```

Aucune information de serveur Web reconnue

Problème

Ce détecteur ne reconnaît aucune information de serveur Web.

Solution

En l'absence d'informations sur le serveur Web, consultez les journaux pour savoir si les commandes **AdsiDump** et **AdsiEnum** du programme TaddmTool ont abouti ou échoué.

Vérifiez si les commandes **QueryRegistry** du programme TaddmTool ont abouti. Deux chemins du registre font l'objet d'une requête.

- `HKLM\SOFTWARE\Microsoft\W3SVC`
- `HKLM\SYSTEM\CurrentControlSet\Services\W3SVC`

  La première clé fournit des informations logicielles générales pour IIS et la seconde fournit des informations liées aux services.

Serveur Web en double

Problème

Lors de la reconnaissance, des serveurs IIS Web sont rencontrés. Ce problème peut se produire quand les serveurs IIS Web ont été reconnus avec une version antérieure de TADDM. Les versions antérieures de TADDM utilisaient le port 0 comme port d'écoute par défaut. Si les mêmes serveurs sont reconnus à l'aide d'un port d'écoute distinct, ils sont dupliqués et ne peuvent pas être automatiquement fusionnés.

Solution

Utilisez une Instruction SQL pour identifier les serveurs IIS Web en double dans la base de données. L'instruction suivante peut être exécutée sur une ligne dans les bases de données DB2 ou Oracle :

```
select
 cast(APPZ.contextip_x as VARCHAR(100)) as CONTEXT_IP, APPZ.guid_x as OLD_GUID,
APPZ.displayname_x as OLD_DISPLAYNAME,
 APPN.guid_x as NEW_GUID, APPN.displayname_x as NEW_DISPLAYNAME
from
 APPSRVR APPZ INNER JOIN APPSRVR APPN ON APPZ.contextip_x = APPN.contextip_x AND
 APPZ.jdoclassx = APPN.jdoclassx
où :
 APPZ.jdoclassx='com.collation.topomgr.jdo.topology.app.web.iis.IIsWebServiceJdo'
and APPZ.displayname_x like '%:0' and APPN.displayname_x not like '%:0'
```

Utilisez l'une des méthodes suivantes pour supprimer les doublons :

- Fusionnez les doublons dans le portail de gestion de données.
- Supprimez manuellement les anciens éléments de configuration.

Pour plus d'informations sur la fusion et la suppression d'éléments de configuration reconnus, voir la rubrique *Tâches de reconnaissance* dans le *Guide d'utilisation* de TADDM.

Echec du système avec une erreur inconnue (0x80005000)

Problème

Lors d'une reconnaissance de IIS8 sur Windows Server 2012 avec le contrôle des comptes activé, l'erreur suivante survient :

```
System.Runtime.InteropServices.COMException (0x80005000):
Unknown error (0x80005000)
```

Solution

Pour résoudre ce problème, procédez comme suit :

1. Sur la machine cible, exécutez l'éditeur de registre, Regedit.exe.
2. Attribuez la valeur 1 à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System LocalAccountTokenFilterPolicy`.
3. Dans la fenêtre du panneau de commande, cliquez sur l'onglet **Outils d'administration** et ouvrez **Local Security Policy**.
4. Développez **Local Policies**, puis cliquez sur **Security Options**.
5. Changez les règles suivantes :
   - Attribuez la valeur **Elever les privilèges sans invite utilisateur** à la règle **Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur**.
   - Attribuez la valeur **Désactivé** à la règle **Contrôle compte d'utilisateur : détecter les installations d'applications et demander l'élévation**.

Pour configurer des règles sur le système avec Active Directory, procédez comme suit :

1. Dans la fenêtre du panneau de commande, cliquez sur l'onglet **Outils d'administration** et ouvrez **Group Policy Management**.
2. Choisissez une forêt et un domaine, puis sélectionnez **Default Domain Policy**.
3. Cliquez sur **Action > Editer**.
4. Ouvrez `Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security options`.
5. Changez les règles suivantes :
   - Attribuez la valeur **Elever les privilèges sans invite utilisateur** à la règle **Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur**.
   - Attribuez la valeur **Désactivé** à la règle **Contrôle compte d'utilisateur : détecter les installations d'applications et demander l'élévation**.

Après la mise à niveau vers la version 7.3, des erreurs liées à une insuffisance de mémoire se produisent lors de l'exécution du détecteur de serveur Web IIS Microsoft

Problème

Lorsque vous exécutez la reconnaissance à l'aide du détecteur de serveur Web IIS Microsoft après la mise à niveau vers TADDM 7.3, des erreurs de mémoire insuffisante se produisent.

Solution

Si, dans TADDM 7.2.2, vous avez défini la propriété `com.collation.discover.agent.IIsWebServiceAgent.discoverIISParameters` sur `false` dans le fichier `collation.properties`, c'est ce qui explique le problème. Dans TADDM 7.3, cette propriété ne se trouve plus dans le fichier `collation.properties`. Par conséquent, après la mise à niveau, sa valeur est définie sur `true`.

Pour modifier la valeur de la propriété, ouvrez la configuration du détecteur dans le portail de gestion de reconnaissance et recherchez `discoverIISParameters`. Spécifiez la valeur `false`.

détecteur NFS

Le détecteur NFS reconnaît les serveurs Network File System (NFS).

Nom du détecteur utilisé dans l'interface graphique et les journaux

NFSServerSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.NFSExport
- sys.NFSSAP
- sys.NFSService
- sys.ServiceAccessPoint

Détecteur Oracle Application Server

Le détecteur Oracle Application Server reconnaît des serveurs Oracle Application Server.

Nom du détecteur utilisé dans l'interface graphique et les journaux

OracleAppSensor et OracleAppOpmnSensor

Prérequis

Prenez connaissance des prérequis suivants :

- La reconnaissance du système informatique doit s'effectuer correctement.
- Un compte Oracle Application Server doit être entré dans la liste d'accès.
- Un compte disposant de privilèges d'administration est requis (un ID en lecture seule peut être utilisé).
- Les bibliothèques Oracle Application Server doivent être mises à disposition sur le serveur TADDM.
- Les chemins relatifs sont associés à `$COLLATION_HOME`.
- Requiert deux sous-répertoires :
  - j2ee
  - opmn

    Ces fichiers peuvent être copiés ou montés sur NFS à partir d'une installation Oracle Application Server existante.

  Les fichiers JAR requis sur le serveur TADDM sont :
  - `j2ee/home/lib/ejb.jar`
  - `j2ee/home/lib/adminclient.jar`
  - `j2ee/home/lib/javax77.jar`
  - `j2ee/home/lib/jmxcluster.jar`
  - `j2ee/home/lib/jmx_remote_api.jar`
  - `j2ee/home/lib/jmxri.jar`
  - `j2ee/home/oc4jclient.jar`
  - `opmn/lib/argus.jar`
  - `opmn/lib/ons.jar`
  - `opmn/lib/opmnconfig.jar`
  - `opmn/lib/optic.jar`
  - `opmn/lib/repositorycheck.jar`
- Indiquez l'emplacement des fichiers dans l'entrée `com.collation.oracleapp.root.dir` du fichier `collation.properties`.
- Ces fichiers doivent disposer des droits d'accès en lecture pour l'utilisateur de Collation.

Objets de modèle créés

OracleAppAgent crée les objets modèles suivants :

- app.AppConfig
- app.ConfigFile.SoftwareContainer
- app.j2ee.EJB

- app.j2ee.EntityBean
- app.j2ee.J2EEComponent
- app.j2ee.J2EEDeployedObject
- app.j2ee.J2EEModule
- app.j2ee.J2EEResource
- app.j2ee.JSP
- app.j2ee.MessageDrivenBean
- app.j2ee.oracleapp.OracleAppCluster
- app.j2ee.oracleapp.OracleAppConnectorModule
- app.j2ee.oracleapp.OracleAppDomain
- app.j2ee.oracleapp.OracleAppEJBModule
- app.j2ee.oracleapp.OracleAppJ2EEApplication
- app.j2ee.oracleapp.OracleAppJ2EEServer
- app.j2ee.oracleapp.OracleAppJ2EEWebSite
- app.j2ee.oracleapp.OracleAppJDBCConnectionPool
- app.j2ee.oracleapp.OracleAppJDBCDataSource
- app.j2ee.oracleapp.OracleAppJDBCDriver
- app.j2ee.oracleapp.OracleAppJMSDestination
- app.j2ee.oracleapp.OracleAppJMSServer
- app.j2ee.oracleapp.OracleAppJSPContainer
- app.j2ee.oracleapp.OracleAppJTAResource
- app.j2ee.oracleapp.OracleAppProcessManager
- app.j2ee.oracleapp.OracleAppResourceAdapter
- app.j2ee.oracleapp.OracleAppServlet
- app.j2ee.oracleapp.OracleAppWebModule
- app.j2ee.StatefulSessionBean
- app.j2ee.StatelessSessionBean
- core.LogicalContent
- enums.StatusEnum
- net.BindAddress
- net.IpAddress
- sys.ComputerSystem

OracleAppOpmn crée les objets modèles suivants :

- app.AppConfig
- app.ConfigFile
- app.j2ee.oracleapp.OracleAppCluster
- app.j2ee.oracleapp.OracleAppProcessManager
- app.web.oracleapp.OracleAppHTTPServer
- core.LogicalContent
- enums.StatusEnum
- net.BindAddress
- net.IpAddress
- sys.ComputerSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Ajoutez une entrée à la liste d'accès du système sur lequel Oracle Application Server est exécuté.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

com.collation.oracleapp.root.dir=lib/oracleapp
La valeur par défaut est `lib/oracleapp`.

Cette propriété indique l'emplacement des bibliothèques Oracle Application Server sur le serveur TADDM.

Vous pouvez indiquer un chemin d'accès absolu ou relatif pour l'emplacement du répertoire. Si la valeur pour cette propriété est un chemin d'accès au répertoire relatif, ce chemin d'accès est ajouté à au chemin `$COLLATION_HOME`.

com.collation.platform.os.ignoreLoopbackProcesses=true
La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Oracle Application Server et propose des solutions à ces problèmes.

Démarrage impossible du détecteur

Problème
Le programme **lsof** n'est pas correctement configuré pour renvoyer des informations sur l'ensemble des processus.

Solution
Assurez-vous que vous reconnaissez une version prise en charge d'Oracle Application Server.

Le détecteur Oracle Application exécute la commande **opmnctl status**. Vérifiez que l'utilisateur système qui est utilisé pour la reconnaissance dispose des droits d'accès nécessaires pour exécuter cette commande.

La liste suivante décrit d'autres raisons possibles pour lesquelles le détecteur ne démarre pas :

- Le programme LiSt Open Files (lsof) n'est pas correctement configuré pour renvoyer des informations sur l'ensemble des processus. L'une des exigences suivantes pour l'exécution du programme lsof doit être satisfaite :
  - L'indicateur du droit d'accès setuid (définir l'ID utilisateur) doit être défini pour le fichier de programme lsof.
  - L'utilisateur doit utiliser la commande **sudo** pour exécuter le programme lsof.
- La valeur de la propriété com.collation.platform.os.ignoreLoopbackProcesses dans le fichier `$COLLATION_HOME/etc/collation.properties` est définie à `false`. Cette valeur doit être définie à `true` pour que le détecteur démarre. Une valeur à `true` indique que les processus qui écoutent sur les interfaces de bouclage doivent être ignorés.
- Les bibliothèques d'Oracle Application Server ne sont pas accessibles sur le serveur TADDM. Les bibliothèques Oracle Application Server doivent être mises à disposition sur le serveur TADDM. Utilisez la propriété suivante pour spécifier l'emplacement de ces bibliothèques :

  com.collation.oracleapp.root.dir=lib/oracleapp

  La valeur par défaut de cette propriété est `lib/oracleapp`. Si la valeur de cette propriété est un répertoire relatif, le répertoire est relatif à `$COLLATION_HOME`, comme illustré dans l'exemple suivant : `$COLLATION_HOME/lib/oracleapp`.

  Que le chemin soit relatif ou absolu, il doit contenir les deux sous-répertoires suivants :
  - j2ee
  - opmn

  Les bibliothèques Oracle Application Server peuvent être copiées ou montées à l'aide du système de fichiers réseau (NFS) à partir d'une installation existante d'Oracle Application Server. La liste suivant identifie les fichiers jar requis :
  - j2ee/home/lib/ejb.jar
  - j2ee/home/lib/adminclient.jar
  - j2ee/home/lib/javax77.jar
  - j2ee/home/lib/jmxcluster.jar
  - j2ee/home/lib/jmx_remote_api.jar
  - j2ee/home/lib/jmxri.jar
  - j2ee/home/oc4jclient.jar
  - opmn/lib/argus.jar
  - opmn/lib/ons.jar
  - opmn/lib/opmnconfig.jar
  - opmn/lib/optic.jar
  - opmn/lib/repositorycheck.jar

Le détecteur Oracle Application Server échoue

Problème

La reconnaissance d'Oracle Application Server n'est pas prise en charge sur toutes les plateformes.

Solution

Assurez-vous que TADDM prend en charge la reconnaissance d'Oracle Application Server sur votre système d'exploitation.

Panne du détecteur dans un serveur distant

Problème

Le détecteur tombe en panne dans le serveur distant et affiche une erreur `Fermeture de l'agent suite au dépassement du délai limitnull`.

TADDM ne peut pas identifier les bibliothèques Oracle Application Server.

Solution

Vérifiez le paramètre de la propriété `com.collation.oracleapp.root.dir`.

Panne du détecteur lors d'une tentative d'exécution de la méthode discoverOpmnctl()

Problème

Le détecteur tombe en panne lorsqu'il essaie d'exécuter la méthode discoverOpmnctl(). Le chemin d'accès du compte de service de TADDM figurant dans le système Oracle Application Server ne contient pas le répertoire `bin` d'Oracle Application Server ou l'utilisateur ne dispose pas de privilèges de lecture ou d'exécution pour exécuter la commande **opmnctl status**.

Solution

Ajoutez le répertoire `bin` d'Oracle Application Server au chemin d'accès du compte de service de TADDM dans le système d'Oracle Application Server.

Panne du détecteur dans un serveur distant avec le message d'erreur Nom introuvable dans le fichier journal

Problème

Le détecteur échoue et l'erreur suivante s'affiche dans le fichier journal :

```
javax.naming.NameNotFoundException: oc4j:internal/ResourceFinder not found
```

Solution

Ajoutez l'adresse IP et le nom d'hôte d'Oracle Application Server au fichier `/etc/hosts` sur le serveur TADDM.

Détecteur Oracle VM

Fix Pack 4

Le détecteur Oracle VM reconnaît les principaux éléments du serveur Oracle VM, à savoir les pools de serveurs, les serveurs VM et les machines virtuelles VM.

Le détecteur est démarré après le détecteur de port.

Systèmes cibles pris en charge

Pour obtenir la liste des systèmes cibles pris en charge par ce détecteur, voir le document PDF TADDM 7.3 : Détecteurs et systèmes cible pris en charge.

Nom du détecteur utilisé dans l'interface graphique et les journaux

OracleVMSensor

Prérequis

- Créez un utilisateur de la reconnaissance et affectez-lui des droits d'accès en lecture seule.
- Ouvrez un port pour les communications entre le serveur TADDM et Oracle VM Manager. Il s'agit par défaut du port 7002. Si vous utilisez un autre port, indiquez son numéro dans la propriété `httpsPort` du profil de reconnaissance du détecteur.
- Assurez-vous qu'Oracle VM Manager est en cours d'exécution.

Connexion aux serveurs avec des certificats SSL

Le détecteur Oracle VM peut se connecter au serveur Oracle VM Manager avec SSL en deux modes, le mode par défaut et le mode strict.

Mode par défaut
Le mode par défaut ne vérifie pas complètement le certificat d'un serveur. Ce mode autorise une connexion même si le certificat est autosigné, expiré ou avec un nom d'hôte non valide. Il refuse la connexion si d'autres problèmes sont découverts, par exemple une erreur de chaînage de certificats. Le mode par défaut est exploitable avec les certificats Oracle VM par défaut.

Mode strict
Le mode strict vérifie complètement le certificat d'un serveur. Vous pouvez l'activer en définissant la propriété de configuration `strictCertificateCheck` sur `true` dans le profil de reconnaissance du détecteur.

Lorsque ce mode est activé, seuls les certificats valides signés par des autorités de certification de confiance sont acceptés. Avant de pouvoir vous connecter avec un tel certificat, vous devez l'importer dans TADDM. Ainsi, les certificats autosignés sont des certificats de confiance, leur validité est toujours vérifiée.
Pour importer de tels certificats, procédez comme suit :

1. Accédez au répertoire `taddm/dist/osgi/plugins/com.ibm.cdb.discover.sys.vmware.vmwarecommon_*` où `*` est le numéro de version du détecteur.
2. A partir du répertoire spécifié, exécutez la commande suivante :

   ```
   java -cp lib/vmwarecommon.jar com.ibm.cdb.discover.sys.vmware.
   VmCertificateCollector OracleVM IP:port
   ```

   où *IP* est l'adresse IP de l'hôte du serveur Oracle VM Manager et *port* est le port SSL de cet hôte. Par exemple :

   ```
   java -cp lib/vmwarecommon.jar com.ibm.cdb.discover.sys.vmware.
   VmCertificateCollector OracleVM 12.234.255.4:7002
   ```

Reconnaissance des données plus détaillées

Le détecteur Oracle VM reconnaît les données de base de l'infrastructure du serveur Oracle VM. Si vous souhaitez reconnaître des informations plus détaillées, par exemple sur des machines virtuelles VM, vous pouvez exécuter les détecteurs de système informatique appropriés. Ainsi, si les machines virtuelles exécutent le système d'exploitation Linux, vous pouvez exécuter le détecteur de système informatique Linux. Une fois la reconnaissance terminée, les objets créés par les deux détecteurs sont fusionnés dans un objet unique contenant l'intégralité des données sur la machine virtuelle reconnue.

Configuration du détecteur Oracle VM

Avant d'exécuter une reconnaissance, vous devez configurer le détecteur Oracle VM.

Configuration de la liste d'accès :

Vous devez indiquer les détails d'accès corrects du détecteur Oracle VM.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Oracle VM** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) de l'utilisateur de la reconnaissance que vous avez créé pour ce détecteur. Pour plus d'informations, voir «Prérequis», à la page 142.

Configuration du profil de reconnaissance :

Vous pouvez configurer le détecteur Oracle VM en modifiant les attributs du profil de reconnaissance.

Vous pouvez configurer le détecteur Oracle VM dans la console de gestion de reconnaissance en définissant les attributs suivants :

strictCertificateCheck
: Si la valeur de cet attribut est définie sur `true`, le détecteur effectue une vérification complète des certificats des serveurs Oracle VM Manager. Les certificats doivent être valides et signés par des autorités de certification dignes de confiance.

  La valeur par défaut est `false`.

httpsPort
: Cette propriété indique un numéro de port utilisé pour les communications entre le serveur TADDM et Oracle VM Manager.

  La valeur par défaut est `7002`.

Objets de modèle avec attributs associés

Le détecteur Oracle VM crée des objets de modèle associés à des attributs. Les attributs indiquent le type d'informations que le détecteur collecte à propos de l'infrastructure Oracle VM.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

app.AppServer

- PrimarySAP

dev.StorageVolume

- Capacity
- ManagedSystemName
- Name
- Type
- XA
- XD

net.IpInterface

- IpAddress

- L2Interface
- Parent

net.L2Interface (pour le réseau de machines virtuelles)

- HwAddress
- Name
- Parent

net.L2Interface (pour le serveur de machines virtuelles)

- HwAddress
- Mtu
- Name

phys.physcomp.CPUCore

- IndexOrder
- MasterCPU
- State

simple.SLogicalGroup

- Description
- HierarchyDomain
- HierarchyType
- Name
- OpenId

storage.StoragePool

- Description
- GroupMembers
- HierarchyDomain
- HierarchyType
- Members
- Name
- OpenId

sys.linux.LinuxUnitaryComputerSystem (pour le serveur de machines virtuelles Oracle)

- Description
- Manufacturer
- Model
- Name
- OSName
- OSVersion
- SerialNumber
- UUID

Plusieurs machines virtuelles Oracle, telles que les systèmes suivants :

sys.ComputerSystem
sys.linux.LinuxUnitaryComputerSystem
sys.sun.SunSPARCUnitaryComputerSystem
sys.windows.WindowsComputerSystem

Les attributs suivants sont associés à ces objets de modèle :

- Host
- MemorySize
- Name
- NumCPUs
- SystemBoardUUID
- UUID
- VirtualMachineState
- Virtual

Détecteur de serveur SAP CCMS

Le détecteur de serveur SAP CCMS reconnaît les systèmes SAP, les serveurs SAP (ABAP et Java) et les composants SAP.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CCMSServerSensor

Prérequis

Le détecteur de serveur SAP CCMS requiert des bibliothèques JCo pour fonctionner. Pour plus d'informations sur les bibliothèques JCo, voir «Installation des bibliothèques SAP Java Connector (JCo)».

Selon l'application spécifique des systèmes SAP NetWeaver, vous pouvez utiliser le détecteur de serveur SAP CCMS et/ou le détecteur de serveur SAP SLD pour reconnaître ces systèmes. Les applications SAP sont installées sur deux schémas distincts de base de données, chacune étant ensuite accessible via son environnement d'exécution. Il existe un environnement d'exécution pour les instances Java (pile Java) et un pour les instances ABAP (Advanced Business Application Programming, pile ABAP):

- Utilisez le détecteur de serveur SAP CCMS pour reconnaître des informations quand le système SAP NetWeaver a des applications uniquement basées sur la pile ABAP.
- Utilisez le détecteur de serveur SAP SLD pour reconnaître des informations quand le système SAP NetWeaver a des applications uniquement basées sur la pile Java.
- Utilisez le détecteur de serveur SAP CCMS et/ou le détecteur de serveur SAP SLD pour reconnaître des informations quand le système SAP NetWeaver a des applications basées sur les piles ABAP et Java.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Installation des bibliothèques SAP Java Connector (JCo) :

Vous devez installer les bibliothèques SAP Java Connector (JCo) 2.*x* pour les systèmes d'exploitation spécifiques des serveurs TADDM et/ou des ancres dans l'environnement TADDM.

Pour installer les fichiers de bibliothèque JCo, procédez comme suit, où *système_exploitation* représente `AIX`, `Linux`, `Linuxs390x` ou `Windows`:

1. Sélectionnez les bibliothèques SAP JCo appropriées qui sont fournies avec TADDM. La seule version fournie avec TADDM est 2.1 32 bits.

   Le tableau suivant répertorie les formats de nom standard des packages de bibliothèques SAP JCo, en fonction du système d'exploitation.

Tableau 13. Noms de package des fichiers de bibliothèque SAP JCo 2.x

Système d'exploitation	Nom du package
AIX (32 bits)	sapjco21P_10-10002239.zip
AIX (64 bits)	sapjco21P_10-10002882.zip
Windows Server on x86_32 (32 bits)	sapjco21P_10-10002243.zip
Windows on x86_64 (64 bits)	sapjco21P_10-20001730.zip
Linux on x86_32 (32 bits)	sapjco21P_10-20007301.zip
Linux on x86_64 (64 bits)	sapjco21P_10-20007300.zip
Linux on zSeries (64 bits)	sapjco21P_10-10002245.zip
Linux on Power (64 bits)	sapjco21P_10-20007302.zip

2. Sauvegardez le répertoire suivant : `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*.
3. Copiez les fichiers suivants du package vers les répertoires suivants :

   Pour les systèmes d'exploitation UNIX ou Linux :
   - `librfccm.*` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*
   - `libsapjcorfc.so` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*
   - `sapjco.jar` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*`/lib`

   Systèmes d'exploitation Windows :
   - `librf32.dll` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*
   - `sapjcorfc.dll` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*
   - `sapjco.jar` dans `$COLLATION_HOME/lib/JCo/`*`système_exploitation`*`/lib`
4. Redémarrez le serveur TADDM.

Exécutez la commande **ldd** sur les bibliothèques pour afficher les dépendances et s'assurer qu'elles sont prises en charge. Le système d'exploitation de base prend en charge la plupart des dépendances.

Sous le système d'exploitation Linux, il est possible que la bibliothèque `libstdc++-libc6.2-2.so.3` ne soit pas installée par défaut. Dans ce cas, vous devez installer le package Red Hat `compat-libstdc++-296` pour récupérer les fichiers de bibliothèque `libstdc++-libc6.2-2.so.3`.

Si les dépendances de bibliothèque ne sont pas prises en charge, le message suivant est affiché :

```
Sensor failed in remote server: JCO.classInitialize ():  Could not load middleware layer
'com.sap.mw.jco.rfc.MiddlewareRFC' JCO.nativeInit (): Could not initialize dynamic link library sapjcorfc
 [Can't find library sapjcorfc  (libsapjcorfc.so) in sun.boot.library.path or java.library.path sun.boot.
library.path={full-path-list}
```

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Computing Center Management System (CCMS)** comme **Type de composant**.

2. Indiquez les informations requises suivantes :
   a. Nom d'utilisateur (le nom d'utilisateur doit posséder au minimum toutes les autorisations mentionnées dans la liste suivante)
   b. Mot de passe
   c. ID client

Les autorisations requises par l'utilisateur SAP utilisé pour la reconnaissance du détecteur CCMS sont répertoriées ci-dessous. Accordez tous (*) les privilèges aux objets d'autorisation suivants :

S_RFC
Contrôle d'autorisation pour un accès RFC

S_ADMI_FCD
Autorisations du système

S_DATASET
Autorisation d'accès au fichier.

Les autorisations d'accès minimales sont :

- READ
- READ avec FILTER

Important : N'accordez pas toutes (*) les autorisations.

S_LOG_COM
Autorisation d'exécution des commandes logiques du système d'exploitation

S_RZL_ADM
Poste de contrôle CC : administration de système

Les autorisations d'accès minimales sont :

- DISPLAY

Important : N'accordez pas toutes (*) les autorisations.

S_XMI_LOG
Autorisation d'accès interne pour le journal XMI

S_XMI_PROD
Autorisation pour les interfaces de gestion externes (XMI)

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

com.collation.platform.os.ignoreLoopbackProcesses=`true`
La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si

le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur SAP CCMS et propose des solutions à ces problèmes.

Panne du détecteur dans un serveur distant

Problème

Les erreurs suivantes se produisent, ce qui indique que le chemin d'accès de la classe ne contient aucun chemin d'accès pour le fichier `sapjco.jar` :

```
Sensor failed in remote server: com/sap/mw/jco/JCO
MSG_ERROR: java.lang.NoClassDefFoundError: com/sap/mw/jco/JCO
```

Solution

Le fichier `sapjco.jar` doit se trouver dans le répertoire `$COLLATION_HOME/lib/JCo/lib`, le chemin d'accès de ce fichier doit se trouver dans le chemin d'accès aux classes.

Identifiez le message suivant dans le fichier `DiscoverManager.log` :

```
ajout de ce fichier jar à la liste : {jar-file-path}
```

L'élément *jar-file-path* doit être `$COLLATION_HOME/lib/JCo/lib/sapjco.jar`.

Le détecteur ne peut pas identifier le fichier de bibliothèque

Problème

Les erreurs suivantes se produisent, ce qui indique que le détecteur ne peut pas identifier le fichier de bibliothèque `libsapjcorfc.so` dans les chemins d'accès `sun.boot.library.path` ou `java.library.path` :

```
Sensor failed in remote server:
JCO.classInitialize (): Could not load middleware layer
'com.sap.mw.jco.rfc.MiddlewareRFC'
JCO.nativeInit (): Could not initialize dynamic link library sapjcorfc
[Can't find library sapjcorfc (libsapjcorfc.so) in sun.boot.library.path
or java.library.path sun.boot.library.path={full-path-list}
```

Solution

Vérifiez que le fichier de bibliothèque `libsapjcorfc.so` se trouve dans le chemin `$COLLATION_HOME/lib/JCo/`*`système d'exploitation`*.

La version du fichier de bibliothèque doit être la version de 64 bits, car les serveurs TADDM, et/ou les ancres de l'environnement TADDM exécutent un système d'exploitation 64 bits.

Assurez-vous également que ce chemin d'accès se trouve dans *full-path-list* du fichier `sun.boot.library.path` mentionné dans le message d'erreur. Si c'est le cas, l'incident peut provenir des dépendances de bibliothèques qui n'ont pas été respectées. Exécutez la commande **`ldd`** en fonction du fichier de bibliothèque `libsapjcorfc.so` pour obtenir une liste des dépendances de bibliothèques et vérifier que votre environnement les prend en charge.

Aucune liste d'accès au CCMS pour une adresse IP

Problème

L'erreur suivante se produit :

```
ERROR collation. AnchorClient - No CCMS access list provided for:
{ip-address}
```

Cette erreur peut se produire pour l'une des raisons suivantes :

- Aucune liste d'accès n'est fournie pour le détecteur.
- Le détecteur ne peut pas se connecter correctement à l'adresse IP avec les informations de la liste d'accès fournies par l'utilisateur.

Solution

Si vous avez indiqué les droits d'accès requis de la liste d'accès, vérifiez les éléments suivants :

- Assurez-vous que l'ID utilisateur répond à un nombre minimal d'exigences d'autorisation spécifiées.
- Assurez-vous que le serveur SAP ABAP est accessible.
- Identifiez le message suivant dans le fichier `local-anchor*.log` et assurez-vous que le *nomutilisateur* et le *id-client* qui sont spécifiés correspondent à ceux que vous avec définis :

  ```
  Checking connection with username: {nomutilisateur} and
  clientID: {id-client}
  ```

  Vous pouvez également attribuer une autorisation SAP_ALL à l'utilisateur et essayer de vous connecter au serveur SAP ABAP directement via l'interface graphique SAP, si elle est disponible.

Détecteur de serveur SAP SLD

Le détecteur de serveur SAP SLD reconnaît les systèmes SAP, les serveurs SAP (ABAP et Java) et les composants SAP.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SLDServerSensor

Prérequis

Le serveur SAP System Landscape Directory (SLD) doit être en cours d'exécution.

Selon l'application spécifique des systèmes SAP NetWeaver, vous pouvez utiliser le détecteur de serveur SAP CCMS et/ou le détecteur de serveur SAP SLD pour reconnaître ces systèmes. Les applications SAP sont installées sur deux schémas distincts de base de données, chacune étant ensuite accessible via son environnement d'exécution. Il existe un environnement d'exécution pour les instances Java (pile Java) et un pour les instances ABAP (Advanced Business Application Programming, pile ABAP):

- Utilisez le détecteur de serveur SAP CCMS pour reconnaître des informations quand le système SAP NetWeaver a des applications uniquement basées sur la pile ABAP.
- Utilisez le détecteur de serveur SAP SLD pour reconnaître des informations quand le système SAP NetWeaver a des applications uniquement basées sur la pile Java.
- Utilisez le détecteur de serveur SAP CCMS et/ou le détecteur de serveur SAP SLD pour reconnaître des informations quand le système SAP NetWeaver a des applications basées sur les piles ABAP et Java.

Remarque : Fix Pack 5 Si vous souhaitez modifier le port SLD en appliquant un port différent du port par défaut répertorié, vous pouvez définir la nouvelle liste de ports dans le panneau de configuration du détecteur. La connexion SLD sera établie à l'aide des nouveaux ports répertoriés.

Objets de modèle avec attributs associés

Le détecteur de serveur SAP SLD crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur à propos des systèmes SAP, des serveurs SAP (ABAP et Java) et des composants SAP de votre environnement informatique.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

AppConfig

- Content
- Parent

Fix Pack 2 **DatabaseServer**

- HierarchyDomain
- HierarchyType
- Host
- OpenId
- ProductVersion
- VendorName

Dans TADDM 7.3.0.2 et versions ultérieures, le détecteur de serveur SAP SLD reconnaît également d'autres bases de données qu'Oracle, DB2 et MS SQL Server. Par exemple, il reconnaît la base de données SAP HANA. Le détecteur crée un type d'objet de modèle pour ces bases de données, nommé `DatabaseServer`. Pour différencier les bases de données au sein de cette classe, les attributs `hierarchyDomain` et `hierarchyType` sont définis pour chaque objet. Par exemple, les attributs sont définis sur les valeurs suivantes pour l'objet `HDB` :

```
hierarchyDomain="app.db.hdb.mysap"
hierarchyType="HDBDatabaseServer"
```

FunctionalGroup

- App
- GroupName
- Members

MySAPABAPApplicationServer

- BasisAppSystemNumber
- Host
- KeyName
- MySAPKernelRelease
- PrimarySAP
- ProcessPools
- ProductName
- SAPSystemSID
- Status
- SystemHome

MySAPCluster

- SAPSystemSID
- Servers
- Status

- SystemHome

MySAPClusterNode

- ClusterNodeID
- Parent
- Type

MySAPDb2Instance

- Host
- Owner
- ProductVersion
- SAPSystemSID
- SID
- SystemHome
- VendorName

MySAPJ2EEEngineInstance

- ClusterNodes
- ConfigContents : cet attribut est disponible uniquement pour l'objet MySAPJ2EEEngineInstance pour lequel le détecteur a été démarré
- Host
- JavaInstanceId
- IsSDM
- PrimarySAP : cet attribut est disponible uniquement pour l'objet MySAPJ2EEEngineInstance pour lequel le détecteur a été démarré
- ProcessPools : cet attribut est disponible uniquement si l'objet MySAPJ2EEEngineInstance est membre de l'objet SAPSystem
- SAPSystemSID
- Status : cet attribut est disponible uniquement si l'objet MySAPJ2EEEngineInstance est membre de l'objet SAPSystem
- SystemHome
- VersioningAndPatchInfo

MySAPJavaCentralSystem

- ClusterNodes
- Host
- JavaInstanceId
- IsSDM
- ProcessPools : cet attribut est disponible uniquement si l'objet MySAPJavaCentralSystem est membre de l'objet SAPSystem
- SAPSystemSID
- Status : cet attribut est disponible uniquement si l'objet MySAPJavaCentralSystem est membre de l'objet SAPSystem
- SystemHome
- VersioningAndPatchInfo

MySAPOracleInstance

- Home
- Host
- HostName

- Owner
- ProductVersion
- SAPSystemSID
- SID
- SystemHome
- VendorName

MySAPSqlServer

- Host
- KeyName
- Owner
- ProductName
- ProductVersion
- SAPSystemSID
- SID
- SystemHome
- VendorName

ProcessPool

- Name
- Parent
- RuntimeProcesses

RuntimeProcess

SAPComponent

- Description
- HighestSupportPackage
- Name
- Parent
- PatchLevel
- Release

SAPSystem

- AppVersion
- BasisVersion
- Contact
- DeployedComponents
- Description
- Groupes
- InstallationNumber
- LicenseExpiryDate
- Name
- SAPSystemSID
- SystemHome
- Vendor

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Serveur annuaire de l'infrastructure du système (SLD)** en tant que **type de composant**.
2. Entrez les informations requises suivantes, **Nom d'utilisateur** et **Mot de passe**.

Vous devez affecter les rôles `SAP_SLD_GUEST` et `SAP_J2EE_GUEST` au compte SAP et, en fonction de votre configuration, vous devez éventuellement lui affecter aussi le rôle `SAP_J2EE_ADMIN`.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

com.collation.discover.agent.SLDServerAgent.connectionTimeout=30
La valeur par défaut est `30`, ce qui signifie 30 secondes. La valeur doit être un entier.

Cette propriété indique la durée maximale (en secondes) à attendre pour le test initial de connexion à SLD.

Les expirations de délai de connexion sont enregistrés dans le fichier `DiscoveryManager.log`. Si ces délais d'attente se produisent, augmentez la valeur de cette propriété.

La propriété peut être sectorisée pour un nom d'hôte ou une adresse IP spécifique, comme illustré dans l'exemple suivant :

```
com.collation.discover.agent.SLDServerAgent.connectionTimeout.Linux.1.2.3.4=60
com.collation.discover.agent.SLDServerAgent.connectionTimeout.SunOS=45
```

com.collation.platform.os.ignoreLoopbackProcesses=true
La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

com.collation.discover.agent.SLD.PoolSize
Cette propriété indique le nombre maximum de pools de connexions à conserver pour un serveur SLD. Ces connexions peuvent être réutilisées pour des demandes supplémentaires. La valeur par défaut est `16`.

com.collation.sudoCommand
Cette propriété indique le nom de la commande sudo. La valeur par défaut est `sudo`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur SAP SLD et propose des solutions à ces problèmes.

Erreurs du délai de connexion à SLDServerAgent

Problème

Les erreurs du délai de connexion à SLDServerAgent se trouvent dans le fichier `DiscoverManager.log`.

Solution

Dans le fichier `$COLLATION_HOME/etc/collation.properties`, augmentez la valeur de la propriété `com.collation.discover.agent.SLDServerAgent.connectionTimeout` jusqu'à ce que la connexion aboutisse.

détecteur de serveur SMB

Le serveur SMB reconnaît les serveurs de fichiers SMB (Server Message Block).

Nom du détecteur utilisé dans l'interface graphique et les journaux

SMBServerSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.ServiceAccessPoint
- sys.SMBExport
- sys.SMBSAP
- sys.SMBService

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur SMB et propose les solutions à ces problèmes.

Message d'erreur relatif à une exception non interceptée lors de l'exécution d'une reconnaissance

Problème

Le message suivant s'affiche lors de l'exécution d'une reconnaissance :

```
Exception non interceptée lors de l'appel de GetSystemInfo:
  System.NullReferenceException:
 La référence d'objet n'est pas définie à une instance d'un objet
```

Solution

Ce message indique qu'il y a un problème avec le service WMI (Windows Management Instrumentation). Pour plus d'informations sur les problèmes et les solutions WMI, voir la rubrique Détecteur de système informatique Windows«Identification et résolution des problèmes liés au détecteur», à la page 416.

Détecteur de serveur SMS

Le détecteur de serveur SMS reconnaît les serveurs Microsoft Systems Management Server (SMS).

Nom du détecteur utilisé dans l'interface graphique et les journaux

SMSServerSensor

Limitations

Le détecteur ne reconnaît pas les informations sur les systèmes informatiques client du serveur SMS en tant qu'instances CDM ComputerSystem, il les reconnaît en tant qu'instances CDM SMSCollectionClients.

Par conséquent, la reconnaissance d'un serveur SMS ne peut pas être utilisée à la place de la reconnaissance directe des hôtes faisant partie de l'infrastructure du serveur SMS.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.sms.SMSAdvertizements
- app.sms.SMSCollections
- app.sms.SMSCollectionClients
- app.sms.SMSHierarchy
- app.sms.SMSPackage
- app.sms.SMSProgram
- app.sms.SMSQuery
- app.sms.SMSReports
- app.sms.SMSResource
- app.sms.SMSServerProcess
- app.sms.SMSSiteBoundaries
- app.sms.SMSSiteComponents
- app.sms.SMSSiteServer

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.discover.agent.SMSServerAgent.GetReports
: Si cette entrée est définie à true, les informations de rapport SMS sont capturées par le détecteur et sont stockées sous forme d'instances de la classe CDM SMSReports. La valeur par défaut est false.

com.collation.discover.agent.SMSServerAgent.GetQueries
: Si cette entrée est définie à true, les requêtes prédéfinies du serveur SMS sont capturées par le détecteur et sont stockées sous forme d'instances de la classe CDM SMSQuery. La valeur par défaut est false.

com.collation.discover.agent.SMSServerAgent.GetClients
: Si cette entrée est définie à true, les informations sur les clients de collecte du serveur SMS sont capturées par le détecteur et sont stockées sous forme d'instances de la classe CSM SMSCollectionClients. La valeur par défaut est false.

com.collation.discover.agent.SMSServerAgent.MaxNrClients
Nombre maximum de clients pour lesquels des informations sont capturées par le détecteur. La valeur par défaut est 100.

détecteur SysImager

Le détecteur SysImager reconnaît des clusters SystemImager High Performance Computing (HPC).

Nom du détecteur utilisé dans l'interface graphique et les journaux

SysImagerServerSensor et SysImagerNodeSensor

Prérequis

Le détecteur GenericComputerSystemSensor et les autres détecteurs requis doivent être activés dans le profil de reconnaissance utilisé pour la reconnaissance du cluster SysImager.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.hpc.cm.ConfigurationManagementCluster
- sys.hpc.cm.ConfigurationManagementNode
- sys.hpc.cm.ConfigurationMangementNodeGroup
- sys.hpc.cm.ConfigurationManagementClusterConfigFile
- sys.hpc.cm.SysImagerNode
- sys.hpc.cm.SysImagerNodeImage
- sys.hpc.cm.SysImagerOverride

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Pour configurer le profil de reconnaissance, procédez comme suit :

1. Créez un profil de reconnaissance et sélectionnez une configuration d'agent de type SysImagerServerAgentConfiguration.
2. Définissez les attributs requis suivants :

   masterServerNames
   Les adresses IP ou noms d'hôte des noeuds maîtres SysImager. Cette propriété doit être définie pour démarrer le détecteur de serveur SysImager.
3. Si approprié, définissez certains des attributs suivants, ou acceptez les valeurs par défaut.

   configFileLocation
   Emplacement du fichier de configuration SysImager. La valeur par défaut est `/etc/systemimager/systemimager.conf`.

clusterXMLFileLocation
Emplacement du fichier de configuration du cluster SysImager. La valeur par défaut est `/etc/systemimager/cluster.xml`.

clusterConfigCommand
Commande permettant d'afficher les informations de configuration relatives au cluster SysImager. La valeur par défaut est**`si_clusterconfig -g`**.

lsImageCommand
Commande permettant d'afficher les images du cluster SysImager. La valeur par défaut est **`si_lsimage -v`**.

imagesDiscoveryMode
Cette propriété n'est pas utilisée.

overridesDiscoveryMode
Profondeur de capture de fichier pour des substitutions. Les valeurs admises sont les suivantes :

- `0` : aucune information de fichier n'est capturée.
- `1` : seuls le nom de fichier et les informations relatives au fichier sont capturés.
- `2` : toutes les informations de fichier et le contenu sont capturées.

La valeur par défaut est 1.

overridesDiscoveryPattern
Modèle de nom de fichier des fichiers figurant sous le répertoire des substitutions. La valeur par défaut est "`*`".

preInstallScriptsContent
Profondeur de capture de fichier des scripts exécutés avant l'installation. Les valeurs valides sont les suivantes :

- `0` : aucune information de fichier n'est capturée.
- `1` : seuls le nom de fichier et les informations relatives au fichier sont capturés.
- `2` : toutes les informations de fichier et le contenu sont capturées.

La valeur par défaut est 1.

postInstallScriptsContent
Profondeur de capture de fichier des scripts exécutés après l'installation. Les valeurs admises sont les suivantes :

- `0` : aucune information de fichier n'est capturée.
- `1` : seuls le nom de fichier et les informations relatives au fichier sont capturés.
- `2` : toutes les informations de fichier et le contenu sont capturées.

La valeur par défaut est 1.

nodesScope
Portée des adresses IP auxquelles les détecteurs de noeud SysImager sont limités.

doPingNodes
Indique si les détecteurs ping sont exécutés sur les noeuds SysImager reconnus.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

SysImagerServerSensor utilise l'entrée d'accès de SysImager Server. Si cette entrée n'est pas disponible, le détecteur utilise l'entrée d'accès ComputerSystem pour accéder au serveur SysImager.

SysImagerNodeSensor utilise l'entrée d'accès ComputerSystem pour accéder aux noeuds SysImager.

Détecteur de cluster Veritas

Le détecteur de cluster Veritas reconnaît les serveurs de cluster Veritas.

Le détecteur collecte des informations générales sur le serveur de cluster Veritas et les services installés sur ce serveur. Les services sont organisés en groupes et contiennent des informations sur les ressources employées.

Le détecteur peut créer des relations entre les services et les applications installés sur un cluster.

Nom du détecteur utilisé dans l'interface graphique et les journaux

VeritasClusterSensor

Problèmes de sécurité

Le compte utilisateur utilisé pour la reconnaissance des systèmes informatiques est également utilisé pour exécuter les commandes Veritas. Par défaut, l'autorisation d'exécution dans le répertoire et les commandes Veritas Cluster est requise. Le détecteur utilise les commandes suivantes :

- **hastatus**
- **haclus**
- **hasys**
- **hares**
- **hagrp**
- **hatype**
- **hauser**

Avant d'exécuter les commandes Veritas, une connexion au cluster est exécutée sur les systèmes qui prennent en charge la commande Veritas **halogin**. Il s'agit des systèmes UNIX avec VCS version 4.1 et ultérieure. Le détecteur se connecte en utilisant le nom d'utilisateur et le mot de passe de l'entrée de la liste d'accès des solutions à haute disponibilité.

Pour indiquer que le détecteur doit utiliser **sudo** lors de l'exécution des commandes Veritas Cluster Server sous des systèmes Linux ou UNIX, configurez les paramètres appropriés dans le fichier collation.properties.

Pour exécuter les commandes sans utiliser la commande **sudo**, le compte de service TADDM doit être un membre du groupe d'administration Veritas sur la cible.

Fix Pack 5 Les commandes suivantes doivent être exécutées manuellement sur la cible Veritas pour vérifier si les droits sont suffisants pour reconnaître le détecteur VeritasClusterSensor correctement :

- **halogin [utilisateur] [motdepasse]**
- **halogout -endallsessions**
- **halogout -endsession localhost**
- **haclus -display**
- **hasys -display**
- **hares -dep**
- **hares -display**
- **hagrp -resources [groupe]**
- **hagrp -dep [groupe]**
- **hagrp -display**
- **hatype -display**

Vous devez configurer `sudo ndd with NOPASSWORD` pour l'utilisateur de l'accès.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.ConfigFile
- app.SoftwareInstallation
- app.veritas.cluster.VCSCluster
- app.veritas.cluster.VCSHADServer
- app.veritas.cluster.VCSLocalServiceGroup
- app.veritas.cluster.VCSResourceConfiguration
- app.veritas.cluster.VCSServiceGroup
- app.veritas.cluster.VCSSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

L'attribut **VeritasClusterSensor** suivant peut être modifié :

discoveryMode

La valeur par défaut de l'attribut **discoveryMode** est 1 (Le détecteur s'exécute en mode léger).

Pour générer davantage d'éléments de configuration et les stocker dans la base de données, indiquez `0`.

Sinon, ouvrez `$COLLATION_HOME/etc/discover-sensors/VeritasClusterSensor.xml` et modifier l'attribut.

Lorsque vous utilisez un détecteur de cluster Veritas et un détecteur pour reconnaître une instance Oracle, des doublons peuvent apparaître. Ceci se produit parce que le détecteur de cluster Veritas utilise des majuscules pour le SID de l'instance et le détecteur Oracle utilise les minuscules pour le même SID. Pour

éviter ce problème, modifiez le fichier `dist/etc/discover-sensors/VeritasClusterSensor.xml` en changeant la ligne suivante :

```
<source>Sid</source>
```

pour la ligne suivante :

```
<source>%{Sid}</source>
```

Après ce changement, le détecteur de cluster Veritas crée des instances Oracle avec le SID en minuscule.

Remarque : Si vous changez la ligne après l'exécution des reconnaissances où aucun doublon n'est apparu, de nouveaux doublons pourraient apparaître.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **High Availability Solutions** en tant que **Type de composant**.
2. Entrez les informations requises suivantes, **Nom d'utilisateur** et **Mot de passe**.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Les propriétés suivantes indiquent que le détecteur utilise **sudo** pour élever les privilèges lors de l'exécution des commandes Veritas Cluster Server :

- `com.collation.discover.agent.command.hastatus.Linux=sudo /opt/VRTSvcs/bin/hastatus`
- `com.collation.discover.agent.command.haclus.Linux=sudo /opt/VRTSvcs/bin/haclus`
- `com.collation.discover.agent.command.hasys.Linux=sudo /opt/VRTSvcs/bin/hasys`
- `com.collation.discover.agent.command.hares.Linux=sudo /opt/VRTSvcs/bin/hares`
- `com.collation.discover.agent.command.hagrp.Linux=sudo /opt/VRTSvcs/bin/hagrp`
- `com.collation.discover.agent.command.hatype.Linux=sudo /opt/VRTSvcs/bin/hatype`
- `com.collation.discover.agent.command.hauser.Linux=sudo /opt/VRTSvcs/bin/hauser`

Vous pouvez configurer chaque propriété pour un système d'exploitation ou d'une adresse IP spécifique, comme dans les exemples suivants :

- `com.collation.discover.agent.command.hastatus =sudo /opt/VRTSvcs/bin/hastatus`
- `com.collation.discover.agent.command.hastatus.Linux=sudo /opt/VRTSvcs/bin/hastatus`
- `com.collation.discover.agent.command.hastatus.Linux.192.168.1.1=sudo /opt/VRTSvcs/bin/hastatus`

Indiquez l'option **sudo** pour un système d'exploitation uniquement si elle est requise pour tous les systèmes qui exécutent ce système d'exploitation ; sinon, indiquez l'option uniquement pour les adresses IP spécifiques où la commande **sudo** est configurée. Vous devez configurer `sudo ndd with NOPASSWORD` pour l'utilisateur de l'accès.

Sur chaque système cible pour lequel une escalade des privilèges est nécessaire, configurez la commande **sudo** avec l'option NOPASSWD. Sinon, la reconnaissance se bloque jusqu'au dépassement du délai du serveur TADDM.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de cluster Veritas et présente des solutions à ces problèmes.

Le détecteur échoue

Problème

Le détecteur VeritasClusterSensor échoue.

Solution

Si le détecteur échoue et que les journaux signalent l'expiration du délai de certaines commandes, cette erreur pourrait indiquer l'échec d'une connexion au cluster. Vérifiez que le nom d'utilisateur et le mot de passe corrects de Veritas Cluster sont utilisés.

Détecteur de serveur VMware VirtualCenter

Le détecteur de serveur VMware VirtualCenter reconnaît les serveurs VMware VirtualCenter ainsi que les éléments gérés par les serveurs. VMware VirtualCenter est maintenant connu sous l'intitulé VMware vCenter Server.

Nom du détecteur utilisé dans l'interface graphique et les journaux

VirtualCenterSensor

Eléments reconnus par le détecteur

Le détecteur reconnaît les éléments suivants qui sont gérés par le serveur VirtualCenter :

- Pools de ressources UC
- Centres de données dans un centre virtuel
- Domaines du magasin de données pour VMware vSphere 4
- Magasins de données créés dans chaque centre de données
- Commutateurs virtuels distribués, liens ascendants et groupe de ports dans chaque commutateur virtuel distribué
- Pools de ressources mémoire
- Numéro de série des serveurs ESX
- Commutateurs virtuels et groupes de ports dans chaque commutateur virtuel
- Clusters VMware créés dans chaque centre de données
- Serveurs VMware ESX gérés par un centre virtuel
- Adresses IP des machines virtuelles

Les serveurs VMware ESX, reconnus par les détecteurs de serveur VMware ESX et VirtualCenter, sont fusionnés après la reconnaissance.

Dans la console de gestion de reconnaissance, une machine virtuelle est représentée par une icône de système informatique bleu transparent.

Le détecteur de serveur VirtualCenter utilise l'API VMware pour reconnaître des données. Cette API collecte les données suivantes :

- les données d'attribut requises pour correspondre au règles de nommage et pour créer une instance de machine virtuelle autonome valide,
- certaines informations de base que le serveur VMware ESX fournit via la commande **vmware-cmd**,
- l'attribut `primaryMACAddress`, requis pour faire correspondre l'instance virtuelle superficielle à une instance physique pouvant être reconnue,
- l'attribut `vmwareUUID`, requis pour faire correspondre les instances d'ordinateur virtuel reconnues avant et après les migrations à l'aide de VMotion.

Il existe quatre scénarios utilisateur pour une reconnaissance de serveur VirtualCenter et ESX :

- Intégrale : La portée de la reconnaissance contient les serveurs ESX et VirtualCenter.

  Le résultat affiche les serveurs ESX et VirtualCenter. Les serveurs ESX qui sont gérés par les serveurs VirtualCenter sont affichés dans un des centres de données ou clusters du centre virtuel. Toutes les instances virtuelles et physiques reconnues par les détecteurs VirtualCenter et ESX font l'objet d'un rapprochement. Les instances physiques sont dotées d'un attribut virtuel dont la valeur est true.
- Serveur ESX uniquement : la portée de la reconnaissance contient les serveurs ESX.

  Le résultat présente les serveurs ESX qui sont reconnus par le détecteur ESX. Les serveurs ESX avec les attributs standard, par exemple modèle, sont affichés. Le détecteur VirtualCenter n'est pas démarré.
- Serveur VirtualCenter uniquement : la portée de la reconnaissance contient les serveurs VirtualCenter.

  Le résultat affiche les serveurs ESX et les ordinateurs virtuels qui sont reconnus par le détecteur VirtualCenter.
- VirtualCenter et machine virtuelle : la portée de la reconnaissance contient les serveurs VirtualCenter et tous les ordinateurs virtuels.

  Les résultats présente tous les ordinateurs virtuels, avec tous les attributs physiques et virtuels définis à true. Les ordinateurs virtuels apparaissent sous l'onglet **Systèmes virtuels** du serveur ESX respectif.

Prérequis

Le service du serveur VMware Virtual Center est en cours d'exécution sur l'ordinateur Windows cible. L'écoute de port et/ou la correspondance de modèle de processus permettent de démarrer le détecteur de serveur VMware Virtual Center. Par défaut, le détecteur est démarré par la correspondance de modèle de processus.

Restriction : Ce prérequis ne s'applique pas à vCSA (Virtual Center Server Appliance). vCSA est basé sur la technologie Linux et est détecté par TADDM au moyen des autorisations standard, sans autre prérequis nécessaire.

Fix Pack 3 Pour que la reconnaissance de VMware vCenter Server Appliance 6 s'effectue correctement, des ports doivent être définis pour la communication des

services Web. Par défaut, les ports 80 et 443 sont définis. Si votre VMware vCenter Server Appliance 6 utilise des ports non standard, modifiez la valeur de la propriété `portList` dans le profil de reconnaissance. Pour plus d'informations, voir «Configuration du profil de reconnaissance», à la page 169.

Prise en charge de la reconnaissance de Virtual Center System Appliance via des ports Web

Cette amélioration peut vous permettre d'effectuer la reconnaissance VCSA en utilisant des interfaces Web. Une nouvelle option de configuration a été ajoutée au détecteur PortScan pour permettre d'utiliser la spécification des ports d'écoute VCSA (vcsaListPortListEcoute) pour déclencher la distribution du VirtualCenterSensor.

Limitations

- Si le port mentionné dans `vcsaListeningPortList` est ouvert par un processus autre que VCSA, le détecteur de serveur VMware Virtual Center génère une erreur.

Problèmes de sécurité

Pour reconnaître le serveur VMware Virtual Center, vous devez définir des droits d'accès en lecture seule pour le compte de service TADDM. Le compte de service doit disposer de droits administrateur.

Connexion aux serveurs avec SSL

Le détecteur VMware VirtualCenter peut se connecter au serveur avec SSL en deux modes - le mode par défaut et un nouveau mode.

Mode par défaut
Le mode par défaut ne vérifie pas complètement le certificat d'un serveur. Ce mode autorise une connexion même si le certificat est autosigné, expiré ou avec un nom d'hôte non valide. Il refuse la connexion si d'autres problèmes sont découverts, par exemple une erreur de chaînage de certificats. Le mode par défaut peut s'utiliser avec les certificats VMware par défaut.

Nouveau mode
Le nouveau mode vérifie complètement le certificat d'un serveur. Vous pouvez activer ce mode en définissant la propriété de configuration `strictCertificateCheck` à `true`. Si ce mode est activé, seuls les certificats valides signés par des autorités de certification de confiance sont acceptés.

Importation de certificats autosignés dans TADDM
En définissant la propriété `strictCertificateCheck` à `true`, vous pouvez vous connecter avec des certificats autosignés. Vous devez d'abord importer ce certificat dans TADDM. Ainsi, les certificats autosignés sont des certificats de confiance, leur validité est toujours vérifiée.

Pour importer de tels certificats, procédez comme suit :

1. Ouvrez le répertoire `taddm/dist/osgi/plugins/com.ibm.cdb.discover.sys.vmware.vmwarecommon_*` où `*` est le numéro de version du détecteur.
2. Lancez la commande suivante :

```
java -cp lib/vmwarecommon.jar com.ibm.cdb.discover.sys.vmware.
VmCertificateCollector ip:port
```

où *ip* est l'adresse IP de l'hôte du détecteur de VMware VirtualCenter et *port* est le port SSL de cet hôte.

Configuration recommandée

Vous devez sélectionner le port de configuration de manière logique pour éviter toute distribution erronée du détecteur VirtualCenterSensor (VCSA). Cette configuration fonctionne mieux si ces ports sont reconnus comme un centre virtuel unique. S'il existe une liste spécifique de ports, les ports énumérés doivent spécifier les mêmes programmes d'écoute. Ces ports tiennent compte des changements de configuration sur les instances pour éviter la collision.

Exemple :

1. Exemple : 80 TCP vCenter Server nécessite le port 80 pour les connexions HTTP directes. Le port 80 redirige la demande vers le port HTTPS 443. Cette redirection est utile si vous utilisez involontairement http://server au lieu de https://server.
2. Port TCP 443 par défaut utilisé par le système vCenter Server pour écouter les connexions à partir du client Web vSphere. Pour permettre au système vCenter Server de recevoir des données du client Web vSphere, ouvrez le port 443 dans le pare-feu.

Les ports 80 et 443 sont très répandus et peuvent sembler un mauvais choix pour la distribution du VirtualCenterSensor car ils peuvent provoquer de nombreux faux positifs pour les appels de capteurs. Il est recommandé de fournir un autre port, de préférence unique, ou des listes des valeurs possibles de ce port dans un déploiement client, qui seront utilisé(e)s dans PortScanSensors `vcsaListeningPortList`.

1. Port TCP/UDP 514 de vSphere Syslog Collector pour vCenter Server sous Windows et port de service vSphere Syslog pour vCenter Server Appliance.
2. Port TCP/UDP 902 par défaut utilisé par le système vCenter Server pour envoyer des données aux hôtes gérés. Les hôtes gérés envoient également un signal de présence régulier via le port UDP 902 au système vCenter Server. Ce port ne doit pas être bloqué par des pare-feux entre le serveur et les hôtes ou entre les hôtes.

Objets de modèle avec attributs associés

Le détecteur de serveur VMware Virtual Center crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les ressources VMware Virtual Center dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

dev.StorageExtent

- ManagedSystemName
- Name

net.IpInterface

- Name (pour le serveur ESX)
- IpAddress

net.L2Interface

- Name (pour le serveur ESX)

- HwAddress

process.CPUResourcePool

- Name
- Label
- Limit
- Reservation
- SharesLevel
- SharesValue

process.MemoryResourcePool

- Name
- Label
- Limit
- Reservation
- SharesLevel
- SharesValue

relation.AllocatedTo

- Source (MemoryResourcePool ou CPUResourcePool)
- Target (Memory ou CPU)

relation.DonatedTo

- Source (pour le serveur ESX uniquement)
- Target (MemoryResourcePool ou CPUResourcePool)

sys.CPU

- NumCPUs
- Parent

sys.DNSResolveEntry (pour le serveur ESX uniquement)

- ServerIP
- Parent

sys.Memory

- MemorySize
- Parent

sys.NFSFileSystem

- serverName
- MountPoint
- Type
- Capacity
- AvailableSpace
- MaxFileSize
- StorageExtent
- FileSystemBlockSize
- MaxBlocks

sys.unix.UnixFileSystem (pour Virtual Machine File System)

- MountPoint
- Type

- Capacity
- AvailableSpace
- MaxFileSize
- StorageExtent
- FileSystemBlockSize
- MaxBlocks

sys.vmware.DataCenter

- Name
- Label
- Parent
- Systèmes
- Clusters
- VirtualSwitches

sys.vmware.VirtualCenter

- Name
- Host
- UID
- VersionString
- ApiVersion
- Vendor
- BuildLevel
- VirtualCenterPort
- MaxDBConnections
- ClientTimeoutNormal
- ClientTimeoutLong
- WebServiceHttpPort
- WebServiceHttpsPort

sys.vmware.VMWareCluster

- Name
- Label
- DPMEnabled
- DRSEnabled
- HAEnabled
- Parent
- RootMemoryResourcePool
- RootCPUResourcePool

sys.vmware.VMWareDataStore

- Name
- Label
- Type
- DataStoreURL
- Capacity
- FreeSpace
- IsAccessible

- AccessMode
- IsMultipleHostsAccess
- BasedOn
- DataCenter

sys.vmware.VmwareESX

- OSName
- OSVersion

sys.vmware.VMWarePortGroup

- ActiveUplinks
- L2Interfaces
- Name
- Parent
- StandbyUplinks
- Liaisons montantes

sys.vmware.VmwareUnitaryComputerSystem

- Name
- Fqdn
- ObjectType
- Manufacturer
- Model
- CPUSpeed
- CPUType
- LifecycleState
- NumCPUs
- MemorySize
- AvailableMemoryForAllVMs
- CurrentMemoryForAllVMs
- SwapMemorySize
- ServiceConsoleMemorySize
- VmotionEnabled

sys.vmware.VMWareVirtualSwitch

- DataCenter
- Name
- MTU
- NumPorts
- NumPortsAvailable
- ObjectType
- PortGroups
- Parent
- UplinkPortGroups
- Interfaces

sys.vmware.VMWareDVUplink

- L2Interfaces
- Name

Plusieurs machines virtuelles, telles que les systèmes d'exploitation et les systèmes virtuels suivants :

sys.darwin.Darwin
sys.darwin.DarwinUnitaryComputerSystem
sys.dos.Dos
sys.dos.DosUnitaryComputerSystem
sys.freebsd.FreeBSD
sys.freebsd.FreeBSDUnitaryComputerSystem
sys.linux.Linux
sys.linux.LinuxUnitaryComputerSystem
sys.netware.Netware
sys.netware.NetwareUnitaryComputerSystem
sys.sun.Solaris
sys.sun.SunSPARCUnitaryComputerSystem
sys.windows.WindowsComputerSystem
sys.windows.WindowsOperatingSystem

Les attributs suivants sont associés à ces objets de modèle :

- uuid
- VMID
- OSName
- Fqdn (si VMware Tools s'exécute sur une machine virtuelle)
- MemorySize
- NumCPUs
- FaultTolerance

Configuration du détecteur

Vous devez configurer le détecteur de serveur VMware Virtual Center avant de l'utiliser.

Configuration d'utilisateurs non-administrateurs pour exécuter le détecteur :

Un utilisateur non-administrateur doit disposer d'autorisations pour exécuter le détecteur de serveur VMware Virtual Center. Vous pouvez attribuer les autorisations requises à l'aide du client VMware Infrastructure Client.

Remarque : Les comptes administrateurs disposent des autorisations nécessaires par défaut et ne nécessitent pas cette procédure.

Pour attribuer les autorisations nécessaires à un compte utilisateur non-administrateur, procédez comme suit :

1. Depuis VMware Infrastructure Client, connectez-vous au serveur VMware Virtual Center en utilisant un compte administrateur.
2. Cliquez sur l'onglet **Autorisations**.
3. Attribuez le rôle **Lecture seule** au compte utilisateur non-administrateur dont que vous souhaitez pouvoir exécuter le détecteur. Pour plus d'informations sur l'attribution des rôles aux utilisateurs, consultez la documentation VMware.

Configuration du profil de reconnaissance :

Par défaut, le détecteur de serveur VMware VirtualCenter est activé pour une reconnaissance de niveau 3. Le détecteur reconnaît tous les invités, y compris les systèmes invités qui sont éteints. Pour reconnaître uniquement les systèmes invités en cours d'exécution, créez un profil de reconnaissance de niveau 3 pour le détecteur de serveur VMware VirtualCenter, et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

1. Dans le tiroir **Reconnaissance** de la console de gestion de reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil. Dans la liste **Cloner le profil existant**, sélectionnez **Reconnaissance de niveau 3**, puis cliquez sur **OK**.
4. Sous l'onglet **Configuration du détecteur**, sélectionnez le détecteur **VirtualCenterSensor** et cliquez sur **Nouveau**.
5. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration, puis sélectionnez la case à cocher **Activer la configuration**.
6. Dans la section **Configuration** de la fenêtre Créer la Configuration, cliquez sur **discoverNonRunningGuests**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne, et entrez `false`.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Propriétés

Vous pouvez modifier les propriétés suivantes :

`ordinalESXviaVCserialDiscovery`
Reconnaît un numéro de série à l'aide de l'API VMware. Il s'agit d'une méthode standard utilisée pour reconnaître le numéro de série. Elle est plus rapide que l'utilisation de l'API CIM, requiert moins de privilèges mais est aussi davantage sujette aux erreurs.

La valeur par défaut est `false`.

`directESXserialDiscovery`
Reconnaît un numéro de série à l'aide de l'API CIM. Cette méthode reconnaît toujours le numéro de série mais elle est plus lente et les contraintes suivantes s'appliquent :

- L'utilisateur de la reconnaissance doit disposer du privilège `Hôte > CIM > Interation CIM`.
- La connexion entre TADDM et le serveur ESX est requise.

Pour plus d'informations, reportez-vous également à la note technique à l'adresse http://www-01.ibm.com/support/docview.wss?uid=swg21638454.

Important : Si vous exécutez le serveur ESX sur du matériel virtualisé tel que Cisco UCS, vous devez reconnaître le numéro de série en utilisant l'API CIM et non l'API VMware, car sinon une fusion pourrait se produire.

La valeur par défaut est `false`.

shallowVMdiscovery
Reconnaît des données limitées pour une machine virtuelle.

La valeur par défaut est `false`.

discoverNonRunningGuests
Reconnaît des machines virtuelles non en cours d'exécution.

La valeur par défaut est définie sur `true`.

strictCertificateCheck
Force le détecteur à se connecter aux serveurs VirtualCenter qui sont sécurisés avec des certificats signés d'autorités de certification et valides.

La valeur par défaut est `false`.

enableVMDiscovery
Active la reconnaissance des machines virtuelles.

La valeur par défaut est définie sur `true`.

shallowESXDiscovery
Active la reconnaissance ESX superficielle. Les serveurs ESX sont reconnus uniquement avec un nom, des informations de magasins de données et des informations au centre de données. La propriété peut être utilisée avec un détecteur ESXi pour une reconnaissance plus rapide de l'environnement complet.

La valeur par défaut est `false`.

Fix Pack 3 **portList**
Contient une liste séparée par des virgules des ports utilisés par VMware vCenter Server Appliance 6 pour la communication avec les services Web. Modifiez la valeur de cette propriété si votre VMware vCenter Server Appliance 6 utilise des ports non standard.

La valeur par défaut est `80,443`.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour accéder au serveur VMware Virtual Center à l'aide d'un compte bénéficiant des privilèges de l'administrateur, procédez comme suit :
  1. Utilisez **ComputerSystem (Windows)** comme **Type de composant**.
  2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe).

     Utilisez cette méthode pour accorder un accès au système informatique hôte et au serveur VMware Virtual Center.
- Pour accéder au serveur VMware Virtual Center à l'aide d'un compte bénéficiant des privilèges En lecture seule, procédez comme suit :
  1. Utilisez **Virtual Center Server** comme **Type de composant**.
  2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe).

     Utilisez cette méthode pour reconnaître les serveurs VMware Virtual Center dans un environnement IBM Tivoli Monitoring. Elle accorde un accès uniquement au serveur Virtual Center, mais pas au système informatique hôte. Dans le profil de reconnaissance, incluez le détecteur de serveur VMware Virtual Center et le détecteur de portée IBM Tivoli Monitoring.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur VMware Virtual Center et propose des solutions à ces problèmes.

Numéro de série et ID système ne sont pas définis dans le panneau Détails du serveur VMware ESX

Problème

Les attributs Numéro de série et ID système ne sont pas définis dans le panneau Détails du serveur VMware ESX. Les attributs du système de fichiers ne sont pas reconnus.

Solution

TADDM utilise l'interface de programme d'application SMASH pour se connecter directement au serveur ESX. Assurez-vous que la connexion est ouverte pour le port indiqué dans la propriété `com.collation.discover.vmware.cimport` (par défaut, la valeur est 5989), ou utilisez plutôt un ancre. ESX doit prendre en charge le programme d'application SMASH.

Vérifiez que les serveurs ESX et Virtual Center sont inclus dans la portée de la reconnaissance. Vérifiez les données d'identification pour vous assurer que les autorisations correctes sont utilisées pour accéder aux serveurs ESX et Virtual Center, puis exécutez la reconnaissance de nouveau. Pour la couche L2Interface, le détecteur collecte uniquement le nom et les adresses matérielles.

Le détecteur échoue avec une erreur de délai d'attente

Problème

Si le serveur Virtual Center gère de nombreux hôtes et ordinateurs virtuels ESX, le détecteur peut échouer avec un message d'erreur de délai d'attente, `Une erreur s'est produite. Le délai du détecteur a expiré.`

Solution

Dans le fichier `etc/collation.properties`, augmentez la valeur afin que le serveur puisse être exécuté, où *valeur* correspond au nombre de millisecondes autorisées pour l'exécution du détecteur :

`com.collation.discover.agent.VirtualCenterSensor.timeout=`*`value`*

La valeur par défaut est `3600000` .

Des éléments gérés par le serveur VMware Virtual Center ne sont pas reconnus

Problème

Des éléments ne sont pas reconnus sur VMware vCenter Server version 4.1 exécuté sous Microsoft Windows Server 2003. Les messages d'erreur suivants sont présents :

- Le journal `VirtualCenterServer` contient les lignes suivantes :

```
AxisFault
 faultCode: {http://xml.apache.org/axis/}HTTP
 faultSubcode:
 faultString: (503)Service Unavailable
 faultActor:
 faultNode:
```

```
 faultDetail:
 {}:return code:  503
503 Service Unavailable {http://xml.apache.org/axis/}HttpErrorCode:503
  (503)Service Unavailable )
```

- Le journal vpxd du serveur VMware Virtual Center contient les lignes suivantes :

```
Connection to localhost:8085 failed with error class Vmacore::SystemException
(Normally allowed each socket address (protocol / network address / port)
is used only once.
```

- L'exécution d'une commande **netstat -ban | findstr 8085** émise à partir du serveur VMware Virtual Center affiche de nombreux ports TCP/IP restés ouverts dans l'état LAST_ACK.

Solution

Le comportement apparaît se produit car des ports éphémères, ports temporaires utilisées pour des communications du serveur client, ne sont pas fermés après usage. Les ports temporaires sont limités à une plage de ports et ne sont valides que pour la durée de la connexion. Dans ce cas, sur certains systèmes d'exploitation Microsoft Windows, certaines connexions laissent les ports dans l'état Last_ACK sur le serveur Virtual Center. La plage de ports peut être épuisée après un temps et si cette situation se produit, la connectivité peut échouer tant qu'un port n'est pas libéré.

Pour prévenir cette éventualité, accédez au site Web de Microsoft à http://support.microsoft.com et recherchez KB979230. Vous pourrez ensuite télécharger et installer le correctif.

Détecteur WebLogic

Le détecteur WebLogic reconnaît des serveurs d'application Oracle WebLogic Server et des informations de version de serveur WebLogic.

Les fichiers JAR de toutes les éditions de WebLogic 9 peuvent être utilisés pour reconnaître toutes les éditions de WebLogic 9 et 10.

Nom du détecteur utilisé dans l'interface graphique et les journaux

- WeblogicSensor
- WeblogicSensor2
- WeblogicServerVersionSensor

Prérequis

Le détecteur WeblogicSensor nécessite des fichiers JAR supplémentaires qui font partie de l'installation d'Oracle WebLogic Server. Vous devez copier ces fichiers JAR dans les répertoires suivants du serveur TADDM :

- Pour les systèmes d'exploitation Linux, AIX et Linux sous System z :
  - $COLLATION_HOME/lib/weblogic/9.0
  - $COLLATION_HOME/lib/weblogic/10.0
- Pour les systèmes d'exploitation Windows :
  - %COLLATION_HOME%\lib\weblogic\9.0
  - %COLLATION_HOME%\lib\weblogic\10.0

Vous devez configurer le nom spécifique du répertoire `$COLLATION_HOME/lib/weblogic/$VERSION_DIR` dans le fichier `$COLLATION_HOME/etc/discover-sensors/WeblogicVersionSensor.xml`.

Il n'existe aucune limite au nombre de répertoires $VERSION_DIR que vous pouvez créer dans le répertoire `$COLLATION_HOME/lib/weblogic/`. Toutefois, chaque répertoire doit être configuré dans le fichier `WeblogicVersionSensor.xml` .

Problèmes de sécurité

Le serveur TADDM exige le nom de connexion et le mot de passe du système WebLogic utilisés pour la connexion à la console produit WebLogic.

Limitations

TADDM ne prend pas en charge la reconnaissance WebLogic avec le détecteur WebLogic lors de l'utilisation de SSL.

Le détecteur WebLogic doit être exécuté avec les détecteurs connectables WebLogic SSH dans le même répertoire. N'activez pas le détecteur WebLogic ni les détecteurs connectable SSH WebLogic dans le même profil de reconnaissance.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.AppServer
- app.ConfigFile
- app.j2ee.weblogic.WebLogicServer
- app.j2ee.J2EEComponent
- app.j2ee.J2EEDeployedObject
- app.j2ee.J2EEDomain
- app.j2ee.J2EEModule
- app.j2ee.J2EEResource
- app.j2ee.weblogic.WebLogicCluster
- app.j2ee.weblogic.WebLogicConnector
- app.j2ee.weblogic.WebLogicConnectorModule
- app.j2ee.weblogic.WebLogicDomain
- app.j2ee.weblogic.WebLogicEJBModule
- app.j2ee.weblogic.WebLogicJ2EEApplication
- app.j2ee.weblogic.WebLogicJDBCConnectionPool
- app.j2ee.weblogic.WebLogicJDBCDataSource
- app.j2ee.weblogic.WebLogicJDBCDriver
- app.j2ee.weblogic.WebLogicJDBCMultiPool
- app.j2ee.weblogic.WebLogicJDBCTxDataSource
- app.j2ee.weblogic.WebLogicJMSServer
- app.j2ee.weblogic.WebLogicJMSStore
- app.j2ee.weblogic.WebLogicJTA
- app.j2ee.weblogic.WebLogicMachine
- app.j2ee.weblogic.WebLogicSSLSettings

- app.j2ee.weblogic.WebLogicServer
- app.j2ee.weblogic.WebLogicServlet
- app.j2ee.weblogic.WebLogicVirtualHost
- app.j2ee.weblogic.WebLogicWebContainer
- app.j2ee.weblogic.WebLogicWebModule
- app.ProcessPool
- app.SoftwareContainer
- app.web.WebVirtualHost

Configuration du détecteur

Vous devez configurer le détecteur WebLogic avant de l'utiliser.

Copie des fichiers JAR dans le serveur TADDM :

Vous devez copier des fichiers JAR supplémentaires qui font partie de l'installation du serveur WebLogic Oracle Server dans le serveur TADDM.

Avant de démarrer une reconnaissance, copiez les fichiers JAR requis pour votre version de WebLogic dans le répertoire `$COLLATION_HOME/lib/$version_dir/ / WebLogic` :

Tableau 14. Fichiers JAR WebLogic obligatoire

Version de WebLogic	Fichiers JAR requis
WebLogic version 9 (toutes éditions)	• `$WEBLOGIC_HOME/server/lib/weblogic.jar` • `$WEBLOGIC_HOME/server/lib/webservices.jar` • `$WEBLOGIC_HOME/server/lib/wljmxclient.jar`
WebLogic version 10.0 à 10.2	
WebLogic version 10.3	• `$WEBLOGIC_HOME/server/lib/wlfullclient.jar`

Vérifiez que l'utilisateur utilisé pour exécuter TADDM dispose de droits d'accès en lecture aux fichiers JAR copiés.

Création d'un fichier wlfullclient.jar pour le détecteur WebLogic :

Vous devez créer un fichier `wlfullclient.jar` pour une application client. Ce fichier JAR est obligatoire pour WebLogic version 10.3 ou ultérieure.

Pour créer un fichier `wlfullclient.jar` pour le détecteur WebLogic, procédez comme suit :

1. Accédez au répertoire dans lequel le serveur WebLogic est installé :
   ```
   cd WL_HOME/server/lib
   ```
2. Créez le fichier `wlfullclient.jar` :
   ```
   java -jar ../../../modules/com.bea.core.jarbuilder_X.X.X.X.jar
   ```
   où *X.X.X.X* représente le numéro de version du module `JarBuilder` dans le répertoire `WL_HOME/server/lib`. Par exemple :
   ```
   java -jar ../../../modules/com.bea.core.jarbuilder_1.0.1.0.jar
   ```
3. Copiez et regroupez le fichier `wlfullclient.jar` avec l'application client.
4. Ajoutez le fichier `wlfullclient.jar` dans votre chemin de classe Java.

Edition du fichier WeblogicVersionSensor.xml :

Vous devez éditer le fichier `WeblogicVersionSensor.xml` .

Le fichier de configuration se trouve dans les répertoires suivants :

- Sous les systèmes d'exploitation Linux, Solaris, AIX et Linux sous System z, le fichier est dans le répertoire *$COLLATION_HOME*`/etc/discover-sensors/`.
- Sous les systèmes d'exploitation Windows, le fichier est dans le répertoire *%COLLATION_HOME%*`\etc\discover-sensors\`.

L'exemple de code figurant dans cette section vous présente comment configurer les répertoires et Java à l'aide de balises XML. Dans cet exemple, les associations suivantes de répertoires et de JRE sont configurées :

- Les fichiers JAR du répertoire `lib/weblogic/10.0` sont associés à Java SDK version 1.5.0 JRE.
- Les fichiers JAR du répertoire `lib/weblogic/9.0` sont associés à Java SDK version 1.5.0 JRE.

La balise `<entry>` configure le nom du répertoire utilisé pour stocker les fichiers JAR WebLogic. Les fichiers JAR WebLogic doivent se trouver dans le répertoire `lib/weblogic`.

De même, la balise `<jdk>` configure la version SDK Java utilisée. La seule valeur valide est `1.5.0`. Si le détecteur WeblogicServerVersionSensor ne reconnaît pas le serveur BEA WebLogic en cours d'exécution, vous pouvez utiliser la balise `<WeblogicClassPathDefault>` pour forcer la configuration.

```
<SensorPlugin xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:noNamespaceSchemaLocation="http://www.ibm.com/xml/schemas/taddm/FixedSensorSchema.xsd">
    <name>WeblogicServerVersionSensor</name>
    <osgiId>com.ibm.cdb.discover.sensor.app.j2ee.weblogicserverversion_7.1.0</osgiId>

    <sensorClassName>com.collation.discover.agent.app.j2ee.WeblogicServerVersionAgent</sensorClassName>
    <seedClassName>com.collation.discover.seed.app.j2ee.WeblogicVersionSeed</seedClassName>
    <resultClassName>com.collation.discover.result.app.j2ee.WeblogicVersionResult</resultClassName>
    <convertorClassName>com.collation.discover.engine.seedfactory.WeblogicVersionConvertor</convertorClassName>

    <defaultProfiles>
        <profile>Level 3 Discovery</profile>
    </defaultProfiles>

    <configuration className="com.ibm.cdb.discover.sensor.configuration.WeblogicServerVersionAgentConfiguration">
        <weblogicClassPath>
            <item>
                <entry>10.0</entry>
                <jdk>1.5.0</jdk>
            </item>
            <item>
                <entry>9.0</entry>
                <jdk>1.5.0</jdk>
            </item>
        </weblogicClassPath>
        <!--<weblogicClassPathDefault>
            <entry>10.0</entry>
             <weblogicVersion>10</weblogicVersion>
            <jdk>1.5.0</jdk>
        </weblogicClassPathDefault>-->
    </configuration>
</SensorPlugin>
```

Dans l'exemple, le détecteur WeblogicServerVersionSensor utilise les fichiers JAR du répertoire `lib/weblogic/10.0` avec Java SDK version 1.5.0 et suppose que le serveur WebLogic 10.x est en cours de fonctionnement.

Edition du fichier WeblogicSensor2.xml :

Vous devez éditer le fichier `WeblogicSensor2.xml`.

Le fichier de configuration se trouve dans les répertoires suivants :

- Sous les systèmes d'exploitation Linux, Solaris, AIX et Linux sous System z, le fichier est dans le répertoire *$COLLATION_HOME*`/etc/discover-sensors/`.
- Sous les systèmes d'exploitation Windows, le fichier est dans le répertoire *%COLLATION_HOME%*`\etc\discover-sensors\`.

Utilisez les balises suivantes pour modifier le fichier `WeblogicSensor2.xml` :

```
<SensorPlugin xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.ibm.com/xml/schemas/taddm/FixedSensorSchema.xsd">
    <name>WeblogicSensor2</name>
    <osgiId>com.ibm.cdb.discover.sensor.app.j2ee.weblogic2_7.1.0</osgiId>

    <sensorClassName>com.collation.discover.agent.app.j2ee.WeblogicAgent2</sensorClassName>
    <seedClassName>com.collation.discover.seed.app.j2ee.WeblogicSeed2</seedClassName>
    <resultClassName>com.collation.discover.result.app.j2ee.WeblogicServerResult2</resultClassName>
    <convertorClassName>com.collation.discover.engine.seedfactory.SoftwareConvertor</convertorClassName>

    <defaultProfiles>
        <profile>Level 3 Discovery</profile>
    </defaultProfiles>

    <configuration className="com.ibm.cdb.discover.sensor.configuration.WeblogicServerAgent2Configuration">
        <allowSensorToBePooledInJVM>true</allowSensorToBePooledInJVM>
        <domains>
            <item>
                <domainAddress>
                    <address>DOMAIN_IP</address>
                    <port>DOMAIN_PORT</port>
                </domainAddress>
                <addresses>
                    <item>
                        <address>IP_OF_FIRST_INTERFACE_ADMIN_SERVER_IS_USING</address>
                        <port>PORT_ ADMIN_SERVER_IS_USING </port>
                    </item>
                    <item>
                        <address>IP_OF_SECOND_INTERFACE_ADMIN_SERVER_IS_USING</address>
                        <port>PORT_ ADMIN_SERVER_IS_USING </port>
                    </item>
                </addresses>
            </item>
        </domains>
    </configuration>
</SensorPlugin>
```

Vous pouvez utiliser cette configuration lorsque le serveur WebLogic utilise plusieurs interfaces sur le serveur d'administration de domaine.

Dans ce cas, la valeur de `DOMAIN_IP` et de `DOMAIN_PORT` est utilisée à la place de `IP_OF_FIRST_INTERFACE_ADMIN_SERVER_IS_USING:PORT_ ADMIN_SERVER_IS_USING` et de `IP_OF_SECOND_INTERFACE_ADMIN_SERVER_IS_USING:PORT_ ADMIN_SERVER_IS_USING`.

Copie des fichiers JAR pour reconnaître les anciennes versions des serveurs d'applications WebLogic :

Pour reconnaître des serveurs qui exécutent des anciennes version de WebLogic, copiez les fichiers JAR dans le serveur TADDM.

Dans la plupart des cas, si vous possédez des fichiers JAR de la version actuelle de WebLogic, vous pouvez également reconnaître les serveurs exécutant les versions antérieures de WebLogic. Si cette méthode ne fonctionne pas, procédez comme suit :

1. Exécutez une reconnaissance avec l'ensemble actuel de fichiers JAR.
2. Arrêtez le serveur TADDM.

3. Copiez les fichiers JAR de la version ancienne ou différente du serveur WebLogic dans les répertoires correspondants.
4. Démarrez le serveur TADDM.
5. Exécutez la reconnaissance pour le serveur WebLogic.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Serveurs d'applications** en tant que **Type de composant**.
2. Sélectionnez **Weblogic** comme **Fournisseur**.
3. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

Assurez-vous que l'utilisateur WebLogic que vous ajoutez à la liste d'accès dispose des informations suivantes :

- Droits d'administrateur
- Mot de passe

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur WebLogic.

Fix Pack 3

com.collation.discover.agent.WeblogicSensor.UseDomainForClusterName=false

Cette propriété permet de personnaliser l'attribut `displayName` pour les clusters Weblogic. Par défaut, `displayName` est défini à l'aide du nom du cluster Weblogic. Deux clusters Weblogic peuvent avoir le même nom, mais peuvent appartenir à des domaines Weblogic différents. Dans ce cas, une personnalisation est nécessaire.

Lorsque cette propriété est définie sur `true`, ObjectDisplayNameAgent recalcule l'attribut `displayName` pour que le cluster Weblogic incorpore le nom de son domaine Weblogic. Par exemple, si le domaine Weblogic est `webl-dom-dr.mycompany.com:9111` et que le cluster est `webl_c1`, l'attribut `displayName` pour ce cluster est `webl-dom-dr.mycompany.com:9111:webl_c1`.

La valeur par défaut de cette propriété est `false`.

Après avoir modifié la valeur de la propriété, vous devez redémarrer TADDM.

com.collation.agent.weblogic.domainsconfiguration

Utilisée lorsque le serveur WebLogic utilise plusieurs interfaces sur le serveur Domain Admin Server (domain_ipX:domain_portX est utilisé à la place de listen_ipN:listen_portN).

La syntaxe de la propriété est la suivante :

```
com.collation.agent.weblogic.domainsconfiguration
domain_ipA:domain_portA listen_ip1:listen_port1,listen_ip2:
listen_port2;domain_ipB:domain_portB ...
```

Par exemple :

```
com.collation.agent.weblogic.domainsconfiguration=
   9.158.143.20:7001-9.158.143.20:7002,9.158.143.50:7001;9.158.143.20:
   7001-9.158.143.20:7002,9.158.143.50:7003
```

com.collation.agent.weblogic.protocols

Par défaut, cette propriété est désactivée et le protocole T3 est utilisé. Si vous supprimez la mise en commentaire de cette propriété, vous pouvez indiquer la liste des protocoles (séparés par des virgules) que les détecteurs WebLogic doivent utiliser, comme illustré dans l'exemple suivant :

```
com.collation.agent.weblogic.protocols=t3,http
```

Dans cet exemple, le protocole T3 est le premier protocole choisi. Si ce protocole échoue, le protocole HTTP est utilisé. Si vous voulez utiliser le protocole HTTP pour vous connecter à une instance de serveur WebLogic, vous devez activer l'établissement de tunnels HTTP pour cette instance à l'aide de la console WebLogic.

Les seules valeurs valides sont `t3` et `http`. Si vous codez une valeur incorrecte, comme une valeur avec des erreurs typographiques, le serveur WebLogic ne peut pas traiter correctement la demande et peut s'arrêter.

com.collation.platform.os.ignoreLoopbackProcesses=true

La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur WebLogic et propose des solutions à ces problèmes.

Des domaines WebLogic en double risquent d'être créés

Problème

Des domaines WebLogic en double risquent d'être créés lorsqu'un hôte d'un serveur admin d'un domaine WebLogic possède plusieurs adresses IP.

Solution

Fix Pack 3 Pour supprimer les doublons, assurez-vous que WebLogicDomainConsolidationAgent est exécuté après la reconnaissance des domaines WebLogic.

Le détecteur WebLogic ne démarre pas

Problème

Le détecteur WebLogic ne démarre pas.

Solution

Réalisez les opérations suivantes :

- Pour chaque version du serveur WebLogic, copiez les fichiers JAR dans le répertoire `$COLLATION_HOME/lib/weblogic/VERSION` à partir de l'installation de WebLogic. Vérifiez la configuration du détecteur dans le fichier `$COLLATION_HOME/etc/discover-sensors/WeblogicVersionSensor.xml`.
- Vérifiez que le port et l'adresse IP du serveur Weblogic sont accessibles et que le serveur Weblogic utilise le protocole de communication Java Management Extensions (JMX) qui est pris en charge par TADDM. Configurez la propriété com.collation.agent.weblogic.protocols dans le fichier `collation.properties`.
- Si le détecteur Weblogic démarre lorsque vous utilisez l'adresse d'hôte local (127.0.0.1) et échoue ou ne reconnaît rien, définissez la valeur de la propriété suivante dans le fichier `collation.properties` sur `true` :

  ```
  com.collation.platform.os.ignoreLoopbackProcesses=true
  ```

Le détecteur WebLogic échoue

Problème

Le détecteur WeblogicServerVersion échoue.

Solution

Copiez dans l'installation TADDM les fichiers JAR WebLogic requis (pour plus d'informations, voir la configuration du détecteur). Les informations d'authentification sont manquantes ou incorrectes.

Panne du détecteur dans un serveur distant

Problème

L'erreur suivante se trouve dans le fichier `local-anchor*.log`, ce qui indique généralement que les informations d'authentification de sécurité de WebLogic sont manquantes ou incorrectes :

```
Sensor failed in remote server:
An error occurred in the null sensor.
```

Solution

Assurez-vous que vous disposez d'informations d'authentification de sécurité correctes. Le serveur TADDM exige le nom de connexion et le mot de passe du système WebLogic utilisés pour la connexion à la console produit WebLogic.

Un message indique qu'il n'y a rien à reconnaître

Problème

Le détecteur WebLogic s'exécute et se termine avec succès, avec le message suivant :

```
Il n'y avait rien à reconnaître.
```

Solution

Ce message s'affiche lors de la reconnaissance d'un serveur d'application WebLogic. Cette situation ne pose pas de problème, mais assurez-vous que le détecteur WebLogic s'exécute par rapport au serveur d'administration WebLogic.

Echec du détecteur avec WebLogic 10.x

Problème

Le détecteur WeblogicServerVersion échoue uniquement avec WebLogic 10.x.

Solution

Le détecteur WeblogicVersionSensor utilise une commande externe pour identifier la version de WebLogic. Sur certaines installations WebLogic 10.x, cette commande renvoie une chaîne vide inattendue qui entraîne l'échec du détecteur WeblogicVersionSensor.

Pour résoudre ce problème, utilisez les fichiers JAR d'une installation WebLogic 9.x. Les fichiers JAR WebLogic 9.x peuvent être utilisés avec WebLogic 10.x.

Le détecteur WebLogic ne reconnaît pas le serveur WebLogic Administration Server

Problème

Pendant la tentative de reconnaissance d'un serveur WebLogic Administration Server, le détecteur WebLogic échoue suite au non fonctionnement d'un DNS.

Solution

Les reconnaissances impliquant les détecteurs liés aux serveurs WebLogic Administration Servers doivent disposer de DNS opérationnels. Pour résoudre ce problème, définissez la valeur de `com.collation.platform.os.disableRemoteHostDNSLookups` sur true, et assurez-vous que le serveur TADDM dispose toujours du chemin d'accès à la recherche DNS correct.

Le détecteur Weblogic échoue en raison d'une expiration de délai

Problème

Le détecteur Weblogic échoue en raison d'une expiration de délai.

Solution

Augmentez la valeur de la propriété d'expiration de délai com.collation.discover.agent.*NOM* dans le fichier `collation.properties`, où *NOM* représente le nom du détecteur qui est configuré dans le fichier XML du répertoire `$COLLATION_HOME/etc/discover-sensors`. Les exemples suivants indiquent comment coder cette propriété :

```
com.collation.discover.agent.WeblogicSensor2.timeout=7200000
com.collation.discover.agent.WeblogicSensor.timeout=7200000
```

Le détecteur WebLogic échoue après la migration

Problème

Le détecteur Weblogic échoue après la migration.

Solution

Vérifiez que le script `$COLLATION_HOME/bin/template-upgrade.sh` est exécuté.

Panne du détecteur suite à un incident T3

Problème

Le détecteur WeblogicServerVersion échoue en raison d'un protocole T3 inaccessible.

Solution

Dans certaines installations, le protocole T3 peut être bloqué. Dans ce cas, configurez les serveurs WebLogic et les détecteurs WeblogicSensors pour utiliser le protocole http.

Par exemple :

```
com.collation.agent.weblogic.protocols=t3,http
```

WeblogicServerVersion échoue en raison d'un délai d'attente lors de l'émission d'une commande version

Problème

weblogicServerVersion a dépassé le délai d'attente lors de l'émission de la commande version. Cela peut être dû au fait que le port est bloqué par le pare-feu. L'exemple suivant illustre le numéro de port 6079 bloqué par un pare-feu :

```
2009-09-09 12:29:38,802 DiscoverManager
DiscoverWorker-11 WeblogicServerVersionSensor-169.70.70.100-6079 DEBUG
j2ee.WeblogicServerVersionAgent - Executing command: -cp
/opt/IBM/taddm/dist/lib/weblogic/10.0/weblogic.jar:/opt/IBM/taddm/dist/lib
/weblogic/10.0/webservices.jar:/opt/IBM/taddm/dist/lib/weblogic/10.0/wljm
xclient.jar -Duser.language=en -Duser.region=US weblogic.Admin -url
t3://169.70.70.100:6079 -username confadmin -password XXX VERSION 2009-09-09
12:29:39,133 DiscoverManager DiscoverWorker-11
WeblogicServerVersionSensor-169.70.70.100-6079 DEBUG util.OsCommand - Command
executed, capturing output 2009-09-09 12:33:03,526 DiscoverManager
DISCOVER_SENSOR_CLEANUP_DiscoverWorker-11
WeblogicServerVersionSensor-169.70.70.100-6079 DEBUG
j2ee.WeblogicServerVersionAgent - JavaCommand error
java.lang.InterruptedException at java.lang.Object.wait(Native Method) at
java.lang.Object.wait(Object.java:231) at java.lang.Thread.join(Thread.java:680)
at com.collation.platform.util.OsCommand.execute(OsCommand.java:411)
```

Solution

Ce détecteur utilise un protocole autre que SSH pour accéder à l'hôte. Le port approprié doit être ouvert entre le serveur TADDM et la cible. Si un pare-feu empêche l'accès direct depuis le serveur de reconnaissance à certains hôtes ou périphériques, vous pouvez indiquer un système informatique qui ne peut pas accéder aux hôtes ou périphériques en tant qu'hôte d'ancrage.

Certaines dépendances JDBC ne sont pas créées entre un serveur WebLogic et des serveurs de base de données

Problème

TADDM reconnaît le serveur WebLogic et un serveur associé de base de données mais ne crée pas de relation entre eux. Une telle relation est basée sur les propriétés de connexion JDBC qui sont définies sur le serveur d'applications.

Solution

Le problème peut être causé par l'un des cas suivants :

- Les dépendances sont créées par l'agent JDBCDependencyAgent qui s'exécute dans le groupe d'agents de topologie des dépendances. Assurez-vous que l'agent est exécuté après la reconnaissance des serveurs WebLogic.
- JDBCDependencyAgent traite uniquement les serveurs d'applications récemment reconnus. Si certaines dépendances sont toujours manquants une fois que l'agent a été exécuté, relances la reconnaissance des serveurs WebLogic, et attendez que les agents de topologie s'exécutent de nouveau.
- Assurez-vous que le serveur de base de données prend en charge la création de dépendances transactionnelles entre lui et le serveur d'applications WebLogic. Les bases de données suivantes sont prises en charge :
  - Oracle
  - IBM DB2

– Microsoft SQL Server
– Sybase

Fix Pack 5

Le détecteur WebLogic échoue avec l'erreur : "java.lang.OutOfMemoryError: Java heap space"

Problème

Si une machine cible est dotée de plusieurs serveurs WebLogic qui s'exécutent sur des adresses IP virtuelles différentes, l'erreur `OutOfMemory` peut s'afficher pour TADDM lors de l'exécution des détecteurs WebLogic. Cette erreur peut être due aux valeurs de départ des détecteurs WebLogic qui contiennent tous la liste de processus exécutés sur le système.

Certains processus WebLogic peuvent alors comporter des milliers d'objets **BindAddress** et **LogicalConnection** dans l'objet de départ, occupant ainsi une grande quantité de mémoire. Lorsque beaucoup de détecteurs WebLogic sont appelés, ils créent leur propre copie de la liste des processus avec des données identiques, ce qui entraîne une augmentation de la consommation de mémoire pour les mêmes données.

Solution

Vous pouvez partager la liste des processus de cibles identiques entre les valeurs de départ de détecteurs WebLogic différents, ce qui permet de réduire la mémoire requise, en activant les propriétés suivantes dans le fichier collation.properties :

```
com.collation.discover.WeblogicApplicationSeed.processlist.shared=true
com.collation.discover.WeblogicDomainSeed.processlist.shared=true
com.collation.discover.WeblogicLauncherSeed.processlist.shared=true
com.collation.discover.WeblogicServerSeed.processlist.shared=true
```

Leur valeur par défaut est `false`.

Détecteur WebLogic SSH

Le détecteur WebLogic SSH analyse les fichiers de configuration du serveur WebLogic et se sert de ces informations pour reconnaître les composants du serveur WebLogic et leur configuration. L'ensemble de détecteurs connectables peut se connecter au système cible via SSH, WMI ou d'autres protocoles pris en charge par le détecteur de système informatique générique.

Nom du détecteur utilisé dans l'interface graphique et les journaux

- WeblogicLauncherSensor
- WeblogicApplicationSensor
- WeblogicDomainSensor
- WeblogicServerSensor

Problèmes de sécurité

Les détecteurs connectables WebLogic requièrent les autorisations d'accès du système informatique ou de WebLogic.

Limitations

Pour permettre l'exécution d'une reconnaissance, les détecteurs connectables WebLogic doivent disposer d'un accès aux fichiers de configuration de domaine. L'emplacement du répertoire de configuration du domaine peut être déterminé par le détecteur dans les situations spécifiques suivantes :

- Le serveur WebLogic est démarré comme un service Windows.
- Le serveur WebLogic est démarré comme un processus Windows ou UNIX, il est lancé avec l'argument suivant :

  `-Dpredefined.domain.config.dir=`*`répertoire_domaine`*
- Le serveur WebLogic est démarré comme un processus Windows ou UNIX, il est lancé avec l'argument suivant :

  `-Dweblogic.RootDirectory=`*`répertoire_domaine`*
- Le serveur WebLogic est démarré comme un processus UNIX, et l'emplacement du répertoire de configuration de domaine est défini comme l'une des variables d'environnement de traitement suivantes :
  - DOMAIN_HOME
  - LONG_DOMAIN_HOME
  - PWD
  - OLD_PWD
  - OLDPWD
- Le serveur WebLogic est démarré comme un processus Windows ou UNIX et le processus contient une variable avec le chemin d'accès au sous-répertoire `domains`. Tous les domaines sont dans le répertoire *`répertoire_projet_utilisateur`*`/domaines/`*`nom_domaine`*. Une recherche du fichier de configuration est exécutée sur le répertoire et tous les sous-répertoires définis dans le chemin d'accès pour les `domains`.

  Par exemple, si un processus contient la variable *-Dweblogic.system.BootIdentityFile=/home/weblogic/bea/my_user_projects/domains/domain92/aaa/boot.properties*, les chemins d'accès suivants sont recherchés pour le *nom_fichier_config* :
  - `/home/weblogic/bea/my_user_projects/domains/domain92/`
  - `/home/weblogic/bea/my_user_projects/domains/domain92/config/`
- Le serveur WebLogic est démarré comme un processus Windows ou UNIX et le processus contient une variable avec le chemin d'accès au sous-répertoire `servers`. Le répertoire servers se trouve dans le répertoire de base Domain. Une recherche du fichier de configuration est exécutée sur le répertoire et tous les sous-répertoires définis dans le chemin d'accès pour les `servers`.

  Par exemple, si un processus WebLogic contient la variable *-Dweblogic.system.BootIdentityFile=/home/weblogic/bea/my_user_projects/domains/domain92/servers/MS92_1/data/nodemanager/boot.properties*, les chemins d'accès suivants sont recherchés pour *nom_fichier_config* :
  - `/home/weblogic/bea/my_user_projects/domains/domain92/`
  - `/home/weblogic/bea/my_user_projects/domains/domain92/config/`
- Le serveur WebLogic est démarré comme un processus Windows ou UNIX et le processus contient une variable avec le chemin d'accès au sous-répertoire `user_project`. Le répertoire `user_projects` est le répertoire par défaut qui contient les projets WebLogic. Une recherche du fichier de configuration est exécutée sur le répertoire et tous les sous-répertoires définis dans le chemin d'accès pour les projets utilisateurs `user_projects`.

Par exemple, si un processus WebLogic contient la variable *-Dweblogic.system.BootIdentityFile=/home/weblogic/bea/my_user_projects/domains/domain92/servers/MS92_1/data/nodemanager/boot.properties*, les chemins d'accès suivants sont recherchés pour *nom_fichier_config* :

  - `/home/weblogic/bea/user_projects/domains/domain92/`
  - `/home/weblogic/bea/user_projects/domains/domain92/config/`
- Le détecteur de programme de lancement WebLogic contient les informations suivantes :
  - Le répertoire de configuration du domaine.
  - L'adresse IP sur laquelle la console d'administration WebLogic est en mode écoute.
  - Le numéro de port sur lequel la console d'administration WebLogic est en mode écoute.

  Pour plus d'informations, voir «Configuration du détecteur», à la page 187.

Sous Windows, le détecteur de programme de lancement WebLogic n'est normalement pas démarré si le processus WebLogic n'est pas démarré comme un service Windows. Il peut démarrer correctement si les variables d'environnement requises ont été définies.

Sous UNIX, lorsqu'une installation non standard est réalisée, il peut être nécessaire de définir des informations de configuration dans le fichier de configuration du détecteur de programme de lancement WebLogic.

Pour le serveur géré WebLogic, le nom du processus WebLogic doit être appelé avec l'argument suivant :

`-Dweblogic.management.server=`*`nom_serveur`*

Les détecteurs connectables WebLogic SSH ne doivent pas être exécutés avec le détecteur WebLogic dans le même répertoire, en conséquence vous ne devez pas activer les détecteurs connectables WebLogic dans le même profile de reconnaissance.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.AppServer
- app.ConfigFile
- app.j2ee.weblogic.WebLogicServer
- app.j2ee.J2EEComponent
- app.j2ee.J2EEDeployedObject
- app.j2ee.J2EEDomain
- app.j2ee.J2EEModule
- app.j2ee.J2EEResource
- app.j2ee.weblogic.WebLogicCluster
- app.j2ee.weblogic.WebLogicConnector
- app.j2ee.weblogic.WebLogicConnectorModule
- app.j2ee.weblogic.WebLogicDomain
- app.j2ee.weblogic.WebLogicEJBModule

- app.j2ee.weblogic.WebLogicJ2EEApplication
- app.j2ee.weblogic.WebLogicJDBCConnectionPool
- app.j2ee.weblogic.WebLogicJDBCDataSource
- app.j2ee.weblogic.WebLogicJDBCDriver
- app.j2ee.weblogic.WebLogicJDBCMultiPool
- app.j2ee.weblogic.WebLogicJDBCTxDataSource
- app.j2ee.weblogic.WebLogicJMSServer
- app.j2ee.weblogic.WebLogicJMSStore
- app.j2ee.weblogic.WebLogicJTA
- app.j2ee.weblogic.WebLogicMachine
- app.j2ee.weblogic.WebLogicSSLSettings
- app.j2ee.weblogic.WebLogicServer
- app.j2ee.weblogic.WebLogicServlet
- app.j2ee.weblogic.WebLogicVirtualHost
- app.j2ee.weblogic.WebLogicWebContainer
- app.j2ee.weblogic.WebLogicWebModule
- app.ProcessPool
- app.SoftwareContainer
- app.web.WebVirtualHost

Ressources reconnues par le détecteur

Cette rubrique décrit les ressources pouvant être reconnus par les détecteurs connectables WebLogic ainsi que le fonctionnement de ces reconnaissances.

Les informations sont collectées à partir des fichiers de configuration XML sur la machine cible. Les propriétés WebLogic par défaut sont stockées dans un schéma XSD, et non dans des fichiers de configuration XML.

Détecteur de programme de lancement WebLogic

Le détecteur de programme de lancement WebLogic est démarré, après le détecteur de serveur générique, à l'aide d'un modèle connectable, configuré dans `plugin.xml`. Il reconnaît la plupart des installations WebLogic standard et peut être configuré manuellement, si nécessaire.

Il reconnaît les informations suivantes :

- Le chemin d'accès au répertoire contenant des fichiers de configuration associés au domaine.
- La version WebLogic installée sur la machine cible.
- Si la cible est un serveur d'administration ou un serveur géré.
- L'IP et le port d'écoute du serveur d'administration.
- Les informations de base sur la structure du domaine WebLogic et des serveurs.

Le détecteur de programme de lancement WebLogic crée les objets suivants :

- L'objet du modèle de domaine WebLogic avec seulement les attributs qui sont inclus dans la règle de nommage.
- Les objets du modèle de serveur WebLogic avec seulement les attributs qui sont inclus dans la règle de nommage.

Le détecteur de programme de lancement WebLogic démarre les détecteurs suivants :

- Le détecteur de domaine WebLogic pour un serveur d'administration
- Le détecteur de serveur WebLogic pour un serveur d'administration

Détecteur de domaine WebLogic

Le détecteur de domaine WebLogic reconnaît les informations sur la totalité du domaine WebLogic.

Les informations suivantes (disponibles dans des fichiers de configuration XML) sont reconnues :

- Détails du domaine
- Détails de la machine
- Détails du cluster
- Paramètres SSL
- Analyseur JTA
- Pool de connexions JDBC
- Source de données JDBC
- Multi pool JDBC
- Serveur JMS
- Paramètres du gestionnaire de noeuds

Le détecteur de domaine WebLogic crée l'objet de domaine WebLogic.

Détecteur de serveur WebLogic

Le détecteur de serveur WebLogic reconnaît les informations sur la totalité du serveur WebLogic ainsi que des informations de base sur le domaine WebLogic.

Les informations suivantes (disponibles dans des fichiers de configuration XML) sont reconnues :

- Détails du serveur
- Pool de connexions JDBC
- Source de données JDBC
- Multi pool JDBC
- Serveur JMS

Le détecteur de serveur WebLogic crée l'objet de modèle du serveur WebLogic.

Le détecteur de serveur WebLogic démarre le détecteur d'applications WebLogic.

Détecteur d'applications WebLogic

Le détecteur d'applications WebLogic reconnaît les applications WebLogic déployées sur le serveur WebLogic et les applications WebLogic déployées sur le domaine WebLogic.

Les informations suivantes concernant le déploiement sont stockées :

- Application ou module, par exemple J2EEApplication, EJBModule, WebModule ou ConnectorModule.

- Détails de l'application ou du module, y compris J2EEDeployedObjects, par exemple WebLogicEntityEJB, WebLogicServlet et WebLogicConnector.
- Informations de sous-déploiement de l'application.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur WebLogic SSH prend en charge une reconnaissance asynchrone et basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Les détecteurs suivants, descendants du détecteur WeblogicLauncherSensor , ne nécessitent pas de configuration :

- WeblogicApplicationSensor
- WeblogicDomainSensor
- WeblogicServerSensor

Limitations

Les dernières dates de modification des fichiers de configuration collectés ne sont pas disponibles.

La reconnaissance de descripteur d'application n'est pas pris en charge.

Configuration du détecteur

Les détecteurs WebLogic connectables peuvent être configurés en éditant le fichier de configuration `plugin.xml`.

Vous pouvez exécuter une configuration spécifique de WebLogic en éditant l'élément `<configuration>` pour les détecteurs connectables WebLogic suivants :

- Détecteur de programme de lancement WebLogic
- Détecteur de serveur WebLogic
- Détecteur d'applications WebLogic

Configuration du détecteur de programme de lancement WebLogic

Le fichier `plugin.xml` du détecteur de programme de lancement WebLogic se trouve dans le répertoire `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.app.j2ee.weblogic.sensor.weblogiclaunchersensor_1.2.0`.

Dans l'élément `<configuration>`, vous pouvez configurer des informations relatives au répertoire de configuration pour chaque domaine. Placez les informations pour chaque domaine dans un élément `<item>` distinct. Pour chaque domaine, vous pouvez configurer les éléments suivants :

`<configDirectory>`
Le répertoire de configuration du domaine.

<adminServer>

Contient des informations sur l'adresse IP et le numéro de port sur lesquels la console d'administration WebLogic est en mode écoute. Les éléments suivants sont utilisés pour indiquer ces informations :

<listenAddress>

L'adresse IP sur laquelle la console d'administration WebLogic est en mode écoute.

<listenPort>

Le numéro de port sur lequel la console d'administration WebLogic est en mode écoute.

Le fichier de configuration, en exemple ci-après, affiche l'utilisation standard de l'élément <configuration>, et ses éléments enfant :

```
<configuration className="com.ibm.cdb.discover.app.j2ee.weblogic.configuration.WeblogicLauncherConfigurationItem">
 <domain>
  <item>
   <configDirectory>/opt/bea10/wl_10.0/domains/medrec/config</configDirectory>
   <adminServer>
    <listenAddress>127.0.0.1</listenAddress>
    <listenPort>7011</listenPort>
   </adminServer>
  </item>
  <item>
   <configDirectory>/opt/bea/user_projects2</configDirectory>
   <adminServer>
    <listenAddress>127.0.0.1</listenAddress>
    <listenPort>7002</listenPort>
   </adminServer>
  </item>
 </domain>
</configuration>
```

Vous pouvez également indiquer l'emplacement du répertoire de configuration du domaine en démarrant le serveur WebLogic avec l'argument suivant :

`-Dpredefined.domain.config.dir=`*`répertoire_domaine`*

Configuration du détecteur de serveur WebLogic

Le fichier `plugin.xml` associé au détecteur de serveur se trouve dans le répertoire `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.app.j2ee.weblogic.sensor.weblogicserversensor_1.2.0`.

Dans le fichier de configuration `plugin.xml`, vous pouvez configurer les éléments suivants :

<discoverAppDescriptors>

Indique si la reconnaissance des descripteurs d'applications est activée. La reconnaissance des descripteurs d'applications peut être gourmande en temps car les descripteurs sont définis dans des fichiers de configuration supplémentaires sur la machine distante où WebLogic est installé.

<discoverJdbcDetails>

Indique si la reconnaissance des descripteurs JDBC est activée. La reconnaissance des descripteurs JDBC peut être gourmande en temps car les descripteurs sont définis dans des fichiers de configuration supplémentaires sur la machine distante où WebLogic est installé.

Le fichier de configuration ci-dessous en exemple affiche l'usage standard des éléments <discoverAppDescriptors> et <discoverJdbcDetails> :

```
<configuration
className="com.ibm.cdb.discover.app.j2ee.weblogic.configuration.WeblogicServerConfigurationItem">
 <discoverAppDescriptors>true</discoverAppDescriptors>
 <discoverJdbcDetails>true</discoverJdbcDetails>
</configuration>
```

Configuration du détecteur d'application WebLogic

le fichier `plugin.xml` du détecteur d'application WebLogic se trouve dans le répertoire suivant :

```
$COLLATION_HOME/osgi/plugins/
com.ibm.cdb.discover.app.j2ee.weblogic.sensor.weblogicapplicationsensor_1.2.0
```

Dans le fichier de configuration `plugin.xml`, vous pouvez configurer les éléments suivants :

<discoverApplicationDetails>
Indique si la reconnaissance des caractéristiques application/module est activée. La reconnaissance des descripteurs d'application/module (descripteurs J2EE) peut être gourmande en temps car les descripteurs sont définis dans des fichiers de configuration supplémentaires sur la machine distante dans laquelle WebLogic est installé.

Le fichier de configuration suivant affiche l'usage standard de l'élément `<discoverApplicationDetails>` :

```
<configuration
className="com.ibm.cdb.discover.app.j2ee.weblogic.configuration.WeblogicApplicationConfigurationItem">
 <discoverApplicationDetails>true</discoverApplicationDetails>
</configuration>
```

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur WebLogic SSH.

Fix Pack 3

com.collation.discover.agent.WeblogicSensor.UseDomainForClusterName=false
Cette propriété permet de personnaliser l'attribut `displayName` pour les clusters Weblogic. Par défaut, `displayName` est défini à l'aide du nom du cluster Weblogic. Deux clusters Weblogic peuvent avoir le même nom, mais peuvent appartenir à des domaines Weblogic différents. Dans ce cas, une personnalisation est nécessaire.

Lorsque cette propriété est définie sur `true`, ObjectDisplayNameAgent recalcule l'attribut `displayName` pour que le cluster Weblogic incorpore le nom de son domaine Weblogic. Par exemple, si le domaine Weblogic est `webl-dom-dr.mycompany.com:9111` et que le cluster est `webl_c1`, l'attribut `displayName` pour ce cluster est `webl-dom-dr.mycompany.com:9111:webl_c1`.

La valeur par défaut de cette propriété est `false`.

Après avoir modifié la valeur de la propriété, vous devez redémarrer TADDM.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur WebLogic SSH et propose des solutions à ces problèmes.

Des domaines WebLogic en double risquent d'être créés

Problème
Des domaines WebLogic en double risquent d'être créés lorsqu'un hôte d'un serveur admin d'un domaine WebLogic possède plusieurs adresses IP.

Solution

Fix Pack 3 Pour supprimer les doublons, assurez-vous que WebLogicDomainConsolidationAgent est exécuté après la reconnaissance des domaines WebLogic.

Le détecteur échoue avec une erreur Domain config dir not found

Problème

Le répertoire de configuration du domaine n'a pas été trouvé. Vérifiez la sortie `PS` pour le processus et vérifiez dans la section limitations si la configuration est prise en charge.

Solution

Utilisez l'une des méthodes suivantes :

- Exécutez le serveur WebLogic en utilisant l'argument `-Dpredefined.domain.config.dir=`*`répertoire_domaine`* ou `–Dweblogic.RootDirectory=`*`répertoire_domaine`*
- Configurez le chemin d'accès au serveur administrateur de domaine dans la configuration du détecteur de programme de lancement WebLogic. Pour plus d'informations, voir «Configuration du détecteur», à la page 187.

WeblogicLauncherSensor échoue car la sortie ps est coupée sur HP-UX

Problème

WeblogicLauncherSensor échoue lors de la tentative de reconnaissance de WebLogic sur HP-UX et le message d'erreur suivant s'affiche dans le fichier journal du détecteur : "Cannot find server name in command line: `<COMMAND LINE>`". Une cause possible de cet échec est la coupure de la sortie de commande ps, un comportement connu de HP-UX.

Solution

1. Paramétrez `com.ibm.cdb.discover.WeblogicLauncherSensor.parseConfigXml=true` dans `collation.properties`.
2. Redémarrez TADDM et réexécutez la reconnaissance.

Si l'extraction du nom de serveur de la ligne de commande échoue, WeblogicLauncherSensor lit cette information dans le fichier de configuration locale (`config.xml`).

Certaines dépendances JDBC ne sont pas créées entre un serveur WebLogic et des serveurs de base de données

Problème

TADDM reconnaît le serveur WebLogic et un serveur associé de base de données mais ne crée pas de relation entre eux. Une telle relation est basée sur les propriétés de connexion JDBC qui sont définies sur le serveur d'applications.

Solution

Le problème peut être causé par l'un des cas suivants :

- Les dépendances sont créées par l'agent JDBCDependencyAgent qui s'exécute dans le groupe d'agents de topologie des dépendances. Assurez-vous que l'agent est exécuté après la reconnaissance des serveurs WebLogic.

- JDBCDependencyAgent traite uniquement les serveurs d'applications récemment reconnus. Si certaines dépendances sont toujours manquants une fois que l'agent a été exécuté, relances la reconnaissance des serveurs WebLogic, et attendez que les agents de topologie s'exécutent de nouveau.
- Assurez-vous que le serveur de base de données prend en charge la création de dépendances transactionnelles entre lui et le serveur d'applications WebLogic. Les bases de données suivantes sont prises en charge :
  - Oracle
  - IBM DB2
  - Microsoft SQL Server
  - Sybase

Détecteur de cloud

Fix Pack 5

Détecteur AWS

Le détecteur AWS commence par reconnaître les informations des composants de service EC2 et S3 à partir des environnements AWS du cloud public, permettant ainsi une reconnaissance automatique détaillée et profonde sans faille des composants EC2 reconnus et des informations associées.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AwsSensor

Eléments reconnus par le détecteur

Le détecteur reconnaît les éléments suivants :

- Aws
- AwsS3Bucket
- AwsS3BucketContent
- ComputerSystem (instances EC2)

Dans la console de gestion de reconnaissance et le portail de gestion de données, un type de composant de cloud est représenté par une icône de conception du cloud de couleur blanche, tandis qu'AWS est représenté par une icône en forme de cube de couleur orange.

Le détecteur AwsSensor interagit avec l'environnement AWS par le biais de l'interface Web pour extraire les informations de gestion de premier niveau. Les données extraites se composent principalement des données d'attribut nécessaires pour établir une correspondance avec des règles de dénomination et créer des objets de modèle valides.

Prérequis

Les prérequis d'AWS sont les suivants :

- L'URL publique d'AWS est accessible à partir du serveur de reconnaissance TADDM

- L'ID de la clé d'accès de sécurité et le jeton secret sont configurés correctement sur TADDM pour permettre la connexion au compte/à l'environnement AWS
- Les instances EC2 doivent être configurées dans l'environnement AWS (à reconnaître)
- Les instances EC2/machines virtuelles doivent être accessibles à partir du serveur de reconnaissance TADDM pour la reconnaissance de niveau 2 afin de pouvoir extraire les détails
- Les prérequis spécifiques aux détecteurs (comme ceux liés aux ports, aux droits, etc.) doivent être remplis pour la reconnaissance de niveau 2 afin de pouvoir fonctionner parfaitement pour les instances EC2
- Assurez-vous que les données d'identification correspondant aux machines virtuelles/instances EC2 configurées sont correctement définies sur TADDM de sorte qu'une session puisse être établie avec succès (détecteur de session) pendant la reconnaissance de niveau 2
  - Les fichiers PEM correspondant aux instances EC2 sont stockés de manière sécurisée et placés sur le chemin approprié de la machine TADDM, comme configuré dans les propriétés du détecteur AWS
  - Le nom d'utilisateur et le mot de passe (le cas échéant) sont configurés dans la section Liste d'accès
- Les compartiments doivent être configurés dans l'environnement AWS à reconnaître

Entrées de la liste d'accès

Le connecteur AWSsensor a besoin d'avoir des entrées distinctes dans la liste d'accès, qui correspondent au compte AWS et aux instances EC2 hébergées.

AWSAccount

Vous devez créer des données d'identification de la liste d'accès en sélectionnant 'Cloud' comme **Type de composant** et 'AWS' comme 'Fournisseur' pour la connexion au compte AWS. L'ID de la clé d'accès de sécurité est indiqué dans le 'nom d'utilisateur', et le jeton secret dans le 'mot de passe'.

Instances EC2

Deux scénarios sont possibles :

1. Lorsque l'instance EC2/la machine virtuelle autorise la connexion à l'aide du fichier *.PEM, le nom d'utilisateur correspondant doit être fourni et la zone de mot de passe doit être vide lors de la configuration de l'entrée de la liste d'accès.
2. Lorsque l'instance EC2/la machine virtuelle autorise le mécanisme d'authentification basé sur le mot de passe, l'entrée correspondante doit être ajoutée dans la liste d'accès selon la procédure habituelle.

Connexion à l'environnement AWS

Le détecteur AWSsensor se connecte de manière sécurisée (via https) à l'environnement AWS du cloud public. S'il s'avère que des configurations de proxy sont nécessaires pour l'accès, elles doivent être définies correctement dans les propriétés du détecteur. Pour plus d'informations, voir Configuration du profil de reconnaissance et des «Prérequis», à la page 191.

Objets de modèle avec attributs associés

Le détecteur AWS crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur l'environnement AWS du cloud public.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont affichés sous le nom de l'objet de modèle :

com.collation.platform.model.topology.cloud.aws.Aws

- Endpoint
- Identity
- AuthName
- Name
- GroupMembers (Ec2Instances)
- GroupMembers (Ec2Instances)
- XA
  - TotalVmInstances

com.collation.platform.model.topology.cloud.aws.AwsS3Bucket

- Name
- LastStoredTime
- AwsS3BucketContent

com.collation.platform.model.topology.cloud.aws.AwsS3BucketContent

- Name
- URI
- ContentType
- Size
- LastModifiedTime

com.collation.platform.model.topology.sys.ComputerSystem (corresponding to EC2 instances)

- AwsInstanceId
- Name
- Type
- Description
- IpInterfaces
- OSRunning
- CPU
- StorageExtent
- MemorySize
- VirtualMachineState

Configuration du détecteur

Avant d'utiliser le détecteur AWS, vous devez configurer le profil de reconnaissance.

Configurer le profil de reconnaissance

Par défaut, le détecteur AWS est activé pour la reconnaissance de niveaux 2 et 3. Il reconnaît les informations configurées à l'aide des services EC2 ou

S3, puis déclenche une reconnaissance profonde ou de niveau 2 correspondant aux instances EC2. Pour désactiver la reconnaissance de niveau 2 ou modifier d'autres paramètres de configuration, créez un profil de reconnaissance pour le détecteur AWS et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

1. Dans le tiroir Reconnaissance de la console de gestion de la reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil. Dans la liste Cloner le profil existant, sélectionnez **Reconnaissance de niveau 3**, puis cliquez sur **OK**.
4. Dans l'onglet Configuration du détecteur, sélectionnez le détecteur **AwsSensor** et cliquez sur **Nouveau**.
5. Dans la fenêtre Créer une configuration, entrez le nom et la description de votre configuration, puis cochez la case **Activer la configuration**.
6. Dans la section Configuration de la fenêtre Créer une configuration, cliquez sur **discoverNonRunningContainers**. Cliquez deux fois sur la zone Valeur dans la ligne et entrez ***false***.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Propriétés

Vous pouvez modifier les propriétés et les attributs ci-dessous :

proxyIp

Fait référence à l'adresse IP du proxy (si nécessaire) permettant d'accéder à l'URL publique d'AWS à partir du serveur TADDM.

proxyPassword

Fait référence au mot de passe du proxy (si proxyIp est configuré).

proxyPort

Fait référence au port du proxy (si proxyIp est configuré).

proxyTimeout

Fait référence aux valeurs de délai du proxy en millisecondes (si proxyIp est configuré).

proxyType

Fait référence au type du proxy (valeurs autorisées : HTTP ou HTTPS) permettant d'accéder à l'URL publique d'AWS depuis le serveur TADDM.

La valeur par défaut est HTTPS.

proxyUser

Fait référence au nom d'utilisateur du proxy (si proxyIp est configuré).

secretPemFileDirectoryPath

Chemin d'accès local du serveur de reconnaissance TADDM où tous les fichiers *.PEM sont placés. Il est utilisé pendant l'établissement de session lors de la reconnaissance de niveau 2.

Configuration de la passerelle

Suivez la procédure ci-dessous :

1. Configurez une machine de passerelle.
2. TADDM

   a. Assurez-vous que la machine de passerelle a été ajoutée à la section **Reconnaissance**>**Ancres** et **Passerelles** de la console de gestion de reconnaissance.

   b. Les données d'identification des accès des instances EC2 et de passerelle Windows doivent être fournies dans les détails de la liste d'accès de TADDM.
3. AWS

   Configurez le groupe de sécurité à l'aide des règles d'entrée mentionnées ci-dessous pour les composants suivants :

Tableau 15. Passerelle Windows

Type	Protocole	Plage de ports	Source
SSH	TCP	22	TADDM
TCP personnalisé	TCP	135	TADDM

Tableau 16. Cible (instance EC2)

Type	Protocole	Plage de ports	Source
TCP personnalisé	TCP	135	Passerelle Windows
TCP personnalisé	TCP	49152 – 65535	Passerelle Windows
TCP personnalisé	TCP	49152 – 65535	TADDM

4. Dans l'onglet Configuration du détecteur, sélectionnez le détecteur **DockerHostSensor** et cliquez sur **Nouveau**.
5. Dans la fenêtre Créer une configuration, entrez le nom et la description de la configuration du détecteur et cochez la case **Activer la configuration**.
6. Dans la section Configuration de la fenêtre Créer une configuration, cliquez sur **discoverNonRunningContainers**. Cliquez ensuite deux fois sur la zone Valeur dans la ligne et entrez *false*.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Configuration de l'ancre

Suivez la procédure ci-dessous :

1. Configurez une machine d'ancre.
2. TADDM

   a. Assurez-vous que la machine d'ancre a été ajoutée à la section **Reconnaissance**>**Ancres** et **Passerelles** de la console de gestion de reconnaissance et dans la portée de reconnaissance TADDM appropriée.
3. AWS

   a. Des privilèges d'élévation **sudo** doivent être fournis pour la commande `lsof`. Pour ce faire, mettez à jour la ligne suivante dans le fichier "collation.properties", comme suit :

   ```
   com.collation.discover.agent.command.lsof.Linux=sudo lsof
   ```

b. Créez un répertoire sur une machine d'ancre (en utilisant le chemin indiqué dans les propriétés de configuration du détecteur AWS), puis placez_y les fichiers *.PEM.

c. Configurez un groupe de sécurité à l'aide des règles d'entrée mentionnées ci-dessous.

Tableau 17. Ancre

Type	Protocole	Plage de ports	Source
SSH	TCP	22	TADDM
TCP personnalisé	TCP	8497	TADDM

Tableau 18. Cible (instance EC2)

Type	Protocole	Plage de ports	Source
SSH	TCP	22	Ancre

d. Dans Windows, une passerelle est configurée au-delà d'une ancre.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur AWS et propose des solutions pour y remédier.

Le détecteur échoue avec la description suivante : 'Erreur CTJTD1595E – Aucune donnée d'identification AWS dans la liste d'accès de TADDM'

Problème

Il est possible qu'aucune donnée d'identification de compte AWS ne soit configurée dans la liste d'accès de TADDM.

Solution

Dans l'interface utilisateur de la console de gestion de reconnaissance TADDM, dans **Reconnaissance**>**Liste d'accès**, vérifiez si des données d'identification de compte propres à AWS ont été configurées ou pas.

Le détecteur échoue avec la description suivante : 'Erreur CTJTD1596E – Aucun compte AWS reconnu, vérifiez la configuration du détecteur'

Problème

Ce problème peut survenir en raison d'éléments de configuration erronés pendant l'exécution du détecteur AWS.

Solution

Validez les paramètres de configuration du détecteur AWS dans l'interface utilisateur de la console de gestion de reconnaissance TADDM. Ces paramètres peuvent être en lien avec :

- L'exactitude de l'URL
- L'exactitude des données d'identification de la liste d'accès
- Les propriétés de configuration du détecteur AWS
- Un problème de connectivité du réseau (l'URL d'AWS publique peut ne pas être accessible à partir du serveur TADDM)

Détecteurs de base de données

Les détecteurs de base de données reconnaissant les bases de données utilisées dans l'environnement.

Détecteur IBM DB2

Le détecteur IBM DB2 reconnaît des serveurs IBM DB2 Universal Database (UDB).

Nom du détecteur utilisé dans l'interface graphique et les journaux

Db2Sensor et Db2WindowsSensor

Prérequis

Ce détecteur requiert les conditions suivantes :

- La reconnaissance du système informatique doit s'effectuer correctement.
- DB2 doit être installé dans le répertoire principal du propriétaire de l'instance.

Problèmes de sécurité

Les autorisations d'accès de l'utilisateur de DB2 doivent appartenir au groupe d'administration de DB2.

La reconnaissance s'effectue à l'aide de scripts de shell qui exécutent les commandes DB2 suivantes :

db2 Commande d'appel de l'interpréteur de commandes

db2ilist
Commande d'instances de liste

db2set Commande de registre de profil DB2

db2licm
Commande d'outil de gestion de licence

db2level
Affiche la commande de niveau de service DB2

db2 get dbm cfg

Limitations

Des caractères incorrects peuvent être reconnus si vous utilisez une instance DB2 32 bits sur un système d'exploitation Windows 64 bits. Ce problème de codage de caractères tient à la limitation du système d'exploitation Windows 64 bits, qui masque des commandes comme **chcp** aux applications 32 bits comme le programme **db2cmd.exe**.

Si plusieurs versions de DB2 sont installées sur le même système informatique Windows, le détecteur ne peut pas reconnaître le serveur IBM DB2 Universal Database (UDB).

TADDM exécute le processus de génération de la topologie de façon régulière. Jusqu'au terme de ce processus après une reconnaissance, les noms des bases de données qui s'affichent pour les systèmes distants peuvent ne pas être uniques. Une fois le processus de génération de la topologie terminé, le nom de la base de données contient le numéro de port et l'adresse IP de la base de données distante.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.db.db2.Db2AdminServer
- app.db.db2.Db2Alias
- app.db.db2.Db2BufferPool
- app.db.db2.Db2ConfigValue
- app.db.db2.Db2Container
- app.db.db2.Db2Database
- app.db.db2.Db2DatabaseConfigValue
- app.db.db2.Db2Instance
- app.db.db2.Db2InstanceConfigValue
- app.db.db2.Db2Module
- app.db.db2.Db2Schema
- app.db.db2.Db2Server
- app.db.db2.Db2ServerProcess
- app.db.db2.Db2System
- app.db.db2.Db2SystemConfigValue
- app.db.db2.Db2TableSpace

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur IBM DB2 prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Limitations

Les limitations suivantes s'appliquent :

- Pour une reconnaissance basée sur un script, le détecteur requiert des droits d'accès à la base de données. Si ces droits d'accès ne sont pas fournis, le détecteur se termine avec l'erreur suivante :

  ```
  Aucun système n'a été détecté
  ```

- La reconnaissance de descripteurs d'application n'est pas prise en charge.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Base de données** comme **Type de composant**.
2. Sélectionnez **DB2** comme **Fournisseur**.
3. Indiquez les informations requises suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

Le détecteur DB2 UNIX utilise les données d'identification extraites de la liste d'accès dans l'ordre suivant :

1. Le détecteur recherche dans la liste d'accès les données d'identification de l'utilisateur de DB2.

   Il s'agit du propriétaire de l'instance DB2 actuelle.
2. En cas d'échec de l'étape 1, le détecteur tente de se connecter à DB2 en utilisant chacune des informations d'identification d'utilisateur DB2 contenues dans la liste d'accès.
3. En cas d'échec de l'étape 2, le détecteur tente de se connecter à l'aide des informations d'identification d'utilisateur du système informatique (à l'aide des informations d'identification d'utilisateur provenant de la liste d'accès du système informatique).

Pour la reconnaissance de plusieurs installations DB2 sur une machine unique : DB2, les informations d'identification d'utilisateur extraites de la liste d'accès doivent appartenir au groupe d'administration de DB2 pour toutes les installations de DB2.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur IBM DB2.

Le détecteur DB2 qui s'exécute sur un système Windows (Db2WindowsSensor) se sert de la propriété suivante :

com.collation.discover.agent.Db2WindowsAgent.sshSessionCommandTimeout =300000

La valeur par défaut est `300000`. La valeur doit être un entier.

Cette propriété indique la durée maximale (en millisecondes) pendant laquelle le détecteur DB2 peut exécuter la commande **db2dfind** sur un système Windows.

Pour être utile, la valeur de cette propriété doit être :

- Supérieure à la valeur de la propriété `com.collation.SshSessionCommandTimeout`, qui contrôle le temps que la commande SSH est autorisée à s'exécuter sur la passerelle Windows. Si la valeur de la propriété `Db2WindowsAgent.sshSessionCommandTimeout` est inférieure à celle de la propriété `com.collation.SshSessionCommandTimout`, la valeur `com.collation.SshSessionCommandTimout` est employée.
- Inférieure à la valeur de la propriété `com.collation.discover.agent.Db2Sensor.timeout` (ou `com.collation.discover.DefaultAgentTimeout` si le délai spécifique de DB2 n'est pas défini). Le détecteur ne pouvant pas s'arrêter avant d'avoir terminé la collecte des informations, la valeur de la propriété du délai

Db2Sensor doit être supérieure à celle de la propriété `com.collation.discover.agent.Db2WindowsAgent.sshSessionCommandTimeout`.

Si nécessaire, vous pouvez changer les valeurs des propriétés `com.collation.SshSessionCommandTimeout` et `com.collation.discover.agent.Db2Sensor.timeout`. La propriété `com.collation.discover.agent.Db2Sensor.timeout` est spécifique du détecteur DB2 et remplace la valeur de la propriété `com.collation.discover.DefaultAgentTimeout`.

Pour les propriétés suivantes, vous pouvez aussi indiquer une adresse IP, comme illustré dans l'exemple suivant :

```
com.collation.discover.agent.DB2Agent.db2findscript.1.2.3.4=sudo
```

com.collation.discover.agent.DB2Agent.db2findscript=sudo
Cette valeur permet l'accès au script `db2find.sh` exécuté lors de la reconnaissance à l'aide de la commande **SUDO**.

com.collation.discover.agent.DB2Agent.db2findschemascript=sudo
Cette valeur permet l'accès au script `db2findschema.SH` exécuté lors de la reconnaissance à l'aide de la commande **SUDO**.

com.collation.discover.agent.DB2Agent.systemcommand=sudo
Cette valeur permet l'accès à la commande système exécuté lors de la reconnaissance à l'aide de la commande **SUDO**.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM DB2 et propose des solutions à ces problèmes.

Le détecteur DB2 échoue lors de la reconnaissance.

Problème
Le détecteur DB2 arrive à expiration lors l'exécution de la reconnaissance.

Solution
Augmentez la valeur de la propriété **com.collation.discover.agent.Db2WindowsAgent.sshSession CommandTimeout** dans le fichier `collation.properties`. De plus, vous pouvez augmenter la propriété **com.collation.discover.agent.Db2Sensor.timeout** afin de vous assurer qu'elle est toujours supérieure à la propriété **com.collation.discover.agent.Db2WindowsAgent.sshSession CommandTimeout**.

Des dépendances existent entre une base de données et une application de gestion business application mais elles ne sont pas détectées

Problème
Bien que des dépendances existent entre une base de données et une application de gestion, aucune dépendance n'est détectée parce que l'utilisateur défini dans la liste d'accès de reconnaissance pour DB2 n'est pas le propriétaire de l'instance.

Solution
Pour que les processus de reconnaissances trouvent les commandes DB2

pour répertorier les bases de données, l'utilisateur défini dans la liste d'accès à la reconnaissance pour DB2 doit extraire le profil de DB2 dans le profil de l'utilisateur.

Le volet des détails d'un composant DB2 reconnu est vide.

Problème

Lors de l'exécution d'une reconnaissance, le volet des détails sous l'onglet Licence d'un composant DB2 reconnu est vide. Ce problème affecte tous les niveaux de TADDM, sur toutes les plateformes.

Solution

Sous UNIX et Linux, la routine exécutable **db2licm** doit disposer des autorisations appropriées pour l'utilisateur spécifié dans la console de gestion de reconnaissance pour la connexion à la base de données. Pour extraire les informations de licence, l'utilisateur de la reconnaissance doit également posséder le groupe principal du propriétaire de l'instance DB2 dans sa liste de groupes.

CTJTP1127E La commande copy échoue durant une reconnaissance de DB2.

Problème

Le message d'erreur suivant s'affiche dans la console de gestion de reconnaissance lors de la reconnaissance de DB2 :

```
CTJDT0234E L'erreur suivante se produit : CTJDT0235E L'erreur suivante
s'est produite lors de l'exécution du script de reconnaissance
de DB2 (db2find.sh) :
 sh coll/bin/db2-db2find.sh.
```

De plus, les informations suivantes sont affichées dans le journal du détecteur DB2 :

```
com.collation.discover.agent.AgentException : CTJDT0235E L'erreur suivante
s'est produite lors de l'exécution du script de reconnaissance
de DB2 (db2find.sh) :
sh coll/bin/db2-db2find.sh.
at com.ibm.cdb.discover.sensor.app.db.db2.Db2Sensor.runDb2Find(Db2Sensor
.java:414)
at com.ibm.cdb.discover.sensor.app.db.db2.Db2Sensor.findSystems(Db2Sensor
.java:275)
at com.ibm.cdb.discover.sensor.app.db.db2.Db2Sensor.discover(Db2Sensor
.java:212)
at com.collation.discover.engine.AgentRunner.run(AgentRunner.java:131)
at com.collation.discover.engine.DiscoverEngine.processWorkItem
(DiscoverEngine.java:1247)
at com.collation.discover.engine.DiscoverEngine$DiscoverWorker.run
(DiscoverEngine.java:816)
Caused by:
com.collation.platform.session.SessionClientException: CTJTP1127E The copy
command failed for java.io.EOFException: SSHSCP1: premature EOF.
at com.collation.platform.session.Ssh2SessionClient.copyToRemote
(Ssh2SessionClient
.java:441)
at com.collation.platform.session.Ssh2SessionClient.copyToRemote
(Ssh2SessionClient
.java:397)
at com.collation.platform.session.SessionClientPool.copyToRemote
(SessionClientPool
.java:236)
at com.ibm.cdb.discover.sensor.app.db.db2.Db2Sensor.prepareScript
```

```
(Db2Sensor.java:726)
at com.ibm.cdb.discover.sensor.app.db.db2.Db2Sensor.runDb2Find
(Db2Sensor.java:383)
... 5 autres
```

Solution

Ce message d'erreur s'affiche car la commande secure copy (**scp**) n'est pas située dans le PATH de l'ID utilisateur utilisé par le système informatique distant pour reconnaître DB2.

Pour résoudre ce problème, éditez ou créez un fichier nommé `environment` dans le répertoire `<taddmusr>/.ssh` du système informatique distant en cours de reconnaissance. Définissez la variable d'environnement PATH <*taddmusr*> PATH dans ce fichier. Veillez à inclure le chemin d'accès complet de la commande **scp** dans la variable d'environnement PATH.

Le détecteur DB2 échoue avec l'erreur CTJTD0234E

Problème

Le détecteur DB2 échoue avec l'erreur CTJTD0234E et le message d'erreur suivant :

```
Attribute not set: instances
```

Solution

Ce message s'affiche car la variable PATH n'inclut pas les commandes DB2 requises par le script `db2find.sh`.

Pour corriger ce problème, ajoutez les chemins requis à l'entrée suivante dans le fichier `collation.properties` :

```
com.collation.discover.agent.path.system_uname
```

Si le problème persiste, vous pouvez exécuter les scripts du détecteur via sudo, pour lesquels vous devez avoir accès à des commandes telles que **db2licm** et**db2set**. Pour exécuter le script via sudo, utilisez la propriété suivante :

```
com.collation.discover.agent.DB2Agent.db2findscript.1.2.3.4=sudo
com.collation.discover.agent.DB2Agent.db2findschemascript.1.2.3.4=sudo
com.collation.discover.agent.DB2Agent.systemcommand1.2.3.4=sudo
```

Un avertissement est généré pendant une reconnaissance basée sur le script du détecteur DB2.

Problème

Pendant la reconnaissance basée sur le script, le message d'avertissement suivant s'affiche :

```
CTJTD1006E Invalid data in output file in section: db2findschema
```

Solution

Vérifiez que les données d'identification de l'utilisateur DB2 (propriétaires de toutes les instances DB2) sont ajoutées à la liste d'accès. Si le problème persiste, vérifiez que la commande **db2ilist** fonctionne toujours correctement sur les systèmes reconnus. Pour plus d'informations sur cette commande, consultez la note technique intitulée «DB2ilist does not return the instance» sous : https://www.ibm.com/support/docview.wss?uid=swg21420898.

La reconnaissance de DB2 exécutée sur un système de langue autre que l'anglais échoue

Problème

Lorsque vous voulez reconnaître des cibles dont la langue n'est pas

l'anglais, par exemple des serveurs DB2 de langue japonaise, la reconnaissance échoue. Les fichiers journaux contiennent le message suivant :

```
2016-06-08 21:27:49,778 DiscoverManager
      [DiscoverWorker-3]20160608212657731#Db2Sensor-37.53.105.24-60012
      DEBUGsession.SessionClientPool - PoolEncoding=IBM-943
ClientEncoding=IBM-943
```

De plus, la sortie de la commande **db2find** contient des points d'interrogation, par exemple `?gp?: db2set -g`, au lieu des caractères de tilde, par exemple `~gp~: db2set -g`.

Solution

Ce problème vient du fait que le codage des cibles de la reconnaissance est différent de celui du serveur TADDM. Pour le résoudre, ajoutez la propriété suivante au fichier `collation.properties` :

```
com.collation.platform.session.EncodingOverRide=UTF-8
```

Pour plus d'informations, voir la rubrique *Propriétés de la reconnaissance* dans le *Guide d'administration* de TADDM.

Détecteur IBM Informix

Le détecteur IBM Informix reconnaît les serveurs IBM Informix Dynamic Server.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Informix

Prérequis

Le pilote IBM Informix JDBC doit être installé sur le serveur IBM Informix Dynamic Server.

Limitations

Le serveur Informix Dynamic Server doit être configuré avec les exigences minimales pour la reconnaissance. Ajoutez le compte de service de reconnaissance au groupe Informix sur le serveur Informix Dynamic Server.

Objets de modèle avec attributs associés

Le détecteur IBM Informix crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur à propos des ressources IBM Informix Dynamic Server de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

app.db.ids.IDSAlias

- AliasName
- Parent
- Protocol
- ServiceName

app.db.ids.IDSBufferPool

- BufferPoolID
- NumBuffers
- Size

app.db.ids.IDSChunk

- ChunkNumber
- FreeSpace
- Offset
- Size
- MirrorOffset
- Parent

app.db.ids.IDSConfigValue

- ConfigID
- ConfigName
- DefaultValue
- EffectiveValue
- OriginalValue

app.db.ids.IDSDatabase

- DatabaseLocale
- LoggingType
- Name

app.db.ids.IDSInstance

- BitSize
- ConnectOption
- Home
- Host
- Name
- ProductName
- ProductVersion
- OnConfig
- Protocol
- SQLHostFile
- Status
- VersionString

app.db.ids.IDSSegment

- OS_SHM_ADDR
- OS_SHM_ID
- OS_SHM_KEY
- SegmentClass
- Size

app.db.ids.IDSServerProcess

- OSProcessName
- PID
- VpClass
- VpID

app.db.ids.IDSSpace

- Chunks
- ObjectType
- PageSize
- SpaceName
- SpaceNumber

app.db.ids.IDSStartupEnvironmentVar

- StartupEnvVarName
- StartupEnvVarValue

Configuration de la liste d'accès

Pour fournir au détecteur IBM Informix un accès au serveur Informix Dynamic Server, vous devez configurer la liste d'accès.

Pour configurer la liste d'accès, procédez comme suit :

1. Dans la console de gestion de reconnaissance, créez une portée de reconnaissance qui contient l'adresse IP du serveur Informix Dynamic Server.
2. Pour créer une liste d'accès, cliquez sur l'icône **Liste d'accès**.
3. Dans la fenêtre Liste d'accès, cliquez sur **Ajouter**.
4. Dans la zone **Type de composant** de la fenêtre Caractéristiques de l'accès, cliquez sur **ComputerSystem**.
5. Entrez les accréditations nécessaires pour accéder à la cible Informix Dynamic Server. TADDM utilise une connectivité JDBC pour se connecter au serveur dynamique.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM Informix et propose des solutions à ces problèmes.

Le détecteur ne parvient pas à extraire les informations sur le serveur

Problème

Le détecteur ne peut pas extraire des informations car le serveur Informix Dynamic Server n'est pas démarré.

Solution

Entrez la commande **oninit** pour démarrer le serveur de base de données.

Un message indique qu'il n'y a rien à reconnaître

Problème

Le détecteur s'exécute et se termine correctement, avec le message suivant :

```
Il n'y avait rien à reconnaître.
```

Solution

Aucune instance active d'Informix n'est exécutée sur le système informatique cible.

TADDM ne peut pas se connecter à une base de données Informix

Problème

L'erreur suivante apparaît dans les journaux :

```
erreur survenue : com.informix.asf.IfxASFException:
Echec de la tentative de connexion au serveur de base de données
nom_base_de_données
```

Solution

Vérifiez que la connexion du serveur TADDM au port Informix sur le serveur de base de données est ouverte.

Détecteur Microsoft SQL Server

Le détecteur Microsoft SQL Server reconnaît des serveurs Microsoft SQL Server. Dans TADDM version 7.3.0.2 et ultérieure, vous pouvez utiliser le détecteur en mode basé sur le script.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SqlServerSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- db.mssql.SqlServer
- db.mssql.SqlServerConfig
- db.mssql.SqlServerDatabase
- db.mssql.SqlServerDataFile
- db.mssql.SqlServerModule
- db.mssql.SqlServerProcess

Prérequis

Vous devez effectuer les tâches prérequises suivantes pour que les serveurs Microsoft SQL Server soient reconnus correctement.

Remarque : Les prérequis suivants sont identiques pour la reconnaissance standard et la reconnaissance dépendante d'un script.

Configuration de compte

Vous pouvez exécuter la reconnaissance dans le mode d'authentification Windows ou SQL.

Mode d'authentification Windows

- Créez un nouvel ID de connexion sur SQL Server pour le compte de domaine Windows, utilisé pour la reconnaissance du système d'exploitation Windows. La reconnaissance est ensuite exécutée dans le mode d'authentification Windows.
- Faites correspondre le compte de domaine Windows à l'ID de connexion créé à l'étape précédente.
- Dans la base de données maître SQL, affectez les rôles et droits suivants à l'ID de connexion créé pour le compte de domaine Windows :
  - `public` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Mappage de l'utilisateur, puis sélectionnez le rôle de base de données `public`.

- `db_datareader` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Mappage de l'utilisateur, puis sélectionnez le rôle de base de données `db_datareader`.
- `Connecter SQL` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Eléments sécurisables, puis accordez le droit `Connecter SQL`.
- `Afficher une définition` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Eléments sécurisables, puis accordez le droit `Afficher une définition`.

Ces rôles et droits sont requis pour accéder aux tables suivantes :

- sysdatabases
- syscurconfigs
- sysprocesses
- sysobjects
- syscolumns

- Ouvrez la fenêtre Propriétés de la connexion et accédez à la page Etat. Dans la section des paramètres, sélectionnez **Octroyer** pour le paramètre **Autorisation de se connecter au moteur de base de données**, et **Activé** pour le paramètre **Connexion**.
- Assurez-vous que le groupe d'administrateurs locaux peut accéder à SQL (fait partie de la configuration et de l'autorisation SQL).

Mode d'authentification SQL

- Créez une connexion sur le serveur SQL Server. Sélectionnez l'option **Authentification SQL Server**. La reconnaissance est alors exécutée dans le mode d'authentification SQL.
- Dans la base de données SQL maître, affectez les rôles et droits suivants à la connexion créée pour le compte de domaine SQL :
  - `public` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Mappage de l'utilisateur, puis sélectionnez le rôle de base de données `public`.
  - `db_datareader` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Mappage de l'utilisateur, puis sélectionnez le rôle de base de données `db_datareader`.
  - `Connecter SQL` : ouvrez la fenêtre Propriétés de la connexion, accédez à la page Eléments sécurisables, puis accordez le droit `Connecter SQL`.
- Ouvrez la fenêtre Propriétés de la connexion et accédez à la page Etat. Dans la section des paramètres, sélectionnez **Octroyer** pour le paramètre **Autorisation de se connecter au moteur de base de données**, et **Activé** pour le paramètre **Connexion**.

Configuration requise du réseau

- Selon le système d'exploitation, une configuration réseau de niveau 2 doit être appliquée. L'application est reconnue à l'aide d'un compte de système d'exploitation, par conséquent, la reconnaissance de niveau 2 de TADDM du serveur sur lequel l'application est installée, doit être réussie.

- Les ports d'écoute de Microsoft SQL doivent être ouverts sur les pare-feux entre les passerelles Windows TADDM et les serveurs sur lesquels Microsoft SQL est installé.

Fix Pack 2 **Exigences de la reconnaissance dépendante d'un script**
Dans le mode de reconnaissance dépendante d'un script, installez le module Windows PowerShell `sqlps` ou les composants logiciels enfichables Windows PowerShell SqlServerProviderSnapin100 et SqlServerCmdletSnapin100.

Limitations

Les dépendances transactionnelles entre les serveurs d'applications pris en charge, IBM WebSphere, JBoss, Oracle Weblogic, et le serveur SQL sont uniquement créées pour le port d'écoute stocké dans l'attribut primarySap du serveur SQL.

Si le serveur SQL utilise la configuration TCP/IP générale, l'indicateur *ListenAll* est défini sur true, alors le premier port statique est considéré comme son *primarySAP*. Le reste des ports ne sont pas capturés et donc certaines des dépendances ne peuvent être créées.

Si le serveur SQL utilise la configuration TCP/IP spécifique pour chaque interface IP, l'indicateur *ListenAll* est défini sur false, puis sur le premier non bouclage, *Active*, et *Enabled*, le premier port statique de l'IP est utilisé comme serveur SQL *primarySAP*. Le reste des ports et les ports configurés pour d'autres interfaces IP ne sont pas capturés. Donc, certaines des dépendances ne peuvent être créées.

Si le serveur SQL utilise uniquement la configuration de port dynamique, le port d'écoute d'exécution en cours, qui peut être modifié, n'est pas stocké dans l'attribut *primarySAP*. Au lieu de cela, un indicateur *dynamicPortAllocation* est défini sur true pour l'indiquer.

Les dépendances basées sur le nom de l'instance du serveur SQL, au lieu de son port d'écoute, sont toujours créées.

Fix Pack 2 Le mode de reconnaissance basée sur un script du détecteur Microsoft SQL Server repose sur le module `sqlps`, qui est disponible dans Microsoft SQL Server 2008 et versions ultérieures. Par conséquent, si vous souhaitez reconnaître Microsoft SQL Server 2005, vous devez également disposer d'autres instances telles que Microsoft SQL Server 2008, 2008 R2 ou 2012.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration des méthodes d'authentification :

Il existe deux modes d'authentification pouvant être utilisés par TADDM pour reconnaître un serveur SQL.

Authentification de sécurité intégrée Windows.

- Installez SSH sur la passerelle TADDM comme requis.
- Pour une reconnaissance par passerelle, activez WMI sur tous les systèmes Windows cible. WMI est activé par défaut.

Par défaut, la reconnaissance par passerelle installe automatiquement le fournisseur TADDM WMI sur tous les systèmes Windows cible pendant le processus de reconnaissance.

La reconnaissance d'un serveur SQL Server requiert que le serveur Windows soit éligible pour la reconnaissance et qu'un accès supplémentaire soit accordé à TADDM.

Il existe deux modes d'authentification pouvant être utilisés par TADDM pour reconnaître un serveur SQL Server :

Authentification Windows
Pour une authentification Windows, les exigences suivantes doivent être satisfaites :

- L'utilisateur Windows utilisé pour la reconnaissance du serveur SQL doit posséder le droit utilisateur de `connexion locale` sur le serveur de passerelle.
- L'utilisateur doit disposer de droits d'accès pour se connecter au système SQL Server. Il serait préférable que l'utilisateur soit un utilisateur de domaines et que le système serveur fasse confiance au domaine du serveur de passerelle.
- Ajoutez l'utilisateur et le mot de passe Windows à la liste d'accès pour le serveur SQL Server.

Authentification SQL Server
Pour l'authentification SQL Server, ajoutez l'utilisateur SQL Server à la liste d'accès pour le serveur SQL.

Pour déterminer le type d'authentification que vous devez utiliser, vérifiez avec votre administrateur SQL Server quels noeud sont exécutés par SQL Server. Le mode mixte prend en charge les deux types d'authentification.

Configuration de la liste d'accès :

Décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Utilisez la base de données en tant que type de composant.
2. Utilisez Microsoft SQL Server en tant que fournisseur.
3. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

La liste d'accès SQL Server TADDM s'applique uniquement à l'autorisation SQL Server. Fournissez toujours une entrée d'accès informatique Windows pour que le serveur soit reconnaissable.

Pour la sécurité intégrée, l'ID utilisateur Windows utilisé pour accéder à la passerelle ne doit pas nécessairement être le même que celui utilisé pour se connecter au serveur SQL.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur Microsoft SQL Server.

Le détecteur Microsoft SQL Server utilise les paramètres suivants :

com.collation.discover.agent.SqlServerAgent.UseListeningIp
Cette valeur indique comment sont générés les noms d'affichage des objets d'instances de serveur SQL.

Quand la valeur de la propriété est `false`, les noms d'affichage pour ces objets ont la forme suivante : *host_fqdn* + ":" + *nom_instance_serveur_sql*

Quand la valeur de la propriété est `true`, les noms d'affichage pour les objets ont la forme suivante : *fqdn_écoute_serveur_sql* + ":" + *nom_instance_serveur_sql*

La valeur par défaut est `false`.

Restriction : Vous devez faire une nouvelle reconnaissance du serveur SQL pour que les changements soient visibles.

com.collation.discover.agent.SqlServerAgent.timeout
Cette valeur indique en millisecondes la durée d'exécution du détecteur avant l'expiration du délai d'attente.

Si cette propriété n'est pas définie, le détecteur utilise la délai d'attente par défaut spécifié dans la propriété **`com.collation.discover.DefaultAgentTimeout`**.

Fix Pack 5 **com.collation.discover.agent.sqlserver.skipSqlAuthentication**
Cette valeur indique si l'utilisateur souhaite ignorer l'authentification SQL avant l'authentification Windows dans le détecteur de serveur SQL.

Si la valeur de la propriété est `false`, le détecteur de serveur SQL effectue l'authentification SQL avant l'authentification Windows. Sinon, il ignore l'authentification SQL et tente uniquement d'effectuer l'authentification Windows.

La valeur par défaut de cette propriété est `true`. Cela est dû au mode d'authentification SQL par défaut qui est "Windows".

Cette propriété varie en fonction du détecteur. Vous pouvez rendre ce paramètre configurable par machine.

Exemple :
`com.collation.discover.agent.sqlserver.skipSqlAuthentication.<IP> = true`.

Restriction : Vous devez redémarrer et reconnaître le serveur SQL pour rendre les modifications visibles.

Identification et résolution des problèmes liés au détecteur

Les problèmes qui surviennent avec le détecteur peuvent être les suivants : échec de l'autorisation ou de la reconnaissance etc. Toutefois, vous pouvez résoudre ces problèmes.

Fix Pack 2

La reconnaissance dépendante d'un script du détecteur Microsoft SQL Server échoue

Problème
Lorsque vous exécutez le détecteur Microsoft SQL Server dans le mode basé sur un script, la reconnaissance échoue avec le message suivant :

```
There was an error while Snapins adding...
```

Solution

Vérifiez que le module `sqlps` de Windows PowerShell est installé correctement. Le mode de reconnaissance basée sur un script du détecteur Microsoft SQL Server repose sur ce module. Cependant, le module est disponible uniquement dans Microsoft SQL Server 2008 et versions ultérieures. Par conséquent, si vous souhaitez reconnaître Microsoft SQL Server 2005, vous devez également disposer d'autres instances telles que Microsoft SQL Server 2008, 2008 R2 ou 2012.

Aucun détail n'est disponible pour SQL Server après la reconnaissance

Problème

SQL Server est reconnu mais aucun détail n'est fourni.

Solution

Vérifiez que l'autorisation SQL Server peut accéder aux tables suivantes :

- sysdatabases
- sys.master_files
- syscurconfigs
- sysprocesses

Si aucune autorisation SQL Server n'est utilisée, vérifiez l'autorisation Windows.

Reconnaissance de Microsoft SQL sans droits d'accès datareader

Problème

Est-il possible de reconnaître une base de données Microsoft SQL sans avoir à accorder le rôle db_datareader requis à l'intégralité de la base de données ?

Solution

Pour reconnaître une base de données Microsoft SQL sans avoir à octroyer des droits d'accès à l'intégralité de la base de données, procédez comme suit :

- Créez un utilisateur à l'aide de la procédure de stockage du serveur SQL Server.
- Utilisez la commande **sp_addlogin** pour créer une connexion permettant aux utilisateurs de se connecter au serveur SQL Server à l'aide de l'authentification SQL Server.
- Utilisez la commande **sp_grantlogin** pour permettre à un groupe d'utilisateurs ou un compte utilisateur Windows de se connecter à SQL Server à l'aide de l'authentification Windows.
- Une fois l'utilisateur créé, accordez l'accès aux tables suivantes utilisées par le détecteur de serveur SQL :

  ```
  sysdatabases, sys.master_files, syscurconfigs, sysprocesses
  ```

  Dans l'exemple suivant, l'utilisateur est `taddmusr` :

  ```
  GRANT SELECT on sysdatabases to taddmusr;
  GRANT SELECT on sys.master_files to taddmusr;
  GRANT SELECT on syscurconfigs to taddmusr;
  GRANT SELECT on sysprocesses to taddmusr;
  ```

L'attribut ProductName n'est pas clair

Problème

L'attribut ProductName ne présente pas assez d'informations concernant le produit.

Solution

Si vous avez récemment migré de la version précédente de TADDM, vous devez à nouveau reconnaître les serveurs Microsoft SQL Server. L'attribut comprend le numéro de version de SQL Server, le niveau ServicePack et l'édition de SQL Server.

L'attribut ProductName se présente sous la forme suivante :

- Microsoft SQL Server 2008 R2 SP1 (édition entreprise)

détecteur Oracle

Le détecteur Oracle reconnaît les serveurs de base de données Oracle.

Nom du détecteur utilisé dans l'interface graphique et les journaux

OracleSensor

Prérequis

Les conditions suivantes doivent être remplies :

- La reconnaissance du système informatique doit s'effectuer correctement.
- La connectivité réseau entre le serveur TADDM et le programme d'écoute Oracle Listener doit fonctionner.

Problèmes de sécurité

Les autorisations d'accès de l'utilisateur Oracle utilisées pour reconnaître une base de données Oracle à partir de TADDM doivent disposer de privilèges d'exécution. Pour vous assurer que les privilèges corrects sont accordés à l'utilisateur Oracle, exécutez la commande suivante : `grant execute on` *`système_dbms`* `to` *`utilisateur_oracle`*`;`

Le compte de la base de données Oracle requiert des privilèges CONNECT.

Le rôle de l'utilisateur de la liste d'accès Oracle doit être le suivant : SELECT_CATALOG_ROLE.

Pour reconnaître ASM (Oracle Automatic Storage Management), l'accès en lecture doit être accordé aux tables et vues suivantes : `dba_clusters`, `dba_constraints`, `dba_data_files`, `dba_db_links`, `dba_dimensions`, `dba_indexes`, `dba_mviews`, `dba_profiles`, `dba_role_privs`, `dba_roles`, `dba_rollback_segs`, `dba_segments`, `dba_sequences`, `dba_source`, `dba_synonyms`, `dba_sys_privs`, `dba_tab_privs`, `dba_tables`, `dba_tablespaces`, `dba_ts_quotas`, `dba_users`, `dba_views`, `global_name`, `gv$asm_client`, `gv$instance`, `sys.dba_tables`, `v$asm_diskgroup`, `v$backup`, `v$bgprocess`, `v$controlfile`, `v$database`, `v$datafile`, `v$log`, `v$logfile`, `v$parameter`, `v$pgastat`, `v$process`, `v$session`, `v$sga`, `v$sys_optimizer_env` et `v$version`.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur Oracle prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, vous devez définir le propriétaire du répertoire `Oracle_home` dans la liste d'accès en tant données d'identification de l'utilisateur Oracle. Le détecteur de script localise spécifiquement cet utilisateur pour exécuter les requêtes de base de données Oracle. Si vous ne définissez pas cet utilisateur dans la liste d'accès, le détecteur renvoie l'erreur «CTJTP1186E The entries in the access list are not applicable» (Les entrées de la liste d'accès ne s'appliquent pas).

Remarque : L'utilisateur du système d'exploitation qui démarre le détecteur en utilisant les données d'identification du système informatique doivent avoir un accès en lecture aux fichiers `/etc/oratab` ou `/var/opt/oracle/oratab` pour devenir le propriétaire du répertoire `Oracle_home`.
Procédez comme suit :

1. Sélectionnez **Base de données** comme type de composant.
2. Sélectionnez **Oracle** comme fournisseur.
3. Indiquez les informations obligatoires suivantes :
   - Le nom d'utilisateur du système d'exploitation pour l'utilisateur Oracle
   - Le mot de passe du système d'exploitation pour l'utilisateur Oracle

Limitations

Certaines fonctions fournies par le détecteur Oracle durant une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

Les fonctions suivantes ne sont pas prises en charge :

- Reconnaissance des descripteurs d'application
- Reconnaissance Oracle RAC
- reconnaissance Oracle ASM
- Reconnaissance du schéma brut (la liste des tables figurant dans la base de données est limitée)
- Reconnaissance de l'objet de modèle OracleDBLink
- Reconnaissance de l'objet de modèle OracleListener

Objets de modèle avec attributs associés

Le détecteur Oracle crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur les éléments de configuration de l'environnement Oracle.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

OracleASM

- AsmInstances
- DiskGroups
- Name
- Node
- Rac

OracleASMDisk

- AsmDiskGroup
- State
- Name

OracleASMDiskGroup

- Asm
- AsmDisks
- Name
- State

OracleASMInstance

- BackgroundProcesses
- Database
- Host
- Hostname
- OracleInstanceStatus
- Parameters
- Parent
- Port
- RacDatabase
- SGAValues
- SID
- ServerProcesses

OracleBackgroundProcess

- Description
- Name
- Pid

OracleControlFile

- Nom

OracleDBLink

IpAddress

Port

ServiceName

OracleDataFile

Name

Size

TableSpace

OracleDatabase

ControlFiles

DBName

DBVersion

DataFiles

InitValues

Name

RedoLogFiles

SchemaRawData

Schemas

TableSpaces

OracleInitValue

Description

Name

Value

OracleInstance

BackgroundProcesses

ConfigContents

Database

Host

KeyName

Modules

Name

Port

PrimarySAP

ProcessPools

ProductName

ProductVersion

SGAValues

SID

ServerProcesses

Status

OracleListener
BindAddresses

Name

OracleModule
FileName

Name

Schema

OracleRAC
Asm

HomePath

Name

OCRLocation

PrimaryNode

RacDatabases

VoteDiskPath

OracleRedoLogFile
Name

Size

OracleSGAValue
Name

Value

OracleSchema
Name

Owner

OracleServer
ConfigFile

Listeners

OracleServerProcess
Connections

Name

PID

Ports

OracleTableSpace
Nom

Size

ProcessPool
Nom

RuntimeProcesses

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Copie du pilote JDBC :

Cette rubrique décrit comment copier un pilote JDBC pour le détecteur Oracle.

Important : Si vous utilisez TADDM 7.3.0 ou 7.3.0.1, le détecteur Oracle requiert que le fichier `classes12.jar` soit copié. En plus de ce fichier, vous pouvez aussi copier des versions ultérieures du pilote, par exemple `ojdbc7.jar`, comme décrit dans la procédure qui suit.

Fix Pack 2 Si vous utilisez TADDM 7.3.0.2 ou version ultérieure, un seul fichier est requis. Copiez le pilote compatible avec la dernière version d'Oracle que vous reconnaissez, par exemple `ojdbc7.jar`. Vous pouvez copier plusieurs versions du pilote si nécessaire.

Pour copier le pilote JDBC, procédez comme suit :

1. Obtenez le fichier de pilote JDBC, par exemple `classes12.jar` ou `ojdbc7.jar`, à partir du site Web d'Oracle ou du support d'installation Oracle.
2. Copiez le fichier dans l'emplacement suivant :

   ```
   $COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.oracle.
   oraclecommon_1.0.1/lib/oracle
   ```

3. Ajoutez le nom du fichier de pilote JDBC à l'entrée `Bundle-ClassPath` dans le fichier `MANIFEST.MF` du détecteur OracleCommon.
   a. Accédez au répertoire `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.db.oracle.oraclecommon_1.0.1/META-INF` et ouvrez le fichier `MANIFEST.MF` dans un éditeur de texte.
   b. Vérifiez si l'entrée `Bundle-ClassPath` contient le nom du pilote JDBC que vous souhaitez copier. L'exemple suivant illustre l'entrée correcte pour le fichier `ojdbc7.jar` :

      ```
      Bundle-ClassPath: lib/oracle/ojdbc7.jar,
       lib/oracle/ojdbc6.jar,
       lib/oracle/ojdbc5.jar,
       lib/oracle/classes12.jar
      ```

   c. Si l'entrée ne contient pas le nom du pilote que vous souhaitez copier, ajoutez le nom manuellement en tant que première entrée.
4. Redémarrez le serveur TADDM.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Base de données** comme **Type de composant**.
2. Sélectionnez **Oracle** comme **Fournisseur**.
3. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

   Pour reconnaître des systèmes de fichiers ASM (Oracle Automatic Storage Management), entrez le nom d'utilisateur `sys` et un mot de passe.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

com.collation.discovery.oracle.extended
Cette propriété indique si des valeurs de configuration supplémentaires concernant des liens de la base de données Oracle sont stockées.

La valeur par défaut est `N` (Non).

Si vous définissez la propriété à `Y` (YES/OUI), le détecteur stocke des valeurs de configuration supplémentaires sur les liens de la base de données Oracle.

com.collation.platform.os.ignoreLoopbackProcesses=true
La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

com.collation.discovery.oracle.tablelimit
Cette propriété contrôle la quantité de tables détectées par le détecteur Oracle.

La valeur par défaut est `1000`. Cette propriété prend en charge uniquement les valeurs positives.

Fix Pack 5

com.collation.oracle.sensor.ignoreNonRegisteredSidOfListener=true
La valeur par défaut de cette propriété est `false`.

Lorsque cette propriété a pour valeur True, le détecteur Oracle ignore les SID qui ne sont pas enregistrés dans le programme d'écoute Oracle.
Le détecteur Oracle tente d'abord d'établir une connexion `jdbc` avec le programme d'écoute pour un SID. Si le message d'erreur "`ORA-12505, TNS: listener does not currently know of SID given in connect descriptor`" est généré, le SID est ignoré. Si la connexion échoue en générant une autre erreur, un objet de modèle d'instance Oracle superficiel est créé avec l'adresse IP et le port du programme d'écoute.
Cette propriété a également pour conséquence de ne pas créer les instances Oracle qui n'ont pas été enregistrées dans le programme d'écoute.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur ORACLE et propose des solutions à ces problèmes.

Le détecteur Oracle ne démarre pas

Problème
La signature Oracle ne correspond pas car vous avez renommé les fichiers binaires Oracle, ou vous exécutez une version du serveur Oracle non prise en charge par TADDM (Express Edition, par exemple).

Solution
Ne modifiez pas les noms des fichiers binaires et assurez-vous que vous

utilisez une version d'Oracle prise en charge. Assurez-vous également que le service TNSListener est démarré pour la base de données Oracle.

Echec du détecteur avec l'erreur «Impossible d'identifier les serveurs» error

Problème

Le compte de la base de données Oracle ne fonctionne pas à cause de l'une des raisons suivantes :

- Le mot de passe est incorrect.
- Le compte est verrouillé.
- Le compte ne dispose pas de privilèges de connexion.

Solution

Mettez la liste d'accès à jour, déverrouillez le compte ou ajoutez un privilège de connexion.

Dans l'invite de commande, testez le compte à l'aide de la commande **sqlplus**, comme indiqué dans l'exemple suivant :

```
bash-2.05b$ sqlplus

SQL*Plus: Release 10.2.0.1.0 - Production on Tue Jun 12 08:15:23 2007
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
Enter user-name: system
Enter password:
ERROR:
ORA-28000: the account is locked
```

Des doublons Oracle apparaissent lorsque des instances sont reconnues à la fois par un détecteur de cluster Veritas et un détecteur Oracle

Problème

Lorsque vous utilisez un détecteur de cluster Veritas et un détecteur pour reconnaître une instance Oracle, des doublons peuvent apparaître. Ceci se produit parce que le détecteur de cluster Veritas utilise des majuscules pour le SID de l'instance et le détecteur Oracle utilise les minuscules pour le même SID.

Solution

Pour éviter ce problème, modifiez le fichier `dist/etc/discover-sensors/VeritasClusterSensor.xml` en changeant la ligne suivante :

```
<source>Sid</source>
```

pour la ligne suivante :

```
<source>%{Sid}</source>
```

Après ce changement, le détecteur de cluster Veritas crée des instances Oracle avec le SID en minuscule.

Remarque : Si vous changez la ligne après l'exécution des reconnaissances où aucun doublon n'est apparu, de nouveaux doublons pourraient apparaître.

détecteur Sybase

Le détecteur Sybase reconnaît des serveurs de base de données Sybase Adaptive Server Enterprise (ASE).

Fix Pack 2 Pour reconnaître la base de données Sybase, le détecteur utilise le protocole JDBC avec les indicateurs `ENCRYPT_PASSWORD` et `RETRY_WITH_NO_ENCRYPTION` définis sur `true` par défaut. Cela signifie que le mot de passe est chiffré et que si vous ne parvenez pas à vous authentifier lors de votre premier essai, les mots de passe fournis au cours des tentatives suivantes ne seront pas chiffrés. La connexion est sécurisée si l'entrée de liste d'accès contient un fichier de clés certifiées.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SybaseSensor

Problèmes de sécurité

Pour attribuer les privilèges minimum à l'utilisateur de la reconnaissance Sybase, exécutez la commande suivante :

```
grant select on sysengines from public
```

Les tables suivantes sont interrogées :

- version
- master..sysconfigures
- master..sysusages
- master..syssegments
- master..sysprocesses
- master..sysengines
- master..sysdatabases
- master..sysdevices
- master..syscurconfigs
- master..sysservers
- master..syssrvroles
- master..syslogins
- master..sysloginroles
- master..syspartitions
- master..systhresholds
- master..sysresourcelimits
- master..systimeranges

La requête précédente ne reconnaît que les informations destinées à la base de données maître. Pour reconnaître des informations relatives aux utilisateurs et aux tables issues d'autres bases de données, créez un ID utilisateur sur ces bases de données. Au cours de la reconnaissance, TADDM exécute la requête suivante :

```
select t.segment, u.name from nom_bdd..systhresholds t,nom_bdd..
sysusers u where t.suid=u.suid
```

Exemples :

- La requête suivante est exécutée pour la base de données `tempdb` :

  ```
  select t.segment, u.name from tempdb..systhresholds t,tempdb..sysusers u where
  t.suid=u.suid
  ```

- La requête suivante est exécutée pour la base de données `sybsystemprocs` :

```
select t.segment, u.name from sybsystemprocs..systhresholds t,sybsystemprocs..
sysusers u where t.suid=u.suid
```

Limitations

- Le détecteur Sybase ne collecte pas d'informations sur les schémas appartenant à l'utilisateur dbo.
- Fix Pack 1 La limitation dans le logiciel SAP Sybase ASE identifiée par CR# 751110 affecte TADDM. La connexion à la base de données configurée pour utiliser la couche SSL se bloque lors de la connexion aux serveurs sur lesquels le mode SSL est désactivé. Pour éviter ce type de problème dans TADDM, définissez une valeur pour la propriété de portée suivante :

  `com.collation.sybasesensor.jdbclogin.timeout`

  La valeur par défaut est 15000 ms (15 secondes). Après cette durée, les tentatives de connexion échouent et le détecteur tente d'établir une connexion non sécurisée ordinaire.
- Fix Pack 3 Dans TADDM version 7.3.0.3 et ultérieures, les éléments de configuration suivants ne sont pas reconnus par défaut :
  - `logins`
  - `roles`
  - `rawSchema`
  - `tables`
  - `thresholds`

  Si vous souhaitez que ces éléments soient reconnus, créez une configuration de détecteur dans la console de gestion de reconnaissance, puis définissez les propriétés suivantes sur `true` :
  - **discoverLogins**
  - **discoverRoles**
  - **discoverRawSchema**
  - **discoverTables**
  - **discoverThresholds**

Objets de modèle avec attributs associés

Le détecteur Sybase crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur les ressources de stockage de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

AppConfig
- Content
- Parent

ConfigFile
- FixedPath
- RealFile
- URI

LogicalContent
FixedPath

ProcessPool

- CmdLine
- Env
- Name
- Parent
- RuntimeProcesses

SybaseConfigValue

- ConfigUnit
- Name
- Parent
- RunValue
- Type
- Valeur

SybaseDatabase

- Name
- Options
- Owner
- Parent (SybaseServer)
- SchemasRawData
- Segments
- Tables
- Thresholds
- Users

SybaseDevice

- Description
- FirstVirtualPageNumber
- FixedPath
- IsDefaultDisk
- IsDeviceMirrored
- IsDsyncEnabled
- IsDumpDevice
- IsMasterDeviceMirrored
- IsMirrorEnabled
- IsPhysicalDisk
- IsReadsMirrored
- IsSecondaryMirrorSideOnly
- IsSerialWrites
- IsSkipHeader
- LastVirtualPageNumber
- MirrorPath
- Parent (SybaseServer)
- RealFile
- URI

SybaseEngineProcess

- CmdLine

- Name
- PID
- Parent
- Ports

SybaseLogin

- AccumulatedDate
- FailedLoginCount
- FullName
- IsAccountLocked
- IsPasswordExpired
- Language
- Name
- Parent(SybaseServer)
- PasswordDate
- SybaseRoles
- TotalCPUUsed
- TotalIOUsed

SybaseModule

- Database
- FileName
- Name
- Parent

SybaseRemoteServer

- IsMessageConfidential
- IsMessageIntegrity
- IsMutualAuthentication
- IsNetworkPasswordEncrypted
- IsReadOnly
- IsRPCSecurityModelB
- IsTimeoutEnabled
- Name
- NetworkName
- RemoteNetworkCost
- RemoteServerClass
- SybaseServer

SybaseResourceLimitation

- AppName
- IsEnforcedDuringExecution
- IsEnforcedPriorToExecution
- LimitationExceededAction
- LimitationScope
- LimitType
- LimitValue
- Login

- Name
- Parent (SybaseServer)
- TimeRange

SybaseRole

- FailedLoginCount
- Name
- Parent
- PasswordDate
- Status

SybaseSegment

- Name
- Parent
- Size

SybaseServer

- BindAddresses
- ConfigContents
- ConfigFile
- ConfigValues
- Bases de données
- Périphériques
- EngineProcesses
- FullVersion
- Accueil
- Host
- KeyName
- Logins
- Modules
- Name
- PrimarySAP
- ProcessPools
- ProductName
- ProductVersion
- RemoteServers
- ResourceLimitations
- ServerProcesses
- Status
- SybaseRoles
- TimeRanges

SybaseServerProcess

- Name
- PID
- Parent

SybaseTable

- CreationDate

- Name
- Parent(SybaseDatabase)
- Partitions

SybaseTablePartition

- FirstPage
- NumPages
- Parent (SybaseTable)
- PartitionID

SybaseThreshold

- IsLastChance
- Name
- Parent (SybaseDatabase)
- Segment
- ThresholdExeededProcedure
- ThresholdSize
- User

SybaseTimeRange

- EndDay
- EndTime
- Name
- Parent (SybaseServer)
- StartDay
- StartTime

SybaseUser

- Login
- Name
- Parent (SybaseDatabase)

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Base de données** comme **Type de composant**.
2. Sélectionnez **Sybase** comme **Fournisseur**.
3. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour établir une connexion JDBC avec le serveur Sybase.
4. Fix Pack 1 En fonction de la configuration de votre serveur, indiquez le fichier de clés certifiées SSL avec la phrase secrète dans les paramètres SSL. Ceci s'applique seulement à la reconnaissance qui utilise la connexion SSL.

   Remarque : En raison d'un pilote JDBC Sybase et d'une limitation de la machine virtuelle Java, un seul fichier de clés certifiées peut être utilisé pendant une reconnaissance. Par conséquent, si vous voulez reconnaître un grand nombre de cibles Sybase au-dessus du protocole SSL, vous ne devez ajouter qu'un fichier de clés certifiées contenant tous les certificats obligatoires. Ce fichier doit être ajouté dans la première entrée de liste d'accès du détecteur Sybase dans TADDM. Les autres entrées ne peuvent pas contenir de paramètres

SSL. Vous pouvez créer le fichier de clés certifiées à l'aide des outils `keytool` et `ikeyman`. Les deux outils se trouvent dans le répertoire `$COLLATION_HOME/external/jdk-`*`plateforme_système_exploitation`*`/jre/bin`.

Configuration du profil de reconnaissance

Vous pouvez personnaliser les paramètres du détecteur Sybase si les valeurs par défaut ne répondent pas à vos besoins.

Pour personnaliser les paramètres du détecteur Sybase, vous devez créer une configuration de détecteur. Procédez comme suit :

1. Dans le tiroir **Reconnaissance** de la console de gestion de reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil. Dans la liste **Cloner le profil existant**, sélectionnez **Reconnaissance de niveau 3**, puis cliquez sur **OK**.
4. Sous l'onglet **Configuration du détecteur**, sélectionnez le détecteur **SybaseSensor** et cliquez sur **Nouveau**.
5. Dans la fenêtre Créer une configuration, entrez le nom et la description de votre configuration, puis cochez la case **Activer cette configuration et désactiver la configuration sélectionnée**.
6. Dans la section **Configuration** de la fenêtre Créer une configuration, modifiez tout ou partie des propriétés.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Propriétés

Vous pouvez modifier les propriétés suivantes :

Fix Pack 3 **discoverLogins**
Indique si les données de `logins` (connexions) sont découvertes ou non lors d'une reconnaissance de base de données Sybase.

La valeur par défaut est `false`, ce qui signifie que les données ne sont pas reconnues. Pour reconnaître des `logins`, définissez cette propriété sur `true`.

Fix Pack 3 **discoverRoles**
Indique si les données de `roles` (rôles) sont découvertes ou non lors d'une reconnaissance de base de données Sybase.

La valeur par défaut est `false`, ce qui signifie que les données ne sont pas reconnues. Pour reconnaître des `roles`, définissez cette propriété sur `true`.

Fix Pack 3 **discoverRawSchema**
Indique si les données de `rawSchema` (schéma brut) sont découvertes ou non lors d'une reconnaissance de base de données Sybase.

La valeur par défaut est `false`, ce qui signifie que les données ne sont pas reconnues. Pour reconnaître un `rawSchema`, définissez cette propriété sur `true`.

Fix Pack 3 **discoverTables**
Indique si les données de `tables` (tables) sont découvertes ou non lors d'une reconnaissance de base de données Sybase.

La valeur par défaut est `false`, ce qui signifie que les données ne sont pas reconnues. Pour reconnaître des `tables`, définissez cette propriété sur `true`.

Fix Pack 3 **discoverThresholds**
Indique si les données de `thresholds` (seuils) sont découvertes ou non lors d'une reconnaissance de base de données Sybase.

La valeur par défaut est `false`, ce qui signifie que les données ne sont pas reconnues. Pour reconnaître des `thresholds`, définissez cette propriété sur `true`.

détecteur Sybase IQ

Le détecteur Sybase IQ reconnaît les serveurs de base de données Sybase IQ.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SybaseIQSensor

Problèmes de sécurité

Pour attribuer les privilèges minimum à l'utilisateur de la reconnaissance Sybase, exécutez la commande suivante :

```
grant execute on sp_iqdbsize
```

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.AppConfig
- app.ConfigFile
- app.db.sybase.SybaseConfigValue
- app.db.sybase.SybaseDatabase
- app.db.sybase.SybaseDevice
- app.db.sybase.SybaseEngineProcess
- app.db.sybase.SybaseModule
- app.db.sybase.SybaseServer
- app.ProcessPool
- core.LogicalContent

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Base de données** comme **Type de composant**.
2. Sélectionnez **Sybase** comme **Fournisseur**.
3. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour établir une connexion JDBC avec le serveur Sybase.

Détecteurs génériques

Les détecteurs génériques sont utilisés par les autres détecteurs pour reconnaître des éléments de configuration.

détecteur d'ancrage

Le détecteur d'ancrage est utilisé pour une reconnaissance derrière un pare-feu.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AnchorSensor

Prérequis

Tous les composants logiciels requis pour la reconnaissance à partir de l'ancre distante sont déployés automatiquement durant le processus de reconnaissance. Pour échanger des données, vous devez utiliser le protocole Secure Shell (SSH) version 2.

Si l'ancre est déployé sur des systèmes Linux 64 bits, JBossSensor et StackScanSensor nécessitent également la version 32 bits des bibliothèques libgcc et glibc.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Le serveur TADDM utilise SSH pour communiquer avec le serveur d'ancrage distant. Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour une authentification par clé SSH ou une authentification par connexion SSH sur le serveur d'ancrage distant.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège (généralement effectuée à l'aide de la commande **sudo**).

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration* de TADDM.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur d'ancrage.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

Fix Pack 3 **com.collation.discover.anchor.zone.fromContextIP**

Indique si les zones d'ancrage peuvent être définies à partir du protocole IP du contexte, utilisé pour la reconnaissance. Les valeurs valides sont `true` et `false`. La valeur par défaut est `false`.

Lorsqu'une adresse IP n'est pas incluse dans la portée d'ancrage, la zone d'ancrage n'est pas définie. Par conséquent, l'espace adresse n'est pas défini

pour une adresse IP ou un réseau IP spécifique. Si vous définissez cette propriété sur `true`, les zones d'ancrage sont définies à partir du protocole IP du contexte.

com.collation.discover.agent.AnchorSensor.timeout=3600000
Indique le délai autorisé pour démarrer un nouveau serveur d'ancrage.

com.collation.discover.anchor.forceDeployment=true
La valeur par défaut est définie sur `true`.

Cette propriété définit si les ancrages de la portée reconnue doivent être déployés lors du démarrage de la reconnaissance.

Lorsque vous définissez cette valeur sur `false`, les ancrages sont déployés uniquement si l'une des deux conditions suivantes est remplie :

- Aucune adresse IP de la portée ne répond à une commande ping
- Le port 22 n'est accessible sur aucune adresse IP reconnue

Si des ancres enchaînés existent, cette condition s'applique à tous les ancres de la chaîne. Si un ancre de la chaîne est restreint par une condition, les ancres précédents doivent satisfaire cette condition afin que tous les ancres puissent être déployés.

com.collation.discover.anchor.lazyDeployment=false
Indique si les fichiers doivent être copiés pendant le déploiement de l'ancrage ou pendant le lancement du détecteur nécessitant les fichiers. Dans les deux cas, seuls les fichiers différents sont copiés. Les valeurs valides sont `true` et `false`. La valeur par défaut est `false`.

L'exemple suivant fournit un aperçu de l'impact de cette propriété sur la fonctionnalité TADDM :

Le détecteur WebSphere Application Server contient des dépendances dans le répertoire `dist/lib/websphere` qui occupent 130 Mo. Si l'indicateur est défini sur `false`, ces données sont copiées dans l'hôte cible une fois l'ancrage déployé. Si l'indicateur est défini sur `true`, les données sont copiées lorsque le détecteur WebSphere Application Server s'apprête à être exécuté sur l'ancrage. Si aucun détecteur WebSphere Application Server n'est exécuté dans l'ancrage, les 130 Mo ne sont pas envoyés à l'hôte distant.

com.collation.discover.anchor.connectType=ssh
Indique si la connexion à l'ancrage doit être établie à l'aide d'un tunnel ssh ou d'un socket direct. Les valeurs valides sont `ssh` et `direct`. La valeur par défaut est `ssh`. Pour indiquer le type de connexion pour une adresse particulière, utilisez `com.collation.discover.anchor.connectType.1.2.3.4=`*`ssh`*, où 1.2.3.4 est l'adresse pour laquelle vous voulez indiquer le type de connexion.

com.collation.platform.session.GatewayForceSsh
Indique s'il est nécessaire de forcer la passerelle à agir indépendamment de l'ancre. Les valeurs valides sont `true` et `false`. Spécifiez la valeur `true` pour résoudre les problèmes Cygwin lorsque la passerelle et l'ancre se trouve sur le même système. Lorsque la valeur est true, une session SSH et non une session locale est utilisée pour transférer le trafic entre la passerelle et l'ancre.

Détecteur de reconnaissance asynchrone

Le détecteur de reconnaissance asynchrone est obligatoire pour la reconnaissance asynchrone. Les adresses IP inaccessibles (par une commande PING) sont de bons

candidats pour une reconnaissance asynchrone. Le détecteur de reconnaissance asynchrone tente de déterminer lesquelles des adresses IP inaccessibles sont valides.

Pour plus d'informations sur la reconnaissance asynchrone, voir la rubrique *Reconnaissance asynchrone* dans le *Guide d'administration* de TADDM.

Dans une reconnaissance asynchrone, la sortie du script de reconnaissance est un fichier archive stocké dans un répertoire du serveur TADDM, qui contient les résultats de la reconnaissance. Une adresse IP inaccessible est considérée comme valide s'il existe un fichier archive sur le serveur TADDM pour cette adresse IP. Selon le contenu du fichier archive, les détecteurs appropriés sont planifiés pour la sortie de leur script de reconnaissance. Les détecteurs peuvent exécuter une reconnaissance par le biais d'une analyse syntaxique de la sortie du script au lieu d'accéder directement au système cible, à l'instar d'une reconnaissance non basée sur un script.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ASDSensor

Configuration du détecteur

Le détecteur de reconnaissance asynchrone n'utilise pas la liste d'accès.

Le détecteur de reconnaissance asynchrone utilise les entrées suivantes du fichier `collation.properties` :

- com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory
- com.ibm.cdb.discover.asd.ProcessUnreachableIPs
- com.ibm.cdb.tarpath

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de reconnaissance asynchrone et propose des solutions à ces problèmes.

Le détecteur ne reconnaît pas des objets et échoue avec l'erreur CTJTD3078E

Problème

Le détecteur ASDSensor termine sans objet reconnu et l'erreur suivante est émise :

```
CTJTD3075E Unable to execute command: tar -xf <asdfile> command
exit code: 1.
En outre, dans les journaux, l'erreur suivante apparaît :
tar: can't create ./@LongLink: Permission denied
```

Solution

Votre programme d'archivage sur bande doit prendre en charge les longs chemins d'accès au fichier. L'archivage sur bande GNU 1.13 n'est pas pris en charge car il risque de tronquer les noms de fichier longs.

Détecteur ping de reconnaissance asynchrone

Le détecteur ping d'une reconnaissance asynchrone récupère la première adresse IP valide d'un fichier archive de reconnaissance. Cette adresse IP sert de valeur de

départ au détecteur de reconnaissance asynchrone. Si vous ne pouvez pas définir une portée de reconnaissance et voulez exécuter une reconnaissance asynchrone, vous pouvez utiliser ce détecteur.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ASDPingSensor

Prérequis

Dans un profil de reconnaissance, si vous utilisez le détecteur ping de reconnaissance asynchrone, vous devez le désactiver car vous ne pouvez pas activer ces deux détecteurs à la fois.

Détecteur de serveur d'applications personnalisé

Le détecteur de serveur d'applications personnalisé crée un serveur d'applications personnalisé à partir d'un modèle et des informations sur le processus d'exécution qui sont reconnues par le détecteur de serveur générique. Le détecteur collecte aussi des fichiers de configuration ou des descripteurs d'application s'ils sont indiqués dans le modèle, puis réalise un traitement de l'extension pour collecter plus d'informations.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CustomAppServerSensor

Prérequis

Pour reconnaître des fichiers de configuration, le détecteur a besoin que le programme cksum et les bibliothèques associées soient installés sur le système d'exploitation cible.

Limitations

Les limitations suivantes s'appliquent :

- Le détecteur ne peut pas être exécuté en mode de reconnaissance basée sur un script.
- Les mêmes limitations que celles du «Détecteur de serveur générique», à la page 237 s'appliquent.

Objets de modèle créés

Les objets de modèle suivants permettent de créer des serveurs d'applications génériques :

- app.AppServer
- app.db.DatabaseServer
- app.j2ee.J2EESever
- app.web.WebServer

Les objets de modèle suivants permettent d'étendre les détecteurs d'applications TADDM :

- app.db.db2.Db2Server

- app.db.mssql.SqlServer
- app.j2ee.jboss.JBossServer
- app.j2ee.weblogic.WebLogicServer
- app.j2ee.websphere.WebSphereServer
- app.messaging.exchange.ExchangeServer
- app.messaging.mq.MQQueueManager
- app.sms.SMSiteServer
- app.veritas.cluster.VCSCluster
- app.web.apache.ApacheServer
- app.web.iis.IIsWebServer
- app.web.iplanet.IPlanetServer

Détecteur de système informatique MIB2 personnalisé

Le détecteur de système informatique MIB2 personnalisé crée un système informatique personnalisé basé sur des informations du modèle.

Ces informations de modèle sont semblables pour un ou plusieurs des éléments suivants :

- OID système (SNMPv2-MIB::sysObjectID - .1.3.6.1.2.1.1.2)
- Description du système (SNMPv2-MIB::sysDescr - .1.3.6.1.2.1.1.1) reconnue par le détecteur SNMP MIB2

Le détecteur de système informatique MIB2 personnalisé effectue un traitement des extensions pour collecter des informations supplémentaires.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CustomMib2ComputerSystemSensor

Limitations

Voir les limitations pour le détecteur SNMP MIB2.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.ComputerSystem hierarchy

Détecteur modèle personnalisé

Le détecteur modèle personnalisé peut être utilisé avec des scripts personnalisés pour analyser et améliorer les informations collectées par d'autres détecteurs.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CustomTemplateSensor

Limitations

Le détecteur ne peut pas être exécuté en mode de reconnaissance basée sur un script.

Configuration du détecteur

Vous devez configurer le détecteur modèle avant d'exécuter une reconnaissance.

Par défaut, le détecteur modèle n'est pas activé. Pour l'activer, vous devez créer un profil de reconnaissance, puis activer le détecteur dans le nouveau profil. Vous devez également activer ce profil dans les détecteurs supplémentaires à partir desquels vous souhaitez analyser les résultats.

Vous devez créer un modèle pour le détecteur modèle personnalisé. Ce modèle comprend les fichiers suivants :

template.xml
Ce fichier contient les données de configuration. Dans ce fichier, indiquez l'objet de classe de résultat TADDM que vous souhaitez analyser.

matcher-script.py
Ce script permet d'extraire les objets de modèle indiqués qui seront ensuite traités par le fichier `sensor-script.py`.

sensor-script.py
Ce script peut modifier des objets, créer des objets modèles et stocker des objets modèles.

Vous devez placer ces fichiers dans le répertoire `$COLLATION_HOME/etc/templates/cts/`*`template_name`*. Le nom du répertoire *template_name* doit correspondre exactement au nom indiqué dans le fichier `template.xml`.

Pour exécuter la reconnaissance, vous devez disposer de droits d'accès en lecture au répertoire `templates` et aux fichiers associés.

Les scripts sont des scripts Jython. Pour plus d'informations sur l'interface de programme d'application des extensions de serveur personnalisé, voir le guide du développeur *SDK Developer's Guide*. Des informations générales sur les scripts contenues dans ce guide peuvent être appliquées aux scripts du détecteur modèle personnalisé. Des informations détaillées sur le code associé à l'initialisation de l'environnement, à l'importation d'outils du détecteur TADDM et à la consignation d'erreurs peuvent être utilisées lors de la définition des scripts du détecteur. Vous devez placer ces fichiers dans le répertoire `$COLLATION_HOME/etc/templates/cts/`*`template_name`*.

Template.xml

Le fichier `template.xml` possède la structure suivante :

```
<CTSTemplate>
 <name>template_name</name>
 <result-class>com.ibm.cdb.discover.app.db.db2.result.Db2Result</result-class>
 <plugin-id>com.ibm.cdb.discover.sensor.app.db.db2.db2_7.6.0</plugin-id>
 <engine-id>com.ibm.cdb.core.jython253_2.5.3</engine-id>
 <matcher-script>matcher.py</matcher-script>
 <sensor-script>sensor.py</sensor-script>
</CTSTemplate>
```

Important : Vous devez organiser les éléments du fichier `template.xml` comme dans l'exemple qui précède. Sinon, des erreurs seront générées.

nom Nom du modèle. Par exemple, si le nom du modèle est *example_template*, la structure du répertoire doit être la suivante : `$COLLATION_HOME/etc/templates/cts/example_template`.

result-class
Le nom qualifié complet de la classe de résultat TADDM que vous souhaitez analyser.

plugin-id
Cette valeur *plugin-id* indique l'ID du plug-in fournissant les résultats. Cet ID n'est requis que pour les détecteurs connectables.

engine-id
Cet *engine-id* indique l'IP du plug-in qui fournit le moteur Jython à utiliser, par exemple `com.ibm.cdb.core.jython253_2.5.3`. Si aucun nom n'est spécifié, le moteur par défaut est utilisé.

matcher-script
Nom du script Jython (extension .py) qui répertorie tous les objets répondant aux critères définis dans le script.

sensor-script
Nom du script Jython qui traite la liste d'objets générés à partir du script result-matcher. En fonction de l'objet renvoyé, le script modifie les objets ou crée de nouveaux objets. Ces objets peuvent ensuite être stockés.

Script de correspondance

Ce script est exécuté lorsque l'objet de résultat de la classe indiquée dans le modèle est reconnu. Les informations suivantes sont fournies au script depuis le code `sensorhelper` :

- `ResultMap` est une carte des objets de modèle, de leurs matrices ou de leurs collections. Ces objets sont les propriétés partagées de l'objet de résultat qui sont reliés par le modèle. La carte est indexée par nom de propriété.
- `ReturnList` contient une liste d'éléments nécessitant davantage de traitement. Chaque élément est associé au nom affiché car le détecteur démarre pour cet élément.

Lorsque le script de correspondance des résultats se termine correctement, ces informations sont utilisées pour alimenter le détecteur de modèle personnalisé.

Cet exemple de script illustre les étapes nécessaires pour extraire les objets des résultats de la reconnaissance du détecteur de serveur générique.

```
# Initialisation de l'environnement
import sys
import java

from java.lang import System
coll_home = System.getProperty("com.collation.home")

System.setProperty("jython.home",coll_home + "/osgi/plugins/
com.ibm.cdb.core.jython_1.0.0/lib")
System.setProperty("python.home",coll_home + "/osgi/plugins/
com.ibm.cdb.core.jython_1.0.0/lib")

jython_home = System.getProperty("jython.home")
sys.path.append(jython_home + "/Lib")
sys.path.append(coll_home + "/lib/sensor-tools")
sys.prefix = jython_home + "/Lib"

import traceback

# Importation de sensorhelper
import sensorhelper
```

```
#  Initialisation de l'entrée de script
(resultMap,returnList,log) = sensorhelper.init(targets)
log.debug("CTS result matcher script running")

try:
    #  obtenir la liste des traitements d'exécution des résultats
    runtimeProcesses = resultMap['runtimeProcesses']
    # obtenir le premier des traitements
    rtp = runtimeProcesses[0][0]
    #  L'ajouter à la liste d'éléments nécessitant davantage de traitement
    returnList.add("dummyName",rtp)

except:
    log.error("Error occurred")
```

Vous pouvez utiliser une analyse XPath lorsque vous utilisez la bibliothèque JXPath pour déterminer lesquels de ces objets sont renvoyés. La fonction **findElementsForXPath** peut être utilisée pour interroger et renvoyer une collection d'objets résultant de la requête. L'exemple suivant recherche et imprime une adresse IP à l'aide de la fonction **findElementsForXPath**. Reportez-vous au guide du développeur *SDK Developer's Guide* pour plus d'informations sur cette fonction de programmation.

```
result = IpListResult();
ip1 = IpAddressImpl();
ip1.setStringNotation("9.0.0.1");
ip2 = IpAddressImpl();
ip2.setStringNotation("9.0.0.2");
result.list.add(ip2)
result.list.add(ip1)

elements = sensorhelper.findElementsForXPath(result,"/list[stringNotation='9.0.0.2']")
for e in elements:
    print e
```

Script du détecteur

Ce script démarre séparément pour chaque objet extrait renvoyé depuis le script de correspondance des résultats. En fonction des objets renvoyés, le script modifie, crée et renseigne les objets de modèle. Ces objets peuvent alors être stockés. Les informations suivantes sont fournies au script depuis le code `sensorhelper` :

- L'objet `CTSSeed` qui contient `ResultMap` et la paire de valeurs de nom renvoyés par le script de correspondance des résultats.
- L'objet `CTSResult` est un objet de résultat de modèle personnalisé qui est renseigné par le script du détecter avec les objets de modèles pouvant être stockés.

Cet exemple de script illustre les étapes qui renseigne et stocke les objets de modèle.

```
import sys
import java

from java.lang import System
coll_home = System.getProperty("com.collation.home")

System.setProperty("jython.home",coll_home +
"/osgi/plugins/com.ibm.cdb.core.jython_1.0.0/lib/jython-2.1")
System.setProperty("python.home",coll_home +
"/osgi/plugins/com.ibm.cdb.core.jython_1.0.0/lib/jython-2.1")

jython_home = System.getProperty("jython.home")
sys.path.append(jython_home + "/Lib")
```

```
sys.path.append(coll_home + "/lib/sensor-tools")
sys.prefix = jython_home + "/Lib"

import traceback
import sensorhelper

(ctsResult,ctsSeed,log) = sensorhelper.init(targets)

log.debug("CTS Sensor script running")
#  get value passed by result matcher
runtime_process = ctsSeed.getSeedInitiator().getValue()
#  get name passed by result matcher
name = ctsSeed.getSeedInitiator().getKey()
templateName = ctsSeed.getTemplate().getName();
log.debug("CTS Sensor script running for template " +templateName + "/" + name)
#  process runtime process with user defined function
result = processRuntimeProcess(runtime_process)
#  return resulting model object
ctsResult.addExtendedResult(result)
```

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de modèle personnalisé et propose des solutions à ces problèmes.

Le détecteur de modèle personnalisé ne démarre pas ou échoue

Problème

Il existe plusieurs situations possibles susceptibles d'empêcher le démarrage du détecteur ou de provoquer un échec.

Solution

Vérifiez que les conditions suivantes sont remplies :

- Le détecteur de modèle personnalisé est activé dans le profil de reconnaissance.
- Le modèle est les scripts du détecteur de modèle personnalisé se trouvent dans le répertoire approprié.
- Le nom du répertoire qui stocke le modèle relie le nom indiqué dans le fichier `template.xml`.
- Le format du fichier `template.xml` est valide.
- La classe de résultat *result-class* indiquée dans le fichier `template.xml` existe, et si nécessaire, *plugin-id* est indiqué.
- Les scripts (`matcher-script.py` et `sensor-script.py`) se trouvent dans le bon répertoire et sont correctement définis dans le fichier `template.xml`.
- Les scripts ne contiennent aucune erreur de syntaxe. Les erreurs non traités pour le script `matcher-script.py` sont enregistrées dans le fichier journal mais aucun fichier de départ n'est créé. Les erreurs non traitées pour le script `sensor-script.py` sont traitées dans le fichier journal et sont affichées dans la console Discovery Management Console.
- Le répertoire de modèles et les fichiers associés doivent avoir des droits d'accès appropriés. Vous devez disposer de droits d'accès au répertoire et aux fichiers associés.
- Le détecteur qui collecte les données doit compléter sa reconnaissance sans erreurs.
- La syntaxe du comparateur et des scripts de détecteur doit correspondre à la version de Jython utilisée, comme défini par la balise *engine-id* dans le fichier `template.xml`.

Détecteur de système informatique générique

Le détecteur de système informatique générique reconnaît le type d'un système informatique. Les résultats de ce détecteur sont utilisés pour démarrer un détecteur de système informatique spécifique, tel que le détecteur de système informatique Linux.

Nom du détecteur utilisé dans l'interface graphique et les journaux

GenericComputerSystemSensor

Détecteur de serveur générique

Le détecteur de serveur générique reconnaît les serveurs d'applications qui s'exécutent sur un système informatique hôte.

Le détecteur reconnaît d'abord les ports d'écoute (adresse IP et ports), les connexions établies et les processus en cours d'exécution sur les systèmes informatiques cible. Des modèles permettent de mettre en correspondance les informations de processus d'exécution. Lorsque les critères spécifiés sont remplis, les informations sont utilisées pour démarrer des détecteurs d'applications spécifiques, tels que le détecteur Apache ou un détecteur de serveur d'applications personnalisé.

Les processus peuvent s'exécuter sur des adresses IPv4 ou IPv6. Les processus qui s'exécutent uniquement sur des adresses IPv6 sont reconnus, mais aucune valeur de départ démarrant un détecteur plus spécifique n'est créée.

Des modèles de serveur personnalisés sont utilisés pour reconnaître des serveurs d'applications que TADDM ne catégorise pas automatiquement. Vous pouvez créer des modèles de serveur à l'aide de la console de gestion de reconnaissance. Si plusieurs modèles de serveur personnalisés correspondent aux informations sur le processus d'exécution de l'application, seul le premier modèle entraîne l'exécution du détecteur de serveur d'applications personnalisé.

Nom du détecteur utilisé dans l'interface graphique et les journaux

GenericServerSensor

Limitations

Un détecteur requérant des droits d'accès et un détecteur personnalisé générique peuvent tous deux reconnaître le même système cible durant plusieurs reconnaissances. Selon la nature des données reconnues sans droits d'accès, le système ne peut pas garantir que les objets créés par le modèle de serveur personnalisé sont rapprochés des artefacts créés par le détecteur.

Objets de modèle créés

Le détecteur crée l'objet de modèle suivant :

- sys.RuntimeProcess

Commande `netstat` au lieu de la commande `lsof` pour le système d'exploitation AIX

Le détecteur de serveurs génériques par défaut utilise la commande **`netstat`** au lieu de la commande **`lsof`** sur les systèmes d'exploitation AIX. Ainsi, les processus de partition logique et de partition de la charge de travail sont séparés et le détecteur générique de partition de la charge de travail est exécuté afin d'identifier les applications installées sur les partitions de la charge de travail.
Pour plus d'informations, voir «Détecteur générique de partition de charge de travail», à la page 267.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de serveur générique prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Certaines fonctions fournies par le détecteur de serveur générique durant une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

Sous le système d'exploitation Solaris qui prend en charge la virtualisation, à partir de la zone commune, le détecteur de serveur générique ne prend pas en charge la reconnaissance de processus d'exécution dans des zones locales.

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

com.collation.platform.os.ignoreLoopbackProcesses=`true`

La valeur par défaut est `true`, ce qui signifie que les processus d'écoute sur les interfaces de bouclage sont ignorés. Si un serveur est en mode écoute uniquement sur l'adresse IP de bouclage (127.0.0.1), mais sur aucune autre adresse IP externe disponible, ce serveur ne sera donc pas reconnu.

Cette propriété contrôle la reconnaissance des adresses IP externes.

Si la valeur de cette propriété est définie sur `false`, tous les processus dotés de ports d'écoute sont pris en compte pour la reconnaissance.

Vous devez définir cette propriété à `true` si vous voulez reconnaître un serveur d'applications Oracle ou les détecteurs WebLogic. Par exemple, si le détecteur WeblogicServerVersionSensor tente de démarrer avec une adresse de système hôte local, cette propriété doit être définie à `true`.

com.collation.discover.agent.command.netstat.Windows

Vous pouvez utiliser cette propriété pour indiquer une commande personnalisée à utiliser au lieu de la commande `netstat -nao` sur une cible Windows.

Vous devez vous assurer que toute autre commande que vous indiquez renvoie des informations dans le même format que la commande `netstat-Nao` .

Par exemple,

`com.collation.discover.agent.command.netstat.Windows.`*`adresse_IP`*`=type c:\\\\dossier\\\\mynetstat.txt`

où `mynetstat.txt` contient la sortie de la commande `netstat -nao`, tandis que la commande `type` permet d'imprimer le contenu du fichier.

com.collation.netstatoverlsof.AIX=true

Cette propriété spécifie quelle commande (netstat or lsof) est utilisée pour collecter les informations de processus sur les systèmes d'exploitation AIX. Elle permet essentiellement de déterminer la commande qui va créer la mappe de port et ouvrir le port TCP pour traiter la mappe.

Par défaut, la propriété est définie sur **`true`** et la commande **`netstat` est utilisée.**

Si la propriété est définie sur `false`, la commande **`lsof`** est utilisée. Toutefois, la commande **`netstat`** peut toujours être utilisée dans certains cas, par exemple lorsque vous devez déterminer si les privilèges de la commande **`isof`** sont suffisants ou pas.

Remarque : Il existe une dépendance avec les commandes **`netstat`** et **`kdb`**, même si cette propriété est définie sur `false`. Il est également important de signaler que la commande **`netstat`** est exécutée dans la couche du système d'exploitation et que sa présence est obligatoire, pas seulement pour le détecteur GenericServer.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de serveur générique et propose les solutions à ces problèmes.

Le détecteur de serveur générique ne reconnaît pas les connecteurs ouverts

Problème

Le détecteur de serveur générique ne parvient pas à reconnaître les sockets vides. Le message suivant apparaît dans les journaux d'erreurs :

`CTJTD2522E Le détecteur ne parvient pas à découvrir les ID des processus pour les sockets libres.`

Solution

Consultez les journaux de niveau de débogage du détecteur pour obtenir plus de détails sur la cause de cet incident. Selon la cause, effectuez les tâches suivantes :

- Si le délai d'attente d'une commande a été dépassé, augmentez le délai d'attente en configurant la valeur de la `propriété`

com.collation.discover.agent.command.pidsInfoTimeout. Cette propriété peut être sectorisée à une IP spécifique. Par exemple, la propriété com.collation.discover.agent.command.pidsInfoTimeout.192.168.2.1=1800000 indique un délai d'attente de 30 minutes pour l'IP 192.168.2.1. Pensez à augmenter les valeurs du délai d'attente pour le détecteur de serveur générique ainsi que le détecteur de système informatique AIX d'IBM.

- Si les journaux contiennent l'un des messages suivants :
  - «os.AixOs - Impossible d'obtenir les identifiants des processus pour les sockets libres com.collation.platform.os.OsException : Impossible de trouver <*sctp_pcb_hash_table*>» (pour une reconnaissance standard),
  - «sensor.GenericServerScriptSensor - Impossible de trouver <*sctp_pcb_hash_table*>» (pour une reconnaissance basée sur un script),

  appliquez un correctif pour APAR IZ98746, IZ98842, IV04783, ou IV05965 sur un hôte AIX reconnu.
- Si les journaux contiennent un message semblable à celui-ci :

```
for i in `netstat -Aan| grep tcp|awk '{print $1}'`;do echo \"sockinfo
$itcpcb\"|kdb|grep ACTIVE; echo $i$'\n####';done
open: Permission denied
f1000200000060bb0
####
open: Permission denied
f10002000004ebb0
####
...
```

  effectuez l'une des opérations suivantes :
  - Installez les commandes **netstat**, **sockinfo** et **kdb**. Accordez à l'utilisateur TADDM des droits d'exécution de ces commandes.
  - Si la commande **kdb** est installée, associez-la à sudo en définissant la propriété suivante :

    ```
    com.collation.discover.agent.command.kdb = sudo kdb
    ```
  - Définissez la propriété com.collation.netstatoverlsof.AIX sur false afin d'activer la commande **lsof** pour collecter les informations sur le processus au lieu de la commande **netstat**.

Détecteur d'utilisation d'IBM Tivoli

Le détecteur d'utilisation d'IBM Tivoli collecte les métriques de base à partir d'un système cible. Il utilise l'infrastructure de reconnaissance de TADDM pour déployer des scripts exécutant sur le système cible des commandes de surveillance des performances au niveau du système. A des intervalles spécifiés, le détecteur rassemble des données du système cible et les fournit au serveur TADDM, sur lequel des objets de mesure du système d'exploitation sont créés.

Le détecteur d'utilisation d'IBM Tivoli fournit des métriques ainsi qu'un rapport d'utilisation. Vous pouvez utiliser ces informations avec le rapport de topologie des connexions système afin d'identifier les serveurs qui ne sont pas utilisés pour la capacité et qui ne fournissent pas de services aux autres serveurs.

Nom du détecteur utilisé dans l'interface graphique et les journaux

OperatingSystemUtilizationSensor

Prérequis

Pour que le détecteur puisse reconnaître un système cible, les commandes suivantes doivent y être installées, dans l'emplacement par défaut du système d'exploitation utilisé :

- Commande **compress**
- Commande **netstat**
- Commande **sadc**
- Commande **sar**

Sur les systèmes cible qui exécutent les systèmes d'exploitation suivants, les conditions suivantes doivent être remplies :

- Linux
  - La commande **compress** doit être disponible.
  - La commande **netstat** doit être disponible.
  - La commande **sar** doit être disponible.
  - La commande **sadc** doit être disponible.
- Solaris
  - La commande **compress** doit être disponible.
  - La commande **netstat** doit être disponible.
  - La commande **sar** doit être disponible.
- AIX
  - La commande **compress** doit être disponible.
  - La commande **netstat** doit être disponible.
  - La commande **sar** doit être disponible.
  - Pour exécuter **sar**, le compte de service TADDM doit appartenir au groupe adm.
- HP-UX
  - La commande **compress** doit être disponible.
  - La commande **netstat** doit être disponible.
  - La commande **sar** doit être disponible.
  - Pour planifier les travaux **cron** et **at**, le compte de service TADDM doit être ajouté aux fichiers `cron.allow` et `at.allow`.

Vous devez copier les fichiers JAR suivants dans le répertoire `$COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.sys.utilization_version/lib` :

- `db2jcc.jar`
- `oracle-jdbc-9.2.jar`

Limitations

Le détecteur est pensé pour une utilisation à court terme (par exemple, pendant un mois maximum) en vue d'analyser des serveurs et d'identifier des cibles de consolidation. Le détecteur ne peut être utilisé que pour la zone du pare-feu dans lequel le serveur TADDM réside. L'utilisation d'un serveur d'ancrage n'est pas prise en charge.

Sur une période prolongée, pour déterminer la disponibilité, les performances et l'utilisation du serveur et pour reconnaître les applications qui s'étendent sur les zones de pare-feu, servez-vous du produit IBM Tivoli Monitoring.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur d'utilisation d'IBM Tivoli prend en charge des reconnaissances asynchrones et basées sur un script. Toute fonction fournie par le détecteur lors d'une reconnaissance non basée sur un script est prise en charge dans une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour la reconnaissance asynchrone, commencez par effectuer les étapes décrites dans la rubrique *Configuration de la reconnaissance asynchrone* du *Guide d'administration* de TADDM. Avant d'exécuter une reconnaissance asynchrone, vous devez démarrer le détecteur d'utilisation sur le système cible pour collecter les données d'utilisation. Le module de script de reconnaissance qui est généré pour une reconnaissance asynchrone doit être extrait du système cible. Une fois le module du script de reconnaissance extrait, procédez comme suit :

1. Changez pour le répertoire `taddmasd/com.ibm.cdb.discover.sensor.sys.utilization_version`.
2. Changez les droits d'accès aux fichiers à l'aide de la commande suivante :
   ```
   chmod 700 *.sh
   ```
3. Pour démarrer le détecteur d'utilisation, exécutez la commande suivante :
   ```
   ./utilizationDeployer.sh -c
   ```
   Indiquez l'intervalle de temps et la durée de collecte des données. Avant de démarrer la collecte des données, vous devez attendre que le l'intervalle de temps soit écoulé.
4. Collectez périodiquement des données en exécutant le script `taddmasd/scriptsRunner.sh`. Ce script génère un fichier archive qui contient les données d'utilisation.
5. Déplacez le fichier archive résultant vers le serveur TADDM.
6. Créez un profil de reconnaissance asynchrone pour le détecteur d'utilisation, activez le détecteur, puis exécutez une reconnaissance asynchrone.
7. Lorsque la collecte des données d'utilisation est terminée, pour arrêter le détecteur d'utilisation, changez pour le répertoire `taddmasd/com.ibm.cdb.discover.sensor.sys.utilization_version` et exécutez la commande suivante :
   ```
   ./utilizationDeployer.sh -u
   ```

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Objets de modèle avec attributs associés

Le détecteur d'utilisation d'IBM Tivoli crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur l'utilisation de vos systèmes informatiques dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

metric.OperatingSystemMetric

- Label
- MetricName
- MetricUnitOfMeasure
- MetricValue
- StatisticName

net.IpInterface

- IpAddress

relation.Gauges

- Source (OperatingSystemMetric)
- Target (OperatingSystem)

Les types de système informatique suivants sont reconnus :

sys.aix.AixUnitaryComputerSystem
sys.hpux.HpUxUnitaryComputerSystem
sys.linux.LinuxUnitaryComputerSystem
sys.sun.SunSPARCUnitaryComputerSystem
sys.windows.WindowsComputerSystem

L'attribut suivant est associé à ces objets de modèle :

- signature

Les types de système d'exploitation suivants sont reconnus :

sys.aix.Aix
sys.hpux.HpUx
sys.linux.Linux
sys.sun.Solaris
sys.windows.WindowsOperatingSystem

L'attribut suivant est associé à ces objets de modèle :

- OSName

Configuration du détecteur

Avant d'exécuter le détecteur IBM Tivoli Utilization pour collecter des données à partir d'une machine cible, vous devez le configurer.

Définition des paramètres de configuration :

Vous pouvez configurer le comportement du détecteur IBM Tivoli Utilization en définissant les paramètres de configuration.

La table suivante répertorie les paramètres de configuration du détecteur IBM Tivoli Utilization.

Tableau 19. Paramètres de configuration

Nom du paramètre	Description
operatingMode	Le mode d'opération du détecteur. Les valeurs suivantes sont valides : **ONCE** Indique que les scripts de collecte sont exécutés une seule fois pour les valeurs interval, numDays ou maxFileSize spécifiées, selon la situation qui se présente en premier. Une fois l'exécution des scripts de collecte terminée, les données sont collectées par le détecteur lors de sa prochaine exécution. Les données collectées sont analysées puis stockées sur la base de données TADDM. Tous les fichiers de sortie figurant sur la machine cible sont nettoyés. **RESTART** Indique que les scripts de collecte sont redémarrés lorsqu'ils se terminent normalement. **CLEANUP** Indique que toute opération de collecte en cours d'exécution sur le système est immédiatement arrêtée puis nettoyée. Une fois une opération de collecte appelée, elle peut uniquement être redémarrée sur cette machine en définissant la valeur operatingMode sur RESTART.
collectionMode	Mode de collecte du détecteur. Les valeurs suivantes sont valides : **ALWAYS** Indique que les données sont collectées à chaque exécution du détecteur sur le système cible, que l'exécution des scripts de collecte soit ou non terminée. **END** Indique que les données sont collectées lorsque le détecteur est exécuté sur le système cible, et ce uniquement si l'exécution des scripts de collecte est terminée. Sauf si la valeur operatingMode est définie sur CLEANUP, aucune donnée n'est collectée lorsque les opérations de reconnaissance sont effectuées avant la fin de l'exécution des scripts de collecte.
interval	Intervalle de collecte, en minutes, pour les scripts de collecte en cours d'exécution sur le système cible. Les valeurs admises sont comprises entre 3 et 60 minutes.
numDays	Nombre de jours pendant lesquels les scripts de collecte sont exécutés sur le système cible. Les valeurs admises sont comprises entre 1 jour et 35 jours.
maxFileSize	Taille maximale, en Mo, des fichiers de sortie créés par les scripts de collecte. Les valeurs admises sont comprises entre 1 et 100 Mo.

Configuration des options de nettoyage :

Le détecteur IBM Tivoli Utilization est doté d'une fonction qui nettoie et supprime automatiquement les données et les scripts de collecte stockés sur la machine cible. Le nettoyage peut également être effectué manuellement si nécessaire.

Configuration du nettoyage automatique pendant la reconnaissance

Pour utiliser la fonction de nettoyage automatique, procédez comme suit :

1. Créez une configuration de profil pour le détecteur IBM Tivoli Utilization avec le paramètre operatingMode défini sur CLEANUP.
2. Effectuez une reconnaissance à l'aide du profil dont l'option CLEANUP est définie.

Une fois le nettoyage terminé sur la machine de reconnaissance cible, vous devez effectuer une opération RESTART pour redémarrer les scripts de collecte.

Exécution d'un nettoyage manuel

Procédez comme suit pour effectuer un nettoyage manuel sur une machine cible UNIX :

1. Accédez au répertoire `/var/tmp/`.
2. Exécutez la commande suivante :
   `./scmd_perf.sh -k -c -r`
3. Supprimez le fichier verrou du détecteur IBM Tivoli Utilization.

Procédez comme suit pour effectuer un nettoyage manuel sur une machine cible Windows :

1. Accédez au répertoire `C:\`.
2. Supprimez le script `WINTEL-MAN-PERF.VBS`.
3. Supprimez le fichier `PerformanceData_`*`nomd'hôte`*`.out`.
4. Supprimez le fichier verrou du détecteur IBM Tivoli Utilization.

Configuration du rapport BIRT :

Vous pouvez utiliser le rapport Utilization BIRT pour générer des rapports basés sur les données collectées par le détecteur IBM Tivoli Utilization.

Pourquoi et quand exécuter cette tâche

Important : La configuration du rapport Utilization BIRT n'est possible que si vous avec activé le visualiseur de rapports BIRT. Le visualiseur de rapports BIRT est désactivé en raison de problèmes de sécurité. L'autre moyen de visualiser des rapports BIRT consiste à utiliser Tivoli Common Reporting (TCR) après avoir importé les rapports dans TCR. Si vous êtes conscient des risques, vous pouvez toujours restaurer le visualiseur de rapports BIRT.

Pour savoir comment restaurer le visualiseur de rapports BIRT, voir la rubrique *Restauration du visualiseur de rapports BIRT* dans le *Guide d'administration* de TADDM.

Les étapes 1, 2 et 4 sont spécifiques du visualiseur de rapports BIRT. Si vous visualisez des rapports à l'aide de TCR, vous devez spécifier des valeurs pour les paramètres comme dans l'étape 3.

Procédure

Pour configurer le rapport Utilization BIRT, procédez comme suit dans le portail de gestion de données :

1. Cliquez sur **Analyse** > **Rapports BIRT**. La fenêtre Rapports TADDM BIRT s'affiche.
2. Sélectionnez le rapport **TADDM_SERVER_UTILIZATION**, puis cliquez sur **Exécuter le rapport**.
3. Dans la fenêtre Paramètre, une valeur doit être spécifiée pour chaque paramètre ci-après :

   Portée Dans la liste des portées TADDM disponibles, sélectionnez une portée.

Unité de mesure
Dans la liste des unités de mesure disponibles, sélectionnez l'unité de mesure pour laquelle vous souhaitez afficher des données ou sélectionnez ALL pour afficher les données pour toutes les unités de mesure.

Opérateur
Les opérateurs sont utilisés pour limiter les données affichées dans le rapport. Dans la liste des opérateurs disponibles, sélectionnez un opérateur ou sélectionnez N/A pour afficher toutes les données pour l'unité de mesure sélectionnée.

Valeur Si vous avez indiqué un opérateur, vous devez spécifier une valeur correspondante. Sinon, sélectionnez N/A pour afficher toutes les données pour l'unité de mesure sélectionnée.

Another value
Si vous avez indiqué un opérateur, et qu'il requiert deux valeurs, vous devez spécifier une valeur correspondante pour la seconde valeur. Sinon, sélectionnez N/A pour afficher toutes les données pour l'unité de mesure sélectionnée.

Number of application dependencies
Le nombre de dépendances de l'application est utilisé pour limiter les données affichées dans le rapport. Indiquez le nombre de dépendances de l'application ou sélectionnez N/A pour afficher toutes les données pour l'unité de mesure sélectionnée.

4. Cliquez sur **OK**. La sortie du rapport s'affiche dans BIRT Report Viewer.

Que faire ensuite

Pour configurer le rapport HOURLY Peak Server Utilization BIRT, procédez comme suit dans le portail de gestion de données :

1. Cliquez sur **Analyse** > **Rapports BIRT**. La fenêtre Rapports TADDM BIRT s'affiche.
2. Sélectionnez le rapport **TADDM_SERVER_UTILIZATION_HOURLY_PEAK**, puis cliquez sur **Exécuter le rapport**.
3. Dans la fenêtre Paramètre, une valeur doit être spécifiée pour chaque paramètre ci-après :

   Portée Dans la liste des portées TADDM disponibles, sélectionnez une portée.

   Date Dans la liste des dates disponibles, sélectionnez une date.
4. Cliquez sur **OK**. La sortie du rapport s'affiche dans BIRT Report Viewer.

Configuration du profil de reconnaissance :

Le détecteur IBM Tivoli Utilization est configuré à l'aide des profils de reconnaissance. Un profil de reconnaissance par défaut prêt à l'emploi, appelé Utilization Discovery, est fourni. Il peut être utilisé pour effectuer des reconnaissances ou un profil avec des valeurs de paramètre de configuration personnalisé peut être créé.

Le profil Utilization Discovery prêt à l'emploi est doté des valeurs de propriété par défaut suivantes :

- operatingMode : ONCE
- collectionMode : ALWAYS

- interval : 15
- numDays : 35
- maxFileSize : 100

Il contient les détecteurs par défaut suivants :
- Détecteur Ping
- Détecteur de port
- Détecteur de session
- Détecteur d'ancrage
- Détecteur de système d'exploitation Utilization

Si le profil de reconnaissance par défaut est insuffisant pour couvrir vos besoins, vous pouvez créer un profil avec des paramètres de configuration personnalisés. Procédez comme suit pour créer un profil de reconnaissance personnalisé :

1. Dans le tiroir **Reconnaissance** de la console de gestion de reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la zone **Nom de profil**, entrez le nom du nouveau profil.
4. Dans la zone **Description**, entrez une description du nouveau profil.
5. Dans la liste **Cloner le profil existant**, sélectionnez **Utilization Discovery**.
6. Cliquez sur **OK**.
7. Dans la fenêtre Profils de reconnaissance, sélectionnez le nouveau profil et dans l'onglet **Configuration de détecteur**, sélectionnez le détecteur `OperatingSystemUtilizationSensor`.
8. Pour créer une configuration de détecteur basée sur la configuration par défaut du détecteur `OperatingSystemUtilizationSensor`, cliquez sur **Nouveau**. La fenêtre Créer une configuration s'affiche.
9. Dans la zone **Nom**, entrez le nom de la nouvelle configuration de détecteur.
10. Dans la zone **Description**, entrez une description de la nouvelle configuration de détecteur.
11. Cliquez sur **Activer cette configuration et désactiver la configuration sélectionnée** pour vous assurer que cette configuration est utilisée par défaut par le profil de reconnaissance.
12. Pour chaque paramètre de configuration que vous voulez mettre à jour, exécutez les tâches suivantes :
    a. Dans la section **Configuration**, cliquez deux fois sur le paramètre de configuration que vous souhaitez modifier.
    b. Entrez une nouvelle valeur pour le paramètre de configuration.
13. Cliquez sur **OK**.
14. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques rencontrés par le détecteur IBM Tivoli Utilization et présente des solutions à ces problèmes.

Echec de la reconnaissance à l'aide du processus de nettoyage lors de l'utilisation de données d'identification sans privilèges d'administrateur

Problème

Une reconnaissance effectuée par le détecteur Utilization à l'aide de

l'option `CLEANUP` échoue pour un noeud final lorsque des données d'identification sans privilèges d'administrateur sont utilisées.

Solution

Si la dernière reconnaissance du noeud final a été effectuée par un serveur TADDM utilisant des données d'identification superutilisateur, les scripts du détecteur Utilization déployés sur `/var/temp` disposent d'un accès au système de type superutilisateur. Ces scripts ne peuvent pas être supprimés par l'ID de l'utilisateur non superutilisateur. Pour vous assurer que le nettoyage se termine correctement, effectuez une reconnaissance à l'aide du détecteur Utilization en utilisant l'option `CLEANUP` ainsi que des données d'identification superutilisateur sur ce noeud final. Tous les scripts existants du détecteur Utilization sont supprimés.

Des données de mesure n'ont pas été reconnues dans un ordinateur cible lors de l'exécution d'une reconnaissance asynchrone

Problème

Une reconnaissance asynchrone est exécutée, mais le détecteur IBM Tivoli Utilization ne reconnaît pas les données de mesure sous le système d'exploitation Solaris.

Solution

Vous devez démarrer le détecteur IBM Tivoli Utilization à partir du module de script extrait sur le système cible.

périphérique IP, détecteur

Le détecteur de périphérique IP crée un système informatique léger représentant un périphérique IP sur le réseau.

Nom du détecteur utilisé dans l'interface graphique et les journaux

IpDeviceSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.IpInterface
- sys.ComputerSystem

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur de périphérique IP.

com.ibm.cdb.topomgr.reconciliation.compsys.CompSysReconcilatior.disable LMTupdate=*false*

Indique s'il faut modifier l'heure de la dernière modification d'un système informatique qui est reconnu par le détecteur de périphérique IP, lorsqu'un tel système informatique existe dans la base de données de TADDM et a été reconnu par d'autres détecteurs.

Pour désactiver la mise à jour de l'heure de la dernière modification, définissez cette propriété à *true*. Par défaut, cette propriété est définie sur *false*.

Détecteur d'interface IP

Le détecteur d'interface IP reconnaît des interfaces IP.

Nom du détecteur utilisé dans l'interface graphique et les journaux

IpInterfaceSensor

Limitations

Pour les caractéristiques des routeurs IPv6 et IPv4, l'attribut de transfert IP est défini sur false indépendamment du paramétrage du système Windows reconnu. N'activez pas le détecteur d'interface IP. La fonction fournie par le détecteur d'interface IP est désormais fournie par le détecteur de système informatique approprié. L'activation du détecteur d'interface IP peut provoquer des anomalies de performances.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.IpInterface
- net.IpV4Router
- net.IpV6Router
- sys.ComputerSystem

Détecteur Ping

Le détecteur ping reconnaît les adresses IP accessibles. Il collecte des informations sur les périphériques et systèmes compatibles TCP/IP.

Nom du détecteur utilisé dans l'interface graphique et les journaux

PingSensor

Limitations

- En raison des problèmes liés aux performances, lors de la reconnaissance de ping sur UDP, le détecteur Ping utilise toujours des entrées de liste d'accès SNMPv1 et SNMPv3 entièrement définies, quelque soit les limitations quant à leur portée.

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Vous pouvez configurer PingSensor pour démarrer une session sur des adresses IP qui sont accessibles via une session d'automatisation d'exécution OSLC.

Vous pouvez modifier le comportement des systèmes cible accessibles via une session d'automatisation d'exécution OSLC en définissant la propriété suivante :

`com.ibm.cdb.discovery.StartOSLCSessionDirectly`

Si la propriété est définie à `true`, le détecteur n'envoie pas de commande Ping aux ports et les systèmes cible qui sont accessibles via une session d'automatisation

d'exécution OSLC ne sont pas analysés. Le détecteur de session est démarré directement après une commande PingSensor pour de tels systèmes.

Si la propriété est définie à `false`, PingSensor envoie une commande Ping à tous les systèmes cible.

La valeur par défaut de la propriété est `true`.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur ping.

com.collation.discover.agent.PingSensor.timeout=600000
Cette valeur indique l'intervalle de temps en millisecondes avant un délai d'attente pendant une reconnaissance.

com.collation.pingagent.ports=*xx*, *yy*, ...
Cette propriété n'est pas définie dans le fichier `collation.properties` et doit être ajoutée manuellement si besoin est. Les valeurs valides sont des nombres non négatifs qui représentent des ports pour le détecteur ping.

Par défaut, le détecteur ping utilise le port 22 ; s'il ne peut pas s'y connecter, il utilise le port 135. Pour remplacer l'ensemble de ports TCP par défaut utilisés par le détecteur ping, ajoutez cette propriété au fichier `collation.properties` et séparez les ports TCP par des virgules.

com.ibm.cdb.discover.enablePingDiscoveryOverUdp=false
Si la valeur est définie sur true, le détecteur exécute un ping supplémentaire sur UDP.

Vous pouvez également accéder à la propriété via l'onglet Product Console Platform Properties pour les profils de reconnaissance personnalisés.

Restriction : Les limitations quant à la portée pour cette propriété ne sont pas prises en charge.

com.ibm.cdb.discover.pingUDPPorts=161
Les valeurs valides sont des nombres non négatifs.

Cette propriété indique les ports à scanner pendant la reconnaissance ping UDP. Par défaut, le détecteur Ping utilise le port 161. Vous pouvez également accéder à la propriété via l'onglet Product Console Platform Properties pour les profils de reconnaissance personnalisés.

Restriction : Les limitations quant à la portée pour cette propriété ne sont pas prises en charge.

com.ibm.cdb.discover.SNMPPingWaitTime=2000
Cette propriété indique la durée (en millisecondes) pendant laquelle le détecteur Ping doit attendre pour une requête ping unique envoyée via le protocole SNMP avec des données d'authentification SNMP spécifiques.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Ping et propose des solutions à ces problèmes.

Une reconnaissance du détecteur Ping se termine par le message Impossible d'établir la connexion de bouclage

Problème

Le détecteur échoue lorsque la portée de la reconnaissance est importante, en raison d'une erreur de dépassement du délai d'attente et le message suivant s'affiche :

```
Unable to establish loopback connection
(Impossible d'établir la connexion de bouclage)
```

Afficher le fichier journal pour obtenir une description détaillée du message, par exemple :

```
<log start>
java.io.IOException: Unable to establish loopback connection
at sun.nio.ch.PipeImpl$Initializer.run(PipeImpl.java:172)
at java.security.AccessController.doPrivileged(AccessController.java:246)
at sun.nio.ch.PipeImpl.<init>(PipeImpl.java:188)
at sun.nio.ch.SelectorProviderImpl.openPipe(SelectorProviderImpl.java:45)
at java.nio.channels.Pipe.open(Pipe.java:148)
at sun.nio.ch.WindowsSelectorImpl.<init>(WindowsSelectorImpl.java:192)
at sun.nio.ch.WindowsSelectorProvider.openSelector(WindowsSelectorProvider.java:53)
at java.nio.channels.Selector.open(Selector.java:224)
at com.collation.platform.session.Ping$Connector.<init>(Ping.java:303)
at com.collation.platform.session.Ping.pingArray(Ping.java:656)
at com.collation.platform.session.Ping.pingLoop(Ping.java:574)
at com.collation.platform.session.Ping.ping(Ping.java:557)
at com.ibm.cdb.discover.sensor.net.ping.PingSensor.do_ping(PingSensor.java:75)
at com.ibm.cdb.discover.sensor.net.ping.PingSensor.discover(PingSensor.java:92)
at com.collation.discover.engine.AgentRunner.run(AgentRunner.java:214)
at com.collation.discover.engine.DiscoverEngine.processWorkItem(DiscoverEngine.java:1184)
at com.collation.discover.engine.DiscoverEngine$DiscoverWorker.run(DiscoverEngine.java:867)
Caused by: java.nio.channels.ClosedByInterruptException
at java.nio.channels.spi.AbstractInterruptibleChannel.end(AbstractInterruptibleChannel.java:216)
at sun.nio.ch.SocketChannelImpl.connect(SocketChannelImpl.java:543)
at java.nio.channels.SocketChannel.open(SocketChannel.java:161)
at sun.nio.ch.PipeImpl$Initializer.run(PipeImpl.java:120)
... 16 de plus
<log end>
```

Solution

Utilisez l'une des méthodes suivantes pour résoudre les problèmes :

- Exécutez la reconnaissance sur une portée plus petite.
- Dans le fichier `collation.properties`, augmentez la valeur du délai d'attente afin d'obtenir un temps de reconnaissance plus long pour la propriété suivante :

  ```
  com.collation.discover.agent.PingSensor.timeout=600000
  ```

La reconnaissance du détecteur ping se termine avec l'erreur CTJTD0510E

Problème

Si vous activez la reconnaissance ping sous UDP, il est possible que, lors de la reconnaissance de grandes portées, le détecteur se termine avec le message d'erreur suivant car il dépasse la limite de sockets ouverts :

```
CTJTD0510E The following error occurred in the ping sensor:
Too many open files.
```

Afficher le fichier journal pour obtenir une description détaillée du message, par exemple :

```
<log start>
sensor.PingSensor - Exception in Ping Broadcast Agent
java.io.IOException: Too many open files
    at sun.nio.ch.IOUtil.makePipe(Native Method)
  at sun.nio.ch.EPollSelectorImpl.<init>(EPollSelectorImpl.java:77)
    at sun.nio.ch.EPollSelectorProvider.openSelector(EPollSelectorProvider.java:48)
    at java.nio.channels.Selector.open(Selector.java:238)
    at com.collation.platform.session.Ping$TcpConnector.<init>(Ping.java:354)
    at com.collation.platform.session.Ping$TcpConnector.<init>(Ping.java:349)
    at com.collation.platform.session.Ping.pingArray(Ping.java:926)
    at com.collation.platform.session.Ping.pingLoop(Ping.java:840)
```

```
    at com.collation.platform.session.Ping.ping(Ping.java:821)
    at com.ibm.cdb.discover.net.ping.sensor.PingSensor.do_ping(PingSensor.java:81)
    at com.ibm.cdb.discover.net.ping.sensor.PingSensor.discover(PingSensor.java:114)
    at com.collation.discover.engine.AgentRunner.doRegularDiscovery(AgentRunner.java:349)
    at com.collation.discover.engine.AgentRunner.run(AgentRunner.java:271)
    at com.collation.discover.engine.DiscoverEngine.processWorkItem(DiscoverEngine.java:736)
    at com.collation.discover.engine.worker.DiscoverWorker.processWorkItemWithMetrics
(DiscoverWorker.java:100)
    at com.collation.discover.engine.worker.DiscoverWorker.run(DiscoverWorker.java:146)
2012-09-12 16:48:29,076 DiscoverManager [DiscoverWorker-5]
PingSensor-9.156.46.6⌂9.156.46.254 WARN engine.AgentRunner -
[AgentRunner.W.1] AgentException thrown in agent
com.collation.discover.agent.AgentException:
CTJTD0510E L'erreur suivante s'est produite dans le détecteur ping : Trop de fichiers ouverts.
<log end>
```

Solution

Utilisez l'une des méthodes suivantes pour résoudre les problèmes :

- Exécutez la reconnaissance sur une portée plus petite.
- Sous les systèmes UNIX, augmentez la limite de fichiers ouverts sur le serveur de reconnaissance. Pour plus d'informations sur la limite de fichiers ouverts, voir Configuration logicielle du serveur TADDM.

Le détecteur ping échoue avec une erreur d'expiration du délai d'attente

Problème

Pour les grandes portées, le détecteur échoue avec une erreur d'expiration du délai d'attente.

Toutes les actions du détecteur Ping qui sont visibles dans l'interface utilisateur sont exécutées dans une séquence. La valeur d'expiration du délai d'attente indiquée dans le fichier `collation.properties` défini la durée totale requise pour terminer ces actions.

Solution

Utilisez l'une des méthodes suivantes pour résoudre les problèmes :

- Exécutez la reconnaissance sur une portée plus petite.
- Dans le fichier `collation.properties`, augmentez la valeur du délai d'attente afin d'obtenir un temps de reconnaissance plus long pour la propriété suivante :

  ```
  com.collation.discover.agent.PingSensor.timeout=600000
  ```

Le détecteur ne reconnaît pas les noeuds finaux sur le protocole UDP

Problème

Lors de la reconnaissance de noeuds finaux qui sont accessibles uniquement sur le protocole UDP, certains d'entre eux sont manquants.

Solution

Vous devez configurer les propriétés responsables de la reconnaissance sur le protocole UDP. Pour plus d'informations sur ces propriété, consultez la section Configuration du fichier collation.properties.

Pour extraire des informations sur des ports UDP ouverts, le détecteur Ping utilise le protocole SNMP pour interroger les noeuds finaux de reconnaissance. Assurez-vous que les données d'authentification SNMP ou SNMPv3 appropriées sont fournies dans la liste d'accès TADDM. Vous pouvez également vérifier si votre pare-feu transmet le trafic réseau à travers les ports indiqués dans la propriété `com.ibm.cdb.discover.pingUDPPorts`.

Détecteur de port

Le détecteur de port reconnaît les ports ouverts sur un système hôte.

Vous pouvez changer certains aspects du détecteur de port à l'aide du fichier de configuration du détecteur. Vous devez créer un profil de reconnaissance personnalisé pour changer la configuration du détecteur de port. Avant d'éditer le fichier de configuration, contactez le service de support logiciel IBM.

Nom du détecteur utilisé dans l'interface graphique et les journaux

PortSensor

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de port et propose des solutions à ces problèmes.

Le détecteur ne reconnaît aucun port UDP ouvert

Problème

Lors de la reconnaissance des noeuds finaux, le détecteur ne trouve aucun port UDP ouvert.

Solution

Vous devez configurer les propriétés responsables de la reconnaissance sur le protocole UDP. Pour plus d'informations sur ces propriété, consultez la section Configuration du fichier collation.properties. Le détecteur Ping et le détecteur de port utilise les mêmes propriétés pour la reconnaissance sur le protocole UDP.

Pour extraire des informations sur des ports UDP ouverts, le détecteur Port utilise le protocole SNMP pour interroger les noeuds finaux de reconnaissance. Assurez-vous que les données d'authentification SNMP ou SNMPv3 appropriées sont fournies dans la liste d'accès TADDM. Vous pouvez également vérifier si votre pare-feu transmet le trafic réseau à travers les ports indiqués dans la propriété `com.ibm.cdb.discover.pingUDPPorts`.

Détecteur de session

Le détecteur de session crée une session entrée le serveur TADDM et le système informatique cible. En général, la session est de type SSH (Secure Shell) ou WMI (Windows Management Instrumentation).

Nom du détecteur utilisé dans l'interface graphique et les journaux

SessionSensor

Configuration de la liste d'accès

Les entrées de liste d'accès de type `système informatique` sont essayées de façon séquentielle jusqu'à ce qu'une session soit établie. Pour les cibles Windows, les entrées de liste d'accès de type `système informatique (Windows)` sont utilisées.

Identification et résolution des problèmes

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de session et propose des solutions à ces problèmes.

Fix Pack 2

L'adresse IP de la session CTJTD0591W n'a pas été trouvée dans les interfaces IP reconnues

Problème

L'adresse IP en cours de reconnaissance n'existe pas dans la liste d'interface de l'objet.

En règle générale, cela signifie que l'objet en cours de reconnaissance est un équilibreur de charge. La reconnaissance d'équilibreurs de charge peut entraîner un excès de fusions. Par exemple, si trois ordinateurs sont associés à l'équilibreur de charge, les requêtes SSH du détecteur peuvent être transmises à différentes cibles à chaque fois. Cela aurait pour conséquence la fusion progressive des trois ordinateurs.

Solution

Une nouvelle propriété a été ajoutée au détecteur de session : com.collation.discover.agent.sys.SessionSensor.loadBalancerIp

La valeur par défaut est false.

Si cette propriété est définie sur true, elle arrête le détecteur de session si elle détecte cette condition.

Remarque : Après l'échec du détecteur de session, le détecteur SnmpSensor n'est pas déclenché non plus.

Echec des détecteurs avec un message d'erreur d'accès refusé

Problème

Lors d'une reconnaissance de Windows Server 2012 avec le contrôle des comptes activé, le message d'erreur suivant s'affiche :

```
CTJTP1163E The following WMI session and SSH sessions cannot be established
 (WMI: SELECT BuildVersion FROM Win32_WMISetting failed: Access is denied.
```

Solution

Ce message indique que les paramètres de contrôle utilisateur sont trop restrictifs. Pour résoudre ce problème, procédez comme suit :

1. Sur la machine cible, exécutez l'éditeur de registre, Regedit.exe.
2. Attribuez la valeur 1 à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System LocalAccountTokenFilterPolicy`.
3. Dans la fenêtre du panneau de commande, cliquez sur l'onglet **Outils d'administration** et ouvrez **Local Security Policy**.
4. Développez **Local Policies**, puis cliquez sur **Security Options**.
5. Changez les règles suivantes :
   - Attribuez la valeur **Elever les privilèges sans invite utilisateur** à la règle **Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur**.
   - Attribuez la valeur **Désactivé** à la règle **Contrôle compte d'utilisateur : détecter les installations d'applications et demander l'élévation**.

Pour configurer des règles sur le système avec Active Directory, procédez comme suit :

1. Dans la fenêtre du panneau de commande, cliquez sur l'onglet **Outils d'administration** et ouvrez **Group Policy Management**.

2. Choisissez une forêt et un domaine, puis sélectionnez **Default Domain Policy**.
3. Cliquez sur **Action > Editer**.
4. Ouvrez `Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security options`.
5. Changez les règles suivantes :
   - Attribuez la valeur **Elever les privilèges sans invite utilisateur** à la règle **Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur**.
   - Attribuez la valeur **Désactivé** à la règle **Contrôle compte d'utilisateur : détecter les installations d'applications et demander l'élévation**.

La reconnaissance SSH d'une cible Windows avec Tectia SSH Server échoue avec une erreur de chemin virtuel non valide

Problème

La reconnaissance d'un système Windows échoue et les fichiers journaux contiennent le message suivant :

```
java.io.IOException: SSHSCP1.readResponse, error: scp: invalid virtual path
```

Solution

Tectia SSH Server prend en charge des dossiers virtuels. Il est possible de supprimer tous les dossiers virtuels nommés C:, D:, E:, etc. et de définir défini des dossier virtuels nommés C, D, E, etc. Dans un tel cas, des chemins d'accès complets avec un deux-points dans le nom, comme dans `/C:/folder/example.txt`, ne sont pas acceptés par le serveur. Pour résoudre ce problème, procédez comme suit :

- Modifiez la configuration de Tectia SSH Server en définissant des dossiers virtuels avec des deux-points.
- Ajoutez le propriété sectorisée au fichier `collation.properties`.

  ```
  com.ibm.cdb.session.tectia.filepath.removeColon=true
  ```

  Vous ne pouvez définir l'indicateur précédant que pour les IP et ensembles de portées sélectionnés. Par exemple :

  ```
  com.ibm.cdb.session.tectia.filepath.removeColon.10.11.12.13=true
  com.ibm.cdb.session.tectia.filepath.removeColon.scopesetA=true
  ```

L'application ne parvient pas à établir la session WMI

Problème

Les journaux de SessionSensor contiennent le message d'avertissement suivant :

```
SessionSensor-10.4.112.196-[445,135] WARN engine.AgentRunner -
[AgentRunner.W.1] AgentException thrown in agent
com.collation.discover.agent.AgentException: CTJTP1161E The application
cannot establish the following WMI session: SessionClientException:
Uncaught exception invoking InstallProvider: System.
NullReferenceException: Object reference not set to an instance of an
object.
```

Solution

Pour déterminer la cause du problème, procédez comme suit :

1. Testez WMI en local par l'exécution de requêtes simples, pour voir si des données sont renvoyées.
2. Exécutez la commande WMI `verifyrepository` comme suit :

```
Winmgmt  /verifyrepository
```

Si des requêtes simples ne renvoient pas de résultat, ou que la commande `verifyrepository` ne fonctionne pas, le problème vient du référentiel WMI. Si la commande `verifyrepository` échoue, un administrateur de serveur local doit régénérer le référentiel WMI local ou le recompiler entièrement à partir des fichiers présents sur le serveur. Si cela ne résout pas le problème, une recherche supplémentaire est nécessaire.

L'erreur «The RPC server is unavailable» se produit pendant la reconnaissance avec le détecteur de session

Problème

Lorsque vous exécutez une reconnaissance à l'aide du détecteur de session, l'erreur suivante se produit :

```
The RPC server is unavailable. (Exception from HRESULT:0x800706BA>
```

Solution

Vérifiez que la fonction de recherche DNS inversée fonctionne correctement pour la cible en échec. A partir du serveur de reconnaissance TADDM ou du serveur d'ancrage, exécutez la commande suivante :

```
nslookup target-IP-address
```

Check if the IP address of the target is correctly mapped to its FQDN name.

Configuration des entrées du fichier collation.properties

Vous pouvez configurer le détecteur de session en modifiant les entrées du fichier `collation.properties`.

Fix Pack 4 **com.collation.discover.agent.sys.SessionSensor.timeout.snmp=false**

Cette propriété indique si le détecteur SNMP MIB2 doit démarrer après le dépassement du délai d'attente du détecteur de session.

La valeur par défaut est `false`.

Par défaut, lorsque le détecteur de session dépasse le délai d'attente, le détecteur SNMP MIB2 n'est pas démarré. Parallèlement, lorsque le détecteur de session échoue pour un autre motif que le dépassement du délai d'attente ou en raison de l'erreur CTJTD0591W, le détecteur SNMP MIB2 est démarré. Si vous souhaitez que le détecteur SNMP MIB2 soit également démarré lorsque le détecteur de session dépasse le délai d'attente, définissez la valeur de cette propriété sur `true`.

Fix Pack 2 **com.collation.discover.agent.sys.SessionSensor.loadBalancerIp=false**

Cette propriété indique si le détecteur de session doit s'arrêter lorsque l'objet reconnu est un équilibreur de charge.

La valeur par défaut est `false`, ce qui signifie que le détecteur n'est pas arrêté.

La reconnaissance des équilibreurs de charge peut entraîner un excès de fusions. Si l'erreur «CTJTD0591W Session IP not found within discovered IP interfaces» se produit, remplacez la valeur de cette propriété par `true`.

Remarque : Lorsque cette propriété est définie sur `true` et que le détecteur de session est arrêté, le détecteur SNMP MIB2 n'est pas démarré.

Détecteur générique de zones Solaris

Le détecteur générique de zones Solaris reconnaît des applications exécutées sur des systèmes de zone locale Solaris.

Les résultats du détecteur permettent de démarrer des détecteurs d'application spécifiques, comme IplanetServerSensor, WeblogicServerSensor ou CustomServerSensor, qui reconnaissent les serveurs d'applications que TADDM ne classe pas automatiquement.

Ce détecteur utilise une approche de reconnaissance qui est différente des autres systèmes UNIX . Au lieu d'effectuer une reconnaissance directement sur les systèmes de zone locale, un système de zone globale est utilisé pour démarrer le détecteur ZonesGenericSensor. Ceci est dû au fait que l'outil lsof n'est pas disponible dans les zones locales. Pour extraire tous les détails relatifs au système d'exploitation de la zone locale, vous devez inclure l'adresse IP de la zone locale dans la portée de la reconnaissance.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ZonesGenericSensor

Prérequis

Les autorisations d'accès des zones locales et globales doivent être entrées dans la liste d'accès (à l'aide d'une authentification par clé SSH ou d'une authentification par connexion SSH).

Problèmes de sécurité

Pour une reconnaissance correcte des applications en cours d'exécution sur une zone locale, le compte du service TADDM figurant dans les zones locales et globales doit pouvoir accéder à la commande **ps** avec des arguments de ligne de commande complets.

Utilisez la méthode suivante, pour garantir l'accès si le compte utilisateur root ou le bit **setuid** n'est pas utilisé. Modifiez les propriétés suivantes dans le fichier `$COLLATION_HOME/etc/collation.properties` pour configurer la commande **ps** pour utiliser **sudo** :

- `com.collation.platform.os.command.ps.SunOS=sudo /usr/ucb/ps axww`
- `com.collation.platform.os.command.psEnv.SunOS=sudo /usr/ucb/ps axwweee`
- `com.collation.platform.os.command.psUsers.SunOS=sudo /usr/ucb/ps auxw`

Limitations

Prenez connaissance des limitations suivantes :

- Le détecteur ne crée pas d'objets ProcessFileSystemMapping pour les zones locales. Lorsqu'un processus en cours d'exécution sur une zone locale utilise un partage NFS, la dépendance entre le serveur d'applications et le serveur NFS n'est pas créée.
- Si WebLogic 8 (toutes éditions) gérés et des serveurs d'administration sont en cours d'exécution sur les zones locales, les informations d'exécution sont stockées à l'aide du détecteur CustomAppServerSensor. Le détecteur CustomAppServerSensor est démarré par le détecteur WeblogicVersionSensor.

Vous devez inclure les adresses IP de toutes les zones locales et globales dans la portée de la reconnaissance. Vous devez également vous assurer que la liste de serveurs personnalisés contient au moins un modèle qui correspond à la ligne de commande WebLogic et que le serveur personnalisé est activé.

- Lors de l'exécution d'une reconnaissance par le biais d'un serveur d'ancrage, incluez les adresses IP des zones locales et globales dans le même ensemble de portée que celui défini pour l'ancrage.
- Internet Protocol version 6 (IPv6) n'est pas pris en charge lors de l'exécution d'une reconnaissance dans une zone locale.

Objets de modèle créés

Le détecteur crée l'objet de modèle suivant :

- sys.RuntimeProcess

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur générique de zones Solaris et propose des solutions à ces problèmes.

Le détecteur générique de zones Solaris ne démarre pas en raison d'une adresse IP incorrecte d'une zone

Problème

Le détecteur générique de zones Solaris ne démarre pas. Dans les fichiers historiques des erreurs, vous trouverez des informations indiquant qu'une zone comporte une adresse IP incorrecte. Les fichiers indiquent que l'adresse IP est générée par la commande `host` *`nom_zone`*.

Fix Pack 2 **Solution**

Si vous utilisez TADDM version 7.3.0.2 ou ultérieure, accédez au fichier `collation.properties` et définissez la propriété `com.collation.hostnameforzoneip` sur `false`.

détecteur d'analyse de piles

Le détecteur d'analyse de piles permet une reconnaissance à droits d'accès moindres (reconnaissance plus discrète) du système d'exploitation installé et des ports ouverts sur un système informatique.

Outre Nmap, le détecteur de reconnaissance peut utiliser Tivoli Remote Execution and Access (RXA) pour la reconnaissanceWindows. Il peut reconnaître une adresse MAC de L2Interface.

Nom du détecteur utilisé dans l'interface graphique et les journaux

StackScanSensor

Prérequis

Le détecteur requiert les logiciels suivants :

- Outil Nmap. Voir «Configuration de Nmap», à la page 260 pour plus de détails.
- Outil WinPcap pour les systèmes d'exploitation Windows . Cet outil est disponible sur le DVD de TADDM, mais vous devez l'installer manuellement car il n'est pas installé lors de l'installation de TADDM.

- Outil sudo pour les systèmes d'exploitation non Windows.

  Pour TADDM sur systèmes d'exploitation AIX : Pour que l'utilisateur TADDM puisse utiliser l'outil nmap via sudo, vous devez installer et configurer sudo version 1.6.7p5. En effet, TADDM rencontre des problèmes avec la version la plus récente de sudo (version 1.6.9p15).

Problèmes de sécurité

Pour configurer l'accès à la commande sudo pour l'utilisateur TADDM, vous devez définir une option nopasswd dans le fichier `/etc/sudoers` pour l'utilisateur TADDM.

Limitations

Les pare-feux situés entre les portées ciblées et le serveur TADDM ou les ancrages distants peuvent détériorer considérablement la fiabilité et les performances du détecteur d'analyse de piles. Si tel est le cas, utilisez les ancrages distants après le pare-feu pour améliorer les performances. Il se peut que la version du système d'exploitation ne soit pas correctement reconnue en fonction des éléments reçus par le détecteur d'analyse de piles depuis Nmap. Par exemple, Windows Server 2008 est classifié en tant que Windows Vista, AIX 6.x en tant qu'AIX 5.x, Linux for System z en tant qu'autre système informatique. La reconnaissance de systèmes informatiques exécutant le système d'exploitation UNIX Tru64 n'est pas pris en charge par Nmap. Utilisez la commande suivante pour vérifier la version de système d'exploitation renvoyée par Nmap :

```
nmap -T Normal -O -sS -sU  -oX - IPaddress
```

Les serveurs d'applications et les services reconnus à l'aide d'une reconnaissance sans droits d'accès (niveau 1) sont rapprochés des serveurs d'applications et des services à l'aide d'une reconnaissance de niveau 2 ou de niveau 3 uniquement si les ports TCP de liaison sont les mêmes. Tous les serveurs d'applications et les services reconnus à l'aide d'une reconnaissance de niveau 1 sont conservés après une reconnaissance de niveau 2 ou de niveau 3, alors que les applications et les services identiques sur les ports de liaison sont fusionnés.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.IpAddress
- net.IpInterface
- net.L2Interface
- sys.aix.Aix
- sys.aix.AixUnitaryComputerSystem
- sys.ComputerSystem
- sys.hpux.HpUx
- sys.hpux.HpUxUnitaryComputerSystem
- sys.i5OS.I5OperatingSystem
- sys.linux.Linux
- sys.linux.LinuxUnitaryComputerSystem
- sys.OperatingSystem
- sys.sun.Solaris

- sys.sun.SunSPARCUnitaryComputerSystem
- sys.tru64.Tru64
- sys.windows.WindowsComputerSystem
- sys.windows.WindowsOperatingSystem
- sys.zOS.ZOS
- sys.zOS.ZSeriesComputerSystem

Configuration du détecteur

Avant d'effectuer une reconnaissance du système d'exploitation installé et des ports ouverts, vous devez configurer le détecteur d'analyse de piles.

Configuration de Nmap :

Le détecteur d'analyse de piles utilise Nmap pour collecter des données sur les cibles pour la reconnaissance sans droits d'accès.

Installation de Nmap

Avant d'installer Nmap pour tout système d'exploitation, reportez-vous au site de support TADDM à l'adresse https://www-947.ibm.com/support/entry/portal/product/tivoli/tivoli_application_dependency_discovery_manager?productContext=267282604 pour toute information récente concernant votre système d'exploitation et les versions de Nmap.

Nmap n'est pas installé pendant l'installation de TADDM. L'outil Nmap est disponible sur le DVD 2 de TADDM et vous devez l'installer manuellement. Installez Nmap sur le serveur TADDM et sur tous les serveurs d'ancrage. Pour plus d'informations, consultez le fichier readme situé dans le répertoire `Nmap` du DVD.

Configuration des droits d'accès de l'administrateur "root"

Pour les plateformes autres que Windows, donnez les droits d'accès de l'administrateur "root" de toutes les commandes à l'ID utilisateur TADDM qui démarre le serveur TADDM.

Si vous utilisez un serveur d'ancrage TADDM, donnez les droits d'accès de l'administrateur "root" au compte du service de reconnaissance du serveur d'ancrage.

En tant que superutilisateur, ajoutez la ligne suivante dans le fichier de configuration `/etc/sudoers`, à l'aide de la commande **`visudo`** :

`idutilisateur_TADDM` `ALL=(ALL) NOPASSWD:`*`ALL`*

où

- *idutilisateur_TADDM* est l'ID utilisateur qui démarre le serveur TADDM ou le compte du service de reconnaissance sur un ancrage.

Si le fichier `sudoers` contient la ligne `Defaults requiretty`, commentez-la ou supprimez-la.

Lorsque le serveur d'analyse de piles est en cours d'exécution avec Nmap, l'ID utilisateur du serveur TADDM peut disposer des droits d'exécution

superutilisateur uniquement pour la commande Nmap. Ajoutez la ligne suivante au fichier de configuration `/etc/sudoers` :

```
idutilisateur_TADDM ALL=(ALL) NOPASSWD:chemin_nmap
```

où

- *idutilisateur_TADDM* est l'ID utilisateur qui démarre le serveur TADDM ou le compte du service de reconnaissance sur un ancrage.
- *chemin_nmap* est le chemin complet de l'emplacement de la commande **nmap**.

Si le fichier `sudoers` contient la ligne `Defaults requiretty`, commentez-la ou supprimez-la.

Configuration de la variable d'environnement Path

Nmap doit être installé sur votre serveur TADDM et sur tous les serveurs d'ancrage. La commande Nmap doit se trouver dans la variable d'environnement $PATH de l'ID utilisateur TADDM qui démarre le serveur TADDM. Si vous utilisez un serveur d'ancrage TADDM, la commande Nmap doit se trouver dans la variable d'environnement $PATH du compte de service de reconnaissance.

Sur les plateformes Windows, procédez comme suit pour définir la variable d'environnement système Path afin qu'elle inclut le répertoire dans lequel Nmap est installé :

1. Cliquez sur **Démarrer** > **Control Panel** > **Système**
2. Cliquez sur l'onglet Avancé et sélectionnez Environment Variables.
3. Modifiez la variable système Path et ajoutez le répertoire où Nmap est installé.
4. Redémarrez l'ordinateur.

   Cette tâche permet aux services sur l'ordinateur d'accéder à Nmap.

Vérifier que Nmap fonctionne

Pour vérifier que Nmap fonctionne, procédez comme suit :

1. Connectez-vous au système à l'aide de l'un des ID utilisateur TADDM suivants :
   - L'ID utilisateur qui démarre le serveur TADDM.
   - L'ID utilisateur qui démarre le compte de service de reconnaissance sur le serveur d'ancrage.
2. Exécutez la commande suivante :

   ```
   sudo nmap -T Normal -O -sS  -oX - adresseIP/32
   ```

   où

   - *adresseIP* est un système hôte valide et opérationnel sur votre réseau.

   La sortie produit un document XML qui affiche les ports et les systèmes d'exploitation présents sur ce système informatique.

Limitation

En raison d'une limitation sur AIX, seules quatre commandes Nmap actives peuvent être exécutées sur la même instance. Pour vous assurer que cette limite de commandes Nmap n'est pas dépassée, procédez comme suit :

1. Créez un profil de reconnaissance.

2. Dans le nouveau profil de reconnaissance, créez une configuration StackScanSensor et activez-la.
3. Définissez les valeurs des propriétés suivantes sur 1 :
   - nmapMaxOsScanTreads
   - nmapMaxPingScanTreads
4. Pour sauvegarder la configuration, cliquez sur **OK**.
5. Pour sauvegarder le profil de reconnaissance, cliquez sur **Sauvegarder**. Utilisez ce profil de reconnaissance pour les reconnaissances StackScan.
6. Si le nombre de systèmes informatiques dans la portée en cours de reconnaissance est supérieur à 2 048, définissez la propriété suivante dans le fichier `collation.properties` :

   ```
   com.collation.discover.dwcount=4
   ```

Configuration du profil de reconnaissance :

Si vous voulez créer des serveurs d'applications basés sur les ports TCP/IP actifs reconnus, mettez à jour le profil de reconnaissance pour le détecteur d'analyse de piles.

Pour configurer le détecteur afin qu'il crée des serveurs d'applications, procédez comme suit :

1. Créez un profil de reconnaissance basé sur un profil TADDM de niveau 1.
2. Créez une configuration de détecteur dans ce nouveau profil basée sur la configuration du détecteur d'analyse de piles.
3. Dans la nouvelle configuration de détecteur, attribuez la valeur `true` à la propriété **enableNmapPortApplicationCreation**.

Pour configurer le détecteur afin qu'il utilise winscanner, procédez comme suit :

1. Créez un profil de reconnaissance basé sur un profil TADDM de niveau 1.
2. Créez une configuration de détecteur dans ce nouveau profil basée sur la configuration du détecteur d'analyse de piles.
3. Dans la nouvelle configuration de détecteur, attribuez la valeur `nmap,winscanner` à la propriété **scanners**.

Vous pouvez ensuite configurer les serveurs d'applications à créer en fonction des ports reconnus à l'aide du fichier `PortAppScanSensor.properties` situé dans le répertoire `osgi\plugins\com.ibm.cdb.discover.sensor.idd.stackscan_7.1.2\etc`. Des instructions spécifiques pour modifier l'association entre les ports et les serveurs d'applications figurent dans la partie supérieure du fichier `PortAppScanSensor.properties`.

Les erreurs de configuration dans le fichier `PortAppScanSensor.properties` sont signalées dans le fichier `PortAppScanSensor.errors`, qui figure dans le répertoire `osgi\plugins\com.ibm.cdb.discover.sensor.idd.stackscan_7.1.2\etc`.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur d'analyse de piles.

Le détecteur d'analyse de piles utilise les entrées suivantes dans le fichier `collation.properties` :

com.collation.sudoCommand=sudo
Cette valeur indique l'emplacement de la commande sudo.

com.collation.discover.agent.StackScanSensor.timeout=7200000
Cette valeur indique l'intervalle de temps en millisecondes avant un délai d'attente pendant une reconnaissance.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques rencontrés par le détecteur d'analyse de piles et propose des solutions à ces problèmes.

L'exécution du détecteur d'analyse de piles se termine avec succès, mais aucun système informatique n'est stocké

Problème

Le détecteur d'analyse de piles a procédé à une reconnaissance de niveau 1 qui a abouti, mais il n'a pas stocké d'informations relatives au système informatique. Le message suivant est affiché dans le fichier `services/DiscoveryManager.log` :

```
2008-03-26 11:05:26,845 DiscoverManager [nmap-ping[0] (i1|s[9.42.36.223])]
WARN cdb.STDERR - Mar 26, 2008 11:05:26 AM   invocation failed:
sudo: sorry, you must have a tty to run sudo
From the TADDM server command line you can successfully do an
su - <run as user>
and then
sudo "nmap -0 10.1.2.3
```

Solution

Pour les plateformes autres que Windows, donnez les droits d'accès de l'administrateur "root" de toutes les commandes à l'ID utilisateur TADDM qui démarre le serveur TADDM. En outre, si vous utilisez un serveur d'ancrage TADDM, donnez les droits d'accès de l'administrateur "root" au compte du service de reconnaissance du serveur d'ancrage. Voir «Configuration de Nmap», à la page 260 pour plus de détails.

Le détecteur d'analyse de piles ne reconnaît pas les systèmes informatiques présents sur un système Linux

Problème

Lors d'une reconnaissance de niveau 1 sur un serveur Linux, le détecteur d'analyse de piles se termine correctement, mais aucun système informatique n'est stocké.

Le message suivant est affiché dans le fichier services/DiscoveryManager.log :

```
2008-03-26 11:05:26,845 DiscoverManager [nmap-ping[0] (i1|s[9.42.36.223])]
WARN cdb.STDERR - Mar 26, 2008 11:05:26 AM   invocation failed: sudo: sorry,
you must have a tty to run sudo
```

Cette erreur se produit même si la commande sudo fonctionne correctement pour l'utilisateur `run_as` à partir de la ligne de commande.

Solution

Procédez comme suit :

1. Entrez la commande `visudo` pour éditer le fichier `/etc/sudoers`
2. Lorsque le fichier s'ouvre, commentez la ligne `Defaults requiretty`.
3. Sauvegardez et fermez le fichier.

La configuration réseau sur les systèmes Linux pour Système z ne crée pas de paquets que Nmap puisse lire

Linux pour System z prend en charge les interfaces réseau OSA et VSWICH fonctionnant en mode Couche 3 (couche réseau) ou Couche 2 (couche de liaison). Si le mode Couche 2 est utilisé, les paquets TCP contiennent un en-tête Couche de liaison ethernet valide requis par Nmap. Cependant, les systèmes utilisant OSA ou VSWITCH et fonctionnant en mode Couche 3 requièrent l'ajout de `QETH_OPTIONS='fake_ll=1'` au fichier de configuration matérielle de l'interface. La section suivante décrit comment modifier le fichier de configuration matérielle qui permet à Nmap d'utiliser les interfaces réseau de Couche 3.

Pour plus d'informations sur OSA et VSWITCH et leur modes d'opération, voir Chapitre 7 «qeth device driver for OSA-Express (QDIO) and HiperSockets» dans *Linux on System z Device Drivers, Features, and Commands* à l'adresse : http://download.boulder.ibm.com/ibmdl/pub/software/dw/linux390/docu/lk31dd03.pdf.

Problème

La configuration réseau du système Linux pour Système z ne crée pas de paquets que le Nmap puisse lire.

Le détecteur d'analyse de piles utilise Nmap pour collecter des données sur les cibles pour la reconnaissance sans droits d'accès. Si Nmap ne fonctionne pas correctement, le détecteur d'analyse de piles ne stocke aucun système informatique.

Bien que le détecteur s'exécute sans erreur, le système Linux pour System z qui s'exécute sur le détecteur d'analyse de piles renvoie le message suivant :

```
Stocké - 0 ComputerSystems dans la base de données
```

Si vous entrez la commande **nmap <hostname>** pour tout système autre que le système hôte local, le message suivant s'affiche :

```
Note : l'hôte semble désactivé. S'il est réellement activé,
mais qu'il bloque nos sondes ping, essayez -P0...
```

Solution

Selon votre système d'exploitation, effectuez les actions suivantes :

Sur les systèmes SUSE Linux pour Système z

Le réseau doit s'exécuter avec l'option suivante :

```
QETH_OPTIONS='fake_ll=1'
```

Ajoutez cette option au fichier de configuration pour le NIC. Selon le NIC utilisé, le nom du fichier change. Contactez votre administrateur système pour connaître le fichier de configuration utilisé par votre système.

Le fichier de configuration doit se trouver dans le répertoire `/etc/sysconfig/hardware`. Le nom de fichier peut être `hwcfg-qeth-bus-ccw-0.0.5000`.

Dans un système RedHat Linux pour Système z

Le réseau doit s'exécuter avec l'option suivante :

```
OPTIONS='fake_ll=1'
```

Ajoutez cette option au fichier de configuration pour le NIC. Selon le NIC utilisé, le nom du fichier change. Contactez votre administrateur système pour connaître le fichier de configuration utilisé par votre système.

Le fichier de configuration doit se trouver dans le répertoire/etc/sysconfig/network-scripts. Le nom de fichier peut être ifcfg-eth0.

Vérifiez que l'alias dans le fichier /etc/modprobe.conf comprenne les informations suivantes :

```
alias eth0 qeth
```

Le système informatique est affiché dans une catégorie incorrecte

Problème

Le système informatique est affiché dans la catégorie **OtherComputerSystem**.

Solution

Vérifiez le type du système d'exploitation. S'il est correct, vérifiez la fiabilité. Si la fiabilité est inférieure à la valeur du seuil de fiabilité (la valeur par défaut est 40), les éléments affichés à l'écran sont prévus.

Vous pouvez modifier le seuil de fiabilité pour que le système informatique soit affiché dans la catégorie correcte. Le seuil est configuré 0 et 100. Vous pouvez le définir au moyen de l'attribut de configuration de détecteur **confidenceThreshold**.

Le débogage amélioré du détecteur d'analyse de piles est requis

Problème

Le débogage amélioré du détecteur d'analyse de piles doit être activé.

Solution

Procédez comme suit :

1. Consultez le fichier local-anchor-<machine>.log pour vérifier si Nmap a été utilisé par le détecteur.
2. Activez davantage le débogage en procédant comme suit :

   Dans le fichier collation.properties, définissez l'une des propriétés suivantes :

   - **com.collation.log.level.StackScanSensor=TRACE**
   - **com.collation.log.StackScanSensor=TRACE**
   - **com.collation.log.level=TRACE**

   Cette méthode génère une trace prolixe de ce que fait le détecteur, des résultats, des configurations utilisées, etc.

Echec du détecteur d'analyse de piles et affiche un message : sudo: sorry, you must have a tty to run sudo

Problème

Au cours d'une reconnaissance, si la console de gestion de reconnaissance où le serveur TADDM a été démarré est fermée, le détecteur échoue. Le message : sudo:sorry, you must have a tty to run sudo s'affiche. Si vous démarrez la console de gestion de reconnaissance et la laissez ouverte, le détecteur fonctionne.

Solution

Mettez en commentaires ou supprimez la ligne `Defaults requiretty` du fichier de configuration `/etc/sudoers` sur le serveur TADDM.

Le détecteur d'analyse de piles est incapable d'exécuter la commande sudo nmap

Problème

Le détecteur d'analyse de piles échoue avec le message d'erreur suivant : "Sorry, sudo has been configured to not allow root to run it." Vous pouvez néanmoins exécuter correctement **`sudo nmap`** sur une ligne de commande.

Solution

Ce problème survient lorsque le système est configuré pour ne pas permettre à le superutilisateur d'exécuter la commande **`sudo`**. Pour résoudre ce problème, éditez le fichier `collation.properties` et définissez la propriété com.ibm.cdb.discover.sensor.idd.stackscan.alwaysUseLocalAnchor à `true`. Redémarrez ensuite le serveur TADDM.

Le détecteur d'analyse de piles ne reconnaît pas des systèmes informatiques sous un système AIX.

Problème

Lors d'une reconnaissance de niveau 1 sur un serveur AIX, le détecteur d'analyse de piles se termine correctement, mais aucun système informatique n'est stocké.

Le message suivant est affiché dans le fichier services/DiscoveryManager.log :

```
2008-03-26 11:05:26,845 DiscoverManager [nmap-ping[0] (i1|s[9.42.36.223])]
 DiscoverManager [nmap-ping[0] (i1|s[9.42.36.223]
)]  DEBUG stackscan.ExecCmd - standard err:/taddm/cmdb/dist/nmap/nmap-4.
76/nmap[25]: 708778 Segmentation fault(coredump)
```

Dans le dossier Nmap un fichier core est créé durant la reconnaissance.

Solution

Créez un profil de reconnaissance ou éditez un profil existant pour le détecteur d'analyse de piles. Dans la section **Configuration** de la fenêtre Créer une configuration, cliquez sur **nmapexec**. Ensuite, cliquez deux fois sur la zone **Valeur** de la ligne et ajoutez `-d` à la valeur `nmap`. Par exemple, la nouvelle valeur devient `nmap -d`.

Après avoir activé winscanner, certains des systèmes informatiques reconnus ont une signature sans adresse MAC.

Problème

Une reconnaissance personnalisée de niveau 1 est exécutée avec uniquement le scanner nmap activé. Ensuite, une autre reconnaissance est exécutée sur la même portée avec nmap et winscanner activés. Les systèmes informatiques reconnus ont des signatures sans adresse MAC.

Solution

Le détecteur Stack Scan stocke uniquement les informations sur les systèmes cible qui ne sont pas encore reconnus. Les systèmes informatique qui sont déjà présents dans la base de données TADDM ne sont pas mis à jour. Supprimez les systèmes informatiques manuellement et exécutez la reconnaissance une nouvelle fois.

Le détecteur Stack Scan met à jour uniquement les objets des éléments de configuration déjà stockés dans la base de données TADDM pendant la reconnaissance de niveau 1

Problème

Lors d'une découverte de niveau 1, le capteur Stack Scan stocke des informations exclusivement (en gras) pour ces nouveaux systèmes d'objets IP qui ne sont pas encore découverts et ce, conformément à la façon dont la découverte de niveau 1 est conçue dans TADDM. Ainsi, les systèmes informatiques des éléments de configuration qui sont déjà présents dans la base de données TADDM ne sont pas mis à jour par le détecteur StackScan en cas de modification. Jusqu' à présent, la seule action possible pour TADDM pour pouvoir mettre à jour les objets des éléments de configuration stockés, qui ont été découverts et stockés comme de faux objets "superficiels" initialement au cours de la première découverte de niveau 1 consiste à supprimer les systèmes informatiques manuellement puis à relancer la découverte, ou même à exécuter une découverte de niveau 3.

Solution

Une nouvelle fonctionnalité a été introduite dans le FP4 afin d'éviter la création TADDM de faux objets "superficiels" qui se produit généralement lorsque vous obtenez des adresses IP pingables sans système correspondant (création de systèmes d'exploitation ComputerSystems superficiels).

com.ibm.idd.stackscanner.confidence.skip=default 0

Détecteur générique de partition de charge de travail

⌂Le détecteur générique de la partition de la charge de travail reconnaît des applications qui s'exécutent sur les systèmes de partition de charge de travail.

Les résultats du détecteur permettent de démarrer des détecteurs d'application spécifiques, comme JBossSensor, WebSphere Sensor, etc.

Le processus de reconnaissance de ce détecteur est différent des autres systèmes UNIX. Au lieu d'effectuer une reconnaissance directement sur les systèmes de partition de la charge de travail, un système de partition logique est utilisé pour démarrer le détecteur. Ce phénomène s'explique par le fait que la commande **kdb** n'est pas disponible sur les partitions de la charge de travail et le détecteur n'est pas capable de convertir les sockets ouverts pour traiter les PID (identifiants de processus). L'ensemble du processus de reconnaissance est basé sur la commande **netstat**. La commande **lsof** n'est pas utilisée.

Nom du détecteur utilisé dans l'interface graphique et les journaux

WPARGenericSensor

Prérequis

Vous devez ajouter les données d'identification pour la partition logique et la partition de la charge de travail à la liste d'accès.

Limitations

Le détecteur ne crée pas d'objets ProcessFileSystemMapping pour la partition logique et les partitions de la charge de travail.

Objets de modèle créés

Le détecteur crée l'objet de modèle suivant :

- sys.RuntimeProcess

Détecteur zEnterprise

Pour reconnaître l'environnement zEnterprise, le détecteur utilise le collecteur ECC (Enterprise Common Collector). Ce dernier est un point d'entrée unique pour la demande de toutes les données d'inventaire sur les composants zEnterprise, tant matériels que logiciels.

Le détecteur zEnterprise TADDM établit une connexion sécurisée avec le collecteur ECC et collecte toutes les données nécessaires à la création d'une arborescence d'objets CDM. Le détecteur les stocke ensuite dans TADDM et ainsi, aucune entrée des composants n'est nécessaire. Le collecteur ECC est une application Web déployée sur un serveur Web. C'est pourquoi, le détecteur zEnterprise dépend du détecteur de ports pour identifier le port sur lequel le collecteur ECC écoute. Le détecteur zEnterprise stocke des objets qui décrivent la structure physique et virtuelle de zEnterprise, zBladeExtension et des systèmes informatiques.

Si vous souhaitez reconnaître un système informatique virtuel, vous devez installer et démarrer les agents Guest Platform Management Provider qui fournissent au collecteur ECC des informations sur les systèmes d'exploitation.

Le détecteur stocke les objets suivants qui décrivent les composants physiques, virtuels et logiques :

- **zEnterprise :** packages physiques, dispositifs
- **zEnterprise BladeCenter Extension :** BladeCenters, châssis, armoires, composants blade
- **Systèmes informatiques :** System z, partitions logiques z/VM, partitions logiques PR/SM
- **Composants logiques :** Ensemble, Groupes de ressources de charge de travail
- **Composants virtuels :** Serveurs virtuels, réseaux virtuels, ressources de stockage virtuelles

Remarque : Pour les systèmes informatiques virtuels, les objets sont des balises.

Nom du détecteur utilisé dans l'interface graphique et les journaux

`com.ibm.cdb.discover.sensor.sys.zenterprise_1.0.0`.

Prérequis

Pour les reconnaissances zEnterprise, assurez-vous que les exigences suivantes sont satisfaites :

- Enterprise Common Collector (ECC) version 1.1.0.2

ECC est fourni en tant que composant distinct. Vous devez l'installer et le configurer séparément. Cependant, le détecteur peut utiliser une instance ECC qui est déjà installée et configurée pour une utilisation par une autre application, telle zEnterprise Monitoring Agent fourni avec IBM Tivoli Monitoring. Pour plus d'informations sur l'installation et la configuration d'ECC, consultez le document *Enterprise Common Collector Configuration Guide and Reference*.

- Agents Guest Platform Management Provider

  Vous devez installer, configurer et exécuter les agents GPMP sur chacun des systèmes informatiques virtuels. Sans ces agents, le détecteur n'est pas en mesure de détecter le système d'exploitation et l'identification unique des systèmes informatiques reconnus.

Problèmes de sécurité

Le détecteur zEnterprise a besoin d'une adresse IP et d'un port pour communiquer avec ECC. Ces informations sont requises car le détecteur appelle l'API ECC RESTful, reçoit les données et les place dans une structure d'objets de données qui est ensuite transmise à TADDM pour être stockée.

Limitations

Systèmes informatiques virtuels

La réconciliation d'objets stockés par le détecteur zEnterprise et les détecteurs de système d'exploitation, tels le détecteur de système informatique Linux, le détecteur de système informatique AIX et le système informatique Windows, n'est pas toujours possible car il existe des cas où le collecteur ECC ne peut pas reconnaître le type de système informatique virtuel ou ses données d'identification si aucun agent Guest Platform Management Provider n'est en cours d'exécution.

Par défaut, le détecteur stocke uniquement des systèmes informatiques virtuels connus avec un ensemble d'identification approprié. Les systèmes informatiques qui ne satisfont pas cette exigence sont ignorés et un message d'avertissement approprié s'affiche.

Vous pouvez, cependant, activer le stockage de tous les systèmes informatiques virtuels reconnus, même ceux de type inconnu. De tels systèmes informatiques sont visibles dans la section **Autre systèmes informatiques**. Si possible, la réconciliation correspond à l'adresse MAC provenant du système informatique inconnu reconnu par le détecteur zEnterprise avec les adresses Mac L2Interfaces des systèmes informatiques reconnus par les détecteurs de plateformes, et les fusionne. Pour fusionner les systèmes informatiques automatiquement, vous devez d'abord exécuter les détecteurs de plateformes, puis le détecteur zEnterprise. La séquence inversée de la reconnaissance, qui lance le détecteur zEnterprise en premier, ne garantit pas une fusion automatique.

Partitions logiques

Avant de reconnaître l'environnement zEnterprise avec le détecteur zEnterprise pour la première fois, vérifiez si des partitions logiques précédemment reconnues font désormais partie de l'environnement zEnterprise, et sont donc visibles via la console de gestion de matériel System z ou le collecteur ECC. Dans ce cas, exécutez une reconnaissance des LPAR avec le détecteur de système informatique Linux afin d'éviter des doublons.

Partage d'une instance ECC commune parmi plusieurs applications

Enterprise Common Collector est un composant commun conçu pour être utilisé par plusieurs applications et ainsi il est possible d'avoir une seule instance ECC servant plusieurs produits IBM. Si vous souhaitez partager une instance ECC, vous devez vous assurer que sa version est compatible avec celles des autres applications.

Pourquoi et quand exécuter cette tâche

Chaque version du collecteur ECC possède une version principale de l'interface de programme d'application et une version secondaire qui y est associée. Vous ne pouvez pas connecter une instance d'une application, telle que le détecteur zEnterprise, à une instance ECC qui ne dispose pas d'une version API compatible. Dans une telle situation, un message d'erreur affiche les versions API détectées et attendues.

Le détecteur zEnterprise version 1.0.0 requiert :

- API ECC version principale 1
- API ECC version secondaire 2 ou version ultérieure

Procédure

1. Utilisez l'adresse URL suivante pour déterminer les versions principales et secondaires d'API d'une instance ECC. Vous pouvez entrer l'adresse URL dans le navigateur Web de n'importe quel système disposant d'une connexion réseau au système sur lequel le collecteur ECC est installé :

   `https://`*`nomhôte_ecc`*`:`*`numéro_port_ecc`*`/eccapi/version`

   Par défaut, le numéro de port est `8443`.
2. Accédez au site Web même si un avertissement s'affiche indiquant que le certificat n'a pas été émis par une autorité de certification agréée.
3. Déterminez le `api-major-version` et `api-minor-version` d'une chaîne JSON ou XML à partir du site Web. Voici un exemple de cette chaîne :

   ```
   {
    "class":"ecc-version",
    "self":"/eccapi/version",
    "name":"ECC version",
    "description":"Information about the ECC and ECC API version",
    "api-major-version":1,
    "api-minor-version":2,
    "ecc-version":"1.1"
   }
   ```
4. En fonction des versions principales et secondaires d'API, complétez une des actions suivantes :
   - La version principale est 1 et la version secondaire est 1. Cette version du collecteur ECC n'est pas compatible avec le détecteur zEnterprise. Vous devez mettre à niveau le collecteur ECC vers la version 1.1.0.2, fournie avec TADDM. Pour plus d'informations sur la mise à niveau d'ECC, consultez le document *Enterprise Common Collector Configuration Guide and Reference*.

     Remarque : Une fois la mise à niveau du collecteur ECC terminée, il peut être nécessaire de mettre à niveau d'autres applications, telles zEnterprise Monitoring Agent d'IBM Tivoli Monitoring, qui utilisent le collecteur ECC.

- La version principale est 1, la version secondaire est 2 ou version ultérieure. Cette version du collecteur ECC est compatible avec le détecteur zEnterprise. Vous pouvez utiliser le détecteur et le collecteur ECC.
- La version principale est 2 ou version ultérieure. Cette version du collecteur ECC n'est pas compatible avec le détecteur zEnterprise. Vous pouvez utiliser cette instance du collecteur ECC, mais vous devez mettre à niveau le détecteur zEnterprise vers une version plus récente.

Objets de modèle avec attributs associés

Le détecteur zEnterprise crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur l'environnement zEnterprise.

Le détecteur crée les objets de modèle suivants :

Application de la console HMC (Hardware Management Console)

- phys.physpkg.PhysicalPackage
- sys.appliance.Appliance
- sys.zOS.ZHMC
- sys.OperatingSystem
- net.L2Interface
- net.IpV4Address
- net.IpV6Address
- net.IpInterface
- net.IpNetwork

Ensemble

- core.Ensemble

Processeur CPC (Central Processor Complex)

- phys.physpkg.PhysicalPackage
- sys.zOS.ZSeriesComputerSystem

zEnterprise BladeCenter Extension (zBX)

- sys.zOS.ZBXFeature

Support

- phys.physpkg.Rack

BladeCenter

- phys.physpkg.Chassis
- sys.ComputerSystem

Blade

- phys.physconn.Slot
- phys.physpkg.Board
- sys.ComputerSystem
- sys.appliance.SmartAnalyticsOptimizer
- sys.appliance.DataPower
- sys.OperatingSystem
- net.L2Interface
- net.IpV4Address

- net.IpV6Address
- net.IpInterface
- net.IpNetwork

Hôte de virtualisation zVM

- sys.zOS.ZVM

Serveur virtuel

- sys.ComputerSystem
- sys.zOS.ZVMGuest
- sys.OperatingSystem
- net.L2Interface
- sys.zOS.ChannelSubSystem

Partition logique (LPAR)

- sys.zOS.LPAR
- sys.OperatingSystem

Réseau virtuel

- net.Vlan

Groupe de ressources de charge de travail

- sys.zOS.WorkoadResourceGroup
- service.ServiceInfrastructurePerformancePolicy
- service.ServiceInfrastructureServiceClass

Ressource de stockage de l'hôte de virtualisation

- dev.StorageVolume

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Les étapes de configuration suivantes sont nécessaires :

- Entrée de liste d'accès avec ID utilisateur et mot de passe pour le collecteur ECC et certificat pour HTTPS
- Configuration de la reconnaissance du détecteur zEnterprise
- Portée

Les configurations suivantes sont facultatives :

- Configuration de l'expiration du délai d'attente
- Configuration de la reconnaissance complète

Configuration de la liste d'accès :

Utilisez les détails d'accès suivants pour configurer la liste d'accès.

Pourquoi et quand exécuter cette tâche

Avant d'interroger l'API Restful, le détecteur doit s'authentifier auprès du contrôleur ECC à l'aide d'un nom d'utilisateur, d'un mot de passe et d'un certificat. Ces données d'identification sont ensuite transmises à TADDM à l'aide d'un nouveau type de composant de la liste d'accès, les collecteurs de données. Une des entrées fournies dans les détails d'accès est un fichier de clés certifiées avec le certificat ECC.

Le détecteur utilise le fichier de clés certifiées pour établir une session sécurisée et chiffrée avec le contrôleur ECC. Elle est créée à l'aide de l'outil de clé, la clé Java et l'utilitaire de gestion des certificats. Tout système informatique sur lequel Java est installé peut être utilisé pour créer un tel fichier de clés certifiées. Si aucun système informatique n'est disponible, utilisez l'environnement JRE installé avec le contrôleur ECC.

Vous pouvez trouver le certificat ECC à l'emplacement suivant, où *alias_clé* correspond à l'alias de clé spécifié lors de l'installation du contrôleur ECC :

chemin_install_ecc/certificates/*alias_clé*.cert

Procédure

1. Pour créer le fichier de clés certifiées et importer le certificat, exécutez la commande suivante. Entrez la commande sur une seule ligne.

   ```
   chemin_jre/bin/keytool -import -noprompt -alias alias_clé
   -file chemin_certificat/alias_clé.cert
   -keystore nom_fichier_clés_certifiées
   -storepass phrase_passe_fichier_clés_certifiées
   -storetype JKS
   ```

   L'exemple suivant présente une commande qui permet de créer un fichier de clés certifiées avec le nom `ze_sensor_truststore` et la phrase passe `Fa8asTek` en utilisant l'environnement JRE ECC.

   ```
   chemin_install_ecc/jre/jre/bin/keytool -import -noprompt
   -alias alias_clé -file <chemin_install_ECC>/certificates/alias_clé.cert
   -keystore ze_sensor_truststore -storepass Fa8asTek -storetype JKS
   ```
2. Copiez le fichier de clés certifiées sur le système dans lequel vous avez configuré la liste d'accès.
3. Dans la fenêtre Détails sur l'accès, sélectionnez **Collecteurs de données** comme **Type de composant**.
4. Indiquez les informations d'accès d'un client ECC avec le rôle Explorateur.
5. Cliquez sur **Paramètres SSL** pour importer le fichier de clés certifiées ECC dans TADDM.
   a. Dans la zone **Transmettre le certificat du fichier de clés certifiées**, indiquez le ficher de clés certifiées.
   b. Dans la zone de phrase passe, indiquez la phrase passe.
   c. Indiquez le type SSL comme étant JKS.
   d. Laissez les zones relatives au **Fichier de clés** vides.
6. Cliquez sur **OK**.

Configuration du profil de reconnaissance :

Vous pouvez utiliser les options suivantes pour configurer la reconnaissance du détecteur zEnterprise.

Configuration du détecteur de ports

Vous devez ajouter le port ECC à l'option **Portlist** de la configuration du détecteur de port et l'indiquer dans l'option **enterpriseCCPortList**. L'option **enterpriseCCPortList** permet de définir quel port parmi ceux répertoriés dans l'option **Portlist** est celui sur lequel le collecteur ECC écoute. Le détecteur utilise cette option également pour établir la liste des ports sujets à des actions supplémentaires, telles l'exécution du détecteur zEnterprise. La même liste de ports doit être spécifiée dans l'option **portList** pour que le détecteur s'exécute.

Configuration du détecteur ZEnterprise

Vous pouvez utiliser cette configuration pour augmenter le délai et le nombre de nouvelles tentatives afin d'optimiser la connexion au collecteur ECC ou pour changer l'URL d'une requête si cette dernière est modifiée dans les versions ultérieures de l'ECC.

Si vous souhaitez capturer l'intégralité du paysage zEnterprise, vous pouvez définir l'indicateur **storeUnknownComputerSystems** sur `true`. Ce paramètre oblige le détecteur à stocker un système informatique de type inconnu ou celui sans ensemble d'identification adéquat.

Configuration de la portée :

La portée doit contenir l'adresse IP de l'hôte sur lequel le collecteur ECC est déployé ainsi que son nom de domaine complet. Ces informations sont requises pour une vérification positive des certificats utilisés dans le processus d'authentification.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur zEnterprise et propose des solutions à ces problèmes.

Erreur lors de l'authentification du détecteur

Problème

Le détecteur échoue lorsqu'il tente de s'authentifier avec le collecteur ECC. Les informations de statut du détecteur contiennent le message d'erreur suivant :

```
CTJTD1541E Erreur lors de l'authentification du détecteur
```

Solution

- Si le problème est associé à la configuration de la couche Secure Socket Layer (SSL), le journal du détecteur zEnterprise contient la trace de pile pour une erreur `javax.net.ssl.SSLHandshakeException`. Configurez les paramètres SSL dans les informations d'accès une nouvelle fois. Il est possible qu'aucun fichier de clés certifiées n'ait été téléchargé précédemment, que le fichier de clés certifiées ne contienne pas le bon certificat pour l'ECC, ou que la phrase passe du fichier de clés certifiées soit incorrecte.
- Si le problème est lié à la connexion au collecteur ECC, les journaux ECC contiennent un des messages suivants :

```
CTGEZ0701E L'authentification a échoué à cause d'un ID utilisateur inconnu id_utilisateur.
CTGEZ0702E L'authentification a échoué à cause d'un mot de passe non valide pour l'ID utilisateur
           id_utilisateur.
CTGEZ0703E L'authentification a échoué à cause d'un ID utilisateur désactivé id_utilisateur.
CTGEZ0704E L'authentification a échoué en raison d'un trop grand nombre de tentatives d'ouverture
           de session non valides par l'ID utilisateur id_utilisateur.
CTGEZ0705E L'authentification a échoué, car le mot de passe de l'ID utilisateur id_utilisateur est expiré.
```

  La solution varie en fonction du message de journal ECC trouvé :
  - Mettez à jour les informations d'accès au collecteur de données en corrigeant le nom d'utilisateur ou le mot de passe incorrect.
  - Mettez à jour la configuration client sur le collecteur ECC :
    - Créez un client
    - Activez le client désactivé
    - Relancez le client qui possède trop de tentatives de connexion non valides

- Modifiez le mot de passe client expiré

- Si le problème n'est pas lié à la configuration SSL ou à la connexion du collecteur ECC, vérifiez que des informations d'accès au collecteur de données existent et qu'elles ne sont pas limitées dans leur portée. Créez des informations d'accès ou modifiez la portée sur des informations d'accès existantes.

Erreur au cours de l'analyse des données ECC

Problème

Le détecteur échoue lorsqu'il tente d'analyser des données qui sont renvoyées par le collecteur ECC, et les informations de statut du détecteur contiennent le message d'erreur suivant :

```
CTJTD1542E The sensor failed when trying to parse data returned from the ECC
```

Solution

Le collecteur ECC a rencontré une erreur. Vérifiez les fichiers journaux ECC afin de déterminer la solution.

Impossible de se connecter au collecteur ECC car la version de l'API n'est pas prise en charge

Problème

La version de l'API ECC n'est pas prise en charge par cette version du détecteur zEnterprise. Les informations de statut du détecteur contiennent le message d'erreur suivant :

```
CTJTD1581E Impossible de se connecter à Enterprise Common Collector avec
le nom d'hôte nomhôte car la version d'API du collecteur n'est pas prise en charge ;
version principale d'API prise en charge : version_principale_prise-en-charge ;
version secondaire d'API minimale prise en charge :
version_secondaire_prise-en-charge ;
version principale d'API réelle : version_principale_réelle ;
version secondaire d'API réelle : version_secondaire_réelle
```

Solution

Mettez à niveau le collecteur ECC ou le détecteur zEnterprise vers une version plus récente.

Le détecteur zEnterprise ne s'exécute pas

Problème

Le détecteur ne parvient pas à se connecter au collecteur ECC, et les informations de statut du détecteur Ping indiquent qu'il a stocké 0 adresse IP dans la base de données. De plus, le détecteur de ports et le détecteur zEnterprise ne sont pas en cours d'exécution, ou le détecteur Ping et le détecteur de ports sont tous deux en cours d'exécution mais le détecteur zEnterprise ne l'est pas.

Solution

Si le détecteur Ping indique qu'il a stocké 0 adresse IP dans la base de données, le système ECC n'est pas joignable. Vérifiez que le nom d'hôte et l'adresse IP fournis pour le collecteur ECC sont corrects. Vérifiez également qu'il n'existe aucun pare-feu entre le détecteur et le collecteur ECC.

Si le détecteur Ping et le détecteur de ports sont tous les deux en cours d'exécution, le collecteur ECC n'écoute pas sur le port attendu. Vérifiez qu'une instance d'ECC est installée et en cours d'exécution sur le système indiqué, et que les attributs **portList** et **enterpriseCCPortList** du détecteur de ports contiennent tous deux le numéro de port ECC. Par

défaut, le collecteur ECC écoute sur le port 8443 mais ce numéro de port peut être modifié pendant l'installation du collecteur ECC.

Le détecteur zEnterprise ne se termine pas correctement

Problème

Le détecteur a rencontré une erreur irrémédiable inattendue. Les informations de statut du détecteur contiennent le message d'erreur suivant :

```
CTJTD1544E Enterprise sensor failed to complete. Pour plus de détails,
vérifiez les fichiers journaux.
```

Solution

Pour plus de détails, consultez le fichier journal.

Le détecteur ignore les systèmes informatiques inconnus

Problème

Le détecteur ne peut pas déterminer le type de système d'exploitation qui est en cours d'exécution sur un serveur virtuel. Les informations de statut du détecteur contiennent le message d'avertissement suivant :

```
CTJTD1567E Système informatique inconnu ignoré : ordinateur
```

Solution

Ce message se produit lorsqu'un serveur virtuel est inactif ou lorsque Guest Platform Management Provider (GPMP) n'est pas en cours d'exécution sur le serveur virtuel. Activez le serveur virtuel, installez et exécutez GPMP.

Sinon, vous pouvez remplacer l'indicateur **storeUnknownComputerSystems** par `true` afin de reconnaître tous les serveurs virtuels de ce type. Dans ce cas, les systèmes sont stockés comme des objets ComputerSystem. Vous pouvez y accéder à partir de la section Autres systèmes informatiques du portail de gestion de données.

Le détecteur ignore les systèmes informatiques inconnus sans identificateurs appropriés

Problème

Le détecteur ne peut pas stocker un serveur virtuel PowerVM dans TADDM. Les informations de statut du détecteur contiennent le message d'avertissement suivant :

```
CTJTD1568E Le système informatique pour lequel aucun identificateur approprié n'a été
défini est ignoré : ordinateur
```

Solution

La console HMC zEnterprise ne fournit pas de valeurs pour tous les attributs requis pour identifier un serveur virtuel PowerVM de manière unique dans la base de données TADDM. La seule façon de reconnaître des serveurs virtuels PowerVM est de remplacer l'identificateur **storeUnknownComputerSystems** de la configuration du détecteur zEnterprise par `true`. Dans ce cas, tous les serveurs virtuels PowerVM et tous les serveurs virtuels pour lesquels le détecteur ne peut pas déterminer le type de système d'exploitation sont reconnus.

Détecteurs de réseau

Les détecteurs de réseau reconnaissent des périphériques réseau.

Présentation des détecteurs SNMP

TADDM fournit des détecteurs SNMP dédiés à la reconnaissance des périphériques réseau SNMP.

Séquence d'appel pour des détecteurs SNMP

La séquence d'appel des détecteurs SNMP dépend des détecteurs activés dans le profil de reconnaissance et des données reconnues.

Dans les profils de reconnaissance de niveau 1, utilisez le détecteur SNMP Light avec le détecteur d'analyse de piles pour améliorer la précision de la reconnaissance. Dans les profils de niveau 2 ou de niveau 3, utilisez le détecteur SNMP MIB2, qui reconnaît des données supplémentaires pour la génération de topologies détaillées de niveau 2.

La figure 1, à la page 278 illustre la séquence d'appel pour le détecteur SNMP Light et le détecteur SNMP MIB2.

Le détecteur ping appelle le détecteur de port.

Si le détecteur SNMP Light est activé, le détecteur de port appelle le détecteur SNMP Light. Si le détecteur de port reconnaît des ports WMI ou SSH et si le détecteur de session est activé, le détecteur de port lance le détecteur de session. Si le détecteur de port ne reconnaît pas de port WMI or SSH, ou si le détecteur de session est dans l'impossibilité d'établir une connexion à l'hôte distant, le détecteur de port appelle le détecteur SNMP MIB2.

La figure 2, à la page 278 illustre la séquence d'appel des détecteurs SNMP, qui démarre après l'appel du détecteur SNMP Light ou du détecteur SNMP MIB2.

Selon les données que le détecteur SNMP Light ou SNMP MIB2 reconnaît à partir des périphériques, les détecteurs suivants sont appelés :

- S'il s'agit de la reconnaissance d'un périphérique Cisco, le détecteur de port Cisco et le détecteur de réseau local virtuel Cisco sont appelées.
- S'il s'agit de la reconnaissance d'un commutateur Fibre Channel, le détecteur de commutateur Fibre Channel est appelé.
- Si aucun commutateur Fibre Channel n'est reconnu, le détecteur Entity MIB et le détecteur Bridge SNMP sont appelées. Ces détecteurs doivent toutefois être activés dans le profil de reconnaissance.
- Si le périphérique reconnu correspond à un modèle de système informatique MIB personnalisé, le détecteur de système informatique MIB2 personnalisé est appelé.

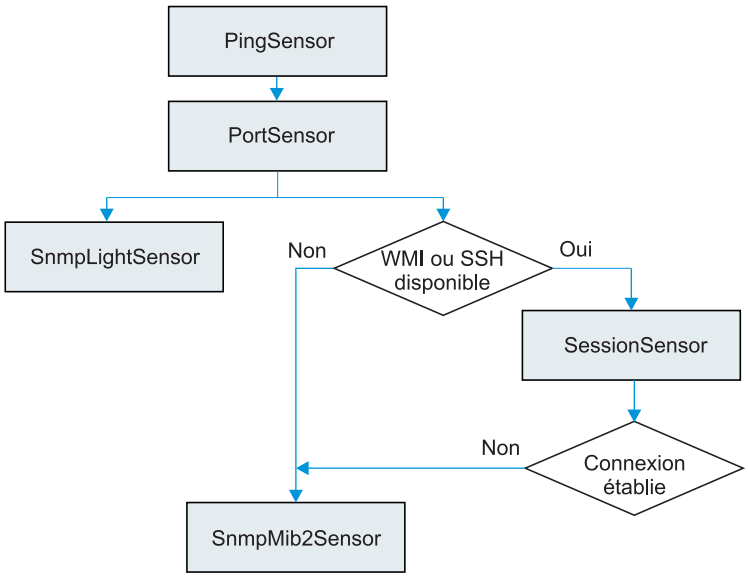

Figure 1. Séquence d'appel pour un détecteur SNMP Light et un détecteur SNMP MIB2

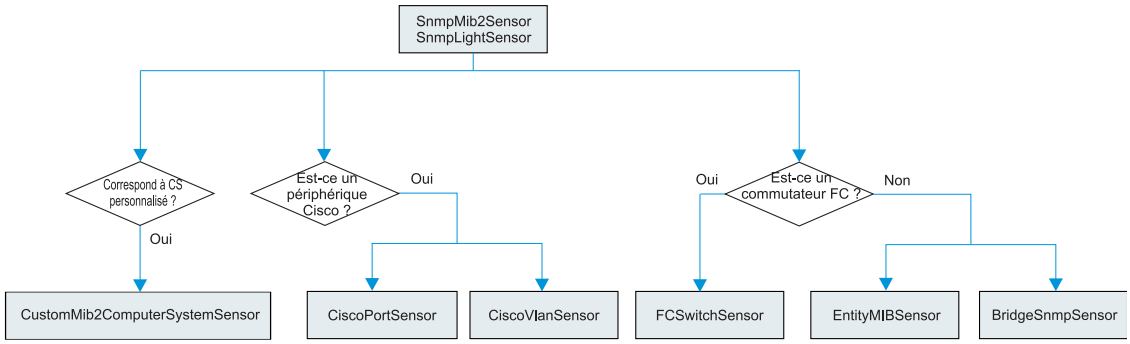

Figure 2. Séquence d'appel pour des détecteurs SNMP qui démarrent après l'appel du détecteur SNMP Light ou du détecteur SNMP MIB2.

Détecteurs SNMP de parcours de MIB et de débogage SNMP

Vous pouvez consigner des requêtes SNMP get envoyées par les détecteurs.

Pour ce faire, ajoutez la propriété suivante au fichier`collation.properties` :

```
com.collation.Discover.jvmargs=-Xmx2048M
-Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
-Dcom.collation.platform.snmp.SnmpPackedPDU.trace=true
```

Vous pouvez ensuite comparer des entrées de la sortie du fichier journal avec les requêtes SNMP directes que vous exécutez pour les périphériques utilisant snmpwalk. Vous pouvez télécharger des outils de requête SNMP qui prennent en charge snmpwalk depuis http://www.net-snmp.org/download.html.

Si une authentification SNMP V3 est utilisée avec un chiffrement, vous devez aussi télécharger OpenSSL à partir de http://www.openssl.org/.

L'exemple suivant présente des requêtes identiques, où la première utilise une authentification V3 (bien que les clés ont été supprimés) et la deuxième une authentification de nom de communauté :

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "mon mot de passe d'authentification"
   -x DES -X "ma clé de chiffrement" 10.199.250.9 .1.3.6.1.2.1.4.20.1
snmpwalk -v 1 -c 5FFGkFaFNs 10.199.250.9 .1.3.6.1.2.1.4.20.1
```

Gestion des modèles de système informatique SNMP et des fichiers de configuration

La vue Système informatique vous permet de gérer la liste des modèles pouvant être utilisée pour reconnaître des périphérique réseau.

Vous pouvez définir partiellement un périphérique, lier cette définition à un modèle, puis utilisez ce dernier pour découvrir davantage d'informations sur le périphérique.

L'OID est attribué au périphérique par le constructeur, et il est unique pour la marque et le modèle de ce périphérique. Des périphériques similaires du même modèle ont le même OID. Généralement, vous pouvez déterminer le type du périphérique que vous avez trouvé par une recherche sur le Web. Cette valeur peut également être obtenue pour le périphérique en interrogeant les tables SNMPv2-MIB pour des valeurs sous le sysObjectID 1.3.6.1.2.1.1.2.

Les modèles SNMP et leurs fichiers de configuration sont chargés dynamiquement durant chaque reconnaissance. Il n'est pas nécessaire de redémarrer le serveur TADDM après avoir modifié les modèles SNMP et leurs fichiers de configuration. Il est important d'utiliser la syntaxe correcte et d'entrer les valeurs correctes lors de l'édition des modèles et des fichiers de configuration.

Si vos périphériques ne sont pas correctement classés après une reconnaissance, vérifiez le fichier `SnmpMib2Sensor log` ou `DiscoveryManager log`.

Pour plus d'informations, voir la rubrique *Ajout d'un modèle de système informatique pour un réseau* dans le *Guide d'utilisation* de TADDM.

Les résultats suivants affichent différents OID reconnus par le biais d'analyses SNMP de quatre périphériques Foundry. Dans un environnement de test, les OID décrits dans le tableau 20 ont été reconnus. Vous pouvez effectuer une recherche sur Internet pour déterminer le type de périphériques. Vous pouvez également demander à votre équipe réseau d'identifier les types de périphérique spécifiques.

Tableau 20. Exemple de mappage d'OID Foundry

Périphérique Foundry	OID	Description
Foundry FESX448-PREM	.1.3.6.1.4.1.1991.1.3.34.2.1.1.2	Routeur
Foundry FastIron SX	.1.3.6.1.4.1.1991.1.3.36.6.2	Inconnu (classé comme commutateur dans nos tests)
Foundry BigIron RX	.1.3.6.1.4.1.1991.1.3.40.1.2	Inconnu (classé comme commutateur dans nos tests)
Foundry NetIron MLX	.1.3.6.1.4.1.1991.1.3.44.2.2	Inconnu (classé comme routeur dans nos tests)

Vous pouvez créer des modèles pour classifier les périphériques Foundry reconnus.

Exemple de commutateur Foundry :

Cet exemple illustre comment créer le modèle de système informatique SNMP pour un commutateur Foundry.

Procédure

1. Dans la console de gestion de reconnaissance, cliquez sur **Reconnaissance** > **Systèmes informatiques**.
2. Dans la vue Systèmes informatiques, cliquez sur **Ajouter**. La fenêtre Caractéristiques du système informatique s'affiche.
3. Dans la zone **Nom**, entrez `Foundry Switch`.
4. Dans la zone **Action**, sélectionnez **Reconnaître**.
5. Sélectionnez **Enabled**.
6. Facultatif : Dans la zone **Icon**, cliquez sur **Browse** pour sélectionner une icône pour le périphérique. Cette icône est utilisée uniquement pour identifier le modèle dans la vue Systèmes informatiques. (Elle n'est pas utilisée pendant ou après la reconnaissance.)
7. Sélectionnez **Base d'informations de gestion**.
8. Dans la zone **Identification des critères**, sélectionnez **Un critère quelconque**.
9. Indiquez les valeurs suivantes pour le premier critère :

OID système	**est**	`.1.3.6.1.4.1.1991.1.3.34.2.1.1.1`

   Puis cliquez sur **Ajouter un critère**.
10. Indiquez les valeurs suivantes pour le second critère :

OID système	**débute-par**	`.1.3.6.1.4.1.1991.1.3.36`

    Puis cliquez sur **Ajouter un critère**.
11. Indiquez les valeurs suivantes pour le troisième critère :

OID système	**débute-par**	`.1.3.6.1.4.1.1991.1.3.40`

    Puis cliquez sur **Ajouter un critère**.
12. Cliquez sur **OK**. Le nouveau modèle est ajouté à la fin de la liste.
13. Pour ajouter un fichier de classe Action pour le modèle, créez un fichier nommé `Foundry Switch.xml` dans le répertoire`$COLLATION_HOME/etc/templates/action`. Ajoutez le contenu suivant au fichier :

```
<?xml version="1.0" encoding="UTF-8"?>
  <results
    xmlns="urn:www-collation-com:1.0"
    xmlns:coll="urn:www-collation-com:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:www-collation-com:1.0
        urn:www-collation-com:1.0/results.xsd">

    <UnitaryComputerSystem array="1" xsi:type=
   "coll:com.collation.platform.model.topology.sys.UnitaryComputerSystem">
      <type>Bridge</type>
      <manufacturer>Foundry Networks</manufacturer>
    </UnitaryComputerSystem>
  </results>
```

   Ce fichier XML indique que tous les périphériques reconnus du système informatique SNMP qui correspondent au modèle `Foundry Switch` utilisent la classe de modèle com.collation.platform.model.topology.sys.UnitaryComputerSystem et que leur attribut *type* est défini sur `bridge` et l'attribut *manufacturer* est défini sur `Foundry Networks`.

Remarque : Le nom du fichier de classe Action (sans l'extension .xml) doit correspondre au nom du modèle de système informatique SNMP.

Que faire ensuite

Le nouveau modèle peut être utilisé immédiatement (il n'est pas nécessaire de redémarrer le serveur TADDM).

Exemple de routeur Foundry :

Cet exemple illustre comment créer le modèle de système informatique SNMP pour un routeur Foundry.

Procédure

1. Dans la console de gestion de reconnaissance, cliquez sur **Reconnaissance** > **Systèmes informatiques**.
2. Dans la vue Systèmes informatiques, cliquez sur **Ajouter**. La fenêtre Caractéristiques du système informatique s'affiche.
3. Dans la zone **Nom**, entrez `Foundry Router`.
4. Dans la zone **Action**, sélectionnez **Reconnaître**.
5. Sélectionnez **Enabled**.
6. Facultatif : Dans la zone **Icon**, cliquez sur **Browse** pour sélectionner une icône pour le périphérique. Cette icône permet d'identifier le modèle dans la vue Systèmes informatiques. (Elle n'est pas utilisée pendant ou après la reconnaissance.)
7. Sélectionnez **Base d'informations de gestion**.
8. Dans la zone **Identification des critères**, sélectionnez **Un critère quelconque**.
9. Indiquez les valeurs suivantes pour le premier critère :

OID système	est	.1.3.6.1.4.1.1991.1.3.34.2.1.1.2

   Puis cliquez sur **Ajouter un critère**.
10. Indiquez les valeurs suivantes pour le second critère :

OID système	débute-par	.1.3.6.1.4.1.1991.1.3.44

    Puis cliquez sur **Ajouter un critère**.
11. Cliquez sur **OK**. Le nouveau modèle est ajouté à la fin de la liste.
12. Pour ajouter un fichier de classe Action pour le modèle, créez un fichier nommé `Foundry Router.xml` dans le répertoire `$COLLATION_HOME/etc/templates/action`. Ajoutez le contenu suivant au fichier :

```
<?xml version="1.0" encoding="UTF-8"?>
  <results
    xmlns="urn:www-collation-com:1.0"
    xmlns:coll="urn:www-collation-com:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:www-collation-com:1.0
        urn:www-collation-com:1.0/results.xsd">

    <UnitaryComputerSystem array="1" xsi:type=
      "coll:com.collation.platform.model.topology.sys.UnitaryComputerSystem">
        <type>Router</type>
        <manufacturer>Foundry Networks</manufacturer>
    </UnitaryComputerSystem>
  </results>
```

Ce fichier XML indique que tous les périphériques reconnus du système informatique SNMP qui correspondent au modèle `Foundry Router` utilisent la classe de modèle com.collation.platform.model.topology.sys.UnitaryComputerSystem et que leur attribut *type* est défini sur `Router` et l'attribut *manufacturer* est défini sur `Foundry Networks`.

Remarque : Le nom du fichier de classe Action (sans l'extension .xml) doit correspondre au nom du modèle de système informatique SNMP.

Que faire ensuite

Le nouveau modèle peut être utilisé immédiatement (il n'est pas nécessaire de redémarrer le serveur TADDM).

Propriétés des détecteurs SNMP

Vous pouvez contrôler l'utilisation des détecteurs SNMP en modifiant les propriétés dans le fichier `collation.properties`.

Fix Pack 2 **com.ibm.cdb.discover.snmp.login.timeout=5000**

Cette propriété indique le laps de temps écoulé avant qu'une tentative de connexion n'échoue.

La valeur par défaut est `5000` (millisecondes).

détecteur de port Alteon

Le détecteur de port Alteon reconnaît les informations de port de commutateur Alteon, notamment les ports qui fonctionnent en mode de négociation automatique et en mode duplex.

Ces ports sont stockés dans L2Interface avec les informations de négociation automatique (activée ou désactivée). Le mode duplex (semi-duplex ou duplex intégral) est également stocké.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AlteonPortSensor

ID objets (OID) utilisés

Le détecteur utilise les OID suivants :

- curCfgTable: .1.3.6.1.4.1.1872.2.1.2.3.2.1
- portInfoTable: .1.3.6.1.4.1.1872.2.1.9.1.1.1

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur Alteon SNMP

Le détecteur SNMP Alteon reconnaît les périphériques de l'équilibreur de charge Alteon.

Le détecteur reconnaît les éléments suivants :

- Serveurs vrais et groupes de serveurs vrais. Les serveurs vrais sont partitionnés dans leurs groupes de serveurs vrais respectifs. Des informations supplémentaires telles que LoadBalancingAlgorithm sont également reconnues et stockées dans le groupe de serveurs vrais.
- Ports virtuels, ports vrais et serveurs virtuels utilisés pour créer et stocker des services virtuels.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AlteonSnmpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- .1.3.6.1.4.1.1872.2.1.5.5.1.1
- .1.3.6.1.4.1.1872.2.1.5.5.1.2
- .1.3.6.1.4.1.1872.2.1.5.5.1.4
- .1.3.6.1.4.1.1872.2.1.5.2.1.1
- .1.3.6.1.4.1.1872.2.1.5.2.1.2
- .1.3.6.1.4.1.1872.2.1.5.2.1.3
- .1.3.6.1.4.1.1872.2.1.5.2.1.10
- .1.3.6.1.4.1.1872.2.1.5.10.1.1
- .1.3.6.1.4.1.1872.2.1.5.10.1.2
- .1.3.6.1.4.1.1872.2.1.5.10.1.3
- .1.3.6.1.4.1.1872.2.1.5.10.1.7

- .1.3.6.1.4.1.1872.2.1.5.8.1.1
- .1.3.6.1.4.1.1872.2.1.5.8.1.2
- .1.3.6.1.4.1.1872.2.1.5.8.1.3
- .1.3.6.1.4.1.1872.2.1.5.8.1.4
- .1.3.6.1.4.1.1872.2.1.5.8.1.5
- .1.3.6.1.4.1.1872.2.1.5.8.1.6

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.vip.RealServerGroup
- net.vip.Vip
- net.vip.VipFunction
- net.vip.Virtualservice
- sys.UnitaryComputerSystem
- sys.Function net.vip.RealServer

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur de réseau local virtuel Alteon

Le détecteur de réseau local virtuel Alteon reconnaît les réseaux locaux Alteon. Ce détecteur utilise la base d'informations de gestion Alteon VLAN Membership MIB pour reconnaître le contenu des réseaux locaux virtuels.

Le détecteur SnmpMib2Sensor appelle le détecteur AlteonVlanSensor lorsque les réseaux locaux virtuels sont configurés pour des périphériques Alteon. Le détecteur AlteonVlanSensor appelle ensuite le détecteur BridgeSnmpSensor2 pour chaque réseau local virtuel reconnu.

Le détecteur reconnaît la table d'appartenance du réseau local virtuel, crée les interface L2Interfaces et les connecte au pont de réseau local virtuel.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AlteonVlanSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- .1.3.6.1.4.1.1872.2.1.4.2.1
- .1.3.6.1.4.1.1872.2.1.2.3.2.1

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Vlan
- net.VlanInterface
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur de port BIG-IP

Le détecteur de port BIG-IP reconnaît les interfaces de port F5 BIG-IP.

Le détecteur SnmpMib2Sensor appelle le détecteur BigIPPortSensor. Le détecteur BigIPPortSensor collecte les ports à partir de la base d'informations de gestion, par exemple, l'interface via laquelle les ports connus peuvent être adressés. Ceci permet la création des vues de topologie L2.

Nom du détecteur utilisé dans l'interface graphique et les journaux

BigIPPortSensor

ID objets (OID) utilisés

Ce détecteur respecte les normes documentées dans la RFC 1212 pour extraire les ports de la MIB. Plus précisément, une requête est effectuée sur l'OID .1.3.6.1.4.1.3375.1.1.5.2.1 pour obtenir l'interface via laquelle le port peut être reconnu à partir de la MIB.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur BIG-IP SNMP

Le détecteur Big-IP SNMP reconnaît les équilibreurs de charge F5 Big-IP .

Le détecteur SnmpMib2Sensor appelle le détecteur BigIPSnmpSensor si ce dernier correspond à l'un des OID suivants :

- .1.3.6.1.4.1.3375
- .1.3.6.1.4.1.2021.250.255

Le détecteur BigIPSnmpSensor collecte des informations sur les IP virtuels et les groupes de serveurs vrais.

Nom du détecteur utilisé dans l'interface graphique et les journaux

BigIPSnmpSensor

ID objets (OID) utilisés

Le détecteur respecte les normes documentées dans la RFC 1212 pour obtenir des entrées de table de base de données de serveurs réels (RSD) et de base de données de serveurs virtuels (VSD).

Le détecteur utilise les OID suivants :

F5 BIG-IP version 4 :

- Table de membres de pool : 1.3.6.1.4.1.3375.1.1.8.2.1
- Table de pools : 1.3.6.1.4.1.3375.1.1.7.2.1
- Table de serveurs virtuels : 1.3.6.1.4.1.3375.1.1.3.2.1

F5 BIG-IP version 9 :

- Table de membres de pool : 1.3.6.1.4.1.3375.2.2.5.3.2
- Table de pools : 1.3.6.1.4.1.3375.2.2.5.1.2
- Table de serveurs virtuels : 1.3.6.1.4.1.3375.2.2.10.1.2
- Table de pools de serveurs virtuels : 1.3.6.1.4.1.3375.2.2.10.6.2
- Table de règles de serveurs virtuels : 1.3.6.1.4.1.3375.2.2.10.8.2
- Table d'adresses virtuelles : 1.3.6.1.4.1.3375.2.2.10.10.2
- sysGeneralChassisSerialNum: 1.3.6.1.4.1.3375.2.1.3.3.3

F5 BIG-IP version 10 :

- Table de membres de pool : 1.3.6.1.4.1.3375.2.2.5.3.2
- Table de pools : 1.3.6.1.4.1.3375.2.2.5.1.2
- Table de serveurs virtuels : 1.3.6.1.4.1.3375.2.2.10.1.2
- Table de règles de serveurs virtuels : 1.3.6.1.4.1.3375.2.2.10.8.2
- Table d'adresses virtuelles : 1.3.6.1.4.1.3375.2.2.10.10.2
- sysGeneralChassisSerialNum: 1.3.6.1.4.1.3375.2.1.3.3.3

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- bigip.BigIPRealServer
- bigip.BigIPRealServerGroup
- bigip.BigIPVip
- bigip.BigIPVipFunction
- bigip.BigIPVirtualService
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.

2. Indiquez le nom de communauté correct.

- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteurs de réseau local virtuel BIG-IP

Le détecteur de réseau local virtuel Big-IP reconnaît des réseaux locaux virtuels F5 Big-IP.

Le détecteur SnmpMib2Sensor appelle le détecteur BigIPVlanSensor. Un objet de modèle VlanInterface est créée pour chaque réseau local virtuel dans la mappe des réseaux locaux virtuels (par exemple, l'interface permettant d'adresser des réseaux virtuels connus). Ceci autorise la création des vues de topologie L2.

Nom du détecteur utilisé dans l'interface graphique et les journaux

BigIPVlanSensor

ID objets (OID) utilisés

Le détecteur BigIPVlanSensor respecte les normes documentées dans la RFC 1212 pour obtenir l'interface de réseau local virtuel. Plus précisément, une requête est effectuée sur l'OID .1.3.6.1.4.1.3375.1.1.10.2.1 pour obtenir l'interface VLAN via laquelle le réseau local virtuel peut être reconnu à partir de la base d'informations de gestion.

Le détecteur BigIPVlanSensor exécute l'étape de reconnaissance de l'agent et reconnaît les éléments Vlan et VlanInterface, et indique une erreur AgentException en cas d'échec de la reconnaissance.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- bigip.BigIPVlan
- net.L2Interface
- net.VlanInterface

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur de pont SNMP

Le détecteur de pont SNMP développe et met à jour les données de port reconnues par le détecteur SNMP MIB2 (il s'agit des données qui sont affichées sous l'onglet Ports du panneau Détails).

Le détecteur SNMP MIB2 appelle le détecteur de pont SNMP. Le détecteur de pont SNMP collecte les données d'adresse MAC des périphériques connectés (notamment, le numéro d'interface par lequel il est possible d'atteindre des périphériques à adressage MAC connue), ce qui est nécessaire pour la génération de vues de topologie de niveau 2.

Le détecteur respecte les normes documentées dans la RFC 1286 pour extraire certaines entrées de la table FDB (Forwarding Database) MAC. Les OID suivants sont interrogés :

- `.1.3.6.1.2.1.17.4.3.1.1`
- `.1.3.6.1.2.1.17.4.3.1.2`

L'OID `.1.3.6.1.2.1.17.4.3.1.1` retourne une liste d'OID pour les adresses MAC connues, comme indiqué dans l'exemple suivant. Ces OID sont ensuite interrogées pour déterminer l'interface permettant d'accéder au périphérique MAC.

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.189.255.1
   .1.3.6.1.2.1.17.4.3.1.1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.18.242.42.208.0 = Hex-STRING: 00 12 F2 2A D0 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.18.242.50.0.0 = Hex-STRING: 00 12 F2 32 00 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.18.242.51.88.0 = Hex-STRING: 00 12 F2 33 58 00
SNMPv2-SMI::mib-2.17.4.3.1.1.0.18.242.218.128.177 = Hex-STRING: 00 12 F2 DA 80 B1
SNMPv2-SMI::mib-2.17.4.3.1.1.0.208.4.45.228.10 = Hex-STRING: 00 D0 04 2D E4 0A

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.189.255.1
   .1.3.6.1.2.1.17.4.3.1.1.0.18.242.42.208.0
SNMPv2-SMI::mib-2.17.4.3.1.1.0.18.242.42.208.0 = Hex-STRING: 00 12 F2 2A D0 00
```

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.189.255.1
   .1.3.6.1.2.1.17.4.3.1.2.0.18.242.42.208.0
SNMPv2-SMI::mib-2.17.4.3.1.2.0.18.242.42.208.0 = INTEGER: 282
```

Le détecteur de pont SNMP fournit également des informations spécifiques sur les interfaces du système informatique ce niveau 2 (L2) qui sont connectées au commutateur. Le détecteur SNMP MIB2 fournit des informations générales sur l'existences des interfaces de périphérique, tandis que le détecteur SNMP de pont fournit des informations détaillées sur les adresses MAC qui sont accessibles via les interfaces d'unité.

Par exemple, le tableau 21 affiche les noms des périphériques MAC reconnus par le détecteur de pont SNMP. TADDM peut déterminer les noms car le système informatique qui propriétaire de ce périphérique MAC a été reconnu. Si le nom du périphérique est inconnu, l'adresse MAC est utilisée.

Tableau 21. Données de topologie de pont de niveau 2

Name	Interfaces L2 du système informatique
ethernet 1/9	NC84CDRS1LDPC02
ethernet 1/10	00040DFDE53
ethernet 1/11	NC84CDRS1LDPC04
ethernet 1/12	NC84CDRS1LDPC03
ethernet 10/2	000CDBF90C19

Le détecteur respecte également les normes qui sont documentées dans la RFC 1286 pour extraire certaines des informations de table de ports. Les OID suivants sont interrogés :

- `.1.3.6.1.2.1.17.1.4.1.1`
- `.1.3.6.1.2.1.17.1.4.1.2`

Nom du détecteur utilisé dans l'interface graphique et les journaux

BridgeSnmpSensor

ID objets (OID) utilisés

Ce détecteur respecte les normes documentées dans la RFC 1286 pour extraire certaines entrées de la table MAC Forwarding Database (fdb). Les OID suivants sont interrogés :

- .1.3.6.1.2.1.17.4.3.1.1
- .1.3.6.1.2.1.17.4.3.1.2

L'OID .1.3.6.1.2.1.17.4.3.1.1 retourne une liste d'OID pour les adresses MAC connues. Ces OID sont ensuite interrogés pour déterminer l'interface permettant d'accéder au périphérique MAC.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Segment

- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Configuration des entrées du fichier `collation.properties`

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

Fix Pack 3 **com.ibm.cdb.discover.sensor.net.BridgeSnmpSensor.dot1dTpFdbStatus**
Cette propriété indique les valeurs de l'objet `dot1dTpFdbStatus`.

Par défaut, TADDM prend en charge les valeurs `1`, `3` et `5`.

Si vous utilisez des commutateurs réseau qui prennent en charge des valeurs personnalisées, ajoutez cette propriété au fichier `collation.property` avec les valeurs spécifiées.

com.collation.discover.agent.net.BridgeSnmpAgent.filterCiscoTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des dispositifs Cisco.

Dans TADDM 7.3.0.2 et versions antérieures, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez activer le protocole CDP pour les commutateurs de reconnaissance et aussi activer CdpSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

Fix Pack 2

com.collation.discover.agent.net.BridgeSnmpAgent.filterLLDPTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des commutateurs FDB.

Dans TADDM 7.3.0.2, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez activer le protocole LLDP pour les commutateurs de reconnaissance et aussi activer LldpSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

Fix Pack 2

com.collation.discover.agent.net.BridgeSnmpAgent.filterExtremeTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des dispositifs Extreme.

Dans TADDM 7.3.0.2, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez également activer le protocole EDP pour les commutateurs de reconnaissance et aussi activer ExtremeVlanSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

détecteur de pont SNMP 2

Le détecteur de pont SNMP 2 développe et met à jour les données de port reconnues par le détecteur SNMP MIB2 pour toutes les zones des réseaux locaux virtuels (VLAN).

Le détecteur de pont SNMP 2 est appelé lorsque des réseaux locaux virtuels sont configurés pour le périphérique. Le détecteur de réseau local virtuel Cisco appelle le détecteur de pont SNMP 2 pour chaque réseau local virtuel qui est reconnue. Les données qui sont reconnues sont les mêmes que pour le détecteur de pont SNMP, mais elles sont reconnues pour tous les réseaux locaux virtuels.

Nom du détecteur utilisé dans l'interface graphique et les journaux

BridgeSnmpSensor2

ID objets (OID) utilisés

Ce détecteur respecte les normes documentées dans la RFC 1286 pour extraire certaines entrées de la table MAC Forwarding Database (fdb). Les OID suivants sont interrogés :

- .1.3.6.1.2.1.17.4.3.1.1
- .1.3.6.1.2.1.17.4.3.1.2.

L'OID .1.3.6.1.2.1.17.4.3.1.1 retourne une liste d'OID pour les adresses MAC connues. Ces OID sont ensuite interrogés pour déterminer l'interface permettant d'accéder au périphérique MAC.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Segment
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Configuration des entrées du fichier `collation.properties`

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

Fix Pack 3 **com.ibm.cdb.discover.sensor.net.BridgeSnmpSensor.dot1dTpFdbStatus**
Cette propriété indique les valeurs de l'objet `dot1dTpFdbStatus`.

Par défaut, TADDM prend en charge les valeurs `1`, `3` et `5`.

Si vous utilisez des commutateurs réseau qui prennent en charge des valeurs personnalisées, ajoutez cette propriété au fichier `collation.property` avec les valeurs spécifiées.

com.collation.discover.agent.net.BridgeSnmpAgent.filterCiscoTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des dispositifs Cisco.

Dans TADDM 7.3.0.2 et versions antérieures, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez activer le protocole CDP pour les commutateurs de reconnaissance et aussi activer CdpSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

Fix Pack 2
com.collation.discover.agent.net.BridgeSnmpAgent.filterLLDPTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des commutateurs FDB.

Dans TADDM 7.3.0.2, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez activer le protocole LLDP pour les commutateurs de reconnaissance et aussi activer LldpSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

Fix Pack 2
com.collation.discover.agent.net.BridgeSnmpAgent.filterExtremeTrunkPort
Cette propriété indique si le détecteur doit ignorer ou non la reconnaissance des adresses MAC sur les ports de liaison des dispositifs Extreme.

Dans TADDM 7.3.0.2, la valeur par défaut est `false`, ce qui signifie que les adresses MAC sont reconnues. Si vous souhaitez désactiver la reconnaissance, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `true`.

Important : Si vous définissez cette propriété sur `true`, vous devez également activer le protocole EDP pour les commutateurs de reconnaissance et aussi activer ExtremeVlanSensor dans le profil de reconnaissance.

Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, la valeur par défaut est `true`. Pour activer la reconnaissance des adresses MAC sur les ports de liaison, ajoutez cette propriété au fichier `collation.properties` et affectez-lui la valeur `false`.

Fix Pack 2

com.collation.discover.agent.BridgeSnmpAgent.MACAddressPrefixSkipList
Cette propriété ignore les adresses MAC d'un périphériques réseau. Utilisez cette propriété pour filtrer les bureaux et tout autre périphérique physique lorsque TADDM analyse les périphériques réseau.

La valeur de cette propriété est une liste de préfixes d'adresse MAC séparés par des virgules, qui correspondent aux entrées que le détecteur trouve dans la table Forwarding Database. Lorsqu'une adresse MAC et qu'une entrée de la table correspondent, le périphérique est ignoré.

détecteur Check Point

Le détecteur Check Point reconnaît Check Point FireWall-1 qui s'exécute sur les plateformes non-Windows, comme des systèmes d'exploitation Solaris ou Check Point IPSO.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CheckpointSensor

Prérequis

Vous devez disposer des droits d'accès suivants :

- Accès SSH pouvant exécuter lsof
- Autorisation de lecture sur le répertoire `$CPMDIR/conf/objects.C` du système dans lequel Check Point FireWall-1 est exécuté
- Autorisation d'exécution pour la commande `$CPMDIR/bin/fw`
- Autorisation de lecture pour les fichiers `$CPMDIR/conf/*.W` qui contiennent les versions éditables des ensembles de règles

La variable d'environnement CPMDIR doit être définie pour l'utilisateur TADDM.

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

Entrées du fichier collation.properties

Les propriétés suivantes peuvent requérir un privilège élevé :

- com.collation.discover.agent.command.cat.SunOS=cat
- com.collation.discover.agent.command.cat.SunOS.1.2.3.4=sudo cat

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classique susceptibles de survenir avec le détecteur Check Point et propose des solutions à ces problèmes.

Impossible d'extraire des informations de la machine hôte du serveur Check Point

Problème

Echec du détecteur Check Point durant une reconnaissance.

Solution

Vérifiez que vous disposez des autorisations suivantes :

- Autorisation de lecture sur le répertoire `$CPMDIR/conf/objects.C` du système dans lequel Check Point FireWall-1 est exécuté
- Autorisation d'exécution pour la commande `$CPMDIR/bin/fw`
- Autorisation de lecture pour les fichiers `$CPMDIR/conf/*.W` qui contiennent les versions éditables des ensembles de règles

détecteur SNMP Check Point SNMP

Le détecteur SNMP Check Point reconnaît des informations SNMP qui sont associées aux pare-feux Check Point FireWall-1.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CheckpointSnmpSensor

Prérequis

L'ID objet système (sysObjectID) doit retourner l'un des ID objet suivants :

- OID = .1.3.6.1.4.1.1919.
- OID = .1.3.6.1.4.1.2620.
- OID.startsWith(.1.3.6.1.4.1.42.2.1.1.)

Limitations

Le détecteur collecte les informations relatives au module, au nom du filtre, à la date d'installation du filtre, au nom du produit, au nom majeur et au nom mineur.

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	Vers ce qui suit :
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Détecteur Cisco Adaptive Security Appliance

Le détecteur Cisco Adaptive Security Appliance (ASA) reconnaît les unités ASA utilisées comme pare-feux d'IP et les dispositifs de conversion d'adresses réseau.

Le détecteur Cisco ASA rassemble des données sur les unités ASA. Il reconnaît par ailleurs les informations suivantes :

- Tous les serveurs réels et les services virtuels en cours d'exécution. Les serveurs réels sont rassemblés dans le groupe de serveurs réels.
- Les éléments virtualIp, realIp, virtualPort et realPort. Le détecteur dérive aussi les IP virtuelles à l'aide des éléments virtualIp, realIp, virtualPort et realPort. Les adresses IP virtuelles sont stockées dans la table Vip.

Nom du détecteur utilisé dans l'interface graphique et les journaux

- ASASensor
- CiscoApplianceVersionSensor

Limitations

Dans les rapports sur l'historique des changements de TADDM, l'unité Cisco ASA apparaît comme une unité PIX.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- cisco.CiscoPixComputerSystem
- core.LogicalContent
- net.L2Interface
- sys.OperatingSystem
- vip.RealServer
- vip.RealServerGroup
- vip.Vip
- vip.VipFunction
- vip.VirtualService

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Unité Cisco** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur, mot de passe et mot de passe d'activation) que TADDM doit utiliser pour l'authentification à l'unité ASA cible.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` que le détecteur Cisco ASA utilise.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.asa.pager.command=terminal pager 0
Ajoutez cette propriété et la valeur si l'utilisateur indiqué dans la liste d'accès n'a pas accès à la commande **`configure terminal`**.

La valeur `terminal pager 0` instruit la commande pager pour forcer l'unité ASA à renvoyer des réponses en un seul lot.

com.collation.CiscoSshTimeout=9000
Augmentez la valeur **`CiscoSshTimeout`** (en millisecondes) si le système cible est disponible et en cours d'exécution, mais que l'erreur suivant s'affiche :

```
The ssh login did not work correctly
```

com.collation.CiscoExpectTimeout=60000
Augmentez la valeur **`CiscoExpectTimeout`** (en millisecondes) sur le système cible est disponible et en cours d'exécution, mais que l'erreur suivant s'affiche :

```
The ssh login did not work correctly
```

détecteur Cisco Discovery Protocol

Le détecteur Cisco Discovery Protocol (CDP) utilise le CDP MIB pour reconnaître des segments de couche 2 sur le réseau.

Le détecteur CdpSensor reconnaît les informations cdpCacheDeviceId et cdpCacheDevicePort et crée l'interface locale des périphériques homologues qui est utilisée pour créer le segment.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CdpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- Global Device Id : 1.3.6.1.4.1.9.9.23.1.3.4.0
- Cache Device Id : .1.3.6.1.4.1.9.9.23.1.2.1.1.6
- Cache Device Port : .1.3.6.1.4.1.9.9.23.1.2.1.1.7

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Segment
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

- Pour permettre à TADDM d'exécuter une reconnaissance complète, SNMP et telnet doivent être activés. Vous devez configurer l'accès Telnet avec un nom d'utilisateur et un mot de passe, et vous devez activer le mot de passe.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit les problèmes classiques qui peuvent survenir avec le détecteur Cisco Discovery Protocol et propose des solutions.

Une fois la reconnaissance effectuée par TADDM, le nom du détecteur apparaît sur l'interface graphique, sauf que l'onglet Fichiers de configuration n'apparaît pas comme prévu.

Problème

L'accès Telnet n'est pas configuré correctement.

Solution

Configurez l'accès Telnet avec un nom d'utilisateur et un mot de passe, et assurez-vous que le mot de passe est activé.

détecteur Cisco IOS

Le détecteur Cisco Internetwork Operating System (Cisco IOS) reconnaît l'équipement de réseau Cisco à l'aide du protocole SSH1, SSH2 ou Telnet.

Le détecteur Cisco IOS prend en charge une authentification en deux étapes :

- Création du client de session approprié pour le protocole SSH1, SSH2 ou Telnet
- Connexion à l'hôte

Nom du détecteur utilisé dans l'interface graphique et les journaux

CiscoIOSSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- agent.CiscoIOSAgentConfiguration
- core.LogicalContent
- sys.ComputerSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Les attributs de détecteur suivants peuvent être modifiés à partir du profil de reconnaissance:

useSshFirst
La valeur par défaut de cet attribut est `false`. Les protocoles sont détectés dans l'ordre suivant : protocole Telnet, SSH2 et SSH1. Si la valeur est `true`, les protocoles sont détectés dans l'ordre suivant : SSH2, SSH1 et protocole Telnet.

commands
Les valeurs par défaut de cet attribut sont `show running-config;show startup-config`, si aucune valeur n'est entrée. Le sortie de chaque commande est enregistrée en tant que fichier de configuration. Pour ajouter des commandes supplémentaires, entrez les commandes par défaut `show running-config;show startup-config` et ajoutez des commandes supplémentaires à la liste. Séparez chaque commande par un point-virgule. Vous pouvez également entrez les commandes que vous voulez exécuter.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Pour **Component Type**, sélectionnez **CiscoDeviceAuth**.
2. Indiquez les informations d'accès (nom d'utilisateur, mot de passe et mot de passe d'activation) que TADDM doit utiliser pour l'authentification auprès du système informatique cible. Ne renseignez pas le mot de passe d'activation si celui-ci n'est pas obligatoire.
3. Si le détecteur Cisco IOS utilise un protocole Telnet et n'affiche pas de message invitant à entrer un nom d'utilisateur, entrez `default` dans la zone du nom d'utilisateur.

détecteur de port Cisco

Le détecteur de port Cisco reconnaît les informations du commutateur de port Cisco.

Le détecteur CiscoPortSensor reconnaît l'index d'interface et l'état duplex du port. Il détermine également le statut d'auto-négociation.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CiscoPortSensor

ID objets (OID) utilisés

Le détecteur utilise l'OID .1.3.6.1.4.1.9.9.87.1.4.1.1 pour des périphériques Cisco 2900 Series. Sinon, l'OID .1.3.6.1.4.1.9.5.1.4.1.1 est utilisée.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

- Pour permettre à TADDM d'exécuter une reconnaissance complète, SNMP et telnet doivent être activés. Vous devez configurer l'accès Telnet avec un nom d'utilisateur et un mot de passe, et vous devez activer le mot de passe.

Détecteur SNMP Cisco UCS

Fix Pack 2

Le détecteur SNMP Cisco UCS reconnaît et collecte des informations de configuration concernant le périphérique Cisco UCS. Il utilise le protocole SNMP (Simple Network Management Protocol) pour reconnaître et interroger les composants d'infrastructure Cisco UCS.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CiscoUCSSensor

Limitations

- Le détecteur ne reconnaît pas certains types de données. Pour plus d'informations, consultez la liste suivante.

  Remarque : Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, ces limitations ne s'appliquent pas.

  – Les informations sur le module d'interconnexion de matrice ne sont pas disponibles dans l'interface utilisateur. Elles ne sont affichables que par le biais de l'interface CLI.
  – La relation entre le module d'interconnexion de matrice et le châssis n'est pas créée.
  – Les modules d'E/S ne sont pas reconnus.
  – L'objet de modèle d'UC du composant Blade et l'attribut Informations sur la mémoire ne sont pas reconnus.
- Le détecteur ne reconnaît pas les objets Cluster Cisco UCS et Pool Cisco UCS.

Objets de modèle avec attributs associés

Fix Pack 2

Le détecteur SNMP Cisco UCS crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte à propos des périphériques Cisco UCS.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

CiscoUCSBladeServer

- AdminState
- DistinguishedName
- Model
- Presence
- RelativePosition
- SerialNumber
- SystemBoardUUID

CiscoUCSChassis

- DistinguishedName
- HWRevision
- Model
- OperationalState
- SerialNumber

CiscoUCSFabricInterconnect

- DistinguishedName
- HWRevision
- Model
- OperationalState

- SerialNumber
- Thermal

CiscoUCSServiceProfile

- AssignedState
- AssocState
- DistinguishedName
- Label
- ProfileType
- OperationalState
- OriginNode

enums.PhysTypeEnum

enums.SlotStateEnum

net.Fqdn

phys.physconn.PhysicalConnector

phys.physconn.Slot

- HWRevision
- Name
- Parent
- PhysicalFrame
- RelativePosition
- SlotState
- Type

phys.physpkg.Board

- DistinguishedName
- Model
- ModuleSide
- Name
- OperationalState
- PhysicalPackage
- Presence
- RelativePosition
- RunningVersion
- SerialNumber
- StartupVersion
- Thermal
- Type

phys.physpkg.Fan

- Name
- HWRevision
- RelativePosition
- SerialNumber

phys.physpkg.PhysicalFrame

phys.physpkg.PowerSupply

- Name
- HWRevision
- RelativePosition
- SerialNumber

sys.ComputerSystem

Configuration du détecteur

Fix Pack 2

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès : Fix Pack 2

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour les reconnaissances SNMP V1 et V2, entrez la chaîne de communauté appropriée dans la liste d'accès.

  Pour cela, vous pouvez utiliser le type de composant (SNMP) du modèle de réseau dans la fenêtre Liste d'accès de la console de gestion de reconnaissance.
- Pour les reconnaissances SNMP V3, entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects dans la liste d'accès, en fonction des informations de mappage de données d'identification SNMP V3 dans le tableau suivant.

Tableau 22. Mappage des données d'identification SNMP V3.

Mappez à partir de ce qui suit :	Vers ce qui suit :
Type d'authentification (par exemple MD5)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

  Pour cela, vous pouvez utiliser le type de composant (SNMPV3) dans la fenêtre Liste d'accès de la console de gestion de reconnaissance.

Configuration du profil de reconnaissance : Fix Pack 2

Cette rubrique décrit comment configurer le profil de reconnaissance.

Vous pouvez configurer le profil de reconnaissance de CiscoUCSSensor dans la console de gestion de reconnaissance en définissant les attributs suivants :

snmpPort
Numéro du port utilisé pour la communication SNMP. La valeur par défaut est `161`.

snmpTimeout
Délai d'attente utilisé pour une requête SNMP unique. La valeur par défaut est `20000` (secondes).

locale Environnement local utilisé pour les requêtes SNMP.

characterEncoding
Codage de caractères utilisé pour les requêtes SNMP.

Lorsque CiscoUCSSensor est activé, vous devez également activer SnmpLightSensor ou SnmpMIB2Sensor pour permettre le fonctionnement correct du détecteur CiscoUCSSensor.

Pour plus d'informations sur les profils de reconnaissance, voir la rubrique *Création de profils de reconnaissance* dans le *Guide d'utilisation* de TADDM.

Identification et résolution des problèmes liés au détecteur

Fix Pack 2

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur SNMP Cisco UCS et propose des solutions à ces problèmes.

Une erreur de délai d'attente SNMP se produit

Problème

Le détecteur génère une erreur de dépassement de délai d'attente SNMP durant la reconnaissance.

Solution

Augmentez la valeur du paramètre `snmpTimeout` pour le détecteur CiscoUCSSensor à l'aide de la console de gestion de reconnaissance.

Détecteur de réseau local virtuel Cisco

Le détecteur de réseau local virtuel Cisco utilise Cisco VLAN Membership MIB pour reconnaître le contenu du réseau local virtuel.

Le détecteur SnmpMib2Sensor appelle le CiscoVlanSensor lorsque des réseaux locaux virtuels sont configurés pour des périphériques Cisco. Le détecteur CiscoVlanSensor appelle ensuite BridgeSnmpSensor2 pour chaque réseau local virtuel à l'aide du protocole Ethernet. Ce détecteur reconnaît la table d'appartenance au réseau local virtuel, crée des interfaces L2Interface et les connecte au pont de réseau local virtuel.

Remarque : Les réseaux locaux virtuels et les réseaux en anneau à jeton par défaut ne génèrent pas de BridgeSnmpSensor2.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CiscoVlanSensor

ID objets (OID) utilisés

Ce détecteur respecte les normes documentées dans la RFC 1286 pour obtenir l'interface de réseau local virtuel. Les OID de haut niveau interrogés sont les suivants :

- OID .1.3.6.1.4.1.9.9.68.1.2.2.1.2 pour obtenir la table d'appartenance au réseau local virtuel
- OID .1.3.6.1.4.1.9.9.46.1.2.1.1 pour obtenir la table de domaine de gestion
- OID .1.3.6.1.4.1.9.9.46.1.3.1.1 pour obtenir la table de réseau local virtuel vtp
- OID .1.3.6.1.4.1.9.9.46.1.6.1.1 pour obtenir les informations relatives au port de liaison du réseau local virtuel.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Vlan
- net.VlanInterface
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

- Pour permettre à TADDM d'exécuter une reconnaissance complète, SNMP et telnet doivent être activés. Vous devez configurer l'accès Telnet avec un nom d'utilisateur et un mot de passe, et vous devez activer le mot de passe.

Détecteur CiscoWorks

Le détecteur CiscoWorks collecte des données pour des serveurs CiscoWorks.

Ce détecteur fonctionne en appelant le servlet RME.

Nom du détecteur utilisé dans l'interface graphique et les journaux

CiscoWorksSensor, CiscoWorks405FileSensor, CiscoWorks405FileUDS, CiscoWorks405UDS, CiscoWorksFileSensor, CiscoWorksFileUDS et CiscoWorksUDS

Limitations

Le détecteur CiscoWorks ne reconnaît pas CiscoWorks LMS ou Cisco Prime LMS quand le mode (HTTPS) sécurisé est activé pour le serveur CiscoWorks ou le serveur principal Cisco.

Commandes exécutées par le détecteur

Le détecteur envoie la méthode de requête HTTP POST à l'URL suivante :

`http://<IP Cisco Works>:1741/rme/cwcli`

Le contenu contient la commande **cwcli export inventory**.

Objets de modèle avec attributs associés

Le détecteur CiscoWorks crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les éléments de configuration à partir des serveurs CiscoWorks.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet modèle.

net.IpAdress

- DotNotation

net.IpInterface

- IpAddress
- L2Interface

net.L2Interface

- Description
- Encapsulation
- HwAddress
- Name

net.Router

- Forwarding
- Name

sys.OperatingSystem

- Description
- Name
- OSName
- OSVersion

sys.UnitaryComputerSystem

- Functions
- Manufacturer
- Model
- Name
- OSRunning
- SerialNumber
- Type

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Pour **Component Type**, entrez **CiscoWorks**.
2. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur
   b. Mot de passe

Identification et résolution des problèmes liés au détecteur

Découvrez les incidents courants pouvant survenir avec le détecteur CiscoWorks et comment les corriger.

Format XML invalide

Problème

Lorsque vous tentez de créer des objets modèles, l'erreur suivante se produit :

```
CTJTD0652E La transformation suivante ne s'est pas effectuée correctement :
CTJTP2203E Le serveur ne peut pas créer d'objets modèles : [PLATFORM.XML.E.1]
L'application est incapable d'analyser l'entrée xml.. .
```

Solution

La cause de l'incident est le guillemet d'ouverture (") trouvé dans la configuration CiscoWorks. Ce caractère n'est pas pris en charge. Pour corriger le problème, supprimez le guillemet d'ouverture de la configuration.

détecteur Entity MIB

Le détecteur Entity MIB ne peut reconnaître que les périphériques connues. Elle respecte les normes qui sont documentées dans RFC 2737 pour extraire certaines des informations de configuration physique relatives au périphérique.

Le détecteur Entity MIB collecte les données qui figurent sous l'onglet Package physique du panneau Détails. Ces données permettent de stocker des informations sur les composants physique du périphérique comme un emplacement, un ventilateur, une trame physique, des détecteurs, des connecteurs physiques, un châssis, une armoire et une alimentation électrique.

Le détecteur interroge les OID suivants :

```
.1.3.6.1.2.1.47.1.1.1.1.2, .1.3.6.1.2.1.47.1.1.1.1.3, .1.3.6.1.2.1.47.1.1.1.1.4,
.1.3.6.1.2.1.47.1.1.1.1.5, .1.3.6.1.2.1.47.1.1.1.1.6, .1.3.6.1.2.1.47.1.1.1.1.7,
.1.3.6.1.2.1.47.1.1.1.1.8, .1.3.6.1.2.1.47.1.1.1.1.9, .1.3.6.1.2.1.47.1.1.1.1.10,
.1.3.6.1.2.1.47.1.1.1.1.11, .1.3.6.1.2.1.47.1.1.1.1.12, .1.3.6.1.2.1.47.1.1.1.1.13.
```

Le détecteur collecte aussi `.1.3.6.1.2.1.55.1.1.0.`, qui contient les informations IPv6 conformément à RFC 2466. L'OID `.1.3.6.1.2.1.17.4.3.1.1` renvoie la liste des OID pour les adresses MAC connues. Ces OID sont ensuite interrogées pour déterminer l'interface permettant d'accéder au périphérique MAC.

Si le détecteur SNMP MIB2 est également exécuté, des informations supplémentaires sont collectées et affichées sous les onglets Détails sur le routeur, Détails sur le pont, IP et Ports.

Nom du détecteur utilisé dans l'interface graphique et les journaux

EntityMIBSensor

ID objets (OID) utilisés

Le détecteur utilise les OID suivants :

- .1.3.6.1.2.1.47.1.1.1.1.2
- .1.3.6.1.2.1.47.1.1.1.1.3
- .1.3.6.1.2.1.47.1.1.1.1.4

- .1.3.6.1.2.1.47.1.1.1.1.5
- .1.3.6.1.2.1.47.1.1.1.1.6
- .1.3.6.1.2.1.47.1.1.1.1.7
- .1.3.6.1.2.1.47.1.1.1.1.8
- .1.3.6.1.2.1.47.1.1.1.1.9
- .1.3.6.1.2.1.47.1.1.1.1.10
- .1.3.6.1.2.1.47.1.1.1.1.11
- .1.3.6.1.2.1.47.1.1.1.1.12
- .1.3.6.1.2.1.47.1.1.1.1.13

Le détecteur interroge l'OID .1.3.6.1.2.1.55.1.1.0. qui contient les informations IPV6 information conformément à RFC 2466. Le détecteur interroge également l'OID .3.6.1.2.1.17.4.3.1.1. qui renvoie la liste des OID pour les adresses MAC connues. Ces OID sont ensuite interrogés pour obtenir l'interface permettant d'accéder au périphérique MAC.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- phys.physconn.Slot
- physconn.PhysicalConnector
- physpkg.Chassis
- physpkg.Fan
- physpkg.PhysicalFrame
- physpkg.PhysicalPackage
- physpkg.otherPhysicalPackage
- physpkg.PowerSupply
- physpkg.Sensor
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur de réseau local virtuel Extreme

Le détecteur de réseau local virtuel Extreme extrait des informations de réseau local virtuel à partir des commutateurs Extreme Networks.

Le détecteur SnmpMib2Sensor appelle le détecteur ExtremeVlanSensor lorsque des réseaux locaux virtuels sont configurés pour ce périphérique.

Nom du détecteur utilisé dans l'interface graphique et les journaux

ExtremeVlanSensor

ID objets (OID) utilisés

Le détecteur utilise les OID suivants :

- L'OID .1.3.6.1.4.1.1916.1.2.1.2.1 permet d'interroger les informations extremeVlanInterface.
- L'OID .1.3.6.1.4.1.1916.1.2.3.1.1 permet d'interroger les informations d'interface d'encapsulation (de liaison).
- L'OID .1.3.6.1.2.1.31.1.2.1 permet d'interroger les informations de pile d'interface.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- sys.UnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Détecteur IBM BladeCenter SNMP

Le détecteur SNMP IBM BladeCenter reconnaît et collecte des informations de configuration sur le châssis IBM BladeCenter. Dans TADDM 7.3.0.3 et versions ultérieures, ce détecteur reconnaît et collecte également des informations de configuration sur le châssis IBM PureFlex System.

Ce détecteur utilise le protocole SNMP (Simple Network Management Protocol) pour reconnaître et interroger les composants d'infrastructure BladeCenter. Le module de gestion (MM, Management Module) et le module de gestion avancé (AMM, Advanced Management Module) constituent les points centraux de gestion pour le châssis IBM BladeCenter.

Fix Pack 3 Le module de gestion de châssis (CMM, Chassis Management Module) constitue le point central de gestion pour le châssis PureFlex.

Nom du détecteur utilisé dans l'interface graphique et les journaux

BladeCenterSnmpSensor

Limitations

Les limitations suivantes s'appliquent à la reconnaissance des châssis IBM BladeCenter et IBM PureFlex System :

- Le détecteur ne peut pas reconnaître un châssis si les modules de gestion ne répondent pas.
- Ce détecteur ne peut pas reconnaître les systèmes BladeCenter dotés de deux interfaces réseau configurées (eth0 et eth1).
- Vous ne pouvez pas démarrer la première reconnaissance de système BladeCenter par rapport à une base de données vide. Les détecteurs de systèmes informatiques qui reconnaissent les systèmes d'exploitation s'exécutant sur des composants blade (tels que Linux et Windows) doivent être exécutés en premier. Cette limitation ne s'applique qu'à la première reconnaissance de BladeCenter.
- Il est possible que le détecteur ne parvienne pas à obtenir des données VDP (Vital Product Data) suffisantes par rapport aux modules Redundant Management Module pour créer certains objets de modèle. Par exemple, il est possible que des instances des classes `ComputerSystem` et `BladeCenterManagementModule` représentant des modules de gestion redondants ne puissent pas être créées. Dans ce cas, des instances de la classe `Board` représentent le module.
- Après la reconnaissance d'un ou de plusieurs systèmes BladeCenter à l'aide du détecteur BladeCenter, les composants BladeCenter et BladeCenter Management Module ne figurent pas dans la liste des types de composant utilisables avec les requêtes personnalisées. Cela signifie que vous ne pouvez pas exécuter une requête personnalisée pour ces types de composant. Ce problème ne concerne que le portail de gestion de données et non la console de gestion de reconnaissance TADDM.
- Le système BladeCenter ne possède pas d'interfaces L2 mais des modules de gestion avec ce type d'interface. Pour afficher les interfaces L2 des modules de gestion figurant dans le système BladeCenter, procédez comme suit :
  1. Dans la sous-fenêtre **Détails**, cliquez sur l'onglet **Boîtier** pour ouvrir le classeur Boîtier.
  2. Cliquez sur l'onglet **MM** pour ouvrir le classeur Module de gestion.

3. Dans la colonne **Système informatique**, cliquez sur BladeCenter Management Module.
4. Cliquez sur l'onglet **IP** pour afficher les détails sur l'interface L2.

Fix Pack 3 Les limitations suivantes s'appliquent à la reconnaissance des châssis IBM PureFlex System uniquement :

- Lorsque le châssis IBM PureFlex System contient le système de stockage IBM Storwize v7000, le détecteur reconnaît les marques de réservation pour les armoires de stockage. La reconnaissance complète des informations concernant ce système de stockage implique également l'exécution du détecteur de stockage SVC. Les données reconnues par le détecteur de stockage SVC sont synchronisées avec ces marques de réservation.
- Lorsque vous reconnaissez le châssis IBM PureFlex System, l'objet de modèle `sys.blade.Alert` n'est pas créé.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- enums.AlertLevelEnum
- enums.PhysTypeEnum
- enums.SlotStateEnum
- IpAddress net
- L2Interface
- net.BindAddress
- net.Fqdn net
- phys.physconn.PhysicalConnector
- phys.physconn.Slot
- phys.physpkg.Board
- phys.physpkg.Chassis
- phys.physpkg.Fan
- phys.physpkg.PhysicalFrame
- phys.physpkg.PowerSupply
- sys.blade.Alert
- sys.blade.BladeCenterManagementModule
- sys.blade.LoginProfile
- sys.ComputerSystem
- sysControlSoftware
- sys.DNSService
- sys.LDAPService
- sys.ServiceAccessPoint
- sys.SMTPService

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Vous pouvez configurer le détecteur BladeCenterSnmpSensor à l'aide de la console de gestion de reconnaissance en définissant les attributs suivants :

snmpPort
Numéro du port utilisé pour la communication SNMP. La valeur par défaut est 161.

snmpTimeout
Délai d'attente utilisé pour une requête SNMP unique. La valeur par défaut est 20000.

locale Environnement local utilisé pour les requêtes SNMP.

characterEncoding
Codage de caractères utilisé pour les requêtes SNMP.

scanL2Interfaces
Obtient les interfaces L2 du châssis, lorsqu'elles sont activées.

Pour plus d'informations, voir la rubrique *Création de profils de reconnaissance* dans le *Guide d'utilisation* de TADDM.

Lorsque BladeCenterSnmpSensor est activé, vous devez également activer SnmpLightSensor ou SnmpMIB2Sensor pour permettre le fonctionnement correct du détecteur BladeCenterSnmpSensor.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur SNMP IBM BladeCenter et propose des solutions à ces problèmes.

Une erreur de délai d'attente SNMP se produit

Problème

Le détecteur génère une erreur de délai d'attente SNMP durant la reconnaissance.

Solution

Utilisez la console de gestion de reconnaissance pour augmentez le paramètre snmpTimeout pour le détecteur BladeCenterSnmpSensor.

détecteur LAN Manager SNMP

Le détecteur SNMP du gestionnaire de réseau local reconnaît un gestionnaire de réseau local et extrait les informations contenues dans les bases de données d'informations de gestion (MIB) SNMP du gestionnaire de réseau local.

Nom du détecteur utilisé dans l'interface graphique et les journaux

LanManagerSnmpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- .1.3.6.1.4.1.77.1.1.1.0
- .1.3.6.1.4.1.77.1.1.2.0
- .1.3.6.1.4.1.77.1.2.3.1.1
- .1.3.6.1.4.1.77.1.2.3.1.2
- .1.3.6.1.4.1.77.1.2.3.1.3
- .1.3.6.1.4.1.77.1.2.3.1.4
- .1.3.6.1.4.1.77.1.2.3.1.5

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.windows.WindowsComputerSystem
- sys.windows.WindowsOperatingSystem
- sys.windows.WindowsService

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	Vers ce qui suit :
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur LDAP

Le détecteur LDAP reconnaît les serveurs LDAP.

Le détecteur LDAP reconnaît toujours une instance LDAP par hôte.

Nom du détecteur utilisé dans l'interface graphique et les journaux

LdapSensor

Objets de modèle créés

Le détecteur crée l'objet de modèle sys.LDAPSAP.

Pour reconnaître tous les attributs, l'utilisateur spécifié dans le liste d'accès doit avoir accès à la sous-arborescence `cn=monitor` sur le serveur LDAP et la sous-arborescence `cn=monitor` doit exister.

Configuration du détecteur

Avant d'exécuter une reconnaissance, vous devez configurer le détecteur LDAP.

Définition des paramètres de configuration du détecteur :

Vous pouvez configurer le comportement du détecteur LDAP en définissant des paramètres de configuration.

Pour modifier la configuration du détecteur, configurez les paramètres suivants :

tryInsecureConnection
Indique s'il faut utiliser une connexion non sécurisée. La valeur par défaut de cette propriété est `true`.

Si ce paramètre est défini à `true`, dans ce cas, lorsque le détecteur se connecte via le protocole LDAPS ou StartTLS et échoue, le détecteur tente de se connecter à LDAP à l'aide d'un protocole standard. Si cette propriété est définie à `false`, le détecteur tente de se connecter à l'aide du protocole LDAPS ou StartTLS uniquement.

Pour plus d'informations sur la configuration des ports LDAP, voir «Configuration des entrées du fichier `collation.properties`», à la page 316.

bypassHostVerification
Indique s'il faut ignorer la procédure de vérification. La valeur par défaut de cette propriété est `true`.

Si cette propriété est définie à `true` et si LDAP est reconnu à l'aide du protocole StartTLS, l'étape de négociation ignore la procédure de vérification de l'hôte. Le détecteur accepte les certificats signés pour un nom d'hôte ou une adresse IP différente du serveur cible qui a été fournie dans la portée utilisée pour la reconnaissance. Si cette propriété est définie à `false`, le détecteur tente d'exécuter la négociation TLS en utilisant l'adresse IP de l'hôte cible.

Configuration de la liste d'accès :

Selon votre configuration, vous devez fournir les détails d'accès nécessaires.

Pour configurer la liste d'accès, procédez comme suit :

1. Pour **Type de composant**, entrez **Service LDAP**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM utilise pour l'authentification auprès du serveur LDAP.
3. Eventuellement, s'il s'agit d'un LDAP sécurisé par les protocoles LDAPS ou StartTLS, fournissez les paramètres SSL, c'est-à-dire un certificat de fichiers de clés certifiées et son mot de passe.

Utilisation de la couche Secure Sockets Layer (SSL)
Le détecteur utilise la première entrée de liste pour se connecter au service LDAP. Pour imposer l'utilisation de la couche Secure Sockets Layer (SSL) placez une entrée d'accès SSL pour LDAP avant les entrées avec des données d'identification standard ou définissez la propriété `tryInsecureConnection` à `false`.

L'installation peut échouer si **SSL** est appliqué. Par défaut, **http** est utilisé (http est codé en dur dans DownloadFilesDeomPrimaryServerAction).

Limitation des fichiers de clés certifiées
En raison d'une limitation de Java, TADDM ne peut gérer qu'un seul fichier de clés certifiées pour une reconnaissance unique du service LDAP. Les certificats qui sont enregistrés dans le fichier de clés certifiées sont chargés lorsque la connexion avec le service LDAP est établie. Seuls ces certificats peuvent être utilisés par TADDM lors d'une reconnaissance entière. Si les certificats de plusieurs fichiers de clés certifiées sont requis, ne les associez pas séparément dans la liste d'accès. Vous devez exporter les fichiers de clés certifiées dans un fichier unique. Lorsque toutes les entrées nécessaires pour chaque serveur LDAP sont dans la liste d'accès TADDM, la première doit avoir le fichier de clés certifiées exporté. Il existe toujours une entrée pour chaque combinaison connexion et mot de passe pour les serveurs LDAP reconnus.

Configuration des entrées du fichier `collation.properties` :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur LDAP.

Le détecteur LDAP utilise les paramètres de détecteur suivant :

`com.collation.ldapsensor.ports.ldaps=636`
Spécifie une liste de ports séparés par des virgules sur laquelle LDAP est exécuté à l'aide du protocole LDAPS.

`com.collation.ldapsensor.ports.starttls=389`
Spécifie une liste de ports séparés par des virgules sur laquelle LDAP est exécuté à l'aide du protocole StartTLS.

Remarque :

- Si la propriété `tryInsecureConnection` est définie à `true` dans la configuration du détecteur, le détecteur tente de se connecter aux ports précédents également en utilisant un protocole LDAP standard, à partir des ports StartTLS.
- PortSensor utilise également les valeurs des deux propriétés pour déterminer quels ports sont ouverts.
- Vous pouvez également définir les deux valeurs sous l'onglet **Propriétés de plateforme** dans des profils.
- Ces propriétés sont des propriétés sectorisées et peuvent être définies pour une adresse IP spécifique de machines cible, par exemple `com.collation.ldapsensor.ports.ldaps.192.168.5.4=755,234,524`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur LDAP et propose des solutions à ces problèmes.

Erreur survenue durant une reconnaissance

Problème

La reconnaissance du détecteur se termine avec le message d'erreur suivant :

```
CTJTD0421E Le serveur LDAP contient les attributs inattendus suivants :
javax.naming.AuthenticationNotSupportedException: [LDAP: error code 13 - confidentiality required]
```

Solution

Le serveur LADP nécessite un chiffrement. Le détecteur LADP ne peut pas effectuer de reconnaissance si le serveur LADP nécessite un chiffrement, désactivez le chiffrement sur le serveur LADP.

Impossible pour le détecteur d'afficher toutes les informations des attributs

Problème

Les informations suivantes relatives aux attributs ne sont pas affichées après l'exécution d'une reconnaissance : `Version LDAP`, `Unités d'exécution` et `Nombre total de connexions`.

Solution

Activer le moniteur d'applications LDAP pour reconnaître `Version LDAP`, `Unités d'exécutionet Nombre total de connexions`.

Instances LDAPService en doublons

Problème

Lorsque le port d'écoute du serveur LDAP change entre deux reconnaissances, des instances LDAPService pourraient apparaître en doublons après chaque reconnaissance.

Solution

Ajoutez à la liste d'accès des données d'identification de session du serveur cible. Vérifiez si les détecteurs de système informatique (ComputerSystem), comme LinuxComputerSystemSensor, sont activés dans le profil de reconnaissance. Après l'exécution de l'agent LDAPServiceAgent, les instances LDAPService sont fusionnées, si reconnues sur le même hôte.

Détecteur Link Layer Discovery Protocol

Le détecteur LLDP (Link Layer Discovery Protocol) utilise la base d'informations de gestion (MIB) pour reconnaître des segments de couche 2 sur le réseau.

LldpSensor reconnaît des informations lldpLocalSystemData, lldpLocPortTable et lldpRemTable et génère l'interface locale pour les périphériques homologues. Cette interface est utilisée pour générer le segment.

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Nom du détecteur utilisé dans l'interface graphique et les journaux

LldpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- lldpLocChassisIdSubtype : .1.0.8802.1.1.2.1.3.1
- lldpLocChassisId : .1.0.8802.1.1.2.1.3.2
- lldpLocSysName : .1.0.8802.1.1.2.1.3.3
- lldpLocPortNum: .1.0.8802.1.1.2.1.3.7.1.1
- lldpLocPortIdSubtype : .1.0.8802.1.1.2.1.3.7.1.2
- lldpLocPortId : .1.0.8802.1.1.2.1.3.7.1.3
- lldpLocPortDesc : .1.0.8802.1.1.2.1.3.7.1.4
- lldpRemTableIdx : .1.0.8802.1.1.2.1.4.1.1.1
- lldpRemChassisIdSubtype : .1.0.8802.1.1.2.1.4.1.1.4
- lldpRemChassisId : .1.0.8802.1.1.2.1.4.1.1.5
- lldpRemPortIdSubtype : .1.0.8802.1.1.2.1.4.1.1.6
- lldpRemPortId : .1.0.8802.1.1.2.1.4.1.1.7
- lldpRemPortDesc : .1.0.8802.1.1.2.1.4.1.1.8

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.L2Interface
- net.Segment
- sys.ComputerSystem

détecteur NetScreen SNMP

Le détecteur NetScreen SNMP reconnaît la configuration NAT à partir des périphériques Juniper Networks NetScreen, puis extrait les valeurs de service comme ServiceIndex, serviceName et ServiceTransProto à partir de NetScreen et recherche l'élément virtualservice.

Le détecteur NetScreenSNMPSensor utilise les bases d'informations de gestion de Netscreen SNMP.

Nom du détecteur utilisé dans l'interface graphique et les journaux

NetscreenSnmpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- .1.3.6.1.4.1.3224.11.1.1.1
- .1.3.6.1.4.1.3224.11.1.1.2
- .1.3.6.1.4.1.3224.11.1.1.3
- .1.3.6.1.4.1.3224.11.1.1.4
- .1.3.6.1.4.1.3224.11.1.1.5
- .1.3.6.1.4.1.3224.11.1.1.6
- .1.3.6.1.4.1.3224.13.1.1.1
- .1.3.6.1.4.1.3224.13.1.1.2
- .1.3.6.1.4.1.3224.13.1.1.4
- .1.3.6.1.4.1.3224.13.1.1.5
- .1.3.6.1.4.1.3224.13.1.1.6
- .1.3.6.1.4.1.3224.13.1.1.7
- .1.3.6.1.4.1.3224.13.1.1.8
- .1.3.6.1.4.1.3224.11.3.1.1.1
- .1.3.6.1.4.1.3224.11.3.1.1.2
- .1.3.6.1.4.1.3224.11.3.1.1.3
- .1.3.6.1.4.1.3224.11.3.1.1.4
- .1.3.6.1.4.1.3224.11.3.1.1.5
- .1.3.6.1.4.1.3224.11.3.1.1.6
- .1.3.6.1.4.1.3224.11.3.2.1.1
- .1.3.6.1.4.1.3224.11.3.2.1.2
- .1.3.6.1.4.1.3224.11.3.2.1.3
- .1.3.6.1.4.1.3224.11.3.2.1.5
- .1.3.6.1.4.1.3224.11.3.2.1.6

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.vip.RealServer
- net.vip.RealServerGroup
- net.vip.Vip
- net.vip.VipFunction
- net.vip.VirtualService
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.

2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur Nokia SNMP

Le détecteur Nokia SNMP reconnaît les informations contenues dans les bases d'informations de gestion de Nokia SNMP.

NokiaSNMPSensor reconnaît les configurations de liste de contrôle d'accès (règles ACL) et les interfaces mappées pour les périphériques Nokia SNMP en fonction du nom de domaine complet, de la signature et de ID_Objet.

Nom du détecteur utilisé dans l'interface graphique et les journaux

NokiaSnmpSensor

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- .1.3.6.1.4.1.94.1.16.4.1.1.1.1
- .1.3.6.1.4.1.94.1.16.4.1.1.1.2
- .1.3.6.1.4.1.94.1.16.4.1.1.1.3
- .1.3.6.1.4.1.94.1.16.4.1.1.1.4
- .1.3.6.1.4.1.94.1.16.4.1.1.1.5
- .1.3.6.1.4.1.94.1.16.4.2.1.1.1
- .1.3.6.1.4.1.94.1.16.4.2.1.1.2
- .1.3.6.1.4.1.94.1.16.4.2.1.1.3
- .1.3.6.1.4.1.94.1.16.4.2.1.1.4
- .1.3.6.1.4.1.94.1.16.4.2.1.1.5
- .1.3.6.1.4.1.94.1.16.4.2.1.1.6
- .1.3.6.1.4.1.94.1.16.4.2.1.1.7
- .1.3.6.1.4.1.94.1.16.4.2.1.1.8
- .1.3.6.1.4.1.94.1.16.4.2.1.1.9
- .1.3.6.1.4.1.94.1.16.4.2.1.1.10
- .1.3.6.1.4.1.94.1.16.4.2.1.1.11
- .1.3.6.1.4.1.94.1.16.4.2.1.1.12
- .1.3.6.1.4.1.94.1.16.4.2.1.1.13
- .1.3.6.1.4.1.94.1.16.4.2.1.1.14
- .1.3.6.1.4.1.94.1.16.4.2.1.1.15

- .1.3.6.1.4.1.94.1.16.4.2.1.1.16

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.acl.Acl
- net.acl.AclFunction
- net.acl.Rule
- net.L2Interface
- sys.ComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur PIX

Le détecteur PIX reconnaît les périphériques Cisco PIX utilisés comme pare-feu IP et dispositifs de conversion d'adresses réseau.

Le détecteur PIX collecte des données sur le système d'exploitation CiscoPIX exécuté sur les unités PIX. Le détecteur effectue également les actions suivantes :

- Reconnaît tous les serveurs réels et les services virtuels en cours d'exécution. Les serveurs réels sont rassemblés dans le groupe de serveurs réels.
- Reconnaît les éléments virtualIp, realIp, virtualPort et realPort, et identifie les adresses IP virtuelles qui les utilisent. Les adresses IP virtuelles sont stockées dans la table Vip.

Nom du détecteur utilisé dans l'interface graphique et les journaux

- CiscoApplianceVersionSensor
- PixSensor

Prérequis

Pour les configurations avec plusieurs configurations de contexte, indiquez dans la portée de la reconnaissance l'adresse IP de «admin context.»

Limitations

Si des topologies sont affichées, les limitations suivantes s'appliquent :

- Pour des configurations de contexte, la même icône représente les contextes virtuels et d'administration.
- Dans la vue de topologie d'infrastructure physique, la connexion entre la «contexte d'administration» et le «contexte virtuel» n'apparaît pas. Cette connexion s'affiche dans la vue de topologie contextuelle.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- cisco.CiscoPixComputerSystem
- core.LogicalContent
- net.L2Interface
- sys.OperatingSystem
- vip.RealServer
- vip.RealServerGroup
- vip.Vip
- vip.VipFunction
- vip.VirtualService

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **Unité Cisco** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur, mot de passe et mot de passe d'activation) que TADDM doit utiliser pour l'authentification à l'unité PIX cible.

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur PIX.

com.collation.pix.pager.command

Cette valeur spécifie l'utilisation de la commande **pager** pour forcer PIX à renvoyer la réponse complète en une seule fois, au lieu de sur un écran à la fois. Ajoutez cette entrée, s'il n'est pas possible d'exécuter la commande **configure terminal**.

détecteur SNMP Light

Le détecteur SNMP Light prend en charge une reconnaissance de niveau 1 des périphériques réseau SNMP.

Dans les profils de reconnaissance de niveau 1, utilisez le détecteur SNMP Light avec le détecteur d'analyse de piles pour améliorer la précision de la

reconnaissance. Dans les profils de niveau 2 ou de niveau 3, utilisez le détecteur SNMP MIB2, qui reconnaît des données supplémentaires pour la génération de topologies détaillées de niveau 2.

Le détecteur SNMP Light collecte les informations affichées sous les onglets suivants du panneau Détails :

- Général
- Informations SNMP

Le détecteur SNMP Light et le détecteur SNMP MIB2 collectent des informations génériques des identificateurs d'objets suivants (OID) :

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-JK9SV-M), Version 12.2(17d)SXB11,
   RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled T

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "Y1UN9;4b/1tz9l#"
   10.199.250.9 .1.3.6.1.2.1.1.2.0
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.400

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "Y1UN9;4b/1tz9l#"
   10.199.250.9 .1.3.6.1.2.1.1.4.0
SNMPv2-MIB::sysContact.0 = STRING: Network Support - CH

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: NC89ZNC01TSL302

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.6.0
SNMPv2-MIB::sysLocation.0 = STRING: NC89ACB01
```

Nom du détecteur utilisé dans l'interface graphique et les journaux

SnmpLightSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.UnitaryComputerSystem
- sys.OperatingSystem
- sys.SnmpSystemGroup

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.

2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

détecteur SNMP MIB2

Le détecteur SNMP MIB2 prend en charge une reconnaissance de niveau 2 des périphériques réseau SNMP.

Dans les profils de reconnaissance de niveau 1, utilisez le détecteur SNMP Light avec le détecteur d'analyse de piles pour améliorer la précision de la reconnaissance. Dans les profils de niveau 2 ou de niveau 3, utilisez le détecteur SNMP MIB2, qui reconnaît des données supplémentaires pour la génération de topologies détaillées de niveau 2.

Le détecteur SNMP MIB2 reconnaît les informations SNMP de base sur le périphérique ainsi que d'autres informations comme les détails du routeur, les détails du pont, les données IP (à la fois IPv4 et IPv6) et les données de port. Le détecteur SNMP MIB2 appelle le détecteur Entity MIB et le détecteur Bridge SNMP s'ils sont activés dans le profil de reconnaissance.

D'autres détecteurs sont appelées puisque le détecteur SNMP MIB2 détecte les périphériques qui prennent en charge TADDM (par exemple, le détecteur de port Cisco et le détecteur de réseau local virtuel Cisco sont appelées si un périphérique Cisco est détecté).

Le détecteur SNMP MIB2 collecte les informations affichées sous les onglets suivants du panneau Détails :

- Général
- Informations SNMP
- Caractéristiques du routeur IPv6
- Caractéristiques du routeur IPv4
- Protocole IP
- Interfaces

Le détecteur SNMP Light et le détecteur SNMP MIB2 collectent des informations génériques des identificateurs d'objets suivants (OID) :

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-JK9SV-M), Version 12.2(17d)SXB11,
   RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled T
```

```
snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "Y1UN9;4b/1tz9l#"
   10.199.250.9 .1.3.6.1.2.1.1.2.0
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.400

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "Y1UN9;4b/1tz9l#"
   10.199.250.9 .1.3.6.1.2.1.1.4.0
SNMPv2-MIB::sysContact.0 = STRING: Network Support - CH

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: NC89ZNC01TSL302

snmpwalk -v 3 -u cmdbadmin -l authPriv -a MD5 -A "" -x DES -X "" 10.199.250.9
   .1.3.6.1.2.1.1.6.0
SNMPv2-MIB::sysLocation.0 = STRING: NC89ACB01
```

Le détecteur SNMP MIB2 reconnaît les informations IPv4 et IPv6. A l'aide des modules IP-MIB et IP-FORWARD-MIB (mis à jour dans RFC 4293 et RFC 4292), le détecteur collecte des informations sur l'interface IP, le transfert et le routage. Les OID suivants sont interrogés :

```
1.3.6.1.2.1.4.34 IP-MIB (ipAddressTable)
1.3.6.1.2.1.4.32 IP-MIB (ipAddressPrefixTable)
1.3.6.1.2.1.4.25 IP-MIB (ipv6IpForwarding)
1.3.6.1.2.1.4.1  IP-MIB (ipForwarding)
1.3.6.1.2.1.4.24.7 IP-FORWARD-MIB (inetCidrRouteTable)
```

ipAddressTable
Cette table répertorie les adresses IPv4 et IPv6.

ipAddressPrefixTable
Cette table répertorie les informations de préfixe de toutes les adresses.

ipv6IpForwarding
Cet indicateur indique si le périphérique cible agit comme un routeur pour transférer des paquets IPv6.

ipForwarding
Cet indicateur indique si le périphérique cible agit comme un routeur pour transférer des paquets IPv4.

inetCidrRouteTable
Cette table de routage IP répertorie les routes pour les interfaces IPv4 et IPv6.

Si le périphérique cible prend en charge les versions nécessaires des modules IP-MIB et IP-FORWARD-MIB, le détecteur SNMP MIB2 collecte toutes les informations requises et la reconnaissance se termine. Si le périphérique cible ne prend pas en charge les versions nécessaires de ces modules, les versions plus anciennes (RFC 2011 et RFC 1213), qui ne collectent que les informations IPv4, sont alors utilisées, et les OID suivants sont interrogés :

```
1.3.6.1.2.1.4.20 IP-MIB (ipAddrTable)
1.3.6.1.2.1.4.1  IP-MIB (ipForwarding)
1.3.6.1.2.1.4.21 RFC1213-MIB (ipRouteTable)
```

En outre, s'il s'agit d'un périphérique cible Cisco, les modules CISCO-IETF-IP-MIB et CISCO-IETF-IP-FORWARDING-MIB sont utilisés pour ne collecter que les informations IPv6, et les OID suivants sont interrogés :

```
1.3.6.1.4.1.9.10.86.1.1.2 CISCO-IETF-IP-MIB (cIpAddressTable)
1.3.6.1.4.1.9.10.86.1.1.1 CISCO-IETF-IP-MIB (cIpAddressPfxTable)
1.3.6.1.4.1.9.10.86.1.2.1 CISCO-IETF-IP-MIB (cIpv6Forwarding)
1.3.5.1.4.9.10.85.7 CISCO-IETF-IP-FORWARD-MIB (cInetCidrRouteTable)
```

Nom du détecteur utilisé dans l'interface graphique et les journaux

SnmpMib2Sensor

Limitations

TADDM prend en charge actuellement un nombre limité de périphériques réseau. En outre, les commutateurs L2 TADDM sont des commutateurs, alors que les commutateurs L3 sont des routeurs. Ainsi, les commutateurs L3 sont affichés en tant que routeur dans l'arborescence de l'infrastructure physique et dans la topologie.

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.Bridge
- net.IpInterface
- net.IpRoute
- net.IpV4Address
- net.IpV6Address
- net.IpV4Router
- net.IpV6Router
- net.L2Interface
- sys.UnitaryComputerSystem
- sys.OperatingSystem
- sys.SnmpSystemGroup

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.

2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Configuration des entrées du fichier `collation.properties` :

Cette rubrique répertorie les entrées du fichier `collation.properties` que le détecteur SNMP MIB2 utilise.

com.collation.discover.agent.net.SnmpMib2Agent.useEntitySerial
Lorsque vous définissez cette propriété sur `true`, elle permet à TADDM de collecter le numéro de série du détecteur EntityMIB.

TADDM ne prend pas en charge la configuration Cisco autorisée pour l'objet chassisId 1.3.6.1.4.1.9.3.6.3. Par conséquent, une information non valide est définie sur l'attribut SerialNumber pour les appareils réseau. Pour éviter ce problème, ajoutez la propriété `com.collation.discover.agent.net.SnmpMib2Agent.useEntitySerial=true` au fichier `collation.properties`.

com.ibm.cdb.discover.sensor.net.snmpmib2.SnmpMib2Sensor.ifType
Cette propriété permet de créer des relations aux appareils réseau qui utilisent des interfaces virtuelles et qui sont reconnus par le détecteur SNMP MIB2. Par défaut, le détecteur ne stocke pas les interfaces virtuelles pour le traitement. Pour que les relations aux interfaces virtuelles apparaissent dans TADDM, ajoutez cette propriété au fichier `collation.properties`.

La valeur de cette propriété correspond au type d'interface de l'interface virtuelle, spécifié par l'attribut `ifType`. Par exemple, si une interface possède l'attribut `ifType=135`, vous devez ajouter la propriété suivante :

```
com.ibm.cdb.discover.sensor.net.snmpmib2.SnmpMib2Sensor.ifType=135
```

Vous pouvez spécifier une liste de types d'interface séparés par des virgules comme valeur de cette propriété.

Par conséquent, la valeur d'attribut `ifType` est traitée comme un port physique et la relation est créée.

La valeur par défaut est `6, 62, 69, 117`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur SNMP MIB2 et propose des solutions à ces problèmes.

Le détecteur SNMP MIB2 ne démarre pas lorsque le détecteur de session dépasse le délai d'attente

Problème

Lorsque le détecteur de session échoue en raison d'un dépassement de délai d'attente, le détecteur SNMP MIB2 ne démarre pas.

Fix Pack 4 **Solution**

Si le détecteur de session échoue en raison d'un dépassement de délai d'attente, le détecteur SNMP MIB2 ne démarre pas par défaut. Si vous souhaitez modifier ce comportement, définissez la propriété `com.collation.discover.agent.sys.SessionSensor.timeout.snmp` sur `true` dans le fichier `collation.properties`. Pour plus d'informations, voir «Configuration des entrées du fichier collation.properties», à la page 256.

Identification incorrecte des commutateurs L3 en tant que routeurs par le détecteur

Problème

Pour les périphériques SNMP qui ne sont pas encore détectés par TADDM, TADDM identifie occasionnellement par erreur des commutateurs L3 comme des routeurs.

Solution

Utilisez les modèles SNMP pour fournir des indications à TADDM concernant l'identification correcte des commutateurs et des routeurs. Pour plus d'informations sur la manière d'utiliser les modèles SNMP pour fournir des indications à TADDM concernant l'identification correcte du commutateur et la catégorisation des routeurs, voir le *Guide d'utilisation* de TADDM.

Le détecteur ne peut pas effectuer de reconnaissance de système d'exploitation

Problème

Le détecteur ne peut pas effectuer de reconnaissance de système d'exploitation.

Solution

Vérifiez les autorisations d'accès fournies dans la liste d'accès et assurez-vous que SNMP est en cours d'exécution sur le client TADDM.

Un périphérique DataPower reconnu avec SnmpMib2Sensor ne fusionne pas avec des données reconnues par d'autres détecteurs.

Problème

Un périphérique DataPower reconnu avec SnmpMib2Sensor ne fusionne pas avec les données reconnues par d'autres détecteurs.

Solution

Si un périphérique DataPower est configuré pour utiliser le protocole SNMP, il peut être reconnu à l'aide de SnmpMib2Sensor. DataPower utilise cependant un ensemble personnalisé d'OID SNMP que SnmpMib2Sensor n'interroge pas. Ces OID sont lus uniquement par le détecteur CustomMib2ComputerSystem en utilisant un script d'extension Jython.

Pour plus d'informations, voir l'étape 6 de la rubrique *Ajout d'un modèle de système informatique pour un appareil réseau* du *Guide d'utilisation* TADDM.

Pour sécuriser un rapprochement correct avec des données enregistrées par des détecteurs DataPower, VMWare et ZEnterprise dans la console de gestion de reconnaissance, vérifiez les prérequis suivants :

- Vérifiez que le modèle DataPowerComputerSystem est activé dans des modèles de systèmes informatiques (ce qui est le paramètre par défaut).
- Assurez-vous que le détecteur CustomMib2ComputerSystem est activé dans le profil de reconnaissance qui est utilisé pour reconnaître des périphériques DataPower.
- Assurez-vous que les fichiers suivants figurent dans l'installation de TADDM :
  - `etc/templates/commands/DataPowerComputerSystem`
  - `etc/templates/commands/extension-scripts/DataPowerComputerSystem.py`

Détecteurs de systèmes d'exploitation

Les détecteurs de systèmes d'exploitation reconnaissent les systèmes d'exploitation exécutés dans l'environnement.

Détecteur Citrix XenServer

Le détecteur Citrix XenServer reconnaît des plateformes Citrix XenServer. Il s'agit d'un détecteur basé sur un script.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Le détecteur Citrix XenServer est un détecteur basé sur un script. Il démarre après GenericServerSensor. Le détecteur reconnaît un hôte avec une liste de machines virtuelles. Domain 0 est reconnu comme une machine virtuelle et contient le numéro de série et l'identificateur unique universel hérités des matériels des serveurs. D'autres machines virtuelles possèdent un numéro de série et un identificateur unique universel généré par un hyperviseur Xen.

XenServerSensor

Eléments reconnus par le détecteur

Le détecteur Citrix XenServer reconnaît des pools de serveurs, des hôtes dans un pool et des machines virtuelles situées sur tous les hôtes d'un pool.

- Le détecteur reconnaît les éléments suivants pour des pools :
  - liste des hôtes
  - nom
- Le détecteur reconnaît les éléments suivants pour des hôtes :
  - liste des machines virtuelles, y compris Domain 0
  - informations sur la mémoire
  - informations sur l'unité centrale
  - nom
  - description
  - état en cours
  - identificateur unique universel
- Le détecteur reconnaît les éléments suivants pour des machines virtuelles :

- nom
- informations sur la mémoire
- nombre d'unités centrales
- état d'alimentation
- PV/HVM
- informations sur le réseau
- type d'amorçage

Prérequis

Les prérequis suivants sont obligatoires :

- lsof doit être installé dans le domaine 0
- xapi doit être en cours d'exécution dans le domaine 0
- Dans le cas d'une machine virtuelle basée sur Linux, les outils invités doivent être exécutés dans DomainU paravirtualisé pour reconnaître ce type de machine virtuelle.
- Dans le cas d'une machine virtuelle basée sur Windows, les outils invités doivent être exécutés dans une machine virtuelle matérielle pour reconnaître les informations sur le réseau et le système d'exploitation.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- simple.SLogicalGroup
- sys.ComputerSystem
- sys.linux.Linux
- sys.linux.LinuxUnitaryComputerSystem
- sys.windows.WindowsComputerSystem
- sys.windows.WindowsOperatingSystem

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Citrix XenServer et propose les solutions à ces problèmes.

Une machine virtuelle Windows est reconnue comme un autre système informatique sans informations du système d'exploitation

Problème

Une machine virtuelle Windows est reconnue comme un autre système informatique et aucune information de système d'exploitation n'est fournie

Solution

Vérifiez que les outils invités sont exécutés dans la machine virtuelle. Les outils sont obligatoires pour une reconnaissance.

Une machine virtuelle Linux n'est pas reconnue.

Problème

Une machine virtuelle Linux n'est pas reconnue et un avertissement s'affiche.

Solution

Vérifiez que les outils invités sont exécutés dans la machine virtuelle. Les outils sont obligatoires pour une reconnaissance.

Détecteur DataPower

Le détecteur DataPower détecte les dispositifs SOA DataPower IBM WebSphere, qui prennent en charge l'interface de gestion des configurations.

Fix Pack 3

Dans TADDM version 7.3.0.3 et ultérieures, le détecteur reconnaît les domaines DataPower et les types de proxys suivants :

- Proxy SSL
- Proxy TCP
- Proxy XSL
- Proxy WS
- Passerelle multiprotocole (MPG)
- Pare-feu XML
- Service HTTP

Les données reconnues sont stockées en tant qu'instances étendues. Pour chaque nouvelle catégorie reconnue un onglet est créé dans le portail de gestion de données, par exemple, **Domaines** ou **Proxy SSL**. Les données sont affichées au format XML.

Nom du détecteur utilisé dans l'interface graphique et les journaux

DataPowerSensor

Prérequis

Le service de gestion des configurations du protocole SOAP des dispositifs DataPower détectés doit être activé.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.appliance.DataPower
- net.L2Interface
- net.IpInterface

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration des numéros de port :

Vous devez définir un numéro de port de l'interface de gestion des configurations SOAP de DataPower dans la configuration du détecteur de port.

Procédure

1. Créez un profil de reconnaissance.
2. Sélectionnez `PortSensor` dans la liste des détecteurs et cliquez sur **Nouveau**.
3. Dans la zone **dataPowerXmlManagementPorts**, entrez une liste de numéros de port séparés par des virgules, qui doivent être traités en tant que ports d'interface de gestion des configurations de protocole SOAP DataPowerenter. Spécifiez les autres informations requises, activez la configuration et sauvegardez-la.

4. Ajoutez DataPowerSensor à votre profil de reconnaissance et sauvegardez-le.

Résultats

Lorsque vous effectuez une détection en utilisant le profil que vous avez créé, le détecteur DataPower est démarré pour chaque serveur. Ces serveurs écoutent tout port fourni dans la liste **dataPowerXmlManagementPorts**.

Configuration de la liste d'accès et des certificats :

Le détecteur DataPower nécessite la saisie correcte du type de composant "DataPower" dans la liste d'accès. Le nom d'utilisateur et le mot de passe doivent être identiques à ceux utilisés pour vous identifier à vos dispositifs DataPower avec WebGUI ou SSH.

Configuration du certificat

Le détecteur DataPower utilise le protocole HTTPS et nécessite un fichier de mémoire protégée avec votre certificat de dispositif, qui doit être joint à l'entrée de la liste d'accès. Chaque entrée de liste d'accès utilise son propre fichier de mémoire protégée et est indépendant des autres entrées de la liste d'accès.

Vous pouvez employer l'utilitaire `iKeyman` (`ikeyman.exe` sous Windows) pour créer un fichier de mémoire protégée. La fonctionnalité est intégrée à l'installation TADDM. Les certificats issus de votre dispositif ou de vos dispositifs DataPower doivent être ajoutés à votre fichier de mémoire protégée en tant que certificats de signataire.

Ignorer la validation des certificats :

Si votre environnement est entièrement sécurisé, vous pouvez configurer le détecteur DataPower de sorte qu'il ignore la validation des certificats.

Procédure

1. Choisissez le profil de reconnaissance utilisé pour la reconnaissance de vos dispositifs DataPower.
2. Sélectionnez `DataPowerSensor` dans la liste des détecteurs et cliquez sur **Nouveau**.
3. Spécifiez la valeur `false` pour la propriété `validateCertificates`, activez la configuration et sauvegardez-la.
4. Sauvegardez le profil de reconnaissance.

Résultats

Lorsque vous exécutez une reconnaissance à l'aide du profil que vous avez créé, le détecteur DataPower ne validant pas les certificats, vous n'avez pas besoin de joindre de fichiers de clés certifiées à vos entrées de liste d'accès.

Activation de la vérification des noms d'hôte :

Lorsque vous utilisez des certificats basés sur le nom de domaine complet, l'étape de vérification du nom d'hôte du protocole SSL est ignorée en raison des restrictions liées à la définition de portées de TADDM. Lorsque vous utilisez des certificats basés sur IP, vous pouvez activer la vérification du nom d'hôte pour sécuriser complètement la connexion SSL.

Pourquoi et quand exécuter cette tâche

Une définition de portée TADDM est basée sur une adresse IP et non sur le nom de domaine complet. Toute valeur de nom de domaine complet qui peut être fournie pendant la création d'une portée est immédiatement résolue pour l'adresse IP. Le nom de domaine complet n'est pas transmis au détecteur lors de l'exécution de la reconnaissance. Le détecteur doit utiliser l'adresse IP en tentant de se connecter au dispositif DataPower. Si le certificat du dispositif DataPower est basé sur le nom de domaine complet, normalement l'erreur de protocole SSL est déclenchée pour indiquer une non-concordance possible entre l'adresse IP fournie et le nom de domaine complet du service lue à partir du certificat. Pour éviter de problème, l'étape de vérification du nom d'hôte est désactivée par défaut.

Lorsque vous utilisez des certificats basés sur IP, vous pouvez activer l'étape de vérification du nom d'hôte pour sécuriser complètement la connexion SSL.

Procédure

1. Choisissez le profil de reconnaissance utilisé pour la reconnaissance de vos dispositifs DataPower.
2. Sélectionnez `DataPowerSensor` dans la liste des détecteurs et cliquez sur **Nouveau**.
3. Spécifiez la valeur `false` pour la propriété `bypassHostnameVerification`, activez la configuration et sauvegardez-la.
4. Sauvegardez le profil de reconnaissance.

Résultats

Lorsque vous exécutez une reconnaissance à l'aide du profil que vous avez créé, le détecteur DataPower est strictement conforme au protocole SSL. L'adresse IP fournie sur la portée TADDM doit correspondre exactement à l'adresse IP indiquée dans le certificat du dispositif DataPower pour que la reconnaissance aboutisse.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur DataPower et propose des solutions à ces problèmes.

Un périphérique DataPower reconnu avec SnmpMib2Sensor ne fusionne pas avec des données reconnues par d'autres détecteurs.

Problème

Un périphérique DataPower reconnu avec SnmpMib2Sensor ne fusionne pas avec les données reconnues par d'autres détecteurs.

Solution

Si un périphérique DataPower est configuré pour utiliser le protocole SNMP, il peut être reconnu à l'aide de SnmpMib2Sensor. DataPower utilise cependant un ensemble personnalisé d'OID SNMP que SnmpMib2Sensor n'interroge pas. Ces OID sont lus uniquement par le détecteur CustomMib2ComputerSystem en utilisant un script d'extension Jython.

Pour plus d'informations, voir l'étape 6 de la rubrique *Ajout d'un modèle de système informatique pour un appareil réseau* du *Guide d'utilisation* TADDM.

Pour sécuriser un rapprochement correct avec des données enregistrées par des détecteurs DataPower, VMWare et ZEnterprise dans la console de gestion de reconnaissance, vérifiez les prérequis suivants :

- Vérifiez que le modèle DataPowerComputerSystem est activé dans des modèles de systèmes informatiques (ce qui est le paramètre par défaut).
- Assurez-vous que le détecteur CustomMib2ComputerSystem est activé dans le profil de reconnaissance qui est utilisé pour reconnaître des périphériques DataPower.
- Assurez-vous que les fichiers suivants figurent dans l'installation de TADDM :
  - `etc/templates/commands/DataPowerComputerSystem`
  - `etc/templates/commands/extension-scripts/DataPowerComputerSystem.py`

Détecteur de système informatique FreeBSD

Le détecteur de système informatique FreeBSD reconnaît les systèmes informatiques exécutant le système d'exploitation FreeBSD basé sur BSD UNIX.

Nom du détecteur utilisé dans l'interface graphique et les journaux

FreeBSDComputerSystemSensor

Prérequis

Pour que le détecteur reconnaisse le système d'exploitation, le script `/bin/sh` doit être configuré comme shell par défaut.

Pour fusionner les données reconnues par le détecteur de système informatique VMware ESX, la commande **`dmidecode`** est requise sur les cibles où le système d'exploitation FreeBSD est installé.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Si la commande suivante se trouve sur le système cible, le détecteur reconnaît les systèmes de fichiers locaux :

```
df -kTP
```

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS,

TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de système informatique FreeBSD prend en charge la reconnaissance basée sur un script.

Conditions requises pour la configuration du détecteur

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Objets de modèle avec attributs associés

Le détecteur de système informatique FreeBSD crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les systèmes informatiques exécutant le système d'exploitation FreeBSD dans votre environnement informatique.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous leur nom.

core.LogicalContent

- Checksum
- Content
- FixedPath
- URI

net.L2Interface

- Promiscious
- Name
- HwAddress
- Mtu
- Speed
- Duplex
- AutoNegotiation
- Broadcast
- Loopback
- InterfaceMTU
- InterfaceName

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

sys.DNSResolveEntry

- ServerIp
- SearchOrder

sys.freebsd.FreeBSD

- FQDN
- Name
- OSName
- OSVersion
- BootTime
- KernelArchitecture
- KernelVersion
- WordSize
- Charset
- OsId
- OSMode
- OSConfidence
- VersionString
- KernelModulesRawData

sys.freebsd.FreeBSDUnitaryComputerSystem

- UUID
- Name
- Type
- SystemId
- Signature
- Fqdn
- SerialNumber
- Manufacturer
- Model
- MemorySize
- BIOSManufacturer
- BIOSDate
- BIOSName
- NumCPUs
- CPUType
- CPUSpeed
- Architecture
- TimeZone
- VirtualMachineState

sys.SoftwareComponent

- SoftwareVersion

- Name

sys.unix.UnixFileSystem

- MountPoint
- Type
- Capacity
- AvailableSpace
- Owner
- Group
- Permissions

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme type de composant.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

En règle générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège, qui peut être effectuée à l'aide de la commande **sudo**.

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Configuration des entrées du fichier `collation.properties` :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

Fix Pack 3 **com.ibm.cdb.discover.sys.freebsd.pkg_info=pkg_info**
Cette propriété indique le chemin d'accès à la commande **pkg_info** sur le système d'exploitation FreeBSD versions 9.*x* ou antérieures. La commande fournit des informations sur tous les packages installés sur le système d'exploitation FreeBSD.

La valeur par défaut est `pkg_info`.

Fix Pack 3 **com.ibm.cdb.discover.sys.freebsd.pkg_info_10=pkg info**
Cette propriété indique le chemin d'accès à la commande **pkg info** sur le système d'exploitation FreeBSD versions 10.*x* ou ultérieures. La commande fournit des informations sur tous les packages installés sur le système d'exploitation FreeBSD.

La valeur par défaut est `pkg info`.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique FreeBSD et présente des solutions à ces problèmes.

Des invités FreeBSD en double sont créés

Problème

Lorsque le même invité sur lequel le système d'exploitation FreeBSD est installé est reconnu par les détecteurs de systèmes informatiques FreeBSD et VMware ESX, les données ne sont pas fusionnées et des doubles sont créés.

Solution

Installez la commande **dmidecode** sur les cibles sur lesquelles le système d'exploitation FreeBSD est installé. Cette commande est requise pour que les données reconnues par le détecteur de système informatique VMware ESX puissent être fusionnées correctement.

Détecteur SNMP HP BladeSystem

Le détecteur SNMP HP BladeSystem reconnaît et collecte des informations de configuration concernant le châssis HP BladeSystem.

Ce détecteur utilise le protocole SNMP (Simple Network Management Protocol) pour reconnaître et interroger les composants d'infrastructure BladeSystem. Le composant SNMP d'administrateur embarqué HP BladeSystem est utilisé pour collecter les données.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HPBladeSystemSnmpSensor

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- enums.PhysTypeEnum
- enums.SlotStateEnum
- enums.BladeCenterManagementModuleTypeEnum
- net.Fqdn
- phys.physconn.PhysicalConnector
- phys.physconn.Slot
- phys.physpkg.Board
- phys.physpkg.Chassis
- phys.physpkg.Fan
- phys.physpkg.PhysicalFrame
- phys.physpkg.PowerSupply
- sys.blade.BladeCenterManagementModule
- sys.ComputerSystem
- storage.FCSwitch

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Vous pouvez configurer le détecteur SNMP HP BladeSystem dans la console de gestion de reconnaissance en définissant les attributs suivants :

snmpPort
Numéro du port utilisé pour la communication SNMP. La valeur par défaut est 161.

snmpTimeout
Délai d'attente utilisé pour une requête SNMP unique. La valeur par défaut est 20000.

locale Environnement local utilisé pour les requêtes SNMP.

characterEncoding
Codage de caractères utilisé pour les requêtes SNMP.

Lorsque le détecteur SNMP HP BladeSystem est activé, vous devez également activer le détecteur SNMP Light ou le détecteur SNMP MIB2 pour que le détecteur SNMP HP BladeSystem SNMP sensor fonctionne correctement.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour les reconnaissances SNMP V1 et V2, entrez la chaîne de communauté appropriée dans la liste d'accès.

  Pour cela, vous pouvez utiliser le type de composant (SNMP) du modèle de réseau dans la fenêtre Liste d'accès de la console de gestion de reconnaissance.
- Pour les reconnaissances SNMP V3, entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects dans la liste d'accès, en fonction des informations de mappage de données d'identification SNMP V3 dans le tableau suivant.

Tableau 23. Mappage des données d'identification SNMP V3.

Mappez à partir de ce qui suit :	Vers ce qui suit :
Type d'authentification (par exemple MD5)	Protocole d'authentification
Clé secrète MD5	Mot de passe et Confirmer le mot de passe
Clé ou description d'authentification privée	Mot de passe privé

  Pour cela, vous pouvez utiliser le type de composant (SNMPV3) dans la fenêtre Liste d'accès de la console de gestion de reconnaissance.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur SNMP HP BladeSystem et propose les solutions à ces problèmes.

Une erreur de délai d'attente SNMP se produit

Problème
Le détecteur génère une erreur de dépassement de délai SNMP au cours d'une reconnaissance.

Solution

Augmentez la valeur du paramètre `snmpTimeout` pour le détecteur SNMP HP BladeSystem à l'aide de la console de gestion de reconnaissance.

Des objets HP Blade System ne se synchronisent pas avec des données de reconnaissance de niveau 2.

Problème

Une reconnaissance de HP Blade System crée des systèmes informatiques qui ne se synchronisent pas avec les données de découverte de niveau 2 lorsque Virtual Connect a des profils de serveur logique activés.

Solution

TADDM inspecte des objets provenant d'une reconnaissance HP Blade System, lorsque les attributs par défaut `manufacturer`, `model` et `serialNumber` ne correspondent pas. Le module d'extension de synchronisation interne logique impose que les attributs `manufacturer`, `model` et `FQDN` soient identiques aux données trouvées au cours d'une reconnaissance de niveau 2 pour activer une reconnaissance entre les deux objets. Si FQDN est indisponible, deux instances du même objet apparaissent dans la base de données.

Détecteur de système informatique HP NonStop

Le détecteur de système informatique HP NonStop reconnaît le système informatique qui exécute le système d'exploitation de logiciel libre HP NonStop. Le détecteur s'exécute uniquement en mode reconnaissance asynchrone.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HpNonStopComputerSystemSensor

Prérequis

Un utilisateur de reconnaissance doit avoir accès à l'environnement OSS et Guardian. Un script ASD est exécuté à partir de l'environnement OSS.

Vous pouvez créer un package ASD à l'aide de la commande suivante :

```
$COLLATION_HOME/bin/makeASDScriptPackage.sh --outputDir rèp_sortie
--uname NONSTOP_KERNEL --ipAddress adresse_IP
--packingMethod tar --sensors computersystem
```

Limitations

Le détecteur est uniquement pris en charge en mode reconnaissance asynchrone (ASD).

Le détecteur reconnaît l'ensemble limité d'informations associées au système informatique. Le détecteur de serveur générique qui lance les détecteurs de niveau 3 n'est pas pris en charge sur la plateforme HP NonStop.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- sys.hpnonstop.HpNonStop

- sys.hpnonstop.HpNonStopComputerSystem

Prise en charge de la reconnaissance asynchrone

Le détecteur de système informatique HP NonStop prend en charge la reconnaissance asynchrone.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Identification et résolution des problèmes liés au détecteur

Les problèmes qui surviennent avec le détecteur peuvent être les suivants : échec de la reconnaissance ou propriétés mal définies. Toutefois, vous pouvez résoudre ces problèmes.

Problèmes génériques

Vérifiez que les détecteur suivants sont activés dans le profil :

- ASDPingSensor
- ASDSensor
- GenericComputerSystemSensor
- HpNonStopComputerSystemSensor

Vérifiez que les packages ASD sont disponibles pour une reconnaissance dans un répertoire défini par la propriété `com.ibm.cdb.discover.asd.AsyncDiscoveryResultsDirectory`.

Détecteur de système informatique HP-UX

Le détecteur de système informatique HP-UX reconnaît un système informatique exécutant le système d'exploitation HP-UX. Lorsqu'un système exécute HP-UX sur une plateforme Itanium avec prise en charge de la virtualisation (HP Integrity Virtual Machines), le détecteur reconnaît les éléments gérés par ce serveur.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HpUxComputerSystemSensor

Prérequis

Pour un système VM Host sur une plateforme Itanium, le compte de service TADDM doit posséder les autorisations d'exécution sur les fichiers binaires **`hpvmstatus`** et**`hpvminfo`**.

Pour un système invité sur une plateforme Itanium, le compte de service TADDM doit posséder les autorisations d'exécution sur les fichiers binaires **`hpvminfo`**.

Le compte de service TADDM doit posséder les autorisations d'exécution sur les fichiers binaires **`machinfo`**.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Les limitations suivantes s'appliquent lors de la reconnaissance des informations sur l'unité centrale via le détecteur de système informatique HP-UNIX :

- Le détecteur ne reconnaît pas 'CPUCoresInstalled' pour l'architecture PA-RISC.
- Le détecteur ne reconnaît pas le nombre d'unités d'exécution pour la configuration Unité d'exécution - HyperThreading.
- Le détecteur ne reconnaît pas 'CPUDiesInstalled' si la commande 'mpsched -K' n'est pas disponible.
- Le détecteur ne reconnaît pas 'CPUCoresInstalled' si la commande 'icapstatus' n'est pas disponible.
- Le détecteur ne reconnaît pas la configuration cpu/cores si la commande 'mpsched -K' n'est pas disponible.

La reconnaissance de l'adresse IPv6 d'un système invité par l'intermédiaire d'un système VM Host n'est pas disponible pour HP-UX sur une plateforme Itanium. La reconnaissance de l'adresse IPv6 d'un système VM Host par l'intermédiaire d'un système invité n'est pas disponible pour HP-UX sur une plateforme Itanium.

Les systèmes invités qui exécutent des systèmes d'exploitation autres que HP-UX ne sont pas créés durant la reconnaissance des systèmes VM Host.

TADDM ne peut pas reconnaître les informations de coeur d'UC de l'invité IVM, qui est directement reconnu par le détecteur. Ceci se produit car la commande **`icapstatus`** n'est pas prise en charge sur l'invité IVM.

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS, TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- sys.hpux.HpUx
- sys.HpUxUnitaryComputerSystem
- sys.OperatingSystem
- sys.SoftwareComponent

Objets de modèle avec attributs associés

Le détecteur informatique HP-UX crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les ressources informatiques HP-UX dans votre environnement informatique.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

sys.hpux.HpUxUnitaryComputerSystem

- Name
- UUID
- Type
- SystemId
- VirtualMachineState
- Signature
- Fqdn
- Manufacturer
- Model
- MemorySize
- NumCPUs
- CPUType
- CPUSpeed
- Architecture
- Virtual
- CPUDiesInstalled
- CPUCoresInstalled
- ChildSystem
- VMID

sys.CPU

- IndexOrder
- CPUType
- NumCPUs
- CPUSpeed
- CPUCoresEnabled
- CPUCore
- Virtual

sys.hpux.HpUx

- Fqdn

- Name
- OSName
- OSVersion
- BootTime
- PatchesInstalledRawData
- KernelVersion
- OsId
- KernelModulesRawData
- OSConfidence
- VersionString

core.LogicalContent

- Checksum
- Content
- URI
- fixedPath

sys.SoftwareComponent

- Name
- SoftwareVersion

sys.unix.UnixFileSystem

- AvailableSpace
- Capacity
- MountPoint

net.L2Interface

- IANAInterfaceType
- interfaceMTU
- interfaceSpeed
- interfaceName
- HwAddress
- Mtu
- Name
- Speed
- Loopback
- Broadcast
- Encapsulation

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Le détecteur de système informatique HP-UX peut être exécuté en utilisant les droits d'accès du système informatique. Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines des commandes utilisées par TADDM lors du processus de reconnaissance peuvent requérir une escalade du privilège. Cette escalade s'effectue généralement à l'aide de la commande **sudo**.

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration* de TADDM.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.platform.os.command.machinfo
Cette propriété indique le chemin d'accès à la commande **machinfo**. Si cette propriété n'est pas définie, la valeur par défaut de `/usr/contrib/bin/machinfo` est utilisée.

com.collation.discover.agent.command.kcmodule
Cette propriété indique le chemin d'accès à la commande **kcmodule**.

com.collation.platform.os.HpUxItanium.Model
Sert de point de démarrage pour HpUx sous Itanium. La valeur par défaut est ia64. Modifiez cette propriété si la sortie de la commande model sur les systèmes HP-UX Itanium ne contient pas ia64.

com.collation.discover.agent.command.hpvminfo
Cette propriété indique le chemin d'accès à la commande **hpvminfo**. Si cette propriété n'est pas définie, la valeur par défaut de `/opt/hpvm/bin/hpvminfo` est utilisée.

com.collation.discover.agent.command.hpvmstatus
Cette propriété indique le chemin d'accès à la commande **hpvmstatus**. Si cette propriété n'est pas définie, la valeur par défaut de `/opt/hpvm/bin/hpvmstatus` est utilisée.

com.collation.platform.os.command.crontabEntriesCommand.HP-UX=crontab -l
Cette propriété sert à reconnaître des entrées **crontab**. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesCommand.HP-UX.1.2.3.4=crontab -l
```

com.collation.platform.os.command.crontabEntriesUsers.HP-UX=root
Cette propriété sert à reconnaître des entrées **crontab** pour un utilisateur déterminé ; pour indiquer plusieurs utilisateurs, séparez-les par des virgules. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

com.collation.platform.os.command.crontabEntriesUsers.HP-UX.1.2.3.4=root,build

com.collation.discover.agent.sys.ComputerSystem.serialNumberSanityChecks= "⌂(?!null);⌂(?!not);⌂(?!n/a);⌂(?!permission);⌂(?!to be);⌂(?!undef); ⌂[-:\.\w]{4,80}$; ^(?!.{8}(\-.{4}){3}\- .{12}_.{2}(:.{2}){5});^(?!none);^(?!x{7});^(?!\ .{9});^(?!0123456789);^(?!0+$)";

Cette propriété sert à valider la propriété serialNumber reconnue par les détecteurs du système d'exploitation (sauf Solaris) afin d'éviter de stocker des valeurs génériques (telles que Not Defined, To be set by OEM ou Permission Denied).

La principale règle par défaut est que le numéro de série contient entre 4 et 80 caractères et ne commence pas par l'une des chaînes suivantes :

- **null** : expression régulière **^(?!null)**
- **not** : expression régulière **^(?!not)**
- **n/a** : expression régulière **^(?!n/a)**
- **permission** : expression régulière **^(?!permission)**
- **to be** : expression régulière **^(?!to be)**
- **undef** : expression régulière **^(?!undef)**
- string in form : **098D8710-E623-3C3B-9F9B-FCBAFF1BF3B6_5C:F3:FC:E8:89:FC** : expression régulière **^(?!.{8}(\-.{4}){3}\-.{12}_.{2}(:.{2}){5})**
- **none** : expression régulière **^(?!none)**
- **xxxxxxx** : expression régulière **^(?!x{7})**
- **.....** : expression régulière **^(?!\.{9})**
- **0123456789** : expression régulière **^(?!0123456789)**
- **0000** : expression régulière **^(?!0+$)**

Si un numéro de série ne suit pas cette règle, il n'est pas défini. La syntaxe d'expression régulière est définie dans le SDK Java pour la classe `java.util.regex.Pattern`. Les expressions régulières doivent être séparées par des points-virgules. Les numéros de série candidats sont toujours convertis en minuscules avant d'être mis en correspondance avec des expressions régulières. Par conséquent, quand vous personnalisez la propriété, prenez uniquement des caractères en minuscules.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique HP-UX et propose des solutions à ces problèmes.

Problèmes génériques

Vérifiez que les attributs, comme architecture, type de processeur, vitesse du processeur, taille de la mémoire ou numéro de série ne sont pas renseignés.

Vérifiez que la sortie de la commande Model contient ia64, et si ce n'est pas le cas, vérifiez que la cible est HP-UX 11.23 sous Itanium. Modifiez la propriété `com.collation.platform.os.HpUxItanium.Model` pour inclure l'identificateur unique à partir de la sortie de la commande model.

Par défaut, l'attribut Numéro de série n'est pas renseigné sous Itanium. Pour activer l'attribut Numéro de série, ajoutez l'entrée suivante dans le fichier `collation.properties` sur le serveur TADDM :

```
com.collation.discover.agent.sys.HpUxComputerSystemItaniumAgent.setSerialNumber=true
```

Pas d'affichage des détails matériel

Problème

Durant une reconnaissance via IBM Tivoli Monitoring, certaines informations détaillées n'est pas affichées pour les systèmes informatiques qui exécutent le système d'exploitation HP-UX.

Solution

Dans le fichier `collation.properties`, ajoutez le modèle `|.*machinfo.*` à la fin de la propriété :

```
com.collation.discover.agent.ITM.CmdWrapperSelectionPattern=|.*machinfo.*
```

Détecteur de système informatique IBM AIX

Le détecteur de système informatique IBM AIX reconnaît les systèmes informatiques qui exécutent le système d'exploitation IBM AIX. En outre, ce détecteur reconnaît le partitionnement de la charge de travail (WPAR) du système d'exploitation IBM AIX 6.1.

Nom du détecteur utilisé dans l'interface graphique et les journaux

AixComputerSystemSensor

Prérequis

L'utilisateur TADDM doit avoir accès à la commande **entstat** sur les systèmes cible AIX.

Dans un environnement de système informatique System P ou System Z, l'ID de partition logique doit être sauvegardé dans l'attribut ID de machine virtuelle (VMID) pour éviter la fusion incorrecte de LPAR différents dans un objet unique.

Dans le cas d'AIX, l'attribut VMID a été converti d'ID de partition logique (numérique) en nom de partition logique (texte). L'ID VMID et la partition logique doivent être définis sur **True**.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Le détecteur reconnaît les WPAR à l'aide du nom WPAR et de l'adresse IP. Après avoir exécuté une reconnaissance, si l'adresse IP ou le nom de la WPAR a été

modifié, effacez les données de topologie avant de réexécuter la reconnaissance. Cette tâche permet d'éviter les situations où des WPAR en double du même nom existe dans la base de donnée. Cette limitation ne s'applique pas aux WPAR dans lesquelles l'adresse IP n'est pas configurée.

Le nom de domaine complet peut être obtenu pour la WPAR à partir du nom d'hôte. Dans ce cas, TADDM ne requiert pas le nom d'hôte du serveur DNS et ce nom n'est pas affiché.

Des informations concernant la taille de la mémoire virtuelle des attributs et l'espace de pagination pour le WPAR sont introuvables.

La fonction de mobilité WPAR qui vous permet de déplacer des instances WPAR en cours d'exécution entre des systèmes physiques n'est pas prise en charge.

Fix Pack 1 Live Partition Mobility (LPM) n'est pas pris en charge dans TADDM 7.3.0. Ce produit est pris en charge dans la version 7.3 groupe de correctifs 1 et ultérieure.

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS, TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de système informatique IBM AIX prend en charge une reconnaissance asynchrone ou basée sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Les modèles et extensions de systèmes informatiques ne sont pas pris en charge par le détecteur de système informatique AIX au cours d'une reconnaissance asynchrone ou basée sur un script.

Objets de modèle avec attributs associés

Le détecteur de système informatique IBM AIX crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les systèmes informatiques dotés du système d'exploitation IBM AIX et les ressources de partitionnement de la charge de travail (WPAR) de votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet modèle.

core.LogicalContent

- Checksum
- Configfile
- Content
- ContentType
- FixedPath
- URI

net.L2Interface

- AlternativeName
- AutoNegotiation
- Broadcast
- Duplex
- Encapsulation
- HwAddress
- InterfaceMTU
- InterfaceName
- Loopback
- Mtu
- Name
- Promiscious
- Speed
- IANAInterfaceType
- Index

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

sys.aix.Aix

- BootTime
- Charset
- FQDN
- KernelModulesRawData

- KernelVersion
- Name
- OSConfidence
- OsId
- OSMode
- OSName
- OSVersion
- PatchesInstalledRawData
- VirtualMemorySize
- WordSize
- VersionString
- Level
- BuildLevel
- ServicePack

sys.aix.AixUnitaryComputerSystem

- Architecture
- BIOSManufacturer
- CPUSpeed
- CPUType
- DesiredProcessingUnits
- Fqdn
- IsVMIDanLPAR
- Manufacturer
- MaxProcessingUnits
- MemorySize
- MinProcessingUnits
- Model
- Name
- NumCPUs
- SerialNumber
- Signature
- SystemId
- TimeZone
- Type
- Virtual
- VMID
- VirtualMachineState
- ChildSystem

sys.AixSoftwareComponent

- InstallState
- Name
- SoftwareVersion
- Type

sys.CPU

- IndexOrder
- CPUType
- NumCPUs
- CPUSpeed
- Virtual

sys.DNSResolveEntry

- SearchOrder
- ServerIp

sys.unix.UnixFileSystem

- AvailableSpace
- Capacity
- Group
- MountPoint
- Owner
- Permissions
- Type

sys.PageSpace

- IsActive
- Name
- Size
- Type

sys.WPARComputerSystem

- AssignedIp
- IsWparActive
- IsWparAutostart
- IsWparCheckpointable
- WparCPULimits
- WparCPUShares
- WparInstalledDirectory
- WparMemoryLimits
- WparMemoryShares
- WparOwner
- WparPerProcessVirtualMemoryLimit
- WparType
- Name
- Type
- Virtual

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Editez le fichier `/etc/sudoers` sur le serveur AIX et ajoutez la ligne suivante :

```
<TADDM_USER> ALL=NOPASSWD:ALL
```

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Utilisez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur, mot de passe) que TADDM doit utiliser pour une authentification basée sur une clé SSH ou une authentification basée sur une connexion SSH sur le système informatique cible.

En règle générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines des commandes utilisées par TADDM lors du processus de reconnaissance peuvent requérir une escalade du privilège. Cette escalade peut être effectuée à l'aide de la commande **sudo**.

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration* de TADDM.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties que le détecteur de système informatique IBM AIX utilise.

Le détecteur utilise l'entrée suivante du fichier `collation.properties` :

com.collation.discover.agent.command.lswpar.AIX=sudo lswpar
La commande **lswpar** requiert les privilèges d'administrateur.

com.collation.platform.os.command.crontabEntriesCommand.AIX=crontab -l
Cette propriété sert à reconnaître des entrées **crontab**. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesCommand.AIX.1.2.3.4=crontab -l
```

com.collation.platform.os.command.crontabEntriesUsers.AIX=root
Cette propriété sert à reconnaître des entrées **crontab** pour un utilisateur déterminé ; pour indiquer plusieurs utilisateurs, séparez-les par des virgules. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesUsers.AIX.1.2.3.4=root,build
```

com.collation.discover.agent.sys.ComputerSystem.serialNumberSanityChecks=
"⌂(?!null);⌂(?!not);⌂(?!n/a);⌂(?!permission);⌂(?!to be);⌂(?!undef); ⌂[
-:\.\w]{4,80}$; ^(?!.{8}(\-.{4}){3}\-
.{12}_.{2}(:.{2}){5});^(?!none);^(?!x{7});^(?!
.{9});^(?!0123456789);^(?!0+$)";

Cette propriété sert à valider la propriété serialNumber reconnue par les détecteurs du système d'exploitation (sauf Solaris) afin d'éviter de stocker des valeurs génériques (telles que Not Defined, To be set by OEM ou Permission Denied).

La principale règle par défaut est que le numéro de série contient entre 4 et 80 caractères et ne commence pas par l'une des chaînes suivantes :

- **null** : expression régulière **^(?!null)**
- **not** : expression régulière **^(?!not)**

- **n/a** : expression régulière **^(?!n/a)**
- **permission** : expression régulière **^(?!permission)**
- **to be** : expression régulière **^(?!to be)**
- **undef** : expression régulière **^(?!undef)**
- string in form : **098D8710-E623-3C3B-9F9B-FCBAFF1BF3B6_5C:F3:FC:E8:89:FC** : expression régulière **^(?!.{8}(\-.{4}){3}\-.{12}_.{2}(:.{2}){5})**
- **none** : expression régulière **^(?!none)**
- **xxxxxxx** : expression régulière **^(?!x{7})**
- **.....** : expression régulière **^(?!\.{9})**
- **0123456789** : expression régulière **^(?!0123456789)**
- **0000** : expression régulière **^(?!0+$)**

Si un numéro de série ne suit pas cette règle, il n'est pas défini. La syntaxe d'expression régulière est définie dans le SDK Java pour la classe `java.util.regex.Pattern`. Les expressions régulières doivent être séparées par des points-virgules. Les numéros de série candidats sont toujours convertis en minuscules avant d'être mis en correspondance avec des expressions régulières. Par conséquent, quand vous personnalisez la propriété, prenez uniquement des caractères en minuscules.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique IBM AIX et propose des solutions à ces problèmes.

Le détecteur ne reconnaît pas les WPAR

Problème

Le détecteur ne parvient pas à reconnaître la WPAR.

Solution

Pour vérifier l'état de la WPAR :

1. Exécutez la commande **`sudo lswpar`** à l'aide des autorisations d'accès de <*Utilisateur_TADDM*>. Si la liste des WPAR ne s'affiche pas, attribuez les autorisations d'accès d'accès à <*Utilisateur_TADDM*> pour exécuter la commande **`lswpar`**.
2. Modifiez la commande spécifique **`sudo`** dans le fichier`collation.properties`.

Les WPAR reconnues n'affichent pas des valeurs d'attribut

Problème

Certaines des WPAR reconnues n'affichent pas de valeurs d'attribut.

Solution

Vérifiez si les WPAR présentes sont dans un état actif ou défini. Pour les WPAR dont l'état est défini, un nombre limité de valeurs d'attribut est affiché.

Détecteur de console IBM HMC (Hardware Management Console)

Le détecteur IBM Hardware Management Console (HMC) reconnaît les consoles IBM Hardware Management Console (HMC) et ses systèmes gérés.

Nom du détecteur utilisé dans l'interface graphique et les journaux

HmcSensor

Ressources reconnues par le détecteur

Le processus de reconnaissance d'une console HMC est semblable à celui utilisé pour une reconnaissance de système informatique standard. Les problèmes les plus importants ayant un impact sur la reconnaissance sont la connectivité et l'authentification. Si le compte configuré dans la liste d'accès de TADDM peut se connecter à la console HMC, la reconnaissance s'effectue correctement.

Les ressources suivantes peuvent être reconnues par l'intermédiaire de la console HMC :

- HMC, la console de gestion matérielle ;
- Les systèmes gérés par la console HMC (systèmes informatiques System p et System i) ;
- les partitions logiques (LPAR) définies dans chaque système géré.
- Si une partition logique est installée avec le serveur VIOS (Virtual I/O Server), ce serveur VIOS est reconnu.

Selon sa portée, la reconnaissance d'un système informatique (LPAR) peut détecter deux instances du système informatique :

- le système informatique (LPAR) reconnu par le détecteur HMC ;
- le système informatique reconnu par le détecteur TADDM normal pour le système d'exploitation particulier, comme Linux ou AIX, entre autres.

  Cette instance est reconnue exactement de la même manière qu'un système informatique Linux ou AIX physique. Il n'existe aucun détecteur TADDM spécifique permettant de reconnaître des systèmes informatiques virtuels d'une manière différente des systèmes informatiques physiques qu'ils émulent.

Le système informatique (LPAR) reconnu par le détecteur HMC est un système informatique superficiel. Les attributs clés suivants, qui forment la règle de nommage, sont reconnus :

- Manufacturer
- Modèle
- Numéro de série
- ID LPAR

Après une reconnaissance, TADDM fusionne les deux instances en un même système informatique.

VIOS est reconnu avec les informations de mappage de stockage suivantes :

- Adaptateurs SCSI virtuels
- Adaptateurs NPIV virtuels
- Unités cible virtuelles
- Volumes physiques
- Chemins MPIO
- HBA

Vous devez vous servir de l'utilisateur `Hmcoperator` pour reconnaître les informations de mappage de stockage.

VIOS est reconnu avec les informations de mappage réseau suivantes :

- Adaptateurs virtuels
- Cartes physiques
- Cartes Ethernet partagées

Grâce à la reconnaissance de la console HMC et des partitions logiques, vous pouvez voir un mappage entre le disque de partition logique et l'unité cible virtuelle d'un VIOS.

Limitations

Fix Pack 1 Live Partition Mobility (LPM) n'est pas pris en charge dans TADDM 7.3.0. Ce produit est pris en charge dans la version 7.3 Fix Pack 1 et ultérieure.

Objets de modèle avec attributs associés

Le détecteur IBM Hardware Management Console crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur IBM Hardware Management Console (HMC) et ses systèmes gérés dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

app.SoftwareFix

- ControlSoftware

dev.FCPort

- DeviceID
- TotalNpivPorts
- AvailableNpivPorts
- Parent
- Description
- PhysicalLocationCode
- Status
- PermanentAddress
- ChildPorts
- SecondaryAddress

dev.BasedOnExtent

- Source
- Target

dev.MediaAccessDevice

- Manufacturer
- Model
- Name
- SerialNumber
- Status
- Type

dev.SCSIProtocolController

- Name
- Parent
- PhysicalLocationCode
- Client
- ServerSlotNumber
- TargetDevices
- ClientSlotNumber
- ObjectType
- Description
- EndPoints

dev.SCSIProtocolEndPoint

- Name
- Parent
- Description

dev.StorageVolume

- Name
- Parent
- Type
- IeeeUniqueVolumeName
- Capacity
- LUN
- Pvid
- NumStalePartitions
- SerialNumber
- SystemPState
- ViosUDID
- VolumeGroupName
- BasedOn
- MpioPaths

dev.vios.MpioPath

- Controller
- Volume
- Connection
- Status

dev.vios.NpivViosVirtualAdapter

- ClientStatus
- FcPorts

dev.vios.VirtualTargetDevice

- BackingDevice
- Status

net.L2Interface

- AlternativeName
- DefaultVlan

- HaMode
- HwAddress
- Index
- IsIEEE8021QCompatible
- IsTrunk
- Name
- NetworkedFromVlan
- Parent
- SwitchPortMode
- TrunkPriority
- ViosType

net.Vlan

- Interfaces
- MgmtDomainName
- VlanId
- VlanName

sys.ComputerSystem

- CPUCoresEnabled
- CPUCoresInstalled
- CPULimit
- CPUSpeed
- CPUType
- ChildSystem
- ContextIp
- Description
- DesiredHugePages
- DesiredMemorySize
- DesiredProcessingUnits
- DesiredProcessors
- Périphériques
- DisplayName
- FileSystems
- Fqdn
- Functions
- Guid
- HostSystem
- IpInterfaces
- IsVMIDanLPAR
- L2Interfaces
- Label
- ManagedSystemName
- Manufacturer
- MaxHugePages
- Memory

- MemoryLimit
- MemorySize
- MinHugePages
- Model
- Name
- NumCPUs
- OSInstalled
- OSRunning
- ObjectType
- PrimaryMACAddress
- SerialNumber
- Signature
- StorageExtent
- SystemId
- Type
- UncappedWeight
- VMID
- Virtual

sys.ControlSoftware

- BuildLevel
- ContextIp
- DisplayName
- Fixes
- Level
- MajorVersion
- Modifier
- Name
- Edition
- VersionString

sys.FileSystem

- Parent
- MountPoint

sys.Function

- Name
- Parent

sys.HMC

- Systemp

sys.LocalFileSystem

- StorageExtent

sys.SystemPComputerSystem

- Architecture
- AvailableSysProcUnits
- CPUCoresEnabled
- CPUCoresInstalled

- CPUSpeed
- CPUType
- ConfigurableNumSysHugePages
- ConfigurableSysProcUnits
- ConfigurableSystemMemory
- DeconfiguredSysProcUnits
- DeconfiguredSystemMemory
- HugePageSize
- Is5250ApplicationCapable
- IsCoDMemoryCapable
- IsCoDProcessorCapable
- IsI5OSCapable
- IsLHCACapable
- IsLHEACapable
- IsMicroPartitioningCapable
- IsSNIMsgPassingCapable
- IsVIOSCapable
- Manufacturer
- MaxNumProcessorsPerLPAR
- MaxsSharedProcessorPools
- MemoryAvailableForPartitions
- MemorySize
- MinProcessingUnitsPerVirtualProcessor
- Model
- SerialNumber

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Par défaut, le détecteur IBM Hardware Management Console (HMC) est activé pour une reconnaissance de niveau 2 ou de niveau 3. Le détecteur reconnaît toutes les partitions logiques (LPAR) que le système soit en cours d'exécution ou non. Pour reconnaître des LPAR uniquement lorsque le système est en cours d'exécution, créez un profil de reconnaissance de niveau 2 ou de niveau 3 pour le détecteur IBM Hardware Management Console (HMC), et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

1. Dans le tiroir **Reconnaissance** de la console de gestion de reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil. Dans la liste **Cloner le profil existant**, sélectionnez **Reconnaissance de niveau 2**, ou **Reconnaissance de niveau 3** et cliquez sur **OK**.
4. Sous l'onglet **Configuration du détecteur**, sélectionnez le détecteur **HmcSensor**.

5. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration, puis sélectionnez la case à cocher **Activer la configuration**.
6. Dans la section **Configuration** de la fenêtre Créer la Configuration, cliquez sur **discoverNonRunningLpars**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne, et entrez `false`.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur.

      Ce nom d'utilisateur doit être doté (au minimum) des droits d'accès indiqués plus bas.
   b. Mot de passe

Dans la console de gestion HMC, créez un compte utilisateur pour l'utilisateur de la reconnaissance TADDM. Ce compte utilisateur doit être basé sur le rôle hmcoperator.

De plus, les tâches de ligne de commande suivantes doivent être affectées à ce compte utilisateur :

Système géré
Nécessaire pour utiliser les commandes **lshwres** et **lssyscfg**

Partition logique
Nécessaire pour utiliser les commandes **lshwres**, **lssyscfg** et **viosvrcmd**

Configuration HMC
Nécessaire pour utiliser la commande **lshmc**

Configuration des entrées du fichier `collation.properties` :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Vous pouvez définir les entrées suivantes dans le fichier `collation.properties` :

com.collation.discover.agent.HmcSensor.timeout
Cette propriété spécifie la durée pendant laquelle le détecteur est autorisé à exécuter la reconnaissance. Si la quantité de données extraites sur le stockage est trop importante, le détecteur risque de ne pas être exécuté dans le délai imparti. Pour collecter tous les détails, augmentez la valeur de cette propriété.

La valeur de cette propriété est exprimée en millisecondes.

com.collation.discover.agent.HMC.discoverStorageMapping=true
Cette propriété est utilisée pour fournir tous les détails sur les données extraites. Si vous ne souhaitez pas collecter tous les détails, spécifiez la

valeur `false` pour cette propriété et réduisez la valeur de la propriété `com.collation.discover.agent.HmcSensor.timeout`.

La valeur par défaut de cette propriété est `true`.

Cette propriété est une propriété sectorisée, vous pouvez ajouter l'adresse IP ou le nom de la portée à cette propriété.

Exemples

Les exemples ci-après montrent les informations extraites, lorsque la propriété `com.collation.discover.agent.HMC.discoverStorageMapping=true` est définie dans le fichier`collation.properties`. Les exemples s'appliquent au système d'exploitation AIX.

discoverDevices

Commande permettant d'obtenir les informations :

```
viosvrcmd -m '{0}' --id '{1}' -c 'lsdev -field name status physloc
description parent -state 1 -fmt ::'
```

discoverPhysicalVolumes

Commande permettant d'obtenir les informations :

```
viosvrcmd -m '{0}' --id '{1}' -c 'lspv -size -fmt ::'
```

discoverVirtualScsiServerAdapters

Commande permettant d'obtenir les informations :

```
viosvrcmd -m '{0}' --id '{1}' -c 'lsmap -all -field svsa physloc
clientid vtd status lun backing -fmt ::'
```

Détecteur IBM Integrated Virtualization Manager

Le détecteur IBM Integrated Virtualization Manager reconnaît des systèmes basés sur des processeurs IBM POWER gérés par un gestionnaire IVM (Integrated Virtualization Manager).

Nom du détecteur utilisé dans l'interface graphique et les journaux

IvmSensor

Ressources reconnues par le détecteur

Le processus de reconnaissance d'un IVM est semblable à celui utilisé pour un système informatique standard. Les problèmes les plus importants ayant un impact sur la reconnaissance sont la connectivité et l'authentification. Si le compte configuré dans la liste d'accès de TADDM peut se connecter à la console IVM, la reconnaissance s'effectue correctement.

Les ressources suivantes peuvent être reconnues par l'intermédiaire de l'IVM :

- la console de gestion intégrée ;
- le système géré par l'IVM (systèmes informatiques System p ou System i) ;
- les partitions logiques (LPAR) définies dans le système géré.

Selon sa portée, la reconnaissance d'un système informatique (LPAR) peut reconnaître en fait deux instances du système informatique :

- le système informatique (LPAR) reconnu par le détecteur IVM ;
- le système informatique reconnu par le détecteur TADDM normal pour le système d'exploitation particulier, comme Linux ou AIX, entre autres.

Cette instance est reconnue exactement de la même manière qu'un système informatique Linux ou AIX physique. Aucun détecteur TADDM spécifique n'a été créé pour reconnaître ces systèmes informatiques virtuels d'une manière différente des systèmes informatiques physiques qu'ils émulent.

Le système informatique (LPAR) reconnu par l'IVM est un système informatique superficiel. Les attributs clés suivants, qui forment la règle de nommage, sont reconnus :

- Manufacturer
- Model
- Numéro de série
- ID LPAR, qui sont des attributs de règle de nommage.

Après une reconnaissance, TADDM fusionne les deux instances en un même système informatique.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- sys.ComputerSystem
- sys.ControlSoftware
- sys.IVM
- sys.SystemPComputerSystem
- sys.VIOS

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations obligatoires suivantes :
   a. Nom d'utilisateur.
   b. Mot de passe

Dans la console de gestion IVM, créez un compte utilisateur pour l'utilisateur de la reconnaissance TADDM avec le rôle Visualisation uniquement.

Détecteur de système informatique IBM i

Le détecteur reconnaît le système d'exploitation IBM i, qui est utilisé sur la famille de serveurs IBM Power Systems et correspond à la prochaine génération du système d'exploitation IBM i5/OS et du système d'exploitation IBM OS/400.

Nom du détecteur utilisé dans l'interface graphique et les journaux

I5OSComputerSystemSensor

Prérequis

Le détecteur requiert que les logiciels suivants soient installés et opérationnels :

- IBM Portable Utilities for i, qui fournit OpenSSH et OpenSSL for IBM i.
- Qshell, qui est un interpréteur de commandes base sur des normes et qui active un environnement de développement.
- Portable Application Solutions Environment (PASE), qui inclut trois shells (Korn, Bourne et C Shell) et plus de 200 utilitaires s'exécutant comme les programmes IBM i PASE.
- IBM Toolbox for Java, qui est une bibliothèque de classes Java offrant aux programmes Java un accès facile aux données et aux ressources IBM i.

Pour IBM i 7.1, il vous faut les versions suivantes du logiciel obligatoire :

- IBM Portable Utilities for i : 5733SC1 *BASE et option 1 (V7R1M0)
- Qshell : 5770SS1 option 30
- PASE : 5770SS1 option 33

Remarque : Dans IBM i 7.1, le logiciel sous licence JC1 (IBM Toolbox for Java) n'est plus fourni à part. Il est à la place inclus dans 5770SS1 option 3.

Pour IBM i 6.1, il vous fait les versions suivantes du logiciel obligatoire :

- IBM Portable Utilities for i : 5733SC1 *BASE et option 1 (V6R1M0)
- Qshell : 5761SS1 option 30
- PASE : 5761SS1 option 33
- IBM Toolbox for Java : 5761JC1

Pour IBM i 5.4 et i5/OS V5R3, il vous faut les versions suivantes du logiciel obligatoire :

- IBM Portable Utilities for i5/OS : 5733SC1 *BASE et option 1
- Qshell : 5722SS1 option 30
- PASE : 5722SS1 option 33
- IBM Toolbox for Java : 5722JC1

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

TADDM ne prend pas en charge la reconnaissance de systèmes IBM i si une authentification par infrastructure PKI (Public Key Infrastructure) est utilisée. Pour initialiser une connexion entre le serveur TADDM et un système IBM i, vous devez utiliser un nom d'utilisateur et un mot de passe.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- dev.MediaAccessDevice
- sys.i5OS.I5OperatingSystem
- sys.i5OS.I5OSSoftwareComponent
- sys.i5OS.I5Profile

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Les utilisateurs doivent disposer des privilèges d'accès suffisants pour reconnaître le système :

- Classe de privilèges : Utilisateur
- Privilèges système :
  - L'accès à tous les objets est requis pour reconnaître tous les profils utilisateur sur le système.
  - Sauvegarde/restauration

système informatique IPSO, détecteur

Le détecteur de système informatique IPSO reconnaît les périphériques pare-feux Nokia qui exécutent le système d'exploitation IPSO.

Nom du détecteur utilisé dans l'interface graphique et les journaux

IPSOComputerSystemSensor

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent net.Firewall
- sys.Function
- sys.ipso.ipso
- sys.ipso.IPSOUnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour une authentification à base de clé SSH ou une authentification basée sur une connexion SSH au système cible.

Détecteur de système informatique Linux

Le détecteur de système informatique Linux reconnaît des systèmes informatiques qui exécutent le système d'exploitation Linux.

Nom du détecteur utilisé dans l'interface graphique et les journaux

LinuxComputerSystemSensor

Prérequis

Si vous reconnaissez Red Hat Enterprise Linux 7, ou CentOS Linux 7 à l'aide du détecteur de système informatique Linux, vous devez installer la commande **`ifconfig`** sur les cibles. Cette commande est fournie dans le package net-tools.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS, TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de système informatique Linux prend en charge les reconnaissances asynchrones et basées sur un script.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Certaines fonctions fournies par le détecteur de système informatique Linux lors d'une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

Les fonctions suivantes ne sont pas prises en charge :

- Modèles et extensions des systèmes informatiques
- Reconnaissance approfondie de niveau 2
- Reconnaissance sur les systèmes Linux qui ne sont pas des systèmes x86

Les attributs suivants ne sont pas pris en charge pour l'objet de modèle L2Interface :

- AutoNegotiation
- Speed
- Duplex

Objets de modèle avec attributs associés

Le détecteur de système informatique Linux crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les systèmes informatiques exécutant le système d'exploitation Linux.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

core.LogicalContent

- Checksum
- Configfile
- Content
- ContentType
- FixedPath
- URI

sys.linux.LinuxUnitaryComputerSystem

- Architecture
- BIOSDate
- BIOSManufacturer
- BIOSName
- CPUCoresInstalled
- CPUDiesInstalled
- CPUSpeed
- CPUType
- Fqdn
- Manufacturer
- MemorySize
- Model
- Name
- NumCPUs
- SerialNumber
- Signature
- SystemId
- TimeZone
- Type
- UUID
- VirtualMachineState

net.L2Interface

- AutoNegotiation
- Broadcast
- Duplex
- Encapsulation
- HwAddress
- InterfaceMTU
- InterfaceName
- Loopback
- Mtu
- Name
- Promiscious
- Speed
- IANAInterfaceType

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

sys.CPU

- IndexOrder
- CPUType
- NumCPUs

- CPUSpeed
- CPUCoresInstalled
- Virtual
- CPUCore

sys.DNSResolveEntry

- SearchOrder
- ServerIp

sys.unix.UnixFileSystem

- AvailableSpace
- Capacity
- Group
- MountPoint
- Owner
- Permissions
- Type

sys.linux.Linux

- BootTime
- Charset
- FQDN
- KernelArchitecture
- KernelModulesRawData
- KernelVersion
- EnvironnementLocal
- Name
- OSConfidence
- OSMode
- OSName
- OSVersion
- OsId
- VirtualMemorySize
- WordSize

sys.PageSpace

- Nom
- PageSpacePriority
- Size
- Type

sys.SoftwareComponent

- Nom
- Publisher
- Edition
- SoftwareVersion

sys.zOS.LPAR

sys.zOS.ZSeriesComputerSystem

sys.zOS.ZVMGuest

Configuration du détecteur

Avant d'exécuter une reconnaissance, vous devez configurer le détecteur de système informatique Linux.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM devrait utiliser pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège (généralement effectuée à l'aide de la commande **sudo**).

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Vous pouvez configurer le détecteur de système informatique Linux dans la console de gestion de reconnaissance en définissant les attributs suivants :

ignoreVMCPCommand=false

Cette propriété est utilisée lorsque la commande **vmcp** échoue ce qui pourrait conduire à des fusions en plus de plusieurs systèmes Linux.

La valeur par défaut de cette propriété est `false`. Si la valeur est définie à `true`, la commande **vmcp** est ignorée.

La valeur `true` peut être utilisée, par exemple, lorsque Linux est installé sur LPAR. Pour changer la valeur pour `true`, vous devez créer une configuration de détecteur sous l'onglet **Profils de reconnaissance**. Dans la fenêtre Créer une configuration, changez la valeur de la propriété de `false` à `true`, et sélectionnez l'option `Activer cette configuration et désactiver la configuration sélectionnée`.

Remarque : Cette propriété est ignorée lorsque la propriété `com.ibm.cdb.discover.zlinux.ignoreVMCPCommand.enabled` est définie sur `true`. Pour plus d'informations, voir la description de cette propriété dans la rubrique «Configuration des entrées du fichier collation.properties» du détecteur de système informatique Linux.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur de système informatique Linux.

Le détecteur utilise la commande **vmcp** du programme de contrôle pour reconnaître un système virtuel Linux qui est exécuté sur un système d'exploitation z/VM. Pour chaque système virtuel Linux, indiquez le chemin d'accès à la commande **vmcp** dans le fichier `collation.properties`.

Fix Pack 5 **com.collation.platform.os.unix.find.excludenfsmount=false**
La valeur par défaut est `false`.

Cette propriété est utilisée lorsque le modèle d'extension `LinuxComputerSystemTemplate` est activé pour rechercher le fichier de saisie. Elle permet d'indiquer s'il convient d'utiliser, ou non, la commande `find` pour rechercher un fichier de capture configuré à l'aide de `LinuxComputerSystemTemplate` dans les points de montage NFS.

Si cette propriété est définie sur `true`, le détecteur LinuxComputerSystem recherche le fichier spécifié sur le serveur local seulement. Sinon, il le recherche également dans les points de montage NFS.

Fix Pack 4 **com.collation.platform.os.command.ifconfig=**
Cette propriété indique le chemin d'accès à une commande qui est utilisée pour configurer des interfaces réseau. Par exemple, **ifconfig**. Vous pouvez toutefois indiquer une autre commande de fonction identique, telle que la commande **ip**. Des interfaces réseau sont requises pour garantir la réussite de la reconnaissance.

Fix Pack 3 **com.collation.platform.os.command.CPUSpeed=cat /proc/cpuinfo | grep 'cpu MHz'|awk '{print $4}'| tail -1**
Cette propriété indique la commande utilisée pour récupérer la valeur de l'attribut CPUSpeed exprimée en MHz. La valeur par défaut de cette propriété est `cat /proc/cpuinfo | grep 'cpu MHz'|awk '{print $4}'| tail -1`.

Fix Pack 2 **com.ibm.cdb.discover.zlinux.ignoreVMCPCommand.enabled=false**
Cette propriété indique si l'attribut `ignoreVMCPCommand` ou la propriété `com.ibm.cdb.discover.zlinux.ignoreVMCPCommand` est utilisé(e). Si elle est définie sur `false`, l'attribut `ignoreVMCPCommand` est utilisé. Si elle est définie sur `true`, la propriété `com.ibm.cdb.discover.zlinux.ignoreVMCPCommand` est utilisée, et tous les détecteurs sont activés afin de reconnaître les attributs VMID et MMS des cibles Linux on System z.

La valeur par défaut de cette propriété est `false`.

Important : Utilisez cette propriété uniquement si vous rencontrez des difficultés avec les signatures qui changent lorsque vous reconnaissez des cibles Linux on System z. Si vous décidez de définir cette propriété sur `true`, vous devez la définir sur cette valeur dans tous les profils de reconnaissance pour lesquels l'attribut `ignoreVMCPCommand` est défini. De la même manière, si cette propriété est définie sur `false`, elle doit être définie sur cette valeur dans tous les profils de reconnaissance.

Pour plus d'informations sur l'attribut `ignoreVMCPCommand`, voir la rubrique «Configuration du profil de reconnaissance», à la page 369 du détecteur de système informatique Linux.

Fix Pack 2 **com.ibm.cdb.discover.zlinux.ignoreVMCPCommand=false**
Cette propriété est utilisée uniquement lorsque la propriété `com.ibm.cdb.discover.zlinux.ignoreVMCPCommand.enabled` est définie sur `true`.

Elle s'utilise de la même manière que l'attribut `ignoreVMCPCommand`, à la différence près qu'elle s'applique à tous les détecteurs qui reconnaissent les cibles Linux on System z, et pas uniquement à LinuxComputerSystemSensor. Elle fournit la valeur de l'attribut `ignoreVMCPCommand` pour tous les détecteurs concernés et permet d'éviter les excès de fusions faisant suite à une valeur erronée de l'attribut VMID, ou à l'absence d'une valeur.

La valeur par défaut de cette propriété est `false`.

Important : Utilisez cette propriété uniquement si vous rencontrez des difficultés avec les signatures qui changent lorsque vous reconnaissez des cibles Linux on System z. Si vous décidez de définir cette propriété sur `true`, vous devez la définir sur cette valeur dans tous les profils de reconnaissance pour lesquels l'attribut `ignoreVMCPCommand` est défini sur `true`. De la même manière, si cette propriété est définie sur `false`, elle doit être définie sur cette valeur dans tous les profils de reconnaissance.

com.collation.discover.agent.command.vmcp.Linux.1.2.3.4={command path}
Cette valeur indique le chemin d'accès de la commande **vmcp** pour différents systèmes virtuels Linux ayant des adresses IP différentes. Par exemple, pour indiquer le chemin d'accès de la commande **vmcp** dans le répertoire `/sbin` d'un hôte Linux avec l'adresse IP 192.168.1.2, ajoutez l'entrée suivante dans le fichier `collation.properties` :

```
com.collation.discover.agent.command.vmcp.Linux.192.168.1.2=sudo /sbin/vmcp
```

com.collation.platform.os.command.crontabEntriesCommand.Linux=crontab -l -u
Cette propriété sert à reconnaître des entrées **crontab**. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesCommand.Linux.1.2.3.4=crontab -l -u
```

com.collation.platform.os.command.crontabEntriesUsers.Linux=root
Cette propriété sert à reconnaître des entrées **crontab** pour un utilisateur déterminé ; pour indiquer plusieurs utilisateurs, séparez-les par des virgules. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesUsers.Linux.1.2.3.4=root,build
```

com.collation.discover.agent.sys.ComputerSystem.serialNumberSanityChecks="⌂(?!null);⌂(?!not);⌂(?!n/a);⌂(?!permission);⌂(?!to be);⌂(?!undef); ⌂[-:\.\w]{4,80}$; ^(?!.{8}(\-.{4}){3}\-.{12}_.{2}(:.{2}){5});^(?!none);^(?!x{7});^(?!\.{9});^(?!0123456789);^(?!0+$)";

Cette propriété sert à valider la propriété serialNumber reconnue par les détecteurs du système d'exploitation (sauf Solaris) afin d'éviter de stocker des valeurs génériques (telles que Not Defined, To be set by OEM ou Permission Denied).

La principale règle par défaut est que le numéro de série contient entre 4 et 80 caractères et ne commence pas par l'une des chaînes suivantes :

- **null** : expression régulière **^(?!null)**
- **not** : expression régulière **^(?!not)**
- **n/a** : expression régulière **^(?!n/a)**
- **permission** : expression régulière **^(?!permission)**

- **to be** : expression régulière **^(?!to be)**
- **undef** : expression régulière **^(?!undef)**
- string in form : **098D8710-E623-3C3B-9F9B-FCBAFF1BF3B6_5C:F3:FC:E8:89:FC** : expression régulière **^(?!.{8}(\-.{4}){3}\-.{12}_.{2}(:.{2}){5})**
- **none** : expression régulière **^(?!none)**
- **xxxxxxx** : expression régulière **^(?!x{7})**
- **.....** : expression régulière **^(?!\.{9})**
- **0123456789** : expression régulière **^(?!0123456789)**
- **0000** : expression régulière **^(?!0+$)**

Si un numéro de série ne suit pas cette règle, il n'est pas défini. La syntaxe d'expression régulière est définie dans le SDK Java pour la classe `java.util.regex.Pattern`. Les expressions régulières doivent être séparées par des points-virgules. Les numéros de série candidats sont toujours convertis en minuscules avant d'être mis en correspondance avec des expressions régulières. Par conséquent, quand vous personnalisez la propriété, prenez uniquement des caractères en minuscules.

com.collation.discover.agent.ignoreVirtualMAC=true
Cette propriété indique si la reconnaissance des adresses matérielles d'interfaces virtuelles sur des cibles Linux est activée. Si vous définissez cette propriété sur `true`, les adresses matérielles sont reconnues.

La valeur par défaut de cette propriété est `true`.

Référence associée:

«Identification et résolution des problèmes liés au détecteur»
Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique Linux et propose des solutions à ces problèmes.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique Linux et propose des solutions à ces problèmes.

Une erreur de signature d'hôte se produit sur les cibles Red Hat Enterprise Linux 7 et CentOS Linux 7

Problème

Lorsque vous reconnaissez des systèmes cibles exécutant Red Hat Enterprise Linux 7 ou CentOS Linux 7, l'erreur suivante se produit :

```
2016-03-31 15:46:31,759 DiscoverManager [DiscoverWorker-7]
SessionSensor-9.1.146.78-[22] DEBUG session.SshSessionClient - Command
[LC_ALL=en_US.UTF-8;LANG=en_US.UTF-8;export LANG LC_ALL;ifconfig  -a]
failed in session
ssh2:/HostAuthcom.collation.platform.security.auth.HostAuth[taddmcfm][XX
XXX]/null@9.1.146.78: exit status 127 (no stdout)
```

Solution

Pour résoudre le problème, vous devez installer la commande **ifconfig** sur les cibles. Cette commande est fournie dans le package net-tools.

Fix Pack 4 Dans TADDM 7.3.0.4 et versions ultérieures, vous n'avez pas à utiliser la commande **ifconfig**. Vous pouvez sélectionner n'importe quelle autre commande capable de gérer des interfaces réseau. Dans ce cas, indiquez son nom et son chemin d'accès dans la propriété `com.collation.platform.os.com mand.ifconfig` du fichier

`collation.properties`. Pour plus d'informations, voir «Configuration des entrées du fichier collation.properties», à la page 369.

Echec du détecteur car l'exécution d'une commande a échoué

Problème

Le message suivant s'affiche :

```
Error Message: CTJTD0431E: The following command failed to run or returns
a blank value: sudo /sbin/vmcp q userid | awk 'print{3}'.
```

L'exécution de la commande **vmcp q userid** a échoué et renvoie une valeur vide au système virtuel Linux cible qui exécute le système d'exploitation z/VM.

Solution

Ce problème est dû à l'une des conditions suivantes :

- La spécification d'un chemin d'accès incorrect pour la commande **vmcp** sur le système virtuel Linux cible.
- L'outil **vmcp** n'est pas installé sur le système virtuel Linux cible.
- La commande **sudo** n'est pas configurée pour exécuter la commande **vmcp**.
- Le nom de système n'est pas configuré sur le système z/VM.

Pour résoudre ce problème, procédez comme suit :

- Vérifiez que le chemin d'accès entré pour la commande **vmcp** est correct dans le fichier `collation.properties`. Pour plus d'informations, voir «Configuration des entrées du fichier collation.properties», à la page 369.
- Vérifiez que le nom de système est configuré dans le système z/VM, le nom de système doit être renseigné.
- Si l'outil **vmcp** n'est pas installé sur le système virtuel Linux, vous devez le charger. Pour charger le pilote de périphérique **vmcp**, exécutez la commande `modprobe vmcp` sur l'invité Linux.
- Vérifiez la disponibilité de la commande **sudo**. Pour cela, exécutez la commande suivante sur l'invité Linux où l'agent de surveillance est installé :

  ```
  sudo vmcp q userid
  ```

  Si la commande **sudo** est active et chargée, elle envoie la commande **q userid** à la machine virtuelle hébergeante qui demande l'ID utilisateur pour l'invité.

  S'il n'existe aucune exigence pour le rapprochement du système virtuel Linux avec le système hôte sur le système d'exploitation z/VM, l'exécution de la commande **vmcp** n'est pas nécessaire. Vous pouvez utiliser la propriété de commande externalisée (com.collation.discover.agent.command.vmcp.Linux=) dans le fichier *collation.properties* pour définir la valeur du système hôte à «dummy». Vous devez pouvoir analyser la commande externalisée avec la commande suivante qui lui est annexée :

  ```
  q userid | awk '{ print $3 }'
  ```

  Par exemple, vous pourriez utiliser :

  ```
  com.collation.discover.agent.command.vmcp.Linux.192.168.1.2=echo A B zVMHost
  ```

Cela génère `echo A B zVMHost q userid | awk '{print $3 }'` qui renvoie le nom `zVMHost`. L'attribut hôte pour vos systèmes virtuels est définie à «zvmhost» au lieu du nom du système hôte réel.

- Vous pouvez désactiver la commande **vmcp** en définissant la commande **ignoreVMCPCommand** à `true`. Pour plus d'informations, voir «Configuration des entrées du fichier collation.properties», à la page 369.

Les invités z/VM peuvent être dupliqués après plusieurs reconnaissances du même système virtuel Linux

Problème

Des doublons peuvent se produire si la commande **vmcp q userid** renvoie une valeur vide sur le système virtuel Linux en cours d'exécution sur un système d'exploitation z/VM.

Solution

Vous devez fusionner manuellement ces doublons.

détecteur de système informatique OpenVMS

Le détecteur de système informatique OpenVMS reconnaît les systèmes informatiques exécutant le système d'exploitation OpenVMS.

Nom du détecteur utilisé dans l'interface graphique et les journaux

OpenVmsComputerSystemSensor

Prérequis

Pour exécuter correctement une reconnaissance avec le détecteur de système informatique OpenVMS, vous devez effectuer les tâches prérequises suivantes :

- Accordez à l'utilisateur de la reconnaissance les privilèges suivants :
  - CMKRNL
  - NETMBX
  - SYSLCK
  - TMPMBX
  - WORLD
- Affectez au paramètre `PGFLQUOTA` la valeur `327680`.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- sys.openvms.OpenVms
- sys.openvms.OpenVmsUnitaryComputerSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM devrait utiliser pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique OpenVMS et propose des solutions.

Le détecteur échoue sans erreur

Problème

Le détecteur de système informatique OpenVMS échoue pendant la reconnaissance, mais n'enregistre aucune erreur. L'état de la reconnaissance est `terminé` comme si la reconnaissance avait réussi.

Solution

Accordez à l'utilisateur de la reconnaissance le privilège SYSLCK.

Erreur INSVIRMEM affichée sous l'onglet Licences logicielles

Problème

L'onglet **Licences logicielles** contient le message suivant :

```
?%LIB-F-INSVIRMEM, mémoire virtuelle insuffisante
```

Solution

Pour résoudre le problème, définissez le paramètre `PGFLQUOTA` sur `327680`.

détecteur de système informatique Solaris

Le détecteur de système informatique Solaris reconnaît les systèmes informatiques exécutant le système d'exploitation Solaris.

Fix Pack 2 Si vous souhaitez reconnaître les systèmes Solaris Virtualization, exécutez le détecteur Sun Sparc Virtualization. Pour plus d'informations, voir «Détecteur Sun Sparc Virtualization», à la page 382.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SunSparcComputerSystemSensor

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Le détecteur reconnaît le nombre de processeurs physiques si l'une des commandes suivantes se trouvent sur le système cible :

- **psrinfo -p**
- **prtconf** et **kstat -m cpu_info**. La commande **kstat** doit renvoyer des statistiques d'implémentation.

Le détecteur reconnaît le nombre de coeurs de processeur quand la commande **kstat -m cpu_info** se trouve sur le système cible. La commande **kstat** doit renvoyer des statistiques core_id.

Pour que le détecteur reconnaisse des informations liées au mode promiscuité sur le système d'exploitation Solaris, la commande suivante doit être disponible pour l'interface réseau sur le système cible :

```
kstat
nom_interface_réseau | grep promisc
```

Le détecteur ne reconnaît pas les systèmes de fichiers ZFS.

Si vous souhaitez reconnaître le système d'exploitation Solaris en exécutant le détecteur de serveur générique, la commande **/usr/ucb/ps** doit être disponible sur le serveur Solaris. Pour installer la commande, installez l'un des packages suivants sur les cibles Solaris :

- Versions Solaris antérieures à la version 10 : installez l'un des packages suivants ou les deux :
  - Solaris 32 bits : package `SUNWscpu`
  - Solaris 64 bits : package `SUNWscpux`
- Solaris 10 : package `SUNWscpu`
- Solaris 11 : package `compatibility/ucb`

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS, TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Prise en charge de la reconnaissance asynchrone et basée sur un script

Le détecteur de système informatique Solaris prend en charge les reconnaissances asynchrones et basées sur un scripts.

Conditions requises pour la configuration du détecteur

Pour une reconnaissance asynchrone, le détecteur ne nécessite aucune configuration.

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Certaines fonctions fournies par le détecteur de système informatique Solaris durant une reconnaissance non basée sur un script ne sont pas prises en charge dans une reconnaissance asynchrone ou basée sur un script.

Les fonctions suivantes ne sont pas prises en charge :

- Modèles et extensions des systèmes informatiques
- Reconnaissance approfondie de niveau 2
- Reconnaissance de zones

Les attributs suivants ne sont pas pris en charge :

- L2Interface
  - AutoNegotiation
  - Speed
  - Duplex
- ComputerSystem (zone globale)
  - Virtual
  - ChildSystem
  - VMID
  - CPUCoresInstalled
  - CPUDiesInstalled
- ComputerSystem (zone locale)
  - Virtual
  - HostSystem

- VMID
- CPUCoresInstalled
- CPUDiesInstalled

Objets de modèle avec attributs associés

Le détecteur de système informatique Solaris crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les systèmes informatiques exécutant le système d'exploitation Solaris.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

sys.sun.SunSPARCUnitaryComputerSystem

- Name
- Type
- SystemId
- VirtualMachineState
- Signature
- Fqdn
- Manufacturer
- Model
- MemorySize
- BIOSDate
- BIOSName
- NumCPUs
- CPUType
- CPUSpeed
- Architecture
- Virtual
- TimeZone
- CPUDiesInstalled
- CPUCoresInstalled
- ChildSystem

sys.CPU

- IndexOrder
- CPUType
- NumCPUs
- CPUSpeed
- CPUCoresInstalled
- Virtual
- CPUCore

sys.sun.Solaris

- Fqdn
- Name
- OSName
- OSVersion

- BootTime
- PatchesInstalledRawData
- KernelArchitecture
- KernelVersion
- WordSize
- Charset
- OsId
- KernelModulesRawData
- OSMode
- OSConfidence
- VersionString

sys.DNSResolveEntry

- SearchOrder
- ServerIp

core.LogicalContent

- Checksum
- Content
- FixedPath
- URI

sys.SoftwareComponent

- Name
- SoftwareVersion

net.L2Interface

- AutoNegotiation
- Broadcast
- Duplex
- Encapsulation
- HwAddress
- InterfaceMTU
- InterfaceName
- Loopback
- Mtu
- Name
- Promiscious
- Speed
- IANAInterfaceType

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

sys.unix.UnixFileSystem

- AvailableSpace
- Capacity
- Group

- MountPoint
- Owner
- Permissions
- Type

Configuration du détecteur

Avant d'entamer une reconnaissance, vous devez configurer le détecteur de système informatique Solaris.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège (généralement effectuée à l'aide de la commande **sudo**).

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier collation.properties utilisées par le détecteur de système informatique Solaris.

Le détecteur utilise l'entrée suivante du fichier `collation.properties` :

com.collation.platform.os.command.crontabEntriesCommand.SunOS=crontab -l
Cette propriété sert à reconnaître des entrées **crontab**. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesCommand.SunOS.1.2.3.4=crontab -l
```

com.collation.platform.os.command.crontabEntriesUsers.SunOS=root
Cette propriété sert à reconnaître des entrées **crontab** pour un utilisateur déterminé ; pour indiquer plusieurs utilisateurs, séparez-les par des virgules. Vous pouvez l'indiquer comme une propriété sectorisée en lui ajoutant une adresse IP ou un nom d'ensemble de portées. L'exemple suivant montre une adresse IP ajoutée :

```
com.collation.platform.os.command.crontabEntriesUsers.SunOS.1.2.3.4=root,build
```

com.collation.discover.agent.useSolarisPfiles=false
La valeur par défaut est `false`.

Lorsque défini sur `true`, cette propriété pousse le détecteur GenericServerSensor à utiliser les commandes **ptree** et **pfiles** sur des systèmes cibles Solaris afin de reconnaître la liste de sockets IP et de ports

associés aux processus en cours d'exécution. La propriété remplace l'utilisation de **lsof** qui risque de ne pas être disponible dans un environnement Solaris.

Fix Pack 5 **com.collation.discover.agent.path.SunOS.prtdiag=/sbin/prtdiag**
La valeur par défaut est `/sbin/prtdiag`.

Cette propriété est utilisée pour indiquer tous les chemins d'accès valides d'où la commande `prtdiag` peut être exécutée sur un serveur Solaris.

Elle est utile lorsque l'environnement comporte plusieurs serveurs Solaris et que des serveurs différents possèdent des chemins d'accès différents d'où la commande `prtdiag` peut être exécutée. Dans de tels scénarios, vous pouvez ajouter tous les chemins d'accès valides connus à l'aide de cette propriété séparée par des deux points (:).

Par exemple : `com.collation.discover.agent.path.SunOS.prtdiag=/usr/sbin/prtdiag:/sbin/prtdiag:/sbin/sparcv9/prtdiag`

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique Solaris et propose des solutions à ces problèmes.

Le détecteur ne démarre pas

Problème

L'utilisateur de la reconnaissance TADDM ne dispose pas des droits d'accès nécessaires pour exécuter la commande **ps** avec les arguments de ligne de commande complets requis pour démarrer le détecteur.

Solution

Exécutez l'une des tâches suivantes :

- Définissez le bit permanent de la commande **ps** à l'aide de la commande suivante :

  ```
  chmod u+s /usr/ucb/ps
  ```

  Remarque : Il se peut que le bit permanent soit remplacé par le système d'exploitation si le module de correction appliqué met à jour la commande **ps**.
- Procédez comme suit pour configurer la commande **ps** pour qu'elle s'exécute avec l'accès à la commande **sudo** pour l'utilisateur de la reconnaissance TADDM :
  1. Définissez les propriétés suivantes dans le fichier$*COLLATION_HOME*/`etc/collation.properties` :
     - `com.collation.platform.os.command.ps.SunOS=sudo /usr/ucb/ps axww`
     - `com.collation.platform.os.command.psEnv.SunOS=sudo /usr/ucb/ps axwweee`
     - `com.collation.platform.os.command.psParent.SunOS=sudo ps -elf -o ruser,pid,ppid,comm`
     - `com.collation.platform.os.command.psUsers.SunOS=sudo /usr/ucb/ps auxw`
  2. Assurez-vous que l'accès à la commande **sudo** a été accordé à l'utilisateur de la reconnaissance TADDM en exécutant la commande suivante sur le système cible :

```
sudo ps
```

Une reconnaissance effectuée par le biais d'IBM Tivoli Monitoring échoue

Problème

Une reconnaissance effectuée à l'aide d'IBM Tivoli échoue en raison d'un problème d'exécution de la commande **cd $HOME;LANG=C zonecfg-z s8-zone info**.

Solution

Dans le fichier `collation.properties file`,ajoutez le modèle `|.*zonecfg.*` à la fin de la propriété :

```
com.collation.discover.agent.ITM.CmdWrapperSelectionPattern=|.*zonecfg.*
```

Une zone locale est reconnue sans adresse IP

Problème

Après la reconnaissance d'une zone commune, une zone locale est reconnue sans adresse IP.

Solution

Pour certaines zones locales utilisant une carte Ethernet exclusive, une adresse IP de zone ne peut pas être déterminée depuis le niveau de zone commune. Vous devez exécuter une reconnaissance directe de cette zone pour obtenir des informations complètes la concernant.

Pour obtenir manuellement la configuration IP d'une zone locale, exécutez la commande suivante depuis le niveau de zone commune :

```
zlogin <zonename> ifconfig -a inet
```

Lorsque vous exécutez le détecteur de serveur générique pour reconnaître des cibles Solaris, des erreurs CTJTD0317E et CTJTP1135E se produisent

Problème

Lorsque vous exécutez le détecteur de serveur générique pour reconnaître des cibles de système d'exploitation Solaris, l'erreur et l'exception suivantes se produisent dans la console de gestion de reconnaissance :

```
CTJTD0317E Une erreur s'est produite. CTJTP1135E Le texte suivant contient le statut de sortie : 1
```

Solution

L'erreur indique que la commande **/usr/ucb/ps** n'est pas installée sur le serveur Solaris. Pour résoudre le problème, installez l'un des packages suivants sur vos cibles Solaris :

- Versions Solaris antérieures à la version 10 : installez l'un des packages suivants ou les deux :
  - Solaris 32 bits : package `SUNWscpu`
  - Solaris 64 bits : package `SUNWscpux`
- Solaris 10 : package `SUNWscpu`
- Solaris 11 : package `compatibility/ucb`

Détecteur Sun Sparc Virtualization

Fix Pack 2

Le détecteur Sun Sparc Virtualization reconnaît les deux types de virtualisation Solaris, à savoir les zones et les domaines logiques, sur un système d'exploitation Solaris.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SunSparcVirtualizationSensor

Portée de reconnaissance du détecteur Sun Sparc Virtualization

Le détecteur reconnaît si les domaines invités sont actifs et récupère toutes les informations s'y rapportant.

Il reconnaît également si les zones non communes sont actives et récupère toutes les informations s'y rapportant.

Dépendance du détecteur Sun Sparc Virtualization

Le détecteur dépend du détecteur de système informatique Solaris, qui s'exécute juste avant le détecteur Sun Sparc Virtualization.

Le détecteur de système informatique Solaris reconnaît le système Solaris et les informations détaillées associées et transmet l'objet SunSPARCUnitaryComputerSystem au détecteur Sun Sparc Virtualization.

Pour cet objet SunSPARCUnitaryComputerSystem, le détecteur Sun Sparc Virtualization :

- reconnaît tous les domaines invités et zones non communes disponibles, et
- pour chacun de ces éléments, créé l'objet superficiel SunSPARCUnitaryComputerSystem.

Le détecteur Sun Sparc Virtualization peut être exécuté sur les systèmes Solaris de type de virtualisation :

Tableau 24. Reconnaissance du type de virtualisation Solaris

Type de virtualisation Solaris	Reconnaît
Zone commune	Zones communes et non communes
Zone non commune*	Zone non commune
Domaine de contrôle	Domaine de contrôle (avec nom principal) et domaines invités
Domaine invité*	Domaine invité

Remarque : *Pour récupérer les informations relatives au système d'exploitation dans le cadre des "zones non communes" et des "domaines invités", vous devez ajouter l'adresse IP des zones et des domaines à la portée de reconnaissance et réexécuter le détecteur de système informatique Solaris.

Objets de modèle avec attributs associés

Fix Pack 2

Le détecteur Sun Sparc Virtualization crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur à propos des systèmes informatiques exécutant le système d'exploitation Solaris avec les zones et les domaines logiques disponibles.

Le détecteur crée les objets de modèle suivants pour les zones et les domaines logiques reconnus. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

Pour les domaines logiques
sys.sun.SunSPARCUnitaryComputerSystem
SystemId

Type

Functions

PrimaryMACAddress

MemorySize

NumCPUs

Pour les zones non communes
sys.sun.SunSPARCUnitaryComputerSystem
Virtual

Type

VMID

Functions

SystemId

Devices

ConfigContents

Fqdn

HostSystem

IsVMIDanLPAR

IpInterfaces

sys.Function
Name

- Pour les domaines logiques : 'Guest domain' ou 'Control domain'
- Pour les zones : 'Zone'

net.IpInterface
IpAddress

détecteur Sun Fire SysControl

Le détecteur Sun Fire SysControl (SC) reconnaît les domaines qui sont configurés sur les systèmes Sun Fire.

Les informations suivantes proviennent du contrôleur système figurant sur le système Sun Fire :

- Opérations d'administration de configuration à distance
- Affectations de carte et état de la carte
- Statistiques d'utilisation actuelles des ressources Capacity on Demand (COD)
- Périphériques de carte mère et informations d'utilisation de ressources
- Rôle ou état de la reprise du contrôleur système
- Type de plateforme, liste de composants disponibles de la carte, état de chaque domaine, informations de Capacity on Demand (COD)

Nom du détecteur utilisé dans l'interface graphique et les journaux

SysControlSensor

Problèmes de sécurité

Le compte de service TADDM doit disposer des droits d'administrateur de la plateforme, ce qui signifie que le compte est un membre du groupe platadmn UNIX. Tout utilisateur qui est membre de du groupe platadmn dispose des privilèges permettant d'exécuter les commandes SMS (System Management Services) suivantes :

- **rcfgadm**
- **showboards**
- **showcodusage**
- **showdevices**
- **showfailover**
- **showplatform**

Objets de modèle avec attributs associés

Le détecteur Sun Fire SysControl (SC) crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les domaines configurés sur des systèmes Sun Fire dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet modèle.

phys.physpkg.Board

- DisplayName
- Name
- Package physique
- RelativePosition

sys.sun.DynamicSystemDomain

- Board
- DisplayName
- Fqdn
- HostSystem
- IsVMIDanLPAR
- Model
- Name
- NumCPUs
- SerialNumber
- Type
- Virtual

sys.sun.SunFireComputerSystem

- ChildSystem
- Devices
- DisplayName

- Manufacturer
- Model
- Name
- SerialNumber
- Type

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

Un compte doté des droits de l'administrateur de la plateforme doit être utilisé.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.discover.agent.path.SunOS
Cette valeur indique la configuration du chemin d'accès pourl'exécution des commandes.

Les commandes suivantes sont des commandes SMS (System Management Services) qui exécutent :

- **`rcfgadm`**
- **`showboards`**
- **`showcodusage`**
- **`showdevices`**
- **`showfailover`**
- **`showplatform`**

Si les commandes sont dans le répertoire `opt/SUNWSMS/bin`, par exemple, entrez la commande suivante sur la même ligne :

```
com.collation.discover.agent.path.SunOS=/usr/local/bin:/bin:/usr/bin:
/usr/X11R6/bin:/usr/sbin:/sbin:/opt/SUNWSMS/bin
```

com.collation.discover.agent.SysControlAgent.timeout=1200000
Cette valeur indique l'intervalle de temps en millisecondes pour l'exécution de la commande.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Sun Fire syscontrol (SC) et propose des solutions à ces problèmes.

Le détecteur échoue avec une erreur d'expiration du délai d'attente

Problème

Le détecteur échoue avec une erreur d'expiration du délai d'attente pendant la reconnaissance.

Solution

Ajoutez la propriété suivante dans le fichier `etc/collation.properties`, où *valeur* correspond au nombre de millisecondes autorisées pour l'exécution du détecteur :

```
com.collation.discover.agent.SyscontrolAgent.timeout=1200000
```

Augmentez la valeur, jusqu'à ce l'erreur d'expiration du délai d'attente ne se produise plus.

Le détecteur échoue avec une erreur getModelObject

Problème

Le message suivant s'affiche :

```
Message d'erreur : CTJTD3021E : Le détecteur a échoué dans un serveur distant :
 discoverSystemController: getModelObject failure
```

Solution

Dans le fichier `etc/collation.properties`, ajoutez la configuration du chemin d'accès pour l'exécution de la commande (par exemple, /opt/SUNWSMS/bin) :

```
com.collation.discover.agent.path.SunOS=/usr/local/bin:/bin:/usr/bin:
/usr/X11R6/bin:/usr/sbin:/sbin:/opt/SUNWSMS/bin
```

détecteur de système informatique Tru64

Le détecteur de système informatique Tru64 reconnaît des systèmes informatiques qui exécutent le système d'exploitation Tru64 UNIX.

Nom du détecteur utilisé dans l'interface graphique et les journaux

Tru64ComputerSystemSensor

Prérequis

Le détecteur requiert les logiciels suivants :

- Outil de commande **sudo**
- Outil de diagnostic **lsof**

Installez les deux outils dans le même chemin d'accès que celui défini dans la liste d'accès pour accéder au système informatique Tru64 UNIX. Cette installation doit être effectuée sur chaque système informatique Tru64 UNIX à reconnaître. Les versions les plus testées sont **sudo-1.6.8p9** et **lsof-4.78**, mais d'autres versions sont susceptibles de fonctionner, sauf dans les cas où le module spécifique ne prend pas en charge Tru64 UNIX. Les versions **sudo-1.6.8p9** et **lsof-4.78** sont disponibles sur les sites Web suivants :

- Pour **sudo-1.6.8p9** : http://www.gratisoft.us/sudo/download.html
- Pour **lsof-4.78** : http://freecode.com/projects/lsof/?branch%20id=6029&release%20id=19567

Consultez le site Web de votre distributeur ou les fichiers readme du logiciel pour obtenir la liste des restrictions, comme l'ajout ou la suppression de la prise en

charge d'une plateforme ou d'une fonction. Si un module particulier fait l'objet de restrictions, celles-ci s'appliqueront à TADDM.

Limitations

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- sys.ComputerSystem
- sys.tru64.Tru64

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration d'un utilisateur non superutilisateur pour exécuter le détecteur :

Vous devez ajouter les droits d'accès des utilisateurs aux utilisateurs non superutilisateur.

Editez le fichier `/etc/sudoers` sous le système informatique Tru64 UNIX et ajoutez la ligne suivante, où *utilisateur_non_superutilisateur* est l'utilisateur qui exécute la commande :

```
<non-rootuser> ANY = NOPASSWD: /sbin/hwmgr
```

The `/etc/sudoers` doit se trouver sur le système informatique Tru64 UNIX qui est en cours de reconnaissance.

Par exemple, pour permettre à l'utilisateur *taddmusr* d'exécuter la commande sur n'importe quel système informatique Tru64 UNIX , entrez la ligne suivante :

```
taddmusr ANY = NOPASSWD: /sbin/hwmgr
```

Par exemple, pour permettre à l'utilisateur *taddmusr* d'exécuter la commande `/sbin/hwmgr` sur un système cible spécifique appelé *cible*, entrez la ligne suivante :

```
taddmusr target = NOPASSWD: /sbin/hwmgr
```

Vous devez trouver deux commandes sur l'emplacement par défaut du système informatique Tru64 UNIX : `/sbin/hwmgr` et `/usr/sbin/ifconfig`.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

Généralement, un privilège autre que superutilisateur peut être utilisé. Les commandes utilisées par le détecteur de système informatique Tru64 effectuant la reconnaissance peuvent nécessiter une escalade des privilèges. Cette escalade est généralement effectuée en définissant les autorisations d'accès du fichier à l'aide de la commande **sudo**.

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique Tru64 et présente des solutions à ces problèmes.

Affichage de messages d'erreur de stockage

Problème

Messages d'erreur de stockage.

Solution

Dans ce cas, le système Tru64 UNIX envoie un message avec un état `Autre périphérique IP`. Vérifiez les emplacements et les autorisations sur les dépendances, puis exécutez de nouveau la reconnaissance.

Détecteur de système informatique VMware ESX

Le détecteur de système informatique VMware ESX Server reconnaît les serveurs VMware ESX.

Nom du détecteur utilisé dans l'interface graphique et les journaux

VmwareComputerSystemSensor

Eléments reconnus par le détecteur

La reconnaissance du serveur VMware ESX (machine hôte) est la même pour tous les systèmes d'exploitation. Les problèmes les plus importants ayant un impact sur la reconnaissance sont la connectivité et l'authentification. Si le compte configuré dans la liste d'accès TADDM peut se connecter à la cible du serveur VMware ESX, la reconnaissance aboutit.

Les reconnaissances sont lancées à l'aide de commandes run sur SSH.

La reconnaissance des machines virtuelles (machines invitées) identifie deux instances d'une machine virtuelle, une instance physique et une instance virtuelle. Après une reconnaissance, TADDM fusionne ces deux instances. Il en résulte une instance unique comportant tous les attributs d'une machine physique, mais avec

l'indication qu'elle est virtuelle. Dans la sortie XML de la base de données, cette sortie est représentée par un attribut tel que :

```
<virtual>true</virtual>
```

Dans la console de gestion de reconnaissance, une machine virtuelle est représentée par une icône de système informatique bleu transparent.

L'instance physique est reconnue par le détecteur TADDM normal pour le système d'exploitation invité particulier comme Linux. La reconnaissance de l'instance physique est identique à celle de la machine physique, incluant la recherche de périphériques et d'attributs standard. Tout comme pour les machines physiques qu'elles émulent, aucun détecteur TADDM spécifique n'est requis pour reconnaître ces machines virtuelles.

L'instance virtuelle est reconnue par le détecteur VMware ESX. Il utilise principalement des commandes et des fichiers (`.vmx`) de configuration sur le serveur VMware ESX pour reconnaître une instance superficielle avec les données suivantes :

- Données d'attribut requises pour correspondre aux règles de nommage et créer une instance de machine virtuelle autonome valide
- Certaines informations de base fournies par le serveur VMware ESX via la commande **`vmware-cmd`**.
- Un attribut (primaryMACAddress) utilisé pour faire correspondre l'instance virtuelle superficielle à une instance physique pouvant être reconnue

Il existe deux scénarios utilisateur pour la reconnaissance d'une machine virtuelle :

- Global : Lorsqu'une portée qui inclut le serveur et les instances physiques est reconnue, tout fonctionne normalement.

  Ceci a pour résultat une instance virtuelle qui apparaît dans le domaine approprié pour correspondre à son nom de domaine. Cette instance virtuelle est renseignée avec tous les attributs qu'une machine physique aurait.

  Elle contient également des données et des relations concernant le serveur ESX hôte, un attribut virtuel qui est défini sur true, et un attribut VMID qui a la même valeur que l'attribut défini dans le fichier de configuration `.vmx`. Ce scénario ne doit poser aucun problème si TADDM est connecté à la machine virtuelle et peut s'authentifier auprès de celle-ci.
- Machine virtuelle uniquement : Lors de la reconnaissance d'une portée contenant uniquement la machine virtuelle, cette dernière est affichée en tant que machine physique avec des attributs standard, mis à part le fait que VMware remplace volontairement certaines données de modèle et de fabricant.

  Par conséquent, il est possible de déterminer si une machine est virtuelle en examinant certains attributs. L'icône est toutefois celle utilisée pour les ordinateurs physiques et l'attribut virtuel n'est pas défini à true.

Pour vous assurer que toutes les informations FQDN sur la machine virtuelle sont collectées, VMware Tools doit être installé sur la machine virtuelle.

Limitations

Les serveurs VMware vCenter ne sont pas reconnus par le détecteur de système informatique VMware ESX. Si vous devez reconnaître ces serveurs, utilisez le détecteur de serveur VMware Virtual Center.

Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :

- bouclage, par exemple, `127.0.0.1`, `0:0:0:0:0:0:0:1`
- liaison locale, par exemple, `169.254.1.1`, `FE80:0:0:0:0:0:0:1`
- multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
- non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Pour un serveur VMware ESX version 2.5 (toutes éditions), vous ne pouvez reconnaître que des systèmes virtuels en cours d'exécution.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- core.LogicalContent
- net.IpInterface
- net.L2Interface
- process.CPUResourcePool
- process.MemoryResourcePool
- process.NetworkAdapterResourcePool
- relation.AllocatedTo
- relation.DonatedTo
- sys.CPU
- sys.darwin.Darwin
- sys.darwin.DarwinUnitaryComputerSystem
- sys.dos.Dos
- sys.dos.DosUnitaryComputerSystem
- sys.DNSResolveEntry
- sys.FileSystem
- sys.freebsd.FreeBSD
- sys.freebsd.FreeBSDUnitaryComputerSystem
- sys.linux.Linux
- sys.linux.LinuxUnitaryComputerSystem
- sys.Memory
- sys.netware.Netware
- sys.netware.NetwareUnitaryComputerSystem
- sys.OperatingSystem
- sys.sun.Solaris
- sys.sun.SunSPARCUnitaryComputerSystem
- sys.UnitaryComputerSystem
- sys.vmware.VmwareESX
- sys.vmware.VmwareUnitaryComputerSystem
- sys.windows.WindowsComputerSystem
- sys.windows.WindowsOperatingSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Par défaut, le détecteur de système informatique VMware ESX est activé pour une reconnaissance de niveau 2 ou de niveau 3. Le détecteur reconnaît uniquement les systèmes invités en cours d'exécution. Pour reconnaître tous les invités, créez un profil de reconnaissance de niveau 2 ou de niveau 3 pour le détecteur de système informatique VMware ESX, et personnalisez les paramètres du détecteur.

Pour créer un profil de reconnaissance, procédez comme suit :

1. Dans le tiroir **Reconnaissance** de la console de gestion de reconnaissance, cliquez sur **Profils de reconnaissance**.
2. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.
3. Dans la fenêtre Créer un profil, entrez le nom et la description du profil. Dans la liste **Cloner le profil existant**, sélectionnez **Reconnaissance de niveau 2**, ou **Reconnaissance de niveau 3** et cliquez sur **OK**.
4. Sous l'onglet **Configuration du détecteur**, sélectionnez le détecteur **VmwareComputerSystemSensor**.
5. Dans la fenêtre de création de la configuration, entrez le nom et la description de votre configuration, puis sélectionnez la case à cocher **Activer la configuration**.
6. Dans la section **Configuration** de la fenêtre Créer la Configuration, cliquez sur **discoverNonRunningGuests**. Cliquez ensuite deux fois sur la zone **Valeur** dans la ligne et entrez `true`.
7. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
8. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège (généralement effectuée à l'aide de la commande **sudo**).

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Le détecteur utilise les entrées suivantes du fichier `collation.properties` :

com.collation.platform.os.command.osVersion.Vmware=/usr/bin/vmware –v
La valeur par défaut est `/usr/bin/vmware –v`.

Commande utilisée pour identifier la version de VMware.

com.collation.platform.os.command.vmwareCmd=/usr/bin/vmware-cmd
La valeur par défaut est `/usr/bin/vmware-cmd`.

Commande utilisée pour exécuter des opérations sur la machine virtuelle.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique VMware ESX et présente des solutions à ces problèmes.

Des machines virtuelles en double sont créées

Problème

Après la reconnaissance, il semble qu'il existe des copies de certaines machines virtuelles.

Solution

TADDM reconnaît deux instances d'une machine virtuelle, une physique et une virtuelle. Si leur rapprochement avec la même machine spécifique n'est pas possible, deux instances peuvent exister dans la base de données avec des attributs similaires. Il ne s'agit pas d'instances en double, mais de deux instances reconnues séparément sur la même machine virtuelle.

Cette distinction est essentielle pour résoudre le problème. Plusieurs choses sont à vérifier, en commençant par TADDM, puis l'environnement VMware et enfin identifier et résoudre les problèmes de l'environnement réseau général.

Problèmes liés à une base de données ou une instance pré-existante

Le premier élément à vérifier lors de la résolution d'un incident de synchronisation est la base de données. Si la transition de la machine virtuelle vers une nouvelle machine virtuelle a été effectuée, il se peut que le rapprochement de l'ancienne machine virtuelle ne soit pas possible.

L'ancienne instance peut être supprimée, de préférence avant de redémarrer la reconnaissance. Si plusieurs exécutions sont nécessaires pour essayer diverses solutions, n'oubliez pas de supprimer toutes les instances de la machine virtuelle existante au préalable.

Vous pouvez également supprimer l'instance du serveur ESX hôte. Si cela est réalisable dans l'environnement, il peut être utile de supprimer et de recréer la base de données TADDM entre des exécutions de reconnaissance. Ensuite, exécutez une nouvelle reconnaissance et vérifiez s'il existe encore des doubles.

attribut <primaryMACAddress>

La raison principale de la non correspondance des deux instances d'une machine virtuelle est qu'elles disposent de valeurs différentes pour l'attribut <primaryMACAddress>. Pour déterminer cette valeur pour chaque instance, vous devez exporter les objets de type ComputerSystem à partir de la base de données TADDM à l'aide de la commande suivante exécutée sur le serveur TADDM :

Système autre que Windows :

```
$COLLATION_HOME/sdk/bin/api.sh -u <username> -p <password>
   find --depth 1 ComputerSystem > <filename>.xml
```

Système Windows :

```
%COLLATION_HOME%\sdk\bin\api -u <username> -p <password>
   find --depth 1 ComputerSystem > <filename>.xml
```

Un fichier XML répertoriant les attributs de premier niveau pour toutes les instances de la classe ComputerSystem est généré. Recherchez le nom abrégé des instances en double et accédez à l'attribut appelé <primaryMACAddress>.

Si la valeur diffère pour les deux instances, il est nécessaire d'identifier et de résoudre les affectations d'adresses MAC dans le fichier de configuration figurant sur le serveur, sur la machine virtuelle proprement dite ou sur les deux.

Configuration de la machine virtuelle

Si une machine virtuelle est configurée dans un noeud NAT ou 'hôte uniquement', le détecteur VMware ESX reconnaît l'instance virtuelle, mais l'instance physique n'est pas reconnue.

Fichiers de configuration de la machine virtuelle sur le serveur hôte ESX

Le détecteur TADDM VMware ESX collecte des informations à partir des fichiers de configuration pour chaque machine virtuelle à reconnaître. Ces fichiers de configuration peuvent être localisés à l'aide de la commande ESX suivante :

```
vmware-cmd –l (il s'agit d'un 'L' en minuscules)
```

Cette commande répertorie le fichier de configuration de chaque machine virtuelle connue du serveur ESX, indiqué par l'extension .vmx.

Ces fichiers sont au format XML et ne sont pas sensibles à la casse. Consultez les informations dans le fichier de configuration de la machine virtuelle dotée d'instances en double.

Validez les informations pour chaque interface afin de vous assurer que l'adresse MAC de chaque ligne correspond à une interface sur la machine virtuelle.

```
ethernet0.present = "true"
ethernet0.networkName ="VM Network"
ethernet0.addressType = "generated"
ethernet0.generatedAddress="00:0c:29:c1:a5:ee"
ethernet0.generatedAddressOffset = "0"
ethernet1.present = "true"
ethernet1.networkName = "VM Network"
ethernet1.addressType = "generated"
ethernet1.generatedAddress="00:0c:29:c1:a5:f8"
ethernet1.generatedAddressOffset = "10"
```

Si les valeurs sont différentes dans le fichier de configuration ou sur la machine virtuelle, corrigez-les et relancez la reconnaissance.

Configuration sur la machine virtuelle

Sur la machine virtuelle, il existe une commande qui affiche les informations pour chaque interface réseau.

Sur les systèmes autres que Windows, la commande est **ifconfig**. Sur les systèmes Windows, la commande est **ipconfig**.

Examinez la sortie et validez les associations interface/MAC par rapport au fichier de configuration ESX. Vous pouvez également vérifier que chaque interface fonctionne en exécutant une commande ping sur l'adresse IP associée. Refaites une tentative de reconnaissance.

Modifications récentes dans une machine virtuelle ou déplacement d'un serveur ESX vers un autre

Si une machine virtuelle a été migrée depuis un serveur ESX vers un autre, il est possible que le fichier de configuration a été modifié et cela peut avoir une incidence sur les reconnaissances.

Si les lignes comportant generatedAddress sont supprimées, cela peut affecter les reconnaissances.

Lors de la migration de machines virtuelles dans un environnement VirtualCenter, toutes les machines virtuelles disposant d'une adresse MAC générée vont la modifier. S'il existe une machine virtuelle sur le serveur ESX qui peut être reconnue, utilisez le fichier de configuration de cette machine virtuelle comme exemple et recherchez les lignes qui pourraient avoir été supprimées.

Le serveur ESX sur lequel la machine virtuelle a été créée peut également être spécifié comme cible dans une portée pour vérifier si la reconnaissance effectuée par la machine virtuelle fonctionne correctement sur ce serveur ESX. Si des lignes ont été supprimées ou modifiées pendant la migration, ajoutez-les ou corrigez-les, puis réexécutez la reconnaissance.

Résolution de noms

Si la machine virtuelle ne peut être résolue en une seule machine sur le réseau, elle peut figurer dans TADDM en tant que deux instances distinctes. Si la machine virtuelle est dotée de plusieurs interfaces et que toutes les interfaces sont visibles sur le réseau, plusieurs instances valides peuvent être identifiées. Il ne sera peut-être pas possible de fusionner toutes les instances en une même instance.

Ceci est généralement dû à une non concordance entre les fichiers hôte, DNS, NIS ou tout autre service de résolution de noms.

La solution consiste à tester la résolution de nom par le nom abrégé de la machine plusieurs fois à partir de la machine virtuelle proprement dite, du serveur ESX et du serveur TADDM. Toutes les réponses doivent correspondre. Si des réponses différentes sont renvoyées, modifiez le nom du service ou les fichiers hôte jusqu'à ce que les résultats soient cohérents. Refaites une tentative de reconnaissance.

Routage & et connectivité réseau générale

Des facteurs réseau globaux doivent être pris en considération lors de la résolution des incidents liés à la reconnaissance TADDM. Comme pour les reconnaissances VMware, un pare-feu ou une autre considération d'architecture en réseau comme SSH peut partiellement bloquer la reconnaissance du serveur ESX ou de la machine virtuelle.

Si la machine virtuelle est reconnue correctement par le détecteur VMware, elle apparaît uniquement avec un nom abrégé sous Infrastructure physique : **Présentation** > **Niveau systèmes** > **Systèmes virtuels** > **VMware ESX**

La machine virtuelle proprement dite apparaît uniquement comme un objet sous l'en-tête d'un autre périphérique IP ou autre système informatique.

Si seule la machine virtuelle est correctement reconnue par le détecteur de système informatique, elle s'affiche comme type de système informatique approprié. L'instance virtuelle n'est pas affichée, et le serveur ESX risquent de ne pas être affichés aussi.

Corrigez la configuration du routage et du pare-feu jusqu'à ce que le serveur TADDM puisse exécuter une commande ping et une commande SSH sur le serveur ESX et directement sur chaque machine virtuelle, puis refaites une tentative de reconnaissance.

Des serveurs VMware ESX ont été créés en double

Problème

Il semble que des serveurs VMware ESX (Version 2.5 (toutes version)) soient en double. Ce problème se produit lorsqu'une reconnaissance séquentielle est exécutée à l'aide du détecteur de système informatique VMware ESX suivie par le détecteur de serveur VMware Virtual Center.

Solution

Vous devez fusionner manuellement des serveurs VMware ESX en double.

Le *Guide d'utilisation* de TADDM contient des informations sur l'utilisation du portail de gestion de données, notamment des renseignements sur les tâches de reconnaissance, et sur la façon de fusionner manuellement les éléments de configuration reconnus.

Détecteur de systèmes informatiques VMware ESXi

Le détecteur de systèmes informatiques VMware ESXi reconnaît les serveurs VMware ESXi.

Le détecteur de systèmes informatiques VMware ESXi reconnaît les serveurs VMware ESXi qui prennent en charge l'interface de programme d'application (API) de VMware.

Le détecteur utilise l'API VMware pour une reconnaissance. L'API VMware est disponible sur les serveurs ESXi et sur les versions ESX 3.x, ESX 4.x. Le détecteur n'utilise pas la console ssh.

Nom du détecteur utilisé dans l'interface graphique et les journaux

VmwareESXiComputerSystemSensor

Eléments reconnus par le détecteur

Pour des machines virtuelles et pour un serveur ESX server, le détecteur reconnaît les mêmes données que le détecteur VirtualCenter. Il ne peut pas reconnaître des objets qui sont plus hauts dans l'arborescence de configuration que ESX, comme des clusters, des centres de données. Les magasins de données sont reconnus avec des données très limitées, avec un nom uniquement.

Il existe deux manières de reconnaître le numéro de série ESX, via l'API VMware à l'instar de toutes les autres données ou via l'API CIM.

Prérequis

L'API VMware doit être présente et activée sur le serveur ESX.

Problèmes de sécurité

Pour reconnaître un serveur ESX, vous devez définir des droits en lecture seule pour le compte de service de TADDM.

Connexion aux serveurs avec SSL

Le détecteur de système informatique ESXi peut se connecter au serveur avec SSL en deux modes - le mode par défaut et un nouveau mode.

Mode par défaut
Le mode par défaut ne vérifie pas complètement le certificat d'un serveur. Ce mode autorise une connexion même si le certificat est autosigné, expiré ou avec un nom d'hôte non valide. Il refuse la connexion si d'autres problèmes sont découverts, par exemple une erreur de chaînage de certificats. Le mode par défaut peut s'utiliser avec les certificats VMware par défaut.

Nouveau mode
Le nouveau mode vérifie complètement le certificat d'un serveur. Vous pouvez activer ce mode en définissant la propriété de configuration `strictCertificateCheck` à `true`. Si ce mode est activé, seuls les certificats valides signés par des autorités de certification de confiance sont acceptés.

Importation de certificats autosignés dans TADDM
En définissant la propriété `strictCertificateCheck` à `true`, vous pouvez vous connecter avec des certificats autosignés. Vous devez d'abord importer ce certificat dans TADDM. Ainsi, les certificats autosignés sont des certificats de confiance, leur validité est toujours vérifiée.

Pour importer de tels certificats, procédez comme suit :

1. Ouvrez le répertoire `taddm/dist/osgi/plugins/com.ibm.cdb.discover.sys.vmware.vmwarecommon_*` où `*` est le numéro de version du détecteur.
2. Lancez la commande suivante :

   ```
   java -cp lib/vmwarecommon.jar com.ibm.cdb.discover.sys.vmware.
   VmCertificateCollector ip:port
   ```

   où *ip* est l'adresse IP de l'hôte du détecteur de système informatique VMware ESXi et *port* est le port SSL de cet hôte.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- net.IpInterface
- net.L2Interface
- process.CPUResourcePool
- process.MemoryResourcePool
- process.NetworkAdapterResourcePool
- relation.AllocatedTo
- relation.DonatedTo
- sys.CPU
- sys.vmware.VMWareDataStore
- sys.unix.UnixFileSystem
- sys.NFSFileSystem

- sys.Memory
- sys.vmware.VMWareVirtualSwitch
- sys.vmware.VMWarePortGroup
- sys.darwin.Darwin
- sys.darwin.DarwinUnitaryComputerSystem
- sys.dos.Dos
- sys.dos.DosUnitaryComputerSystem
- sys.DNSResolveEntry
- sys.FileSystem
- sys.freebsd.FreeBSD
- sys.freebsd.FreeBSDUnitaryComputerSystem
- sys.linux.Linux
- sys.linux.LinuxUnitaryComputerSystem
- sys.Memory
- sys.netware.Netware
- sys.netware.NetwareUnitaryComputerSystem
- sys.OperatingSystem
- sys.sun.Solaris
- sys.sun.SunSPARCUnitaryComputerSystem
- sys.UnitaryComputerSystem
- sys.vmware.VmwareESX
- sys.vmware.VmwareUnitaryComputerSystem
- sys.windows.WindowsComputerSystem
- sys.windows.WindowsOperatingSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Par défaut, le détecteur de système informatique VMware ESXi est activé pour une reconnaissance de niveau 2 ou de niveau 3. Le détecteur ne reconnaît que des systèmes invités qui sont en cours d'exécution et ne reconnaît pas de numéro de série ESX. Pour changer ce comportement, créez un profil et personnalisez la configuration du détecteur.

Les éléments de configuration correspondent à la configuration du détecteur VirtualCenter.

Les propriétés suivantes peuvent être définies sur *true* ou *false* :

`ordinalESXviaVCserialDiscovery`
: Reconnaît un numéro de série à l'aide de l'API VMware. Il s'agit d'une méthode standard utilisée pour reconnaître le numéro de série. Elle est plus rapide que l'utilisation de l'API CIM, requiert moins de privilèges mais est aussi davantage sujette aux erreurs.

  La valeur par défaut est `false`.

directESXserialDiscovery
Reconnaît un numéro de série à l'aide de l'API CIM. Cette méthode reconnaît toujours le numéro de série mais elle est plus lente et les contraintes suivantes s'appliquent :

- L'utilisateur de la reconnaissance doit disposer du privilège `Hôte > CIM > Interation CIM`.
- La connexion entre TADDM et le serveur ESX est requise.

Pour plus d'informations, reportez-vous également à la note technique à l'adresse http://www-01.ibm.com/support/docview.wss?uid=swg21638454.

Important : Si vous exécutez le serveur ESX sur du matériel virtualisé tel que Cisco UCS, vous devez reconnaître le numéro de série en utilisant l'API CIM et non l'API VMware, car sinon une fusion pourrait se produire.

La valeur par défaut est `false`.

shallowVMdiscovery
Reconnaît des données limitées pour une machine virtuelle.

La valeur par défaut est `false`.

discoverNonRunningGuests
Reconnaît des machines virtuelles qui ne sont pas en cours d'exécution.

La valeur par défaut est `false`.

strictCertificateCheck
Force le détecteur à se connecter aux serveurs ESX qui sont sécurisés avec des certificats signés d'autorités de certification et valides.

La valeur par défaut est `false`.

enableVMDiscovery
Active la reconnaissance des machines virtuelles.

La valeur par défaut est définie sur `true`.

Configuration de la liste d'accès :

Découvrez quels accès détaillés sont requis, selon votre configuration.

Un détecteur utilise les données d'identification de système informatique pour se connecter à l'API VMware. L'utilisateur VMware doit avoir des droits en lecture seule pour une reconnaissance.

Identification et résolution des problèmes liés au détecteur

Certains problèmes pourraient apparaître avec le détecteur de système informatique VMware ESXi. Découvrez comment résoudre les problèmes classiques.

Impossible pour le détecteur Ping de trouver un IP accessible

Problème
Le détecteur scanne les ports 22 et 135. Si ces ports ne sont pas trouvés, la reconnaissance se termine. Par défaut, ces ports sont bloqués pour le détecteur ESXi.

Solution
Pour activer la reconnaissance, configurez les ports pour permettre leur

scan dans le fichier `collation.properties` à la propriété `com.collation.pingagent.ports` ou ajoutez une exception sur le pare-feu d'ESX.

Le détecteur ESXi ne démarre pas

Problème

Pour permettre au détecteur ESXi de démarrer après un détecteur de port, le détecteur de port doit reconnaître des ports ESXi. Si les ports sont configurés différemment, le détecteur ESXi ne démarre pas.

Solution

Les valeurs de port par défaut sont 902, 80, 443. Si un détecteur ESXi possède des ports configurés différents, reconfigurez le détecteur de port.

Détecteur de système informatique Windows

Le détecteur de système informatique Windows reconnaît des systèmes informatiques qui exécutent des systèmes d'exploitation Microsoft Windows.

Nom du détecteur utilisé dans l'interface graphique et les journaux

WindowsComputerSystemSensor

Prérequis

Pour une reconnaissance par passerelle, la passerelle doit être accessible via SSH.

Pour reconnaître les systèmes Windows sans utiliser de passerelle :

- Les systèmes Windows doivent être accessibles via SSH.
- Microsoft .NET Framework doit être installé sur les systèmes Windows cibles. Pour plus d'informations, voir la rubrique *Configuration pour la reconnaissance des systèmes Windows* dans le *Guide d'administration* de TADDM.
- Windows Scripting Host (WSH) 5.6 ou version ultérieure doit être installé sur les systèmes Windows cible. Windows Scripting Host est installé avec Internet Explorer 6 Service Pack 1 ou version ultérieure.
-

  Windows Server 2016

  En raison d'un problème Powershell 5, vous **devez** contacter le support IBM et demander l'application d'un eFix Powershell 5 **avant** d'essayer de reconnaître un serveur Windows Server 2016 sans passerelle. La reconnaissance de Windows 2016 Server via SSH direct fonctionnera alors normalement.

Limitations

- Si vous fournissez des données d'identification sans le rôle administrateur, de détecteur informatique Windows n'est pas en mesure de collecter la liste de services et de périphériques associés à Windows Server 2003. Dans les résultats, les tables associées dans le portail de gestion de données sont vides.
- Tous les détecteurs du système informatique et le détecteur SNMP MIB2 ignorent les interfaces réseau qui sont configurés pour être arrêtées. TADDM ne renseigne pas l'attribut `net.IpNetwork` sur les types suivants d'interface IP :
  - bouclage, par exemple, `127.0.0.1, 0:0:0:0:0:0:0:1`
  - liaison locale, par exemple, `169.254.1.1, FE80:0:0:0:0:0:0:1`

– multidiffusion, par exemple, `224.0.0.1`, `FF00:0:0:0:0:0:0:1`
– non spécifié, par exemple, `0.0.0.0`, `0:0:0:0:0:0:0:0`

Par conséquent, les réseaux IP ne sont pas renseignés dans l'interface utilisateur TADDM.

Reconnaissance des interfaces IPv6 et des informations de routage et de transfert IPv6

Ce détecteur reconnaît les interfaces IPv6 et les informations de routage et de transfert IPv6 relatives aux cibles configurés pour prendre en charge IPv6. TADDM exécute les reconnaissances uniquement par rapport aux adresses IPv4. TADDM ne démarre pas de détecteur pour les adresses IPv6. Pour les recherches DNS, TADDM utilise les adresses IPv4 ou IPv6. TADDM ne renseigne pas l'attribut net.IpNetwork sur une interface IPv6 si la valeur de longueur de préfixe n'est pas spécifiée ou est égale à zéro.

Les adresses IPv6 reconnues sont affichées dans l'interface utilisateur de TADDM de la même manière que les adresses IPv4 et sont accessibles à l'aide de l'API TADDM. Comme les adresses IPv6 utilisent une valeur de longueur de préfixe au lieu d'un masque de réseau IPv4, seule l'une de ces valeurs est renseignée pour une adresse IP. Cette valeur dépend du type d'adresse.

Reconnaissance d'informations sur l'unité centrale

La valeur de l'attribut NumCPUs est définie au nombre d'unités centrales logiques sur le système informatique. Si l'hyperthreading est activé sur le système cible Windows, l'attribut NumCPUs inclut aussi les hyperthreads. Par exemple, sur des système doubles avec l'hyperthreading activé, la valeur de l'attribut NumCPUs est 4. Si l'hyperthreading n'est pas activé en revanche, la valeur de l'attribut NumCPUs est 2.

Prise en charge d'une reconnaissance asynchrone et basée sur un script

Le détecteur de système informatique Windows prend en charge la reconnaissance asynchrone et basée sur un script.

Conditions requises pour la configuration du détecteur

Pour plus d'informations sur la configuration de la reconnaissance dépendante d'un script, voir la rubrique *Configuration de la reconnaissance basée sur un script* dans le *Guide d'administration* de TADDM.

Conditions requises pour la configuration de la liste d'accès

Pour la reconnaissance asynchrone, la liste d'accès n'est pas utilisée.

Pour une reconnaissance basée sur un script, la configuration de la liste d'accès est la même que pour les autres types de reconnaissance.

Limitations

Le détecteur nécessite un environnement powershell sur le système cible pour une reconnaissance basée sur un script et asynchrone. La version de powershell doit être 2 ou supérieure.

Une reconnaissance basée sur un script est prise en charge pour les systèmes cible suivants :

- Windows 7
- Windows 8
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016 Standard Edition
- Windows Server 2016 Datacenter Edition

Objets de modèle avec attributs associés

Le détecteur de système informatique Windows crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les systèmes informatiques exécutant le système d'exploitation Windows.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

core.LogicalContent

- Checksum
- Content
- FixedPath
- URI

dev.MediaAccessDevice

- Name
- Type
- Status

sys.DNSResolveEntry

- SearchOrder
- ServerIp

net.L2Interface

- Encapsulation
- HwAddress
- InterfaceName
- Loopback
- Name
- Index
- IANAInterfaceType
- InterfaceSpeed
- Speed

net.IpInterface

- IpAddress
- L2Interface
- IpNetwork

sys.CPU

- IndexOrder
- NumCPUs

- CPUType
- CPUSpeed
- CPUCoresInstalled
- Virtual
- CPUCore

sys.FileSystem

- AvailableSpace
- Capacity
- Group
- MountPoint
- Owner
- Permissions
- Type

sys.SoftwareComponent

- Name
- SoftwareVersion
- Publisher

sys.windows.WindowsService

- ServiceName
- CanBePaused
- CanBeStopped
- DesktopInteract
- ErrorControl
- OperatingState
- Started
- StartMode
- Account
- PathName
- ExitCode
- ServiceSpecificCode
- ServiceType
- Description
- Name
- SoftwareVersion
- ProcessId

sys.windows.WindowsComputerSystem

- UUID
- Name
- Type
- SystemId
- SystemBoardUUID
- VirtualMachineState
- Signature
- Fqdn

- SerialNumber
- Manufacturer
- Model
- MemorySize
- NumCPUs
- CPUType
- CPUSpeed
- Architecture
- CPUDiesInstalled
- CPUCoresInstalled

sys.windows.WindowsOperatingSystem

- Fqdn
- Name
- OSName
- OSVersion
- BootTime
- KernelArchitecture
- KernelVersion
- Charset
- Locale
- OsId
- OSConfidence
- ServicePack
- VersionString

Configuration du détecteur

Vous devez configurer le détecteur de système informatique Windows, avant de l'utiliser.

Complétez la configuration suivante :

- Installez tous les logiciels requis.
- Pour une reconnaissance par passerelle, WMI doit être activé sur tous les systèmes Windows cible. WMI est activé par défaut.

  Par défaut, la reconnaissance par passerelle installe automatiquement le fournisseur TADDM WMI sur tous les systèmes Windows cible pendant le processus de reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Pour une reconnaissance complète des hôtes et logiciels Windows, chaque machine Windows requiert un compte de service dans le groupe d'administration local avec un accès WMI à tous les objets WMI figurant sur cette machine. Ce compte peut être un compte local ou un compte de domaine.

   Le compte de service doit être créé sur la passerelle Windows et tous les systèmes informatiques Windows cible.

2. Les entrées de liste d'accès doivent être créées pour les systèmes informatiques Windows (passerelle et les systèmes Windows cible).

   Lors de la spécification d'un compte utilisateur de domaine Windows pour une entrée de liste d'accès, le nom de domaine et le nom d'utilisateur doivent être séparés par une barre oblique inversée (\) comme indiqué dans l'exemple suivant : `DOMAIN\username`.
3. TADDM prend également en charge une reconnaissance des systèmes Windows basée sur SNMP. Pour prendre en charge une reconnaissance basée sur SNMP, procédez comme suit :
   a. Activez SNMP.
   b. Vérifiez que la chaîne de communauté SNMP MIB2 GET dispose d'une autorisation d'accès aux ressources hôte, aux interfaces étendues, aux interfaces, aux adresses IP et au système MIB2.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur de système informatique Windows.

Le détecteur utilise l'entrée suivante du fichier `collation.properties` :

Fix Pack 1 **com.ibm.cdb.skipWindowsSoftware=false**

Remarque : Cette propriété affecte seulement le mode basé sur un script de la reconnaissance.
Cette propriété indique si le logiciel installé sur le système d'exploitation Windows est reconnu.

La valeur par défaut est `false`, ce qui signifie que le logiciel est reconnu.

Si la quantité de données reconnues est très volumineuse et qu'elle ralentit le processus de reconnaissance, définissez cette propriété sur `true` pour désactiver la reconnaissance de ce type de données.

com.collation.discover.agent.sys.ComputerSystem.serialNumberSanityChecks=
"⌂(?!null);⌂(?!not);⌂(?!n/a);⌂(?!permission);⌂(?!to be);⌂(?!undef); ⌂[
-:\.\w]{4,80}$; ^(?!.{8}(\-.{4}){3}\-
.{12}_.{2}(:.{2}){5});^(?!none);^(?!x{7});^(?!
.{9});^(?!0123456789);^(?!0+$)";

Cette propriété sert à valider la propriété serialNumber reconnue par les détecteurs du système d'exploitation (sauf Solaris) afin d'éviter de stocker des valeurs génériques (telles que Not Defined, To be set by OEM ou Permission Denied).

La principale règle par défaut est que le numéro de série contient entre 4 et 80 caractères et ne commence pas par l'une des chaînes suivantes :

- **null** : expression régulière **^(?!null)**
- **not** : expression régulière **^(?!not)**
- **n/a** : expression régulière **^(?!n/a)**
- **permission** : expression régulière **^(?!permission)**
- **to be** : expression régulière **^(?!to be)**
- **undef** : expression régulière **^(?!undef)**
- string in form : **098D8710-E623-3C3B-9F9B-FCBAFF1BF3B6_5C:F3:FC:E8:89:FC** : expression régulière **^(?!.{8}(\-.{4}){3}\-.{12}_.{2}(:.{2}){5})**

- **none** : expression régulière **^(?!none)**
- **xxxxxxx** : expression régulière **^(?!x{7})**
- **.....** : expression régulière **^(?!\.{9})**
- **0123456789** : expression régulière **^(?!0123456789)**
- **0000** : expression régulière **^(?!0+$)**

Si un numéro de série ne suit pas cette règle, il n'est pas défini. La syntaxe d'expression régulière est définie dans le SDK Java pour la classe `java.util.regex.Pattern`. Les expressions régulières doivent être séparées par des points-virgules. Les numéros de série candidats sont toujours convertis en minuscules avant d'être mis en correspondance avec des expressions régulières. Par conséquent, quand vous personnalisez la propriété, prenez uniquement des caractères en minuscules.

Propriétés de la reconnaissance par passerelle ou SSH

com.collation.AllowPrivateGateways=`true`
La valeur par défaut est `true`.

Cette propriété indique si un système informatique Windows peut être reconnu via des connexions SSH ou IBM Tivoli Monitoring sans demander une passerelle intermédiaire. La valeur par défaut permet des connexions SSH ou IBM Tivoli Monitoring à des systèmes Windows. Si la valeur est définie sur `false`, les cibles Windows sont détectées uniquement si elles sont répertoriées dans la liste de passerelle TADDM. Si elles ne figurent pas dans la liste de passerelle, le détecteur de session Windows subit une panne avec l'erreur CTJTP1100E error.

com.collation.PreferWindowsSshOverGateway=`false`
La valeur par défaut est `false`.

Cette propriété indique s'il faut utiliser SSH au lieu d'une reconnaissance par passerelle si un système informatique Windows prend en charge SSH. Même si un système informatique Windows prend en charge SSH, la valeur par défaut pour cette propriété indique qu'une reconnaissance par passerelle est utilisée. Cette propriété est ignorée si `com.collation.AllowPrivateGateways=false`.

Propriétés liées à WMI

TADDM s'appuie sur Windows Management Instrumentation (WMI) pour reconnaître les systèmes informatiques Windows. TADDM peut être configuré pour redémarrer le service WMI en cas de problème avec WMI. Si le service WMI est redémarré, tous les services dépendant de WMI et exécutés avant le redémarrage sont aussi redémarrés.

Fix Pack 4 **com.collation.discover.agent.windows.useIpAsDomain=`false`**
La valeur par défaut est `false`.

Cette propriété indique le format des données d'identification qui est utilisé pour établir la session WMI. Par défaut, les données d'identification sont utilisées au format *`user`*.

Si vous définissez cette propriété sur `true`, les données d'identification sont utilisées au format *`IP`*/*`user`*, en plus du format par défaut.

Cette propriété étant une propriété sectorisée, vous pouvez lui adjoindre l'adresse IP ou le nom de la portée. Par exemple :

```
com.collation.discover.agent.windows.useIpAsDomain.9.100.100.200=false
com.collation.discover.agent.windows.useIpAsDomain.scope_name1=false
```

com.collation.WmiAccessEnabled=true
La valeur par défaut est `true` et indique que TADDM tente d'établir la session WMI.

Il s'agit d'une propriété de profil de reconnaissance. Vous pouvez la configurer avec la priorité la plus élevée dans l'onglet **Propriétés de plateforme** du panneau Profils de reconnaissance de la console de gestion de reconnaissance. Vous pouvez également la définir pour un ensemble de portées spécifique, ou une adresse IP, dans le fichier `collation.properties`.

com.collation.platform.os.WindowsOs.AutoDeploy=true
La valeur par défaut est `true` et indique que TADDM peut installer automatiquement le fournisseur WMI.

La définition de la valeur à `false` indique que vous pouvez déployer manuellement le fournisseur WMI. Le déploiement manuel n'est pas pris en charge mais peut être utilisé pour l'identification et la résolution des problèmes.

Les propriétés suivantes du serveur TADDM contrôlent le redémarrage de WMI.

Remarque : La valeur par défaut pour le redémarrage de WMI est `false`. La définition des propriétés suivantes à `true` peuvent offrir une reconnaissance Windows fiable, mais vous devez aussi prendre en compte l'impact négatif potentiel du service WMI temporairement arrêté et redémarré.

com.collation.RestartWmiOnAutoDeploy=false
Redémarrez WMI si une erreur WMI se produit lors du déploiement automatique du fournisseur WMI TADDM.

com.collation.RestartWmiOnAutoDeploy.1.2.3.4=false
Redémarrez WMI si une erreur WMI se produit lors du déploiement automatique du fournisseur WMI TADDM.

com.collation.RestartWmiOnFailure=false

Redémarrez WMI si une erreur WMI se produit, sauf lors du déploiement automatique.

com.collation.RestartWmiOnFailure.1.2.3.4=false

Redémarrez WMI si une erreur WMI se produit, sauf lors du déploiement automatique.

Fix Pack 2

Propriétés associées à PowerShell

Fix Pack 3 **com.ibm.cdb.session.ps.urlPrefix=wsman**
La valeur par défaut est `wsman`.

Cette propriété indique la valeur de la propriété `URLPrefix` d'un programme d'écoute WinRM sur le système Windows reconnu. La valeur de cette propriété et la propriété `URLPrefix` sur les cibles Windows doivent être identiques.

Cette propriété est basée sur la portée. Vous pouvez remplacer la valeur globale pour un ensemble de portées spécifique ou une adresse IP dans le fichier `collation.properties`.

com.collation.PowerShellAccessEnabled=false
La valeur par défaut est `false`.

Cette propriété indique si TADDM tente d'établir la session PowerShell. Par défaut, l'accès à PowerShell est désactivé. Si vous souhaitez activer la session PowerShell, définissez cette propriété sur `true`.

Il s'agit d'une propriété de profil de reconnaissance. Vous pouvez la configurer avec la priorité la plus élevée dans l'onglet **Propriétés de plateforme** du panneau Profils de reconnaissance de la console de gestion de reconnaissance. Vous pouvez également la définir pour un ensemble de portées spécifique, ou une adresse IP, dans le fichier `collation.properties`.

com.collation.PreferPowerShellOverWMI=true
La valeur par défaut est définie sur `true`.

Cette propriété indique s'il faut utiliser la session PowerShell ou WMI, si elles sont activées. Par défaut, la session PowerShell est préférée.

Cette propriété est basée sur la portée. Vous pouvez remplacer la valeur globale pour un ensemble de portées spécifique ou une adresse IP dans le fichier `collation.properties`. Par exemple :

```
com.collation.PreferPowerShellOverWMI.myScopeABC=false
com.collation.PreferPowerShellOverWMI.10.100.27.8=true
```

com.collation.PowerShellPorts=5985,5986
La valeur par défaut est `5985,5986`.

Cette propriété indique les ports PowerShell. Par défaut, les ports 5985 et 5986 sont indiqués. PortSensor vérifie si ces ports sont actifs. S'ils le sont, la session PowerShell peut être établie. S'ils ne le sont pas, la session WMI est alors utilisée, sauf si elle est désactivée. Dans ce cas, des messages d'erreur s'affichent.

Il s'agit d'une propriété de profil de reconnaissance. Vous pouvez la configurer avec la priorité la plus élevée dans l'onglet **Propriétés de plateforme** du panneau Profils de reconnaissance de la console de gestion de reconnaissance. Vous pouvez également la définir pour un ensemble de portées spécifique, ou une adresse IP, dans le fichier `collation.properties`.

com.ibm.cdb.session.ps.useSSL=false
La valeur par défaut est `false`.

Cette propriété indique si le script PowerShell utilise le protocole SSL pour se connecter à l'hôte distant. Par défaut, le protocole SSL n'est pas utilisé.

Cette propriété est basée sur la portée. Vous pouvez remplacer la valeur globale pour un ensemble de portées spécifique ou une adresse IP dans le fichier `collation.properties`.

com.ibm.cdb.session.ps.allowDNS=true

Remarque : Vous pouvez utiliser cette propriété uniquement si la propriété `com.ibm.cdb.session.ps.useSSL` est définie sur `true`.

La valeur par défaut est définie sur `true`.

Cette propriété indique si le script PowerShell utilise le DNS sur la passerelle pour résoudre l'adresse IP de l'hôte distant. Par défaut, l'utilisation du DNS est autorisée.

Cette propriété est basée sur la portée. Vous pouvez remplacer la valeur globale pour un ensemble de portées spécifique ou une adresse IP dans le fichier `collation.properties`.

com.ibm.cdb.session.ps.fallbackToIP=true

Remarque : Vous pouvez utiliser cette propriété uniquement si les propriétés `com.ibm.cdb.session.ps.useSSL` et `com.ibm.cdb.session.ps.allowDNS` sont définies sur `true`.

La valeur par défaut est définie sur `true`.

Cette propriété indique si le script PowerShell a recours à l'adresse IP lorsqu'aucune session sécurisée ne peut être établie à l'aide du nom de domaine complet. Par défaut, le script PowerShell a recours à l'adresse IP.

Cette propriété est basée sur la portée. Vous pouvez remplacer la valeur globale pour un ensemble de portées spécifique ou une adresse IP dans le fichier `collation.properties`.

com.collation.PowerShellTimeoutFudge=10000

La valeur par défaut est `10000` (millisecondes).

Cette propriété indique le laps de temps après lequel le protocole SSH dépasse le délai d'attente, en commençant par le délai d'attente dépassé du script Powershell. Par défaut, lorsque le script PowerShell dépasse le délai d'attente, le protocole SSH dépasse le délai d'attente 10 000 millisecondes plus tard.

Configuration d'une reconnaissance Windows non administrateur :

Vous pouvez configurer le détecteur pour exécuter des reconnaissances sans fournir des données d'identification de l'utilisateur doté du rôle d'administrateur.

Pourquoi et quand exécuter cette tâche

Selon le type de session que vous avez activé, les étapes suivantes sont obligatoires :

Session WMI

- «Création d'un compte utilisateur de reconnaissance», à la page 410
- «Définition de la configuration WMI», à la page 411
- «Copie des fichiers TaddmWmi», à la page 412
- «Configuration de l'accès DCOM pour ibmcol», à la page 412

Fix Pack 2 **Session PowerShell**

- «Création d'un compte utilisateur de reconnaissance», à la page 410
- «Définition de la configuration WMI», à la page 411
- «Définition de la configuration PowerShell», à la page 411

Fix Pack 2 **Sessions WMI et PowerShell**

- «Création d'un compte utilisateur de reconnaissance», à la page 410
- «Définition de la configuration WMI», à la page 411
- «Définition de la configuration PowerShell», à la page 411
- «Copie des fichiers TaddmWmi», à la page 412
- «Configuration de l'accès DCOM pour ibmcol», à la page 412

Voir également la rubrique *Configuration pour la reconnaissance des systèmes Windows* dans le *Guide d'administration* de TADDM.

Création d'un compte utilisateur de reconnaissance :

Lorsque vous créez un compte, vous devez choisir les droits appropriés et fournir les informations nécessaires pour exécuter une reconnaissance Windows non-administrateur.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un compte utilisateur de reconnaissance sur le serveur Windows autonome et sur le serveur de domaine Active Directory. Utilisez l'une des instructions suivantes pour exécuter cette tâche.

Création d'un compte utilisateur de reconnaissance sur le serveur Windows autonome :

Créer un compte utilisateur de reconnaissance sur le serveur Windows autonome.

Procédure

1. Pour ouvrir Computer Management Console, exécutez la commande **compmgmt.msc**.
2. Dans l'arborescence de navigation, développez **Outils système > Utilisateurs et groupes locaux > Utilisateurs**.
3. Dans le menu **Action**, cliquez sur **Nouvel utilisateur**.
4. Fournissez les informations suivantes :
   a. **Nom d'utilisateur :** `ibmcol`
   b. **Nom complet :** TADDM discovery user
   c. **Description :** TADDM discovery user
   d. **Mot de passe**
5. Désélectionnez la case à cocher **L'utilisateur doit changer son mot de passe à la prochaine ouverture de session**.
6. Sélectionnez la case à cocher **Le mot de passe n'arrive jamais à expiration**.
7. Cliquez sur **Créer**.
8. Pour vérifier que le nouvel utilisateur est bien un utilisateur standard (par défaut), cliquez avec le bouton droit de la souris sur le nom de l'utilisateur, puis cliquez sur **Propriétés**. Dans la fenêtre **Propriétés**, accédez à l'onglet **Membre de**. Si l'utilisateur est un utilisateur standard, le groupe Administrateurs ne figure pas sur la liste.

Création d'un compte utilisateur de reconnaissance sur un serveur de domaine Active Directory :

Créer un compte utilisateur de reconnaissance sur un serveur de domaine Active Directory.

Procédure

1. Ouvrez Utilisateurs et ordinateurs Active Directory en exécutant la commande **dsa.msc**.
2. Dans l'arborescence de navigation, sélectionnez *nom_domaine*, puis sélectionne le dossier **Utilisateurs**.

3. Cliquez avec le bouton droit de la souris sur le menu et sélectionnez **Nouveau > Utilisateur**.
4. Fournissez les informations suivantes :
   a. **Prénom**:`ibmcol`
   b. **Nom de connexion**:`ibmcol`
5. Cliquez sur **Suivant** et fournissez un mot de passe.
6. Désélectionnez la case à cocher **L'utilisateur doit changer son mot de passe à la prochaine ouverture de session**.
7. Sélectionnez la case à cocher **Le mot de passe n'arrive jamais à expiration**.
8. Cliquez sur **Créer**.
9. Pour vérifier que le nouvel utilisateur est bien un utilisateur standard (par défaut), cliquez avec le bouton droit de la souris sur le nom de l'utilisateur, puis cliquez sur **Propriétés**. Dans la fenêtre **Propriétés**, accédez à l'onglet **Membre de**. Si l'utilisateur est un utilisateur standard, le groupe Administrateurs ne figure pas sur la liste.

Définition de la configuration WMI :

Lors de la définition de la configuration WMI, vous pouvez ajouter l'utilisateur à la liste d'accès afin d'activer les droits requis pour la reconnaissance.

Procédure

1. Dans l'arborescence de navigation de Computer Management Console, développez **Services et applications > Contrôle WMI**.
2. Dans le menu **Action**, cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Sécurité**, sélectionnez l'espace de nom **Root**, puis cliquez sur **Sécurité**.
4. Ajoutez l'utilisateur `ibmcol` à la liste. Les droits suivants doivent être accordés :
   a. Exécuter Méthodes
   b. Activer compte
   c. Activation à Distance
5. Cliquez sur **Avancés** et choisissez l'utilisateur `ibmcol` dans la liste.
6. Remplacez la propriété **Appliquer à** par `Cet espace de noms et ces sous-espaces de nom`.
7. Cliquez sur **OK**.

   Remarque : Pour la configuration du domaine Active Directory, vous devez répéter cette procédure pour chaque ordinateur faisant partie du domaine. Microsoft ne fournit aucun outil de configuration WMI étendu au domaine.

Définition de la configuration PowerShell : Fix Pack 2

Si vous avez activé la session PowerShell, vous devez configurer les systèmes cible de manière à activer la reconnaissance non-administrateur.

Procédure

1. Sur le système cible, exécutez la commande suivante :

   ```
   Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI
   -Force
   ```

   L'option `-Force` permet de ne pas avoir à confirmer l'action.

2. Dans la nouvelle fenêtre qui s'affiche, sélectionnez l'utilisateur `ibmcol`. S'il ne figure pas sur la liste, cliquez sur **Ajouter...** et recherchez-le.
3. Dans la liste des autorisations, sélectionnez **Read(Get,Enumerate,Subscribe)** et **Execute(Invoke)** dans la colonne **Autoriser**.
4. Cliquez sur **OK**.

Copie des fichiers TaddmWmi :

Ces fichiers sont utilisés pour la reconnaissance sans agent. Ils sont nécessaires pour activer l'appel de méthodes supplémentaires via WMI.

Procédure

1. Copiez les fichiers TaddmWmi suivant dans le répertoire `C:\Windows\system32\wbem` sur un système 32 bits et dans le répertoire `C:\Windows\SysWOW64\wbem` sur un système 64 bits :
   - `TaddmWmi.pdb`
   - `TaddmWmi.exe`
   - `TaddmWmi.mof`
   - `TaddmWmi.dll`
2. Compilez et enregistrez `TaddmWMI.dll` en exécutant les commandes suivantes :
   - Sous un système d'exploitation Windows 32 bits :

     ```
     %SystemRoot%\System32\wbem\mofcomp.exe %SystemRoot%\System32\wbem\TaddmWmi.mof
     %SystemRoot%\System32\regsvr32 /s %SystemRoot%\System32\wbem\TaddmWmi.dll
     ```

   - Sous un système d'exploitation Windows 64 bits :

     ```
     %SystemRoot%\SysWOW64\wbem\mofcomp.exe
     %SystemRoot%\SysWOW64\wbem\TaddmWmi.mof
     %SystemRoot%\SysWOW64\regsvr32 /s
     %SystemRoot%\SysWOW64\wbem\TaddmWmi.dll
     ```

   Remarque : Vous pouvez déployer les fichiers WMI automatiquement en exécutant une reconnaissance d'administrateur standard.

Configuration de l'accès DCOM pour ibmcol :

Vous devez configurer l'accès au modèle DCOM pour l'utilisateur afin d'activer les droits qui sont nécessaires pour la reconnaissance.

Pourquoi et quand exécuter cette tâche

Pour configure l'accès au modèle DCOM pour l'utilisateur sur le serveur Windows autonome ou le serveur de domaine Active Directory, utilisez l'une des instructions suivantes.

Configuration de l'accès au modèle DCOM pour ibmcol sur un serveur Windows autonome :

Procédez comme suit pour configurer l'accès au modèle DCOM pour l'utilisateur sur le serveur Windows autonome.

Procédure

1. Ouvrez l'outil d'administration des services de composants en exécutant la commande **`dcomcnfg`**.
2. Dans l'arborescence de navigation, développez **Services de composant** > **Ordinateurs** > **Poste de travail**.

3. Dans le menu **Action**, cliquez sur **Propriétés**, puis accédez à l'onglet **Sécurité COM**.
4. Dans la section **Droits d'accès**, cliquez sur **Editer la valeur par défaut**.
5. Ajoutez l'utilisateur `ibmcol` à la liste et assurez-vous qu'il dispose des droits d'`accès local` et d'`accès distant`, puis cliquez sur **OK**.
6. Dans la section **Autorisations d'accès**, cliquez sur **Modifier les limites**.
7. Si le bouton est grisé, procédez comme suit :
   a. Ouvrez **Local Security Policy** en exécutant la commande **`secpol.msc`**.
   b. Développez **Local Policies**, puis cliquez sur **Security Options**.
   c. Sélectionnez la règle suivante : **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax**.
   d. Cliquez avec le bouton droit de la souris et sélectionnez **Properties** dans le menu. Cliquez ensuite sur **Edit Security**.
8. Ajoutez l'utilisateur `ibmcol` à la liste et vérifiez que les droits `Local Access` (accès local) et `Remote Access` (accès distant) sont activés, puis cliquez sur **OK**.
9. Dans la section **Droits d'accès de lancement et d'activation**, cliquez sur **Editer la valeur par défaut**.
10. Ajoutez l'utilisateur `ibmcol` à la liste et assurez-vous qu'il dispose des droits de `lancement local` et de `lancement distant`, puis cliquez sur **OK**.
11. Dans la section **Autorisations de lancement et d'activation**, cliquez sur **Modifier les limites**.
12. Si le bouton est grisé, procédez comme suit :
    a. Ouvrez **Local Security Policy** en exécutant la commande **`secpol.msc`**.
    b. Développez **Local Policies**, puis cliquez sur **Security Options**.
    c. Sélectionnez la règle suivante : **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax**.
    d. Cliquez avec le bouton droit de la souris et sélectionnez **Properties** dans le menu. Cliquez ensuite sur **Edit Security**.
13. Ajoutez l'utilisateur `ibmcol` à la liste et vérifiez que les droits `Local Launch` (lancement local), `Remote Launch` (lancement distant), `Local Activation` (activation locale) et `Remote Activation` (activation distante) sont activés, puis cliquez sur **OK**.
14. Redémarrez le serveur Windows.

Configuration de l'accès au modèle DCOM pour ibmcol sur un serveur de domaine Active Directory :

Procédez comme suit pour configurer l'accès au modèle DCOM pour l'utilisateur sur le serveur de domaine Active Directory.

Procédure

1. Ouvrez **Group Policy Management** en exécutant la commande **`gpmc.msc`**.
2. Choisissez une forêt et sélectionnez une règle de domaine, par exemple **Default Domain Policy**.
3. Cliquez sur **Action > Editer**.
4. Ouvrez `Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Security options`.
5. Sélectionnez la règle suivante : **DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax**.

6. Cliquez avec le bouton droit de la souris et sélectionnez **Properties** dans le menu. Cliquez ensuite sur **Edit Security**.
7. Ajoutez l'utilisateur `ibmcol` à la liste et vérifiez que les droits Local Access (accès local) et Remote Access (accès distant) sont activés, puis cliquez sur **OK**.
8. Sélectionnez la règle suivante : **DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax**.
9. Cliquez avec le bouton droit de la souris et sélectionnez **Properties** dans le menu. Cliquez ensuite sur **Edit Security**.
10. Ajoutez l'utilisateur `ibmcol` à la liste et vérifiez que les droits Local Launch (lancement local), Remote Launch (lancement distant), Local Activation (activation locale) et Remote Activation (activation distante) sont activés, puis cliquez sur **OK**.
11. Exécutez la commande **gpupdate** pour actualiser les paramètres de sécurité.

Configuration automatique :

La configuration automatique permet de remplacer les étapes d'installation de la configuration WMI, de copie des fichiers TaddmWmi et de configuration de l'accès DCOM pour ibmcol. Si vous utilisez TADDM 7.3.0.3 ou versions ultérieures, l'étape d'installation de la configuration PowerShell peut aussi être automatisée.

Procédure

1. Copiez les fichiers suivants sur le système cible.
   a. Les fichiers script suivants sont accessibles dans le répertoire `$COLLATION_HOME/dist/support/bin`.
      - `copyFiles.ps1`
      - `dcomConfiguration.ps1`
      - `nonadmin.properties`
      - Fix Pack 3 `psSessionConfiguration.ps1`
      - `scriptsRunner.bat`
      - Fix Pack 3 `scriptsRunner.ps1`
      - `wmiConfiguration.ps1`
      - Fix Pack 4 `wrmConfiguration.ps1`
   b. Les fichiers de fournisseur TaddmTool suivants sont accessibles dans le répertoire `$COLLATION_HOME/dist/lib/ms/gateway`.
      - `TaddmWmi.pdb`
      - `TaddmWmi.exe`
      - `TaddmWmi.mof`
      - `TaddmWmi.dll`
2. Configurez le fichier `nonadmin.properties` en mettant à jour les propriétés `nonadmin.user` et `nonadmin.files.path` :

```
nonadmin.user=utilisateur
nonadmin.wmi.namespace=root
nonadmin.files.path=chemin
nonadmin.permissions=Enable,MethodExecute,RemoteAccess
```

   La valeur du paramètre *utilisateur* représente l'utilisateur que vous souhaitez utiliser pour la reconnaissance non administrateur. Si vous spécifiez l'utilisateur local, il vous suffit d'ajouter le nom d'utilisateur. Sinon, indiquez également le

nom de domaine, par exemple, `domaine\utilisateur`. La valeur du paramètre *chemin* représente le chemin d'accès au répertoire dans lequel vous avez copié les fichiers à l'étape 1. Ne modifiez pas les valeurs des autres propriétés.

3. A l'invite de commande, exécutez le fichier `scriptsRunner.bat`.

   Fix Pack 3 Dans TADDM 7.3.0.3 et versions ultérieures, le fichier `scriptsRunner.bat` requiert les paramètres `-wmi` et/ou `-ps`.

   - `scriptsRunner.bat -wmi` : exécute les étapes d'installation de la configuration WMI, de copie des fichiers TaddmWmi et de configuration de l'accès DCOM.
   - `scriptsRunner.bat -ps` : exécute les étapes d'installation de la configuration WMI et PowerShell.
   - `scriptsRunner.bat -wmi -ps` : exécute les étapes des paramètres `-wmi` et `-ps`.

   Fix Pack 4 Dans TADDM 7.3.0.4 et versions ultérieures, vous devez utiliser la commande **set** et au moins l'un des paramètres suivants :

   - `scriptsRunner.bat set -wmi` : exécute les étapes d'installation de la configuration WMI, de copie des fichiers TaddmWmi et de configuration de l'accès DCOM.
   - `scriptsRunner.bat set -ps` : exécute les étapes d'installation de la configuration WMI et PowerShell.
   - `scriptsRunner.bat set -wmi -ps` : exécute les étapes des paramètres `-wmi` et `-ps`.

4. Redémarrez le système.

Que faire ensuite

Fix Pack 4 Si vous décidez de ne plus exécuter de reconnaissances non administrateur, vous pouvez revenir à la configuration initiale. Exécutez le fichier `scriptsRunner.bat` avec l'une des options suivantes :

- `scriptsRunner.bat revert -wmi`
- `scriptsRunner.bat revert -ps`
- `scriptsRunner.bat revert -wmi -ps`

Redémarrez le système.

Référence associée:

«Configuration d'une reconnaissance IIS non administrateur», à la page 132
Vous pouvez configurer le détecteur de serveur Web Microsoft IIS pour qu'il exécute la reconnaissance non administrateur des serveurs IIS. Une telle reconnaissance ne nécessite pas un utilisateur avec des droits d'administrateur. Dans ce mode, l'option de contrôle de compte d'utilisateur peut être activée.

Dépannage :

Certaines erreurs pourraient apparaître lors de l'exécution d'une reconnaissance Windows non administrateur. Vous pourrez trouver ici les descriptions des erreurs les plus courantes et voir comment les corriger.

Le détecteur de session se termine avec l'erreur CTJTP1163E

Problème

L'erreur suivante pourrait se produire si la configuration du modèle DCOM et la configuration de Windows Management Instrumentation (WMI) pour l'utilisateur non administrateur est incorrecte.

```
CTJTP1163E The following WMI session cannot be established
(WMI: SELECT BuildVersion FROM Win32_WMISetting failed: Access is denied.
(Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
System.UnauthorizedAccessException: Access is denied.
(Exception from HRESULT: 0x80070005 (E_ACCESSDENIED));
```

Solution

Suivez les instructions à partir des sections suivantes : «Définition de la configuration WMI», à la page 411 et «Configuration de l'accès DCOM pour ibmcol», à la page 412.

Le détecteur de session se termine avec l'erreur CTJTP1161E

Problème

L'erreur suivante pourrait se produire si un utilisateur non administrateur est configuré correctement, mais les fichiers WMI de TADDM n'ont pas été déployés :

```
CTJTP1161E The application cannot establish the following WMI session:
SessionClientException: InstallProvider failed: could not copy files
 to remote host: System.Exception: WNetAddConnection2: Access is denied.
```

Solution

Suivez les instructions fournis dans la section suivante : «Copie des fichiers TaddmWmi», à la page 412.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de système informatique Windows et propose des solutions à ces problèmes.

Problème lié à WMI

Problème

Windows Management Instrumentation (WMI) tombe en panne sur le système à reconnaître, ce qui provoque un échec de reconnaissance.

Solution

Le redémarrage de WMI peut corriger le problème. Utilisez les commandes suivantes pour redémarrer WMI :

```
net stop winmgmt
net start winmgmt
```

Si le redémarrage de WMI ne résout pas l'incident, utilisez les utilitaires Microsoft suivants pour résoudre les incidents liés à WMI. Ces utilitaires sont disponibles à l'adresse https://technet.microsoft.com/en-us/scriptcenter/dd772288.aspx.

WMIDiag

Suivez les instructions pour installer et exécuter l'utilitaire et vérifiez que WMI fonctionne correctement.

Scriptomatic

L'utilitaire Scriptomatic permet de générer des requêtes WMI qui sont identiques à celles utilisées par TADDM. Les classes WMI suivantes sont quelques unes que TADDM demande :

- Win32_Process
- Win32_OperatingSystem
- Win32_WMISetting
- Win32_ComputerSystem

Vérifiez que ces classes peuvent être demandées en utilisant Scriptomatic localement sur le système cible et à distance depuis la passerelle.

Problème lié au déploiement du fournisseur WMI

Problème

Pour la reconnaissance des systèmes Windows, TADDM déploie un fournisseur WMI sur chaque système cible afin d'activer la reconnaissance sans agent. Des problèmes apparaissent parfois lors de ce déploiement.

Solution

Les fichiers suivants contiennent le fournisseur WMI et se trouvent sur le TADDM dans le répertoire $*COLLATION_HOME*/lib/ms/gateway :

TaddmWmi.dll
Fournisseur WMI, qui exécute TaddmWmi.exe pour la fonctionnalité

TaddmWmi.mof
Spécifie les nouvelles méthodes WMI mises à disposition par le fournisseur WMI (TaddmWmi.dll)

TaddmWmi.exe
Appelé par le fournisseur WMI (TaddmWmi.dll) pour l'exécution d'une commande

TaddmWmi.pdb
Contient les informations de débogage pour le fichier TaddmWmi.dll

Le fournisseur d'installation WMI de TADDM effectue les tâches suivantes :

1. Selon le cas, copie les fichiers de la liste précédente vers le répertoire suivant sur chaque système cible qui se trouve dans la portée de reconnaissance (pour cela, le répertoire Admin$ ou C$ est utilisé) : *%SystemRoot%*\System32\wbem
2. Exécute les commandes suivantes sur chaque système cible :

   Dans un système d'exploitation Windows 32-bit :

   ```
   %SystemRoot%\System32\wbem\mofcomp.exe %SystemRoot%\System32\wbem\TaddmWmi.mof
   %SystemRoot%\System32\regsvr32 /s %SystemRoot%\System32\wbem\TaddmWmi.dll
   ```

   Dans un système d'exploitation Windows 64-bit :

   ```
   %SystemRoot%\SysWOW64\wbem\mofcomp.exe %SystemRoot%\SysWOW64\wbem\TaddmWmi.mof
   %SystemRoot%\SysWOW64\regsvr32 /s %SystemRoot%\SysWOW64\wbem\TaddmWmi.dll
   ```

Pour identifier les incidents de WMI ou les incidents liés à l'accès, vous pouvez exécuter manuellement le fournisseur d'installation WMI de TADDM. Pour installer manuellement le fournisseur sur la passerelle Windows à l'aide du programme TaddmTool, entrez les commandes suivantes :

1. cd WINDOWS\temp\taddm.*nnnn*, où *nnnn* représente une chaîne qui identifie le répertoire de passerelle TADDM. Si des correctifs ont été appliqués au TADDM, il peut y avoir plusieurs répertoires de passerelle. Vous pouvez trouver la chaîne identificateur dans le fichier DiscoveryManager.log après l'élément suivant : DTADDM_ID=
2. set TADDM_USERNAME=*domaine**idutilisateur*
3. set TADDM_PASSWORD=*motdepasse_pour_idutilisateur*
4. set TADDM_INTERACTIVE=1
5. TaddmTool InstallProvider @*adresseip*, où *adresseip* est l'adresse IP du système cible

Erreurs d'accès WMI refusé

Problème

Vous recevez des erreurs d'accès WMI refusé.

Solution

Reportez-vous à l'Annexe F du manuel *Deployment Guide Series: IBM Tivoli Change and Configuration Management Database Configuration Discovery and Tracking v1.1*, une publication IBM Redbooks, disponible à l'adresse http://www.redbooks.ibm.com/abstracts/SG247264.html.

Erreurs de création de processus WMI

Problème

La création de processus WMI échoue avec une erreur d'accès pendant l'installation du fournisseur. Il se peut que le privilège **Windows Remplacer un jeton de niveau processus** ne soit pas accordé aux comptes requis.

Solution

- Ce privilège doit être accordé aux comptes LOCAL SERVICE et NETWORK SERVICE. Pour vérifier cela, procédez comme suit :
  1. Connectez-vous à la machine cible à l'aide de la console ou de Terminal Server Client.
  2. Cliquez sur **Démarrer**.
  3. Sélectionnez **Exécuter**.
  4. Entrez `gpedit.msc` pour lancer l'éditeur Group Policy.
  5. Défilez vers le bas dans l'arborescence des privilèges sous **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.
- Si vous ne pouvez pas modifier les comptes attribués au privilège **Remplacer un jeton de niveau processus**, essayez d'ajouter le compte de la reconnaissance à un groupe disposant de ce privilège.

  Vérifiez si le groupe **Tivoli_Admin_Privileges** dispose de ce privilège. Si tel est le cas, faites du compte de la reconnaissance un membre de ce groupe.

Le nom de réseau spécifié n'est plus disponible

Problème

Si cette erreur se produit, ou si un incident se produit pendant la copie des fichiers sur la cible pendant l'installation du fournisseur, il se peut qu'une connexion ne puisse pas être établie au service (partage de fichiers) SMB sur la machine cible.

Solution

Procédez comme suit :

1. Vérifiez que le port SMB est en mode écoute.
   - Windows 2003 sera en mode écoute sur le port 445.
   - Windows 2000 peut être en mode écoute sur 445 ou 139.
2. Sur la passerelle, vérifiez si une connexion est autorisée ou refusée en ouvrant une fenêtre de commande et en exécutant la commande suivante :

   ```
   telnet <target machine name> 445
   ```

3. Si elle est refusée, répétez l'étape b à l'aide du port 139. Si les deux échouent, vous avez l'un des problèmes suivants :
   - Un pare-feu empêche la passerelle de se connecter au service SMB cible.
   - Le service SMB n'est pas en cours d'exécution ou n'est pas fonctionnel.

Pour déterminer si l'origine du problème est un pare-feu ou le service SMB, procédez comme suit :

1. Connectez-vous à la machine cible via la console ou Terminal Server Client.
2. Exécutez les commandes telnet aux étapes 2 et 3 ci-dessus, où <target machine name> correspond cette fois à la machine locale.

   Si la commande telnet aboutit, un pare-feu est à l'origine du problème. Sinon, il y a un problème avec le service SMB.

Procédez comme suit :

- Affichez le panneau de commande, les services, et vérifiez si le service du serveur est en cours d'exécution.
- Exécutez la commande suivante sur la ligne de commande :

  net share

  Un des partages, c$ ou admin$ doit exister.

Reconnaissance lente des systèmes Windows 2003 SP1 ou des applications en cours d'exécution sur ces systèmes

Problème

La reconnaissance lente des systèmes Windows 2003 SP1 ou des applications en cours d'exécution sur ces systèmes peut être due à une fuite de mémoire dans le service WMI.

Solution

Assurez-vous que le correctif logiciel suivant, disponible depuis Microsoft, est installé : http://support.microsoft.com/kb/911262

Les systèmes Windows 2000 ne sont pas reconnus

Problème

Si les systèmes Windows 2000 ne sont pas reconnus, le problème peut être dû à une version non prise en charge du programme **netstat** installé sur le système cible. Le programme **netstat** permet d'obtenir des informations de port TCP pendant la reconnaissance. Les systèmes Windows 2000 utilisent une version différente du programme **netstat** que celle installée sur les systèmes exécutant les versions ultérieures de Windows.

Solution

Assurez-vous que le correctif logiciel suivant, disponible depuis Microsoft, est installé : http://support.microsoft.com/kb/907980

Reconnaissance TADDM de cibles Windows XP quand le pare-feu local est activé

Problème

Sur les cibles basées Windows XP, le pare-feu local est généralement activé pour une sécurité accrue.

La reconnaissance TADDM sur ces ordinateurs échoue avec l'erreur suivante si le pare-feu bloque l'opération :

```
CTJTP1161E The application cannot establish the following WMI
session: SessionClientException: SELECT BuildVersion FROM
Win32_WMISetting failed (0x800706ba: The RPC server is
unavailable.): 0x800706ba: System.
Runtime.InteropServices.COMException (0x800706BA): The RPC server is
unavailable.
```

Solution

Pour reconnaître une cible Windows quand un pare-feu local est activé, limitez la plage des ports RPC sur la cible Windows XP et ouvrez-les sur le pare-feu.

Procédez comme suit pour restreindre les ports DCOM :

1. Allez au **Panneau de configuration**.
2. Sélectionnez **Outils d'administration**.
3. Sélectionnez **Services de composants**.
4. Sélectionnez **Ordinateurs**.
5. Cliquez avec le bouton droit sur **Poste de travail** et ouvrez **Propriétés**.
6. Cliquez sur l'onglet **Protocoles par défaut**.
7. Double-cliquez sur **TCP/IP orienté connexion**.
8. Sélectionnez **Ajouter** dans la fenêtre Propriétés des services Internet COM.
9. Ajoutez une plage de ports ; par exemple, 5000-5050. Cliquez sur **OK**.
10. Redémarrez l'ordinateur.

Ajoutez les ports DCOM à la liste d'exceptions du pare-feu.

Procédez comme suit pour autoriser tous les ports dans le pare-feu local :

1. Allez au **Panneau de configuration**.
2. Cliquez sur **Pare-feu Windows**.
3. Cliquez sur **Exceptions**.
4. Cliquez sur **Ajouter un port**.
5. Ajoutez un par un tous les ports DCOM aux restrictions.

Echec du détecteur sur des cibles dotées d'un serveur SSH Tectia en raison de l'erreur relative à l'impossibilité de copier le fichier

Problème

Le détecteur échoue sur des cibles dotées d'un serveur SSH Tectia, les fichiers journaux contiennent le message suivant :

```
session.Ssh2SessionClient - failed to copy file: AAAA to: BBBB with retray 0
java.io.EOFException: SSHSCP1: premature EOF
```

Solution

Pour résoudre le problème, procédez comme suit :

1. Installez le client SSH Tectia sur le serveur TADDM.
2. Configurez TADDM pour utiliser la commande externe Tectia **scp**. Définissez la propriété `com.collation.platform.os.scp.command` du fichier `collation.properties` pour pointer sur la commande Tectia **scp**. Par exemple :

   ```
   com.collation.platform.os.scp.command=C:\\SshTectia\\SSH Tectia Client\\
   scp2.exe
   ```

   Vous ne pouvez définir l'indicateur précédant que pour les IP et ensembles de portées sélectionnés. Par exemple :

```
com.collation.platform.os.scp.command.10.11.12.13=C:\\SshTectia\\
SSH Tectia Client\\scp2.exe
com.collation.platform.os.scp.command.scopesetA=C:\\SshTectia\\
SSH Tectia Client\\scp2.exe
```

Remarque : Lorsque TADDM est en mode compatible FIPS 140-2, l'utilisation de la commande externe **scp** risque d'affecter la sécurité. Dans un tel cas, vous devez vous assurer que le programme SCP utilisé est compatible FIPS.

Détecteurs de stockage

Les détecteurs de stockage reconnaissent le stockage utilisé dans l'environnement.

Détecteur de portée EMC Storage Scope

Le détecteur EMC Storage Scope reconnaît les ressources de stockage liées à un réseau de stockage (SAN) en procédant à l'extraction de données depuis une base de données EMC Storage Scope.

Le détecteur reconnaît les ressources de stockage telles que les matrices de stockage, les hôtes, les commutateurs, les ensembles de noeuds, les zones, les volumes de stockage, les ports des commutateurs, les systèmes de fichiers et les unités de disque. Certaines de ces ressources, telles les données associées aux hôtes ou aux commutateurs, peuvent également être reconnues par le détecteur de stockage Hôte ou par le détecteur de commutateur à fibre optique.

La reconnaissance EMC est effectuée par deux détecteurs, le détecteur de portée EMC Storage Scope et le détecteur EMC Storage Scope Detail. Le premier reconnaît des attributs généraux du sous-système de stockage StorageSubSystem ainsi que des informations complets sur le commutateur FC, l'ensemble de noeuds, la Zone et ZoneSet. Ensuite, le détecteur lance le détecteur de détails qui reconnaît les informations sur les hôtes et les matrices EMC. Vous pouvez indiquer le nombre de matrices reconnu par chacun des détecteurs de détails en modifiant le paramètre **arraysDiscoveryChunk**.

Nom du détecteur utilisé dans l'interface graphique et les journaux

EMCStorageScopeSensor, EMCStorageScopeDetailSensor

Prérequis

- Vous devez copier les fichiers JAR Oracle suivant depuis le noeud final de reconnaissance dans le répertoire `dist/osgi/plugins/com.ibm.cdb.discover.sensor.app.srm.emccommon_1.0.0/lib/oracle` :
  - `ojdbc14.jar`
  - `oraclepki.jar`
  - `ojpse.jar`

Limitations

- Pour éviter les doublons, vous devez exécuter la reconnaissance de niveau 2 des noeuds finaux reconnus par le détecteur EMC Storage Scope.
- Pour réduire le nombre d'objets découverts susceptibles de générer des erreurs de manque de mémoire, le détecteur EMC Storage Scope Detail reconnaît uniquement le chemin d'accès SCSI pour chaque Volume, même si plusieurs sont

disponibles. TADDM utilise les chemins d'accès SCSI pour établir une relation entre un système informatique et un sous-système de stockage. Les chemins d'accès sont extraits de la table SRMHostArrayPath.

- Lorsque vous exécutez une reconnaissance, les pools de stockage StoragePools ne sont pas reconnus.

Problèmes de sécurité

- Si vous activez SSL dans la base de données EMC Oracle, vous devez ajouter le fichier `cwallet.sso` à la liste d'accès.

Objets de modèle avec attributs associés

Le détecteur EMC Storage Scope crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources de stockage stockées dans la base de données EMC Storage Scope.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous leur nom.

dev.BasedOnExtent

- Source
- Target

storage.HostBusAdaptor

- Nom
- Parent
- WordlWideName

dev.DiskDrive

- DiskSize
- Nom
- Parent
- SerialNumber
- Type
- Vendor
- Révision
- Status
- DiskSpeed

dev.FCPort

- Description
- Parent
- PermanentAddress
- PortNumber
- PortType
- Status

dev.FCVolume

- Capacity
- Nom
- Parent
- BasedOn

- FreeSpace

net.IpAddress

- DotNotation
- StringNotation

net.IpInterface

- IpAddress
- Parent

relation.ConnectedTo

- Source
- Target
- Type

storage.Fabric

- Fcswitch
- Name
- SourceToken
- ZoneSets
- Zones

storage.FCSwitch

- FCPorts
- ManagementURL
- Manufacturer
- Model
- Name
- ROMVersion
- SerialNumber
- Type
- WorldWideName

storage.StorageSubSystem

- AllocatedCapacity
- AvailabilityState
- AvailableCapacity
- CacheSize
- FCPorts
- Fqdn
- Manufacturer
- Members
- Model
- ROMVersion
- SerialNumber
- Type
- VolumeGroupCapacity
- VolumeGroupFreeSpace

storage.StorageVolume

- Capacity
- Name
- Parent
- RedundancyMethod
- SourceToken

storage.Zone

- Active
- Name
- Parent

storage.ZoneSet

- Active
- Name
- Parent
- Zones

Plusieurs systèmes d'exploitation :

sys.aix.Aix

sys.hpux.HpUx

sys.linux.Linux

sys.OperatingSystem

sys.sun.Solaris

sys.vmware.VmwareESX

sys.windows.WindowsOperatingSystem

Ces objets de modèles sont associés aux attributs suivants :

- FQDN
- OSConfidence
- OSName
- Parent

Plusieurs environnements informatiques :

sys.aix.AixUnitaryComputerSystem

sys.ComputerSystem

sys.hpux.HpUxUnitaryComputerSystem

sys.linux.LinuxUnitaryComputerSystem

sys.sun.SunSPARCUnitaryComputerSystem

sys.vmware.VmwareUnitaryComputerSystem

sys.windows.WindowsComputerSystem

Ces objets de modèles sont associés aux attributs suivants :

- Périphériques
- FCPorts
- FileSystems
- FQDN
- IpInterfaces
- Model

- OSInstalled
- OSRunning
- Signature
- Type
- Name

Plusieurs systèmes de fichiers :

sys.LocalFileSystem

sys.sun.SolarisFileSystem

sys.unix.UnixFileSystem

sys.windows.WindowsFileSystem

Ces objets de modèles sont associés aux attributs suivants :

- AvailableInodes
- AvailableSpace
- Capacity
- MountPoint
- Parent
- StorageExtent
- TotalInodes
- Type

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès

Pour une reconnaissance réussie, le détecteur a besoin des données d'identification suivantes :

- Les données d'identification du système informatique Windows pour le serveur EMC Storage Scope
- Les données d'identification Oracle pour la base de données EMC. Si vous activez SSL pour la connexion JDBC, vous devez également ajouter le fichier `cwallet.sso` à la liste d'accès.

Configuration du profil de reconnaissance :

Le détecteur EMC Storage Scope est activé par défaut dans un profil de reconnaissance de niveau 3.

Restriction : Le détecteur de stockage hôte et le détecteur de commutateur à fibre optique reconnaissent également les hôtes et les commutateurs. Si les deux sont activés, il se pourrait que les ressources soit reconnues en deux fois.

Créez un profil pour modifier les attributs suivants :

discoverHosts

La valeur par défaut de l'attribut **discoverHosts** est `true`. Le détecteur reconnaît les données associées à l'hôte, par exemple, ComputerSystem, disques, ports FC, volumes FC, volumes de stockage, systèmes de fichiers locaux et services de système de fichiers.

Si la valeur est `false`, les données associées à l'hôte ne sont pas reconnues par le détecteur.

discoverSwitch
La valeur par défaut de l'attribut **discoverSwitch** est `true`. Le détecteur reconnaît les données de commutateur, par exemple, commutateur, ports de commutation et ports FC.

Si la valeur est `false`, les données de commutateur ne sont pas reconnues par le détecteur.

discoverArraySerialNumberStartsWith
Par défaut, le détecteur reconnaît toutes les matrices trouvées. Vous pouvez indiquer cet attribut pour limiter leur nombre. Par exemple, si vous souhaitez reconnaître les matrices avec un numéro de série commençant par APM, utilisez le paramètre suivant :

```
discoverArraySerialNumberStartsWith=APM
```

arraysDiscoveryChunk
La valeur par défaut de l'attribut **arraysDiscoveryChunk** est `10`. Cet attribut indique le nombre de matrices traité par chaque détecteur EMC Storage Scope Details.

Restriction : Si la valeur est trop élevée, la reconnaissance peut générer de erreurs de mémoire.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur EMC Storage Scope et propose des solutions à ces problèmes.

Le détecteur ne parvient pas à se connecter à la base de données EMC :

Problème
Le détecteur échoue car il ne parvient pas à se connecter à la base de données EMC.

Solution
Assurez-vous que vos données d'identification pour la base de données EMC sont correctes et que vous avez copié tous les fichiers JAR requis. Si vous activez SSL, vous devez également ajouter le fichier `cwallet.sso` à la liste d'accès.

Le détecteur ne reconnaît par les systèmes de l'ordinateur hôte

Problème
Le détecteur ne reconnaît par les systèmes de l'ordinateur hôte.

Solution
Le détecteur peut uniquement reconnaître les systèmes hôtes qui sont gérés par le centre de contrôle EMC et qui sont synchronisés avec la base de données EMC Storage Scope. Les hôtes doivent également avoir une relation avec le commutateur FC ou avec le sous-système de stockage.

La reconnaissance met trop de temps à terminer

Problème
La reconnaissance met trop de temps à terminer.

Solution
Le détecteur de stockage hôte et le détecteur de commutateur à fibre

optique reconnaissent également les hôtes et les commutateurs. Si les deux sont activés, il se pourrait que les ressources soit reconnues en deux fois. Vérifiez la reconnaissance.

La reconnaissance se termine avec l'erreur CTJTD2312E

Problème

La reconnaissance se termine avec l'erreur CTJTD2312E.

Solution

Dans le fichier journal du détecteur, recherchez la propriété `targetDb.HOSTNAME` et assurez-vous que l'hôte peut être résolu depuis le serveur TADDM.

Le verrouillage de la base de données se produit

Problème

Le verrouillage de la base de données se produit lorsque deux détecteurs essaient de stocker des données similaires dans la base de données en même temps.

Solution

Par défaut, tous les détecteurs Detail stockent leurs données en même temps. Vous pouvez modifier la propriété suivante pour les obliger à le faire un par un :

```
com.collation.discover.observer.topopumpdeadlockstrategy=avoid
```

Restriction : Il se peut que la durée de reconnaissance soit plus longue si les détecteurs stockent leurs données dans une séquence.

Détecteur de commutateur Fibre Channel

Le détecteur de commutateur Fibre Channel reconnaît les commutateurs Fibre Channel (FC) et les informations relatives aux ports FC.

Nom du détecteur utilisé dans l'interface graphique et les journaux

FCSwitchSensor

Objets de modèle avec attributs associés

Le détecteur de commutateur Fibre Channel (FC) crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations collectées par le détecteur sur les ressources de commutateur Fibre Channel dans votre environnement informatique.

Ce détecteur crée les objets de modèle ci-après. Les attributs qui sont associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

dev.FCPort

- DisplayName
- PortNumber
- DeviceID
- PermanentAddress
- PortType
- Speed

relation.ConnectedTo

- Source
- Target

storage.FCSwitch

- Name
- Description
- WorldWideName
- Model
- Manufacturer
- SerialNumber
- Version

sys.ControlSoftware

- Name
- VersionString

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du profil de reconnaissance :

Cette rubrique décrit comment configurer le profil de reconnaissance.

Le détecteur n'est pas activé par défaut. Pour l'activer, vous devez créer un profil de reconnaissance, puis activer le détecteur à partir de ce nouveau profil. Ce détecteur nécessite l'activation de détecteurs supplémentaires suivants dans le profil :

- **AnchorSensor**
- **PingSensor**
- **PortSensor**
- **SessionSensor**
- **SnmpMib2Sensor**

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	Vers ce qui suit :
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe

Mappez à partir de ce qui suit :	Vers ce qui suit :
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de commutateur Fibre Channel et propose des solutions à ces problèmes.

Informations de commutateur reconnues incomplètes

Problème

Le détecteur termine la reconnaissance mais ne collecte pas toutes les informations relatives aux commutateurs.

Solution

Vérifiez que les données suivantes sont disponibles :

- MIB Fibre Alliance (FC-MGMT MIB)
- MIB Cisco (CISCO-FC-FE MIB)
- Informations de modèle de commutateur Brocade (switch.html)

Détecteur de ressources hôte

Le détecteur de ressources hôte utilise la base d'informations de gestion (MIB) des ressources hôte pour reconnaître les caractéristiques du système d'exploitation comme la taille de la mémoire, le système de fichiers, les logiciels installés avec la date et le type, le périphérique d'accès à un support et les zones de stockage logique.

Les détails sur les zones de stockage logique peuvent s'avérer utiles pour l'identification et résolution des problèmes de «manque de mémoire» et de «manque de mémoire tampon».

Nom du détecteur utilisé dans l'interface graphique et les journaux

HostResourcesSensor

Limitations

Les systèmes de fichiers reconnus par le détecteur n'apparaissent pas sur l'interface utilisateur. Cette restriction s'applique aux systèmes informatiques exécutés sur des systèmes d'exploitation autres que le système d'exploitation Windows. Exécutez le script `api.sh` pour afficher les systèmes de fichiers reconnus par ce détecteur.

ID objets (OID) utilisés

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- Taille de la mémoire : .1.3.6.1.2.1.25.2.2.0
- Table de stockage : .1.3.6.1.2.1.25.2.1.2
- Type de périphérique : .1.3.6.1.2.1.25.3.1.1
- Périphérique d'accès à un support : .1.3.6.1.2.1.25.3.2.1.1
- Logiciel installé : .1.3.6.1.2.1.25.6.3.1.1

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- dev.MediaAccessDevice
- sys.ComputerSystem sys.OperatingSystem
- sys.FileSystem
- sys.SoftwareComponent

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, entrez les informations suivantes :

- Pour la reconnaissance SNMP V1 et V2, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMP)** comme **Type de composant**.
  2. Indiquez le nom de communauté correct.
- Pour la reconnaissance SNMP V3, procédez comme suit :
  1. Sélectionnez **Elément de réseau (SNMPV3)** comme **Type de composant**.
  2. Entrez le nom d'utilisateur, le mot de passe et le protocole d'authentification corrects en fonction des informations de mappage des données d'identification SNMP V3 figurant dans le tableau suivant :

Mappez à partir de ce qui suit :	**Vers ce qui suit :**
Type d'authentification (MD5, par exemple)	Protocole d'authentification
Clé secrète MD5	Mot de passe et confirmation du mot de passe
Description ou clé d'authentification privée	Mot de passe privé

Restriction : Pour établir une connexion initiale, le détecteur requiert SNMP version 1.

Détecteur de stockage hôte

Le détecteur de stockage hôte reconnaît le stockage associé à un système informatique, y compris le réseau de stockage SAN. Ce détecteur étend la reconnaissance du stockage fournie par le détecteur de stockage.

Les détecteurs de stockage et de stockage hôte reconnaissent les mêmes ressources de stockage, comme les disques, les partitions, les volumes logiques, les volumes physiques et les systèmes de fichiers. Le détecteur de stockage hôte reconnaît également les ressources de stockage suivantes :

- Volumes FC (canal optique)
- Ports FC
- Adaptateurs de bus hôte

Nom du détecteur utilisé dans l'interface graphique et les journaux

HostStorageSensor

Prérequis

Pour les cibles Linux 64 bits
La bibliothèque glibc 32 bits est requise

Limitations

Lorsque vous reconnaissez un stockage joint à un ordinateur cible utilisant le détecteur de stockage, n'exécutez pas de reconnaissance sur la même système en utilisant ce détecteur.

Vous devez installer les fichiers de bibliothèque d'API HBA (host bus adapter, adaptateur de bus hôte) du fournisseur (32 bits).

Le détecteur ne reconnaît pas les systèmes de fichiers ZFS sur les systèmes cibles Solaris.

N'exécutez pas le détecteur sur des partitions logiques AIX, où la configuration des partitions logiques est attachée au commutateur BR8470 FCoE qui exécute FOS v6.4.3_dcb dans le mode passerelle d'accès, car les systèmes connectés à ce commutateur FC pourraient se comporter de manière inattendue. Utilisez FOS7.0.2e ou versions ultérieures.

Problèmes de sécurité

Par défaut, les privilèges de super-utilisateur sont requis pour la reconnaissance des ressources SAN dans les environnements UNIX. Généralement, cette escalade du privilège s'effectue en définissant les autorisations d'accès aux fichiers à l'aide du terme `setuid` (set-user-ID mode bit) ou de la commande **`sudo`**.

Objets de modèle avec attributs associés

Le détecteur de stockage hôte crée des objets de modèle avec des attributs associés. Les attributs indiquent le type d'informations que le détecteur collecte sur les ressources de stockage de votre environnement informatique.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

dev.BasedOnExtent

- Source
- Target

dev.ControlledBy

- Controller
- Device

dev.Controller

- Name

dev.DiskDrive

- Description
- DiskSize
- Name
- Type

dev.DiskPartition

- BlockSize

- Name
- NumOfBlocks

dev.FCPort

- PermanentAddress
- PortType
- Speed

dev.FCVolume

- BlockSize
- Controller
- DeviceID
- FCPLun
- Name
- NodeWWN
- NumOfBlocks
- PortWWN
- RealizedBy
- SCSIBus
- SCSILun
- SCSITarget
- Type

dev.RealizesExtent

- Source
- Target

dev.SCSIProtocolController

- EndPoints
- FCPorts
- Name

dev.SCSIProtocolEndPoint

- Name
- WorldWideName

dev.SCSIVolume

- BlockSize
- DeviceID
- Name
- NumOfBlocks
- RealizedBy
- SCSIBus
- SCSILun
- SCSITarget
- Type

dev.StorageExtent

- BlockSize
- DeviceID

- Name
- NumOfBlocks

dev.StorageVolume

- BlockSize
- DeviceID
- Name
- NumOfBlocks
- RealizedBy
- Type

phys.physpkg.Card

- FWRevision
- Manufacturer
- Model
- SerialNumber

storage.HostBusAdaptor

- Name
- Package physique
- SCSIProtocolControllers
- WorldWideName

sys.LocalFileSystem

- AvailableSpace
- Capacity
- Label
- MountPoint
- StorageExtent
- Type

sys.NFSFileSystem

- AvailableSpace
- Capacity
- ExportName
- MountPoint
- ServerName

sys.unix.UnixFileSystem

- AvailableSpace
- Capacity
- Description
- MountPoint
- Type

sys.windows.WindowsFileSystem

- AvailableSpace
- Capacity
- Description
- MountPoint

- Type

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Copie du fichier du moteur de collecte vers un emplacement accessible au système hôte cible :

Le détecteur de stockage hôte utilise un programme exécutable, le fichier du moteur de collecte pour reconnaître les données de stockage. Par défaut, le détecteur de stockage hôte copie le fichier de moteur de collecte à un emplacement du système hôte cible. Une fois la reconnaissance terminée, le fichier du moteur de collecte est supprimé de l'hôte. Les privilèges de superutilisateur sont requis pour exécuter le programme du moteur de collecte. La copie d'une application sur un système hôte qui requiert des privilèges de superutilisateur peut introduire un risque pour la sécurité. Pour éviter ce risque, le détecteur prend en charge une configuration qui permet de déployer le moteur de collecte sur un emplacement sécurisé et d'y accéder à partir d'un emplacement sécurisé.

Pour exécuter le moteur de collecte à partir d'un emplacement sécurisé, copiez le fichier du moteur de collecte vers un emplacement accessible au système hôte cible.

Pour copier et configurer le fichier du moteur de collecte, procédez comme suit :

1. A partir du répertoire `taddm_home/dist/osgi/plugins/com.ibm.cdb.discover.sensor.dev.hoststorage_7.2.0/bin/collection-engine` du serveur TADDM, copiez le fichier vers un emplacement accessible au système hôte cible.
2. Restreignez la propriété et l'accès au répertoire au superutilisateur.
3. Indiquez l'emplacement du fichier du moteur de collecte. Cet emplacement doit être accessible à partir du système hôte cible. Pour indiquer l'emplacement du fichier du moteur de collecte, utilisez l'une des options suivantes :
   - Pour les systèmes Windows, modifiez la variable d'environnement *PATH* du système hôte et entrez l'emplacement du répertoire du moteur de collecte.
   - Pour tous les autres systèmes, éditez la propriété *com.collation.discover.agent.path* dans le fichier `collation.properties` du serveur TADDM et entrez l'emplacement du répertoire du moteur de collecte. Indiquez l'emplacement du répertoire du moteur de collecte pour le système d'exploitation cible approprié.
   - Modifiez le profil de reconnaissance du détecteur de stockage hôte sur le serveur TADDM. Saisissez le chemin d'accès du répertoire du moteur de collecte dans l'attribut *CollectionEnginePath* ou *CollectionEngineWindowsPath*, ou les deux, si nécessaire.
4. Modifiez le profil de reconnaissance du détecteur de stockage hôte sur le serveur TADDM. Définissez la valeur de l'attribut **deployCollectionEngine** sur `false`.
5. Vérifiez que les droits d'utilisateur corrects sont accordés.

   Les commandes utilisées par le détecteur de stockage hôte exécutant la reconnaissance peuvent requérir une escalade des privilèges. D'une manière générale, cette escalade du privilège s'effectue en définissant les autorisations d'accès aux fichiers à l'aide du terme **`setuid`** (set-user-ID mode bit) ou de la commande **`sudo`**. Pour les systèmes d'exploitation Windows, l'utilisateur de la reconnaissance doit appartenir au groupe des administrateurs.

Configuration du profil de reconnaissance :

Le détecteur de stockage hôte n'est pas activée par défaut. Pour l'activer, vous devez créer un profil de reconnaissance, puis activer le détecteur à partir du nouveau profil.

Le moteur de collecte utilise l'API HBA (adaptateur de bus hôte) pour reconnaître les HBA et les volumes FC configurés sur le système hôte. Pour permettre l'exécution correcte de la reconnaissance, la bibliothèque des API HBA du fournisseur doit être installée et correctement configurée sur le système hôte.

Les attributs suivants peuvent être modifiés :

Fix Pack 4 **deployCollectionEngineWindows**
La valeur par défaut de l'attribut **deployCollectionEngineWindows** est `true`. Le détecteur copie le fichier du moteur de collecte à un emplacement du système hôte cible Windows. Une fois la reconnaissance terminée, le fichier du moteur de collecte est supprimé de l'hôte. L'emplacement est entré dans l'attribut **collectionEngineWindowsPath**. Si aucun chemin n'est indiqué sur des systèmes Windows, le fichier du moteur de collecte est copié dans le répertoire `TEMP`.

Si la valeur est `false`, le fichier du moteur de collecte n'est pas copié.

deployCollectionEngine
La valeur par défaut de l'attribut **deployCollectionEngine** est `true`. Le détecteur copie le fichier du moteur de collecte sur le système hôte cible. Une fois la reconnaissance terminée, le fichier du moteur de collecte est supprimé de l'hôte. L'emplacement est entré dans l'attribut **collectionEnginePath** ou **collectionEngineWindowsPath**. Si aucun chemin n'est indiqué sur des systèmes Windows, le fichier du moteur de collecte est copié dans le répertoire `TEMP`. Pour tous les autres systèmes, le fichier du moteur de collecte est copié dans le répertoire principal de l'utilisateur (celui qui exécute la reconnaissance) sur le système hôte cible.

Si la valeur est `false`, le fichier du moteur de collecte n'est pas copié.

Important : Fix Pack 4 Dans TADDM 7.3.0.4 et versions ultérieures, cet attribut ne s'applique pas aux cibles Windows. A la place, utilisez l'attribut **deployCollectionEngineWindows**.

collectionEnginePath
Il n'existe pas de valeur de défaut pour l'attribut **collectionEnginePath**. Entrez le chemin d'accès absolu au répertoire du moteur de collecte UNIX, si nécessaire.

collectionEngineWindowsPath
Il n'existe pas de valeur par défaut pour l'attribut **collectionEngineWindowsPath**. Entrez le chemin d'accès absolu au répertoire du moteur de collecte Windows, si nécessaire.

La saisie du chemin d'accès Windows lorsque le répertoire réside sur une unité réseau (créé avec la commande **net use**), peut échouer. A la place, entrez le chemin Windows à l'aide de la méthode UNC (Universal Naming Convention). Par exemple, `\\hostname\share\CollectionEngine`.

collectionEngineSudoCommand
Il n'existe pas de valeur par défaut pour l'attribut

collectionEngineSudoCommand. Saisissez la commande permettant d'obtenir une escalade des privilèges sur les systèmes UNIX.

collectionEngineTimeout
La valeur par défaut de l'attribut **collectionEngineTimeout** est `30`. Cette valeur indique, en minutes, l'intervalle de temps après lequel un dépassement de délai d'attente se produit durant une reconnaissance.

collectionEngineForceUniqueName
La valeur par défaut pour l'attribut **collectionEngineForceUniqueName** est `false`. Si la valeur est `false`, le moteur de collecte n'est pas renommé quand il est copié sur le système cible. Si la valeur est `true`, un horodatage est ajouté au nom du moteur de collecte avant sa copie sur le système cible.

Si vous utilisez la commande **`sudo`** afin d'autoriser l'utilisateur de la reconnaissance à exécuter le moteur de collecte, le nom de ce dernier n'est pas modifiable. Dans ce cas, la valeur par défaut `false` doit être employée.

Si, dans des environnements utilisant des reconnaissances simultanées, plusieurs reconnaissances sont exécutées en même temps par rapport aux mêmes systèmes cible, des collisions peuvent se produire lors du déploiement du moteur de collecte. En pareille situation, l'attribut **collectionEngineForceUniqueName** peut être défini sur `true` pour obliger à ce que le nom du moteur de collecte soit unique sur le système cible. Si cet attribut est défini à true, la commande **`sudo`** ne peut pas être utilisée.

Si le détecteur de stockage hôte est activée, n'activez pas le détecteur de stockage. Si les deux détecteurs sont activés, certaines ressources de stockage sont reconnues deux fois.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

En règle générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Les commandes utilisées par le détecteur de stockage hôte exécutant la reconnaissance peuvent nécessiter une escalade du privilège. D'une manière générale, cette escalade du privilège s'effectue en définissant les autorisations d'accès aux fichiers à l'aide du terme **`setuid`** (set-user-ID mode bit) ou de la commande **`sudo`**.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Ce détecteur utilise les entrées suivantes, qui indiquent explicitement l'emplacement du répertoire du moteur de collecte, dans le fichier `collation.properties` :

com.collation.discover.agent.path.Linux

com.collation.discover.agent.path.SunOS

com.collation.discover.agent.path.HP-UX

com.collation.discover.agent.path.AIX

com.collation.discover.agent.path.Vmnix

Vous pouvez indique chacune de ces propriétés sous forme de propriété sectorisée en leur ajoutant une adresse IP ou un nom d'ensemble de portées ; par exemple, `com.collation.discover.agent.path.Linux.1.2.3.4`.

Si le moteur de collecte existe sur plusieurs ordinateurs cibles dotés du même systèmes d'exploitation, mais que les moteurs de collecte résident dans différents chemins, entrez ces chemins dans le fichier `collation.properties`. en les séparant par un point-virgule.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de stockage hôte et propose des solutions à ces problèmes.

Echec des commandes en raison de privilèges insuffisants

Problème

Des échecs de commande se produisent à cause d'erreurs de droits d'accès refusés et sont enregistrés dans les fichiers journaux.

Solution

Vérifiez que les commandes qui requièrent une escalade des privilèges sont configurés correctement.

L'exécution de la reconnaissance dure un certain temps

Problème

Le temps d'exécution de la reconnaissance est très long.

Solution

Vérifiez si le détecteur **StorageSensor** est activé et désactivez-le. Si les deux détecteurs sont activés, certaines ressources de stockage sont reconnues deux fois.

Les données de stockage hôte ne sont pas reconnues

Problème

Les données de stockage hôte ne sont pas reconnues.

Solution

Vérifiez que les fichiers de bibliothèque d'API HBA (host bus adapter, adaptateur de bus hôte) du fournisseur sont installés et configurés correctement sur le système hôte. Des fichiers de bibliothèque manquants peuvent être identifiés dans le fichier journal HostStorageSensor.

Les informations WWPN et WWNN ne sont pas affichées

Problème

Le nom de port international (WWPN, worldwide port name) et le nom de noeud international (WWNN, worldwide node name) d'un volume FC ne sont pas affichés.

Solution

TADDM utilise l'API HBA pour la reconnaissance des volumes FC. L'API HBA fournit un mappage de l'identification de système d'exploitation d'un

volume SCSI à la représentation FC du volume. La représentation FC inclut le WWPN du port à partir de l'adaptateur HBA qui trouve le volume. Sur les adaptateurs HBA multiports, il est impossible de déterminer le port auquel s'applique un volume SCSI. Cette limitation se situe dans l'API HBA. La spécification de l'API HBA a été mise à jour pour résoudre ce problème, mais cette modification n'est peut-être pas implémentées dans toutes les bibliothèque d'API HBA. Assurez-vous que la dernière version de la bibliothèque d'API HBA du fournisseur HBA est installée sur le système hôte cible. En résumé, si l'API HBA ne peut pas fournir le mappage d'un volume SCSI à sa représentation FC, la détermination du WWPN et du WWNN est impossible.

Le nombre prévu d'adaptateurs HBA n'est pas affiché

Problème

TADDM n'affiche pas le nombre prévu d'adaptateurs HBA.

Solution

TADDM utilise l'API HBA pour la reconnaissance des adaptateurs HBA. Pour chaque adaptateur renvoyé par l'API HBA, TADDM crée un objet de modèle HBA. Le WWNN des adaptateurs est utilisé par TADDM pour nommer l'adaptateur HBA. Le nombre d'adaptateurs peut ne pas correspondre au nombre de cartes HBA physiques installées dans le système informatique hôte ou au nombre de WWNN retournés par les commandes système de base.

La manière dont la bibliothèque d'API HBA interprète les adaptateurs et les WWNN est déterminée par l'implémentation des bibliothèques d'API HBA par le fournisseur de cartes HBA. Par exemple, certains fournisseurs peuvent représenter une carte HBA multiport qui utilise un adaptateur unique avec un WWNN unique. D'autres fournisseurs peuvent représenter une carte HBA multiport qui utilise un adaptateur par port, chaque adaptateur possédant son WWNN unique.

Le type et la vitesse du port ne sont pas affichés

Problème

Le type et la vitesse d'un port FC ne sont pas affichés.

Solution

TADDM utilise l'API HBA pour la reconnaissance des ports FC. Toutefois, certaines bibliothèques d'API HBA peuvent ne pas prendre en charge ces attributs, ou la bibliothèque d'API HBA du fournisseur de cartes HBA peut nécessiter une mise à jour. Assurez-vous que la dernière version de la bibliothèque d'API HBA est installée sur le système hôte cible. Si la bibliothèque d'API HBA ne peut pas déterminer le type et la vitesse du port, ces attributs ne sont pas affichés.

Le bus SCSI, la cible SCSI et le LUN SCSI ne sont pas affichés correctement

Problème

Le bus SCSI, la cible SCSI et le numéro d'unité logique (LUN) SCSI d'un volume FC ne sont pas affichés ou les valeurs correctes ne sont pas affichées.

Solution

TADDM utilise l'API HBA pour reconnaître les informations SCSI sur un volume FC. Toutefois, certaines bibliothèques d'API HBA peuvent ne pas

prendre en charge ces attributs ou ne pas retourner les valeurs correctes pour ces attributs. Pour résoudre ce problème, la bibliothèque d'API HBA du fournisseur de cartes HBA peut nécessiter une mise à jour. Assurez-vous que la dernière version de la bibliothèque d'API HBA est installée sur le système hôte cible. Si la bibliothèque d'API HBA ne peut pas déterminer les informations SCSI, ces attributs ne sont pas affichés ou risquent d'afficher des valeurs incorrectes.

Les informations de volume FC ne s'affichent pas correctement

Problème

Les informations de volume FC ne sont pas affichées ou n'affichent pas les valeurs correctes.

Solution

TADDM utilise l'API HBA pour reconnaître les informations relatives à un volume FC. Toutefois, en cas de problème avec la bibliothèque d'API HBA, TADDM risque d'afficher des valeurs incorrectes pour certains attributs de volume FC, par exemple, la taille de bloc. Pour résoudre ce problème, assurez-vous que la dernière version de la bibliothèque d'API HBA est installée sur le système hôte cible et qu'elle est configurée correctement. Si la bibliothèque d'API HBA n'est pas configurée correctement, les attributs de volume FC risquent de ne pas s'afficher ou d'afficher des valeurs incorrectes.

L'utilisation du commutateur BR8470 FCoE fait que HostStorageSensor a une incidence négative sur les systèmes connectés au commutateur

Problème

Lorsque vous exécutez HostStorageSensor sur des partitions logiques AIX, où la configuration des partitions logiques est attachée au connecteur BR8470 FCoE qui exécute FOS v6.4.3_dcb dans le mode passerelle d'accès, les systèmes connectés à ce commutateur FC se comportent de manière inattendue.

Solution

Il s'agit d'un problème FOS connu. Pour le résoudre, effectuez une mise à niveau vers FOS7.0.2e ou versions ultérieures.

Détecteur IBM Tivoli Storage Productivity Center

Le détecteur IBM Tivoli Storage Productivity Center reconnaît les ressources de stockage liées à un réseau de stockage (SAN) et un stockage en réseau (NAS). Le détecteur extrait des données à partir d'une base de données Tivoli Storage Productivity Center.

Ci-après des exemples de ressources reconnues par le détecteur :

- Tableaux de stockage
- Commutateurs
- Hôtes
- Matrices
- Zones
- Volumes de stockage
- Ports de commutation et tableau
- Systèmes de fichiers
- Partitions de disque

- Données NAS

Certaines de ces ressources peuvent aussi être reconnues par le détecteur de stockage hôte (par exemple, les données liées aux hôtes) et le détecteurs du commutateur de canal optique (par exemple, les données liées aux commutateurs).

Nom du détecteur utilisé dans l'interface graphique et les journaux

TPCStorageSensor

Fix Pack 5

Prérequis

Informations de mappage

Pour obtenir des mappages entre les ressources de stockage (disques de stockage, volumes, hôtes physiques, machines virtuelles VM, SVController utilisés comme virtualiseur STG, commutateurs FC et disque, etc.), utilisez le schéma ci-dessous qui détaille les prérequis au niveau de TPC/Spectrum et au niveau de la reconnaissance TADDM pour chaque cas :

Mappage entre un serveur virtuel (en général des machines virtuelles VMware) et des ressources d'unités logiques de stockage

La relation peut être obtenue après l'exécution des détecteurs HostStorageSensor et TPCStorageServerSensor.

Vous devez toutefois prendre en considération les prérequis et les limitations des deux détecteurs.

Pour connaître les prérequis du détecteur de stockage hôte, reportez-vous au lien https://www.ibm.com/support/knowledgecenter/en/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_sensor_hoststorage.html

Pour les prérequis du détecteur de stockage TPC, reportez-vous au lien https://www.ibm.com/support/knowledgecenter/en/SSPLFC_7.3.0/com.ibm.taddm.doc_7.3/SensorGuideRef/r_cmdb_sensor_tpcstorage.html

Mappage entre les sous-systèmes de stockage et les ressources d'unités logiques de stockage

Il s'agit d'une relation implicite qui apparaît si le sous-système de stockage est correctement reconnu.

Mappage entre les ressources de serveurs physiques et de sous-systèmes de stockage

Cette relation peut être obtenue à partir du détecteur HostStorageSensor. Vous devez toutefois prendre en considération les prérequis et les limitations du détecteur HostStorageSensor.

Remarque : Les relations ci-dessus peuvent être obtenues sans l'installation d'agents TPC SRA sur les hôtes cible dans le domaine TCP de gestion. Il y a généralement des exceptions selon les tables sources TPC Spectrum Control utilisées. Cela peut être dû aux informations insuffisantes qu'elles contiennent pour

identifier un hôte cible connexe (nom d'hôte + adresse IP et/ou adresse MAC, etc.) et pour autoriser toujours TADDM à corréler les hôtes cible à des données de sous-système de stockage.

Mappage entre les volumes de sous-systèmes de stockage et le noeud final cible

Pour obtenir le mappage entre le volume de sous-systèmes de stockage reconnu par TADDM (via le détecteur de stockage TPC) et les serveurs cible de noeud final, TPC a besoin des agents TPC SRA installés sur les hôtes cible qui accèdent à ces volumes car TADDM doit au moins disposer de l'adresse MAC avec le nom d'hôte cible pour indiquer qu'il accèdent à des volumes spécifiques. Une autre alternative consiste à utiliser HostStorageSensor pour chacun des hôtes cible afin de stocker et d'afficher les informations de mappage.

Objets de modèle avec attributs associés

Le détecteur IBM Tivoli Storage Productivity Center crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources de stockage stockées dans la base de données Tivoli Storage Productivity Center.

Ce détecteur crée les objets de modèle ci-après. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet.

dev.BasedOnExtent

- Source
- Target
- Type

dev.Controller

- Name
- Parent

dev.DiskDrive

- DiskSize
- Model
- Name
- Parent
- SerialNumber
- Type
- Vendor

dev.DiskPartition

- Capacity
- Name
- Parent
- PartitionType
- RealizedBy

dev.FCPort

- Label
- Parent
- PermanentAddress
- PortNumber

- PortType
- Speed

dev.FCVolume

- Capacity
- FCPLun
- Name
- Parent
- Type
- PortWWN
- HostPaths
- BasedOn

dev.RealizesExtent

- Source
- Target
- Type

dev.SCSIPath

- ArrayVolume
- HostEndPoint
- LUN
- Parent
- Volume

dev.SCSIProtocolEndPoint

- WorldWideName

dev.TapeDrive

- Label
- Type
- WorldWideName

net.IpAddress

- DotNotation
- StringNotation

net.IpInterface

- IpAddress
- Parent

relation.ConnectedTo

- Source
- Target
- Type

storage.Fabric

- Fcswitch
- Label
- Name
- SourceToken
- Virtual

- ZoneSets
- Zones

storage.FCSwitch

- FCPorts
- FCSwitchStatus
- Fcport
- ManagementURL
- Manufacturer
- Model
- Name
- ROMVersion
- SerialNumber
- Type
- WorldWideName
- IpInterfaces

storage.StoragePool

- AnsiT10Id
- Capacity
- Label
- Members
- Raid Level
- RemainingManagedSpace
- StorageSubSystem
- TotalAvailableSpace
- TotalManagedSpace

storage.StorageSubSystem

- AllocatedCapacity
- AnsiT10Id
- AvailabilityState
- AvailableCapacity
- CacheSize
- FCPorts
- Fqdn
- IpInterfaces
- IsNetworkAttached
- Manufacturer
- Members
- MemorySize
- Model
- NumCPUs
- ROMVersion
- SerialNumber
- StoragePools
- Type

- VolumeGroupCapacity
- VolumeGroupFreeSpace

storage.StorageVolume

- BlockSize
- Capacity
- FreeSpace
- Name
- Parent
- RealizedBy
- RedundancyMethod
- SourceToken
- Type
- Virtual
- Paths

storage.TapeLibrary

- AnsiT10Id
- Description
- Devices
- Manufacturer
- Model
- ROMVersion
- SerialNumber
- TapeMediaChangers
- Type

storage.TapeMediaChanger

- Caption
- Description
- Fqdn
- Label
- ROMVersion
- Type
- WorldWideName

storage.Zone

- Active
- Description
- Name
- Parent

storage.ZoneSet

- Active
- Label
- Name
- Parent
- Zones

Plusieurs systèmes d'exploitation :

sys.aix.Aix
sys.hpux.HpUx
sys.linux.Linux
sys.netware.Netware
sys.OperatingSystem
sys.sun.Solaris
sys.vmware.VmwareESX
sys.windows.WindowsOperatingSystem

Les attributs suivants sont associés à ces objets de modèle :

- FQDN
- OSConfidence
- OSName
- OSVersion
- Parent
- SoftwareComponents
- SystemGuid

Plusieurs environnements informatiques :

sys.aix.AixUnitaryComputerSystem
sys.ComputerSystem
sys.hpux.HpUxUnitaryComputerSystem
sys.linux.LinuxUnitaryComputerSystem
sys.sun.SunSPARCUnitaryComputerSystem
sys.vmware.VmwareUnitaryComputerSystem
sys.windows.WindowsComputerSystem

Les attributs suivants sont associés à ces objets de modèle :

- CPUSpeed
- CPUType
- Devices
- FCPorts
- FileSystems
- Fqdn
- IpInterfaces
- Manufacturer
- MemorySize
- Model
- NumCPUs
- OSInstalled
- OSRunning
- SerialNumber
- Signature
- Type
- Name
- UUID
- MacAddress

- VMID

sys.FileSystemExport

- Name
- Parent

sys.FileSystemService

- Exports
- Host
- Name

sys.NFSExport

- Name
- Parent

sys.NFSService

- Exports
- Host
- Name

Plusieurs systèmes de fichiers :

sys.LocalFileSystem
sys.sun.SolarisFileSystem
sys.unix.UnixFileSystem
sys.windows.WindowsFileSystem

Les attributs suivants sont associés à ces objets de modèle :

- AvailableInodes
- AvailableSpace
- Capacity
- MountPoint
- Parent
- StorageExtent
- TotalInodes
- Type

sys.SMBExport

- Name
- Parent
- Path
- Type

sys.SMBService

- Exports
- Host
- Name

sys.SoftwareComponent

- Name
- Parent
- SoftwareVersion

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration du fichier de propriétés de Tivoli Storage Productivity Center :

Le détecteur Tivoli Storage Productivity Center utilise des requêtes SQL pour extraire des données de la base de données de Tivoli Storage Productivity Center. Les requêtes SQL sont définies dans le fichier `tpc.config` et leur exécution est contrôlée par les propriétés définies dans le fichier `tpc.properties`.

Les fichiers `tpc.config` et `tpc.properties` se trouvent dans :`COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.srm.tpc_xxx`, où *xxx* est la version du plug-in du détecteur.

Le détecteur utilise les entrées suivantes dans le fichier `tpc.properties` pour identifier les requêtes à exécuter :

com.ibm.cdb.discover.app.srm.tpc.sensor.ArrayQueries
Cette propriété est associée aux ressources de tableau. Par défaut, les requêtes suivantes sont activées :
`ARRAY,ARRAY_SUM_SOURCE,ARRAY_VOLUME_GROUP,ARRAY_DRIVE,ARRAY_PORT,ARRAY_VOLUME`.

com.ibm.cdb.discover.app.srm.tpc.sensor.HostQueries
Cette propriété est associée aux ressources hôte. Par défaut, les requêtes suivantes sont activées :
`HOST,HOST_PORT,HOST_DEVICE_GROUP,HOST_DEVICE,HOST_DEVICE_PARTITION,HOST_DEVICE_PARTITION_DEVICE,HOST_FS,HOST_FS_EXPORT,HOST_AGENT,HOST_SCSI_PATH,HOST_SCSI_AGENT_LESS`.

Requête HOST_SCSI_PATH
Cette requête permet de créer le mappage de stockage de bout en bout à partir de volumes FC d'un hôte vers les volumes d'un module de stockage. Cette requête est activée par défaut. Selon la dimension de l'environnement de stockage, l'exécution de cette requête peut accroître de façon significative la durée de la reconnaissance du détecteur. En conséquence, lors de reconnaissance d'environnements de stockage étendus, il est préférable de n'activer la requête `HOST_SCSI_PATH` que de manière occasionnelle. Pour désactiver cette requête, n'incluez pas `HOST_SCSI_PATH` dans la propriété : `com.ibm.cdb.discover.app.srm.tpc.sensor.HostQueries`.

Pour plus d'informations sur l'édition de la propriété, voir «Erreur liée à une insuffisance de mémoire si une requête HOST_SCSI_PATH ou HOST_SCSI_AGENT_LESS est activée», à la page 451.

Requête HOST_SCSI_AGENT_LESS
Cette requête permet de créer un mappage de stockage de bout en bout à partir de volumes FC d'un hôte vers les volumes d'un module de stockage, lorsque les agents de ressources de stockage du serveur TPC ne sont pas déployés sur les noeuds finaux. Cette requête est activée par défaut. Selon la dimension de l'environnement de stockage, l'exécution de cette requête peut accroître de façon significative la durée de la reconnaissance du détecteur. En conséquence, lors de reconnaissance d'environnements de stockage étendus, il est préférable de n'activer

la requête HOST_SCSI_PATH que de manière occasionnelle. Pour désactiver cette requête, n'incluez pas HOST_SCSI_PATH dans la propriété : com.ibm.cdb.discover.app.srm.tpc.sensor.HostQueries.

Pour plus d'informations sur l'édition de la propriété, voir «Erreur liée à une insuffisance de mémoire si une requête HOST_SCSI_PATH ou HOST_SCSI_AGENT_LESS est activée», à la page 451.

L'exemple suivant montre la propriété com.ibm.cdb.discover.app.srm.tpc.sensor.HostQueries avec les requêtes HOST_SCSI_PATH et HOST_SCSI_AGENT_LESS désactivées :
com.ibm.cdb.discover.app.srm.tpc.sensor.HostQueries=HOST,HOST_PORT,
HOST_DEVICE_GROUP,HOST_DEVICE,HOST_DEVICE_PARTITION,
HOST_DEVICE_PARTITION_DEVICE,HOST_FS,HOST_FS_EXPORT,HOST_AGENT.

com.ibm.cdb.discover.app.srm.tpc.sensor.FabricQueries
Cette propriété est associée aux ressources de matrice. Par défaut, les requêtes suivantes sont activées : FABRIC, ZONE_SET, ZONE.

com.ibm.cdb.discover.app.srm.tpc.sensor.SwitchQueries
Cette propriété est associée aux ressources de commutateur. Par défaut, les requêtes suivantes sont activées : SWITCH, SWITCH_PORT.

com.ibm.cdb.discover.app.srm.tpc.sensor.NASQueries
Cette propriété est associée aux ressources NAS. Par défaut, les requêtes suivantes sont activées : NAS_FILER, NAS_CONTROLLER, NAS_VOLUME, NAS_FS, NAS_DEVICE, NAS_FS_EXPORT.

com.ibm.cdb.discover.app.srm.tpc.sensor.TapeQueries
Cette propriété est associée aux ressources TAPE. Par défaut, les requêtes suivantes sont activées : TAPE_LIBRARY, TAPE_MEDIA_CHANGER, TAPE_DRIVE.

com.ibm.cdb.discover.app.srm.tpc.sensor.SummaryQueries
Cette propriété est associée aux ressources SUMMARY. Par défaut, la requête suivante est activée : PORT_CONNECTIVITY.

Les propriétés suivantes permettent de contrôler à l'aide du détecteur IBM Tivoli Storage Productivity Center, la reconnaissance de certains types de systèmes informatiques :

com.ibm.cdb.discover.app.srm.tpc.sensor.ignoreAixCompSys=true
Cette propriété détermine si le détecteur IBM Tivoli Storage Productivity Center reconnaît ou non des systèmes informatiques sous les systèmes d'exploitation AIX. Par défaut, sa valeur est true, ce qui signifie que le détecteur ne reconnaît pas les systèmes informatiques sous les systèmes d'exploitation AIX.

com.ibm.cdb.discover.app.srm.tpc.sensor.IgnoreCSWithoutMacaddr=true
Cette propriété détermine si le détecteur IBM Tivoli Storage Productivity Center reconnaît les systèmes informatiques sans adresse MAC. Par défaut, c'est défini à true, ce qui signifie que le détecteur ne reconnaît pas les systèmes informatiques sans adresse MAC.

Le détecteur utilise les entrées suivantes du fichier collation.properties lorsque la requête HOST_SCSI_PATH ou HOST_SCSI_AGENT_LESS est activée.

com.ibm.cdb.discover.app.srm.tpc.sensor.HOST_SCSI_PATH.maxrows
Cette propriété détermine le nombre maximum de lignes que le détecteur traite lorsque la requête HOST_SCSI_PATH est activée.

La valeur par défaut est 20000.

Si la requête HOST_SCSI_PATH entraîne des exceptions de mémoire insuffisante, réduisez la valeur par défaut. Si vous souhaitez rassembler tous les chemins d'accès en une seule exécution de reconnaissance, en fonction de l'environnement de stockage, augmentez la valeur par défaut.

com.ibm.cdb.discover.app.srm.tpc.sensor.HOST_SCSI_AGENT_LESS.maxrows
Cette propriété détermine le nombre maximum de lignes que le détecteur traite lorsque la requête HOST_SCSI_AGENT_LESS est activée.

La valeur par défaut est 20000.

Si la requête HOST_SCSI_PATH entraîne des exceptions de mémoire insuffisante, réduisez la valeur par défaut. Si vous souhaitez rassembler tous les chemins d'accès en une seule exécution de reconnaissance, en fonction de l'environnement de stockage, augmentez la valeur par défaut.

Configuration du profil de reconnaissance :

Le détecteur **TPCStorageSensor** est activé par défaut dans le profil de reconnaissance.

Créez un profil pour modifier les attributs suivants :

discoverHosts
La valeur par défaut de l'attribut **discoverHosts** est true. Le détecteur reconnaît les données associées à l'hôte, par exemple, ComputerSystem, disques, ports FC, volumes FC, volumes de stockage, partitions de disque, systèmes de fichiers locaux et services de système de fichiers.

Si la valeur est false, les données associées à l'hôte ne sont pas reconnues par le détecteur.

discoverSwitch
La valeur par défaut de l'attribut **discoverSwitch** est true. Le détecteur reconnaît les données de commutateur, par exemple, commutateur, ports de commutation et ports FC.

Si la valeur est false, les données de commutateur ne sont pas reconnues par le détecteur.

restrictByScope
La valeur par défaut de l'attribut **restrictByScope** est false. Le détecteur reconnaît tous les hôtes qui ont déjà été reconnus par le serveur Tivoli Storage Productivity Center.

Si la valeur est true, le détecteur reconnaît les hôtes figurant dans la plage de portée de la reconnaissance du détecteur.

Fix Pack 3 **discoverManagedDisks**
La valeur par défaut de l'attribut **discoverManagedDisks** est false.

Si la valeur est true, le détecteur reconnaît les disques gérés pour SVC (storage virtualization layer) et leurs relations vers le stockage dorsal.

Remarque : Si vous définissez cet attribut sur true, le délai de reconnaissance et de stockage du détecteur IBM Tivoli Storage Productivity Center est plus long car davantage de données sont reconnues.

Le détecteur de stockage hôte et le détecteur de commutateur Fibre Channel reconnaissent également les données associées aux hôtes et aux commutateurs.

Lorsque les attributs **discoverHosts** et **discoverSwitch** sont activés, envisagez de désactiver le détecteur de stockage hôte et le détecteur de commutateur Fibre Channel pour empêcher que des ressources soient reconnues deux fois.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour une authentification auprès du serveur Tivoli Storage Productivity Center.
3. Sélectionnez **Base de données** en tant que **Type de composant** et **DB2** en tant que **Fournisseur**.
4. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que doit utiliser TADDM pour une authentification auprès de la base de données Tivoli Storage Productivity Center.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur IBM Tivoli Storage Productivity Center et présente des solutions à ces problèmes.

Des problèmes de connexion à la base de données Tivoli Storage Productivity Center provoquent un échec du détecteur

Problème

Le détecteur échoue en raison de problèmes de connexion à la base de données Tivoli Storage Productivity Center.

Solution

Vérifiez que les données d'identification DB2 de la base de données Tivoli Storage Productivity Center ont été entrées.

Les ordinateurs hôtes ne sont pas reconnus

Problème

Les ordinateurs hôte ne sont pas reconnus.

Solution

Le détecteur reconnaît uniquement les systèmes hôte gérés par l'agent Tivoli Storage Productivity Center. Vérifiez également que la valeur de l'attribut**discoverHosts** est `true` pour le détecteur.

L'exécution de la reconnaissance dure un certain temps

Problème

Le temps d'exécution de la reconnaissance est très long.

Solution

Si la valeur de l'attribut **discoverHosts** est `true`, vérifiez si le détecteur **HostStorageSensor** est activé, et si tel est le cas, désactivez-le. Si les deux détecteurs sont activés, certaines ressources de stockage sont reconnues deux fois.

Si la valeur de l'attribut **discoverSwitch** est `true`, vérifiez si le détecteur **FCSwitchSensor** est activé, et si tel est le cas, désactivez-le. Si les deux détecteurs sont activés, certaines ressources de stockage sont reconnues deux fois.

Ce problème peut également survenir si certaines requêtes activées génèrent un volume important de données. Par exemple, certaines requêtes pouvant générer des volumes de données importants sont les suivantes : `ARRAY_VOLUME`, `HOST_SCSI_PATH` et `SWITCH_PORT`. Ces requêtes sont activées par défaut.

Les systèmes informatiques ne font pas l'objet d'un rapprochement

Problème

Il n'existe aucun rapprochement entre les systèmes informatiques reconnus par le détecteur TPCStorageSensor et les mêmes systèmes informatiques reconnus par les détecteurs de système informatique.

Solution

Des systèmes informatiques d'un environnement de stockage peuvent être physiquement partitionnés ou virtualisés. Si ces systèmes sont reconnus par TPCStorageSensor, et aussi par un détecteur de système informatique, les deux ensembles de ressources reconnues ne sont pas rapprochés ensembles. Par exemple :

- Les partitions logiques (LPAR) sur pSystems reconnues par les détecteurs TPCStorageSensor et AixComputerSystemSensor
- Le serveur E-S virtuel (VIOS) reconnu par TPCStorageSensor et par le détecteur HMC
- Les partitions de noeud (NPAR) sur les systèmes HP reconnues par les détecteurs TPCStorageSensor et HpUxComputerSystemSensor
- Les zones sur les systèmes Solaris reconnues par TPCStorageSensor et SunSparcComputerSystemSensor

Pour vous assurer que les systèmes informatiques ne sont pas dupliqués, vous devez sélectionner les systèmes informatiques en double dans l'interface utilisateur TADDM et les fusionner manuellement.

Erreur liée à une insuffisance de mémoire si une requête `HOST_SCSI_PATH` ou `HOST_SCSI_AGENT_LESS` est activée

Problème

Selon l'environnement de stockage, les requêtes `HOST_SCSI_PATH` et `HOST_SCSI_AGENT_LESS` peuvent renvoyer un ensemble de résultats important pouvant se traduire par une erreur liée à une insuffisance de mémoire.

Solution

Le détecteur limite le nombre de lignes qu'il traite pour les requêtes `HOST_SCSI_PATH` and `HOST_SCSI_AGENT_LESS`à une valeur par défaut de 20 000 afin de prévenir des erreurs liée à une insuffisance de mémoire. La valeur est basée sur :

- Une taille de segment de mémoire de la machine virtuelle Java de reconnaissance (qui est de 1024 Mo)
- Une valeur par défaut du délai d'attente de l'agent (qui est de 600000 ms)

En outre, vous pouvez configurer le détecteur pour éviter des messages d'erreur liée à une insuffisance de mémoire, si la requête HOST_SCSI_PATH ou HOST_SCSI_AGENT_LESS est activée selon l'une des méthodes suivantes :

Modification du nombre par défaut de lignes traitées par le détecteur

Edition du fichier COLLATION_HOME/osgi/plugins/com.ibm.cdb.discover.sensor.app.srm.tpc_7.2.0/tpc.properties et ajout de la propriété suivante :

```
com.ibm.cdb.discover.app.srm.tpc.sensor.HOST_SCSI_PATH.maxrows=X
com.ibm.cdb.discover.app.srm.tpc.sensor.HOST_SCSI_AGENT_LESS.
maxrows=X
```

où *X* représente le nombre maximal de lignes que détecteur traite pour cette requête.

Si cette valeur est supérieure à 20 000 :

- Augmentez la taille du segment de mémoire pour la machine virtuelle Java de reconnaissance. Editez la propriété $COLLATION_HOME/etc/collation.properties et changez la propriété com.collation.Discover.jvmargs.ibm.

  Par exemple, pour définir la taille de segment de mémoire à 1824 Mo, ajoutez la ligne suivante :

  ```
  com.collation.Discover.jvmargs.ibm=-Xdisableexplicitgc -Xmx1824m
  ```

- Augmentez le délai d'attente de l'agent pour la machine virtuelle Java de reconnaissance. Dans le fichier $COLLATION_HOME/etc/collation.properties, ajoutez la propriété suivante, où *valeur* représente le nombre de millisecondes allouées pour l'exécution du détecteur :

  ```
  com.collation.discover.agent.TPCStorageSensor.timeout=valeur
  ```

  Si vous n'indiquez pas de valeur, la valeur par défaut 600000 est utilisée.

- Redémarrez TADDM.

Limitez la portée des modules de stockage et des systèmes informatiques reconnus

Le nombre de lignes que renvoient les requêtes HOST_SCSI_PATH et HOST_SCSI_AGENT_LESS peut être réduit en limitant la portée des modules de stockage et des systèmes informatiques reconnus.

1. Dans la console de gestion de reconnaissance, cliquez sur l'icône **Portée**. Sélectionnez l'ensemble de portées qui contient le serveur Tivoli Storage Productivity Center à reconnaître. Indiquez l'adresse IP, la plage ou des informations de sous-réseau des modules et des systèmes informatiques à reconnaître. L'adresse IP des modules de stockage et l'adresse IP du système informatique doivent être dans le même ensemble de portée que le serveur Tivoli Storage Productivity Center pour la reconnaissance. Ces valeurs permettent d'inclure les données de chemin d'accès SCSI dans les résultats de la reconnaissance.
2. Dans la console de gestion de reconnaissance, cliquez sur l'icône **Profils de reconnaissance**.
3. Dans la fenêtre Profils de reconnaissance, cliquez sur **Nouveau**.

4. Dans la fenêtre de création de profil, entrez le nom et la description du profil. Dans la zone **Cloner le profil existant**, cliquez sur **Reconnaissance de niveau 3**, puis cliquez sur **OK**.
5. Dans la liste des détecteurs, cliquez sur **TPCStorageSensor**, puis cliquez sur **Nouveau**.
6. Dans la fenêtre Création de configuration, entrez le nom et la description de votre configuration du détecteur TPCStorageSensor, et cochez la case **Activer la configuration**.
7. Dans la section **Configuration** de la fenêtre Activer la configuration, pour restreindre la portée de la reconnaissance, cliquez sur **restrictByScope**. Ensuite, cliquez deux fois sur la zone **Valeur** de la ligne, puis entrez true.
8. Cliquez sur **OK** pour revenir à la fenêtre Profils de reconnaissance.
9. Dans la fenêtre Profils de reconnaissance, cliquez sur **Sauvegarder**.
10. Démarrez une reconnaissance en utilisant le nouveau profil.

Après une reconnaissance à l'aide du détecteur, consultez `$COLLATION_HOME/log/sensors/`*`Id_exécution`*`/TPCStorageSensor-`*`IP-PORT`*`.log(.N)` pour afficher le nombre de chemins d'accès SCSI qui existent pour chaque adresse IP de module de stockage et chaque adresse IP d'hôte. Le texte suivant est un exemple de contenu du fichier journal :

```
SCSI PATH statistics by host ip address :
ip#1/4 with ipAddress 10.3.41.230 has 160 valid scsi paths
ip#2/4 with ipAddress 10.3.41.289 has 527 valid scsi paths
ip#3/4 with ipAddress 10.3.43.19 has 108 valid scsi paths
ip#4/4 with ipAddress 10.3.42.211 has 160 valid scsi paths

SCSI PATH statistics by array ip address:
ip#1/2 with ipAddress 10.0.15.201 has 693 valid scsi paths
ip#2/2 with ipAddress 10.0.17.2 has 736 valid scsi paths
```

Exécutez une reconnaissance avec le serveur Tivoli Storage Productivity Center dans une portée qui lui est propre

Pour obtenir l'ensemble complet des résultats des requêtes `HOST_SCSI_PATH` et `HOST_SCSI_AGENT_LESS` et éviter des erreurs liées à une insuffisance de mémoire, procédez comme suit :

1. Créez un ensemble de portée ne contenant que le serveur Tivoli Storage Productivity Center (sans aucune autre cible).
2. Créez un profil de reconnaissance avec le détecteur **TPCStorageSensor** et ses détecteurs dépendants activés uniquement.
3. Démarrez la reconnaissance de l'ensemble de portée contenant le serveur Tivoli Storage Productivity Center en utilisant le nouveau profil.

Le détecteur ne reconnaît aucun objet du fait des problèmes de recherche DNS

Problème

Le détecteur de centre de productivité d'IBM Tivoli Storage se termine sans avoir reconnu d'objets et l'avertissement suivant est émis :

```
CTJTD0952W None of the DB2 access list entries are able to connect to
the TPC database at URL: jdbc:db2://<hôte>:<port>/<base_de_données>.
```

Solution

Si <*hôte*>, qui est lu à partir du fichier `data/config/server.config` sur votre cible de reconnaissance est un nom de domaine complet ou un nom d'hôte (non une adresse IP standard), TADDM doit être en mesure de la résoudre. Configurez votre système de noms de domaine (DNS) de telle sorte que la commande **`nslookup`** <*hôte*> exécutée sur serveur de reconnaissance TADDM renvoie un IP résolu.

Détecteur NetApp

Le détecteur NetApp reconnaît des ressources de stockage liées à une unité de stockage réseau (NAS) en extrayant les données du système d'exploitation Data ONTAP avec le protocole SNMP.

Le détecteur reconnaît ces ressources de stockage en tant que gestionnaires de fichiers de stockage, clusters, volumes de disque, ports FC, disques physiques, agrégats (représentés comme des pool de stockage), services NFS et SMB.

Une reconnaissance NetApp est exécutée par `CustomMib2ComputerSystem` qui appelle des scripts d'extension. En outre, le détecteur Snap Drive est utilisé du côté hôte pour reconnaître des disques iSCSI définis. Si des données sont reconnues des deux sources et qu'elles correspondent, une relation entre l'hôte et la grappe est créée.

Identificateurs d'objets (OID)

Le détecteur utilise les OID de haut niveau suivants pour récupérer les attributs :

- Informations générales : `.1.3.6.1.4.1.789.1.1`
- Gestionnaire de fichiers virtuel : `.1.3.6.1.4.1.789.1.16`
- Volumes : `.1.3.6.1.4.1.789.1.5.8.1`
- Unités de disque : `.1.3.6.1.4.1.789.1.6.10.1`
- Unités de disque d'unité de secours : `.1.3.6.1.4.1.789.1.6.3.1`
- Unités de disque de cluster : `.1.3.6.1.4.1.789.1.6.2.1`
- Qtree : `.1.3.6.1.4.1.789.1.5.10.1`
- Clusters : `.1.3.6.1.4.1.789.1.25.1`
- Noeuds : `.1.3.6.1.4.1.789.1.25.2.1`
- Pool de stockage : `.1.3.6.1.4.1.789.1.5.11.1`
- Cartes FC : `.1.3.6.1.4.1.789.1.17.17.1.1`

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- dev.StorageVolume
- dev.DiskDrive
- dev.FCPort
- net.BindAddress
- net.IpInterface
- net.IpAddress
- net.Fqdn
- sys.NFSExport
- sys.SMBExport

- sys.function.StorageSubSystemFunction
- sys.ComputerSystemCluster
- sys.NFSSAP
- sys.SMBSAP
- sys.NFSService
- sys.SMBService
- storage.StorageSubSystem
- storage.StoragePool

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour les reconnaissances SNMP V2, entrez le nom de communauté approprié dans la liste d'accès. Vous pouvez utiliser le type de composant du modèle de réseau (SNMP) dans la fenêtre Liste d'accès de la console de gestion de reconnaissance.

Détecteur Snap Drive

Le détecteur Snap Drive reconnaît des ressources de stockage qui sont liées au logiciel NetApp SnapDrive pour Windows.

Le détecteur reconnaît de telles ressources de stockage comme un système de fichiers, des volumes SCSI, des adaptateurs de bus hôte et des noeuds finaux SCSI.

Ce détecteur est une partie de la reconnaissance de ressources de stockage NetApp. Il est nécessaire pour reconnaître des ressources de stockage comme iSCSI sous un système Windows. En outre, il fournit des données permettant de créer une relation avec un tableau.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SnapDriveSensor

Problèmes de sécurité

Le compte utilisateur utilisé pour la reconnaissance des systèmes informatiques est également utilisé pour exécuter les commandes SnapDrive.

Le détecteur utilise les commandes suivantes :

- **sdcli disk list**
- **iscsicli listpersistenttargets**
- **sdcli iscsi_target list -f <target IP>**
- **sdcli sysconfig list**

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- dev.SCSIVolume
- dev.StorageVolume
- dev.BasedOnExtent
- dev.SCSIProtocolEndPoint
- dev.SCSIPath

- storage.HostBusAdaptor
- sys.LocalFileSystem

Configuration de la liste d'accès

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Vous pouvez exécuter le détecteur Snap Drive en utilisant les données d'identification d'accès du système informatique (ComputerSystem) qui sont utilisées pour reconnaître le client.

Détecteur de stockage

Le détecteur de stockage reconnaît le stockage associé à un système informatique.

Ci-après des exemples de ressources reconnues par le détecteur :

- Disques
- Partitions
- Volumes logiques
- Volumes physiques
- Systèmes de fichiers

Nom du détecteur utilisé dans l'interface graphique et les journaux

StorageSensor

Prérequis

Pour les cibles Linux 64 bits

La bibliothèque glibc 32 bits est requise

Limitations

L'accès au répertoire `/dev/dsk` est impossible sur les systèmes cible locaux ou de zone personnalisée Solaris. Toutes les informations de stockage ne sont donc pas récupérées.

Lorsque vous reconnaissez un stockage joint à un ordinateur cible utilisant le détecteur de stockage hôte, n'exécutez pas de reconnaissance sur la même système en utilisant ce détecteur.

Le détecteur ne reconnaît pas les systèmes de fichiers ZFS sur les systèmes cibles Solaris.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- dev.BasedOnExtent
- dev.ControlledBy
- dev.Controller
- dev.DiskDrive
- dev.DiskPartition
- dev.FCVolume
- dev.RealizesExtent

- dev.SCSIVolume
- dev.StorageExtent
- dev.StorageVolume
- sys.NFSFileSystem
- sys.unix.UnixFileSystem
- sys.LocalFileSystem

Configuration du détecteur

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès :

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour configurer la liste d'accès, procédez comme suit :

1. Sélectionnez **ComputerSystem** comme **Type de composant**.
2. Indiquez les informations d'accès (nom d'utilisateur et mot de passe) que TADDM doit utiliser pour l'authentification à base de clé SSH ou l'authentification à base de connexion SSH sur le système informatique cible.

D'une manière générale, vous pouvez utiliser un compte sans privilèges d'administrateur. Toutefois, certaines commandes utilisées par TADDM durant le processus de reconnaissance peut requérir une escalade du privilège (généralement effectuée à l'aide de la commande **sudo**).

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Configuration des entrées du fichier collation.properties :

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Les propriétés suivantes du serveur TADDM indiquent les commandes du système d'exploitation utilisées par TADDM pour récupérer des informations liées au stockage :

- com.collation.platform.os.command.lvm.lvdisplay
- com.collation.platform.os.command.lvm.vgdisplay
- com.collation.platform.os.command.lvm.pvdisplay
- com.collation.platform.os.command.lputil.SunOS

Ces commandes requièrent un privilège élevé pour une exécution sur le système cible et doivent être configurées pour utiliser la commande **`sudo`**.

Pour plus d'informations, voir la rubrique *Commandes pouvant nécessiter des privilèges élevés* dans le *Guide d'administration*.

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de stockage et propose des solutions à ces problèmes.

Problèmes génériques

Déterminez si des informations sont manquantes et identifier tous les échecs de la commande en raison d'erreurs de type accès refusé. Vérifiez que les commandes nécessitant une escalade des privilèges sont correctement configurées. Pour plus d'informations, voir la rubrique Configuration des entrées du fichier collation.properties.

Détecteur de stockage SVC

Fix Pack 1

Le détecteur de stockage SVC reconnaît des ressources de stockage qui sont liées au réseau de stockage SAN (Storage Area Network). Ce détecteur extrait des données du contrôleur de volume IBM Storage.

Les ressources de stockage reconnues par le détecteur de stockage SVC incluent les groupes de stockage, les volumes de stockage, les ports FC, les pools de stockage et les unités de disque. Le détecteur utilise la connexion SSH pour extraire ces données.

Le détecteur de stockage SVC reconnaît le nom WWPN des hôtes pour créer la relation vers les volumes hôte, qui exige l'exécution de HostStorageSensor sur les hôtes.

Il est déconseillé d'exécuter le détecteur de stockage SVC avec le détecteur TPC pour le même noeud final. Cela peut entraîner des différences mineures dans les données reconnues, par exemple les chemins d'accès RAID ou SCSI, et générer des entrées supplémentaires dans l'historique des changements.

Fix Pack 3 Vous pouvez utiliser le détecteur de stockage SVC pour reconnaître les détails de configuration du système de stockage IBM Storwize v7000 inclus dans le châssis IBM PureFlex System. Voir «Détecteur IBM BladeCenter SNMP», à la page 311.

Le détecteur de stockage SVC est activé par défaut dans un profil de reconnaissance de niveau 2 et 3.

Nom du détecteur utilisé dans l'interface graphique et les journaux

SVCStorageSensor

Limitations

Le détecteur ne reconnaît pas l'attribut de niveau RAID pour des objets de pools de stockage et de volume de stockage parce que l'attribut est reconnu par TPCStorageSensor pour les mêmes objets.

Objets de modèle avec attributs associés

Fix Pack 1

Le détecteur SVC Storage crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources de stockage stockées dans SVC.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

dev.DiskDrive

- AdminState
- AnsiT10Id
- DiskSize
- Name
- Parent
- Status

dev.FCPort

- Parent
- PermanentAddress
- PortNumber
- PortType
- Speed

net.IpAddress

- DotNotation
- StringNotation

net.IpInterface

- IpAddress
- Parent

storage.StoragePool

- AdminState
- AnsiT10Id
- Capacity
- Label
- StorageSubSystem
- TotalAvailableSpace

storage.StorageSubSystem

- AllocatedCapacity
- AvailabilityState
- AvailableCapacity
- FCPorts
- Fqdn
- Manufacturer
- Members
- Model
- ROMVersion
- SerialNumber
- StoragePools
- Type
- VolumeGroupCapacity
- VolumeGroupFreeSpace

storage.StorageVolume

- AdminState
- BlockSize
- Capacity
- DeviceID
- IeeeUniqueVolumeName
- IOGroup
- ManagedSystemName
- Name
- Parent
- Paths
- RedundancyMethod

dev.SCSIPath

- arrayVolume
- HostEndPoint
- LUN
- Parent

physpkg.PhysicalFrame

- AdminState
- Label
- Manufacturer
- Model
- Name
- Parent
- Package physique
- RelativePosition

sys.CPU

- CPUSpeed
- IdentifyingNumber
- Manufacturer
- Parent
- VersionString

sys.OperatingSystem

- Name
- OSName
- Parent

Configuration de la liste d'accès

Fix Pack 1

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Le détecteur SVC Storage exige les données d'identification du système informatique du détecteur SVC pour exécuter une reconnaissance réussie.

Un rôle de moniteur doit être affecté aux utilisateurs créés sur SVC afin qu'ils puissent exécuter des reconnaissances. Le rôle leur permet d'exécuter des

commandes telles que **lssystem**, **lsmdisk**, **lsmdiskgrp**, **lsportfc**, **lsvdisk**, **lsnode**, **lsnodevpd**, **lsnodecanister**, **lsenclosure**, **lsvdiskhostmap** ou **lsfabric**.

détecteur Veritas Storage Foundation

Le détecteur VERITAS Storage Foundation reconnaît des systèmes VERITAS Storage Foundation.

Le détecteur Veritas Storage Foundation regroupe les composants principaux suivants et fournit une solution pour la gestion du stockage en ligne :

- VERITAS Volume Manager
- Système de fichiers VERITAS

Les disques physiques sont regroupés dans des volumes logiques pour améliorer l'utilisation du disque et réduire le gaspillage d'espace. VERITAS Volume Manager permet aux administrateurs d'utiliser des noms logiques (volumes) plutôt que d'utiliser un accès direct aux périphériques physiques.

Le système de fichiers VERITAS fournit également au système de fichiers de journalisation d'une entreprise une fiabilité et des performances améliorées.

Le détecteur VERITAS Storage Foundation a pour fonction de reconnaître les configurations Volume Manager générales suivantes :

- Version
- Répertoire d'installation
- Objets contrôlés par VxVM (par exemple, les volumes et les groupes de disques) et les relations entre eux.

Le second composant, le système de fichiers VERITAS, est reconnu comme un système de fichiers local et la version d'agencement du disque est collectée.

Nom du détecteur utilisé dans l'interface graphique et les journaux

VeritasStorageSensor

Problèmes de sécurité

L'utilisateur par défaut permettant de reconnaître le système informatique est utilisé.

Limitations

Les licences ne sont pas prises en charge. Il n'existe aucun descripteur d'application.

Objets de modèle créés

Le détecteur crée les objets de modèle suivants :

- app.ConfigFile
- app.SoftwareInstallation
- dev.MediaAccessDevice
- dev.veritas.VeritasDiskGroup
- dev.veritas.VeritasPlex

- dev.veritas.VeritasSubdisk
- dev.veritas.VeritasVMDisk
- dev.veritas.VeritasVolume
- sys.LocalFileSystem
- sys.veritasVeritasStorageService

Configuration des entrées du fichier collation.properties

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Il se peut que les propriétés suivantes requièrent des privilèges élevés.

- **com.collation.discover.agent.command.vxdisk=vxdisk**
- **com.collation.discover.agent.command.vxdg=vxdg**
- **com.collation.discover.agent.command.vxprint=vxprint**
- **com.collation.discover.agent.command.vxupgrade=vxupgrade**
- **com.collation.discover.agent.command.vxdf=df**

Identification et résolution des problèmes liés au détecteur

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur Veritas Storage Foundation et présente des solutions à ces problèmes.

Le détecteur échoue avec une erreur de dépassement du délai d'attente sur une plateforme Windows

Problème

Le détecteur Veritas Storage Foundation échoue avec une erreur de dépassement du délai d'attente sur une plateforme Windows

Solution

Dans le fichier de configuration, changez la valeur de `liteDiscoveryMode` à `true` si le détecteur est en dépassement de délai d'attente sur une plateforme Windows. L'exemple suivant illustre les attributs dans un fichier de configuration prédéfini :

```
<results xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <VeritasStorageAgentConfiguration
      xsi:type="coll:com.collation.platform.model.discovery.agent.
            VeritasStorageAgentConfiguration">
      <enabled>true</enabled>
      <familyName>DiscoverSensor</familyName>
      <name>VeritasStorageSensor</name>
      <seedClassName>com.collation.discover.seed.app.vsf.VeritasSFSeed
         </seedClassName>
      <agentClassName>com.collation.discover.agent.app.vsf.VeritasSFAgent
         </agentClassName>
      <liteDiscoveryMode>false</liteDiscoveryMode>
   </VeritasStorageAgentConfiguration>
</results>
```

Détecteur de stockage XIV

Fix Pack 1

XIVStorageSensor reconnaît les ressources de stockage relatives à SAN (Storage Area Network) en extrayant des données d'IBM XIV Storage System.

Les ressources de stockage reconnues par XIVStorageSensor incluent les grappes de stockage, les volumes de stockage, les ports FC, les pools de stockage et les unités de disque. Le détecteur utilise la connexion XCLI pour extraire les données.

XIVStorageSensor reconnaît le nom de port universel (WWPN) des hôtes pour la création de la relation pour les volumes hôte, qui exige l'exécution deHostStorageSensor sur les hôtes.

XIVStorageSensor est activé par défaut dans un profil de reconnaissance de niveau 2 et 3.

Nom du détecteur utilisé dans l'interface graphique et les journaux

XIVStorageSensor

Limitations

Le détecteur ne reconnaît pas le type de port FC parce qu'il est reconnu par TPCStorageSensor pour les mêmes objets.

Configuration requise pour l'installation du détecteur

L'application XCLI doit être installée sur l'hôte. Il doit pouvoir accéder à XIV Storage System via le protocole XCLI natif. Configurez l'adresse IP et le chemin d'accès de l'hôte sur lequel l'application XCLI est installée.

Condition requise : XIV Storage System version 4.5 est obligatoire.

SSH n'est peut-être pas activé sur le noeud final XIV et, en conséquence, le détecteur de commande PING ne renvoie aucun objet. Dans ce cas, créez un nouveau profil et activez la propriété de plateforme suivante :

```
com.collation.pingagent.ports=7778,22,135
```

Configuration du détecteur

Fix Pack 1

Vous devez configurer le détecteur avant d'exécuter une reconnaissance.

Configuration de la liste d'accès : Fix Pack 1

Cette rubrique décrit les caractéristiques d'accès requises selon votre configuration.

Pour une reconnaissance réussie, XIVStorageSensor a besoin des données d'identification suivantes :

- Données d'identification XIVStorage d'XIV Storage System (utilisateurs avec des droits en lecture seule).
- Données d'identification du système informatique de l'hôte, sur lequel l'application XCLI est installée.

Configuration des entrées du fichier `collation.properties` : Fix Pack 1

Cette rubrique répertorie les entrées du fichier `collation.properties` utilisées par le détecteur.

Quand le protocole SSH n'est pas disponible, définissez la propriété suivante dans le fichier `collation.properties` :

`com.collation.pingagent.ports=`*`numéros_de_port`*

Objets de modèle avec attributs associés

Fix Pack 1

Le détecteur de stockage XIV crée des objets de modèle avec des attributs associés. Ces attributs indiquent le type d'informations collectées par le détecteur sur les ressources de stockage stockées dans XIV.

Le détecteur crée les objets de modèle suivants. Les attributs associés à chaque objet de modèle sont indiqués sous le nom de l'objet de modèle.

dev.DiskDrive

- Model
- Name
- Parent
- Révision
- SerialNumber
- Status
- Type
- Vendor

dev.FCPort

- AdminState
- Label
- Parent
- PermanentAddress
- PortNumber
- PortType
- Speed
- Status

dev.SCSIPath

- arrayVolume
- HostEndPoint
- LUN
- Parent

net.IpAddress

- DotNotation
- StringNotation

net.IpInterface

- IpAddress
- Parent

physpkg.PhysicalPackage

- FWRevision
- Manufacturer
- Model

- Name
- Parent
- PartNumber
- RelativePosition
- SerialNumber

storage.StoragePool

- AdminState
- AnsiT10Id
- Capacity
- Label
- Name
- RaidLevel
- StorageSubSystem
- TotalAvailableSpace

storage.StorageSubSystem

- AnsiT10Id
- AvailabilityState
- FCPorts
- Fqdn
- Manufacturer
- Members
- Model
- SerialNumber
- StoragePools
- SystemId
- Type

storage.StorageVolume

- BlockSize
- Capacity
- ManagedSystemName
- Name
- Parent
- Paths
- RedundancyMethod
- Type
- Virtuel

Identification et résolution des problèmes liés au détecteur

Fix Pack 1

Cette rubrique décrit des problèmes classiques susceptibles de survenir avec le détecteur de stockage XIV et propose des solutions à ces problèmes.

Temps d'exécution des commandes XCLI prolongé

Problème

Remarque : Le problème suivant ne s'applique pas à XIV Storage System version 4.5 et ultérieure.
Le protocole XCLI est requis pour que XIVStorageSensor puisse reconnaître XIV avec succès. Si le serveur TADDM et le protocole XCLI sont tous deux installés sur le système d'exploitation Windows, l'exécution de chaque commande XCLI peut prendre plus de 2 minutes.

Solution

Pour résoudre le problème, accédez au répertoire `XIVGUI\properties`, ouvrez le fichier `xiv-constants.properties` et modifiez la valeur par défaut de la propriété suivante sur `0` :

```
xcliServerTimeout
```

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus d'informations sur les produits et services actuellement disponibles dans votre pays, consultez votre représentant IBM local. Toute référence à un produit, logiciel ou service IBM n'établit ou n'implique que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout produit, logiciel ou service fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est toutefois de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, programmes ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet en attente 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 souhaitez 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.

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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Certaines juridictions n'autorisent pas l'exclusion des garanties explicites ou implicites dans certaines transactions, 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, améliorer et/ou modifier le(s) produit(s) et/ou logiciel(s) 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 quelque 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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Ces informations peuvent être disponibles et 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 du Livret Contractuel IBM, des Conditions Internationales d'Utilisation de Logiciels IBM ou de tout autre contrat 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. Les questions relatives aux performances de produits non IBM doivent être adressées aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document contient des exemples de données et de rapports utilisés dans les opérations quotidiennes d'une entreprise. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs et toute ressemblance avec des noms et des adresses utilisés par une véritable entreprise serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur ne s'affichent pas.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web «Copyright and trademark information» à l'adresse http://www.ibm.com/legal/copytrade.shtml.

Itanium est une marque d'Intel Corporation ou de ses filiales, aux Etats-Unis et dans d'autres pays.

Java et toutes les marques et logos incluant Java sont des marques d'Oracle et/ou de ses filiales.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits et de services peuvent être des marques ou des marques de service appartenant à des tiers.

Imprimé en France