Guide de l'Assistant de la configuration de TSA (IBM® Technical Support Appliance)

Août 2020

Table des matières

Introduction 3

Problématiques de pré-reconnaissance du réseau 3
Documentation utile 3

Présentation 5

Définir des ensembles de périmètres 5
Facteurs à prendre en compte lors de la création de périmètres 6
Données d'identification de la reconnaissance 8
Facteurs à prendre en compte pour la configuration des données d'identification de la reconnaissance 8

Mise en route 10

Installation initiale et configuration de TSA 10
Préparer les reconnaissances 10
Etapes de la reconnaissance 10

Configuration de la reconnaissance des équipements 12

Operating Systems and Hosts 12
IBM Power Systems 13
Hardware Management Console (HMC) 13
Integrated Virtualization Manager (IVM) 15
Virtual I/O Server (VIOS) Partitions 15
AIX 15
Linux on Power 17
IBM i 19
UNIX Systems 20
Solaris 20
Solaris via Oracle iLOM 21
Linux 21
HP-UX 22
VMware vCenter Server et VMware ESXi 22
Windows 24
Windows via WINRM 25
Windows via SMB1 26
Equipements ATM 29
Module de gestion 29
Equipements du Flex System Manager (FSM) 29
Equipements du module de gestion des châssis (CMM) 30
Equipements du module de gestion avancée (AMM) 30
Serveur lame HP Proliant via HP OnBoard Administrator 30
Equipements des modules de gestion intégrés (IMM et IMM2) 30

Serveurs HP Integrity et HP9000 via iLO 31
Equipements réseau 31
Commutateurs BNT 31
Brocade 32
Check Point 32
Cisco 32
F5 Big-IP (TMOS) 33
Fortinet (FortiOS) 33
Commutateurs IBM SAN de type b 33
Juniper 33
Palo Alto Networks (PAN-OS) 34
Commutateurs QLogic 34
Equipements de stockage 34
Stockage EMC Corporation 35
HP StorageWorks P2000 Modular Smart Array 36
Stockage IBM DS3xxx, DS4xxx ou DS5xxx 36
Stockage IBM DS6xxx / DS8xxx 36
IBM FlashSystem, v9000 37
IBM ProtecTIER 37
Stockage IBM SVC, V7000/V3700 37
Bandothèque IBM TS3100 38
Bandothèque IBM TS3200 38
Bandothèque IBM TS3310 38
Bandothèques IBM TS3494, TS3953 38
Bandothèques IBM TS3500, TS3584 38
Bandothèque IBM TS4500 39
Bandothèque IBM TS7700 39
Stockage IBM V7000 Unified 40
Stockage IBM XIV 40
Stockage nSeries ou NetApp 40
Problématiques des pare-feux 41
Problèmes de reconnaissance 44
Problématiques courantes 45
Identification et résolution des problèmes 46
Session active pour la reconnaissance AMM 46
Annexe A : Termes et définitions 47
Annexe B : Eléments divers 48
Fonctions de téléchargement de l'interface utilisateur 48
Annexe C : Fournisseur CIM pour VMware ESXi 49

Annexe D : Windows avec WINRM 53

Introduction

IBM Technical Support Appliance (TSA) est un outil simple d'emploi qui vous permet de tirer le meilleur parti de vos contrats de support IBM. TSA reconnaît les éléments informatiques clés et leurs relations au sein de votre infrastructure informatique, puis transmet les données de façon sécurisée au support IBM à des fins d'analyse. Ces données permettent au support IBM de bien comprendre les relations complexes qui existent entre les serveurs et les composants réseau dans votre data center.

L'objectif de ce document est de fournir des informations et des conseils sur l'installation, la planification et la configuration de TSA.

Problématiques de pré-reconnaissance du réseau

Avant de configurer TSA pour la reconnaissance initiale et la transmission, assurez-vous que les points suivants ont bien été traités. On suppose que TSA a déjà été installé, que l'interface Web est accessible et que TSA a été mis à jour avec la dernière version disponible. Sinon, consultez le Guide de l'installation de TSA (dénommé "guide d'installation" dans la suite de ce document).

Problématiques de pré-reconnaissance du réseau TSA	
Mise en réseau	
	Ouvrez l'accès au pare-feu de TSA à IBM. Voir la section **Configuration requise pour les connexions au support IBM** dans le guide d'installation.
	Si un proxy If est utilisé pour se reconnecter à IBM, assurez-vous qu'il est configuré dans TSA. Voir la section **Configuration de la connectivité IBM** dans le guide d'installation. - L'inspection SSL n'est pas prise en charge. Si vous utilisez l'inspection SSL sur le proxy, désactivez-la pour ces flux.
	S'il existe des pare-feux entre TSA et les équipements cibles, assurez-vous que les ports requis soient ouverts. Pour plus d'informations, consultez la section "Problématiques des pare-feux", à la page 41.

Documentation utile

Le lien ci-dessous mène directement au site web d'information dédié à Technical Support Appliance. Vous y trouverez tout ce dont vous avez besoin pour commencer à utiliser IBM Technical Support Appliance. Vous pourrez consulter les guides de configuration et la documentation relative à la sécurité, étudier des exemples de rapports et télécharger le code d'installation de TSA à partir d'ibm.com.

Pour savoir plus sur Technical Support Appliance : https://ibm.biz/TSAdemo

Présentation

TSA peut obtenir des informations sur votre infrastructure informatique, qui comprend les composants de système d'exploitation déployés, les composants firmware, les serveurs physiques, les équipements du réseau, les réseaux locaux virtuels, etc. Afin d'optimiser l'étendue et la précision des informations collectées, des tâches de configuration sont requises dans TSA afin d'identifier les équipements de reconnaissance.

TSA tente de limiter au maximum les impacts sur l'environnement réseau du client. Ainsi, le processus de reconnaissance utilise une approche itérative et mesurée qui peut faire durer une reconnaissance complète jusqu'à 72 heures. Le statut de la tâche de reconnaissance peut être suivi dans la section **Récapitulatif de la tâche** de la page **Récapitulatif**.

Dans le cadre du processus de reconnaissance, TSA tente avant tout de détecter les équipements dans le périmètre défini sans utiliser de données d'identification. Cela implique d'utiliser Nmap pour reconnaître et classifier les équipements via des techniques de balayage, de prise d'empreinte et de mappage de port IP peu intrusives. En général, cette activité n'est pas suffisamment significative pour déclencher un système de détection d'intrusion (IDS) mais cela peut arriver s'il y a des paramètres locaux contraignants.

Pour permettre à TSA de collecter des informations sur votre infrastructure informatique, vous devez lui fournir les éléments suivants :

- Périmètres
- Données d'identification d'accès

Définir des ensembles de périmètres

Un ensemble de périmètres est un groupement logique de périmètres individuels. Les périmètres utilisent les adresses IP pour dire à TSA où commencer la reconnaissance de l'environnement. Un ensemble de périmètres est composé d'un ou plusieurs périmètres. Il existe trois types d'entrées de périmètre :

- Sous-réseau - Défini par une adresse IP et un masque de sous-réseau. Les sous-réseaux sont limités aux sous-réseaux de classe C.
- Plage d'adresses IP - Comprend toutes les adresses IP du début à la fin.
- Adresse IP / Hôte - Adresse IP ou nom d'hôte individuel(le).

> Le nom d'hôte est résolu au moment de l'entrée, pas au moment de la reconnaissance. Pour plus de détails, consultez la section "Facteurs à prendre en compte lors de la création de périmètres," à la page 6.

Si vous le souhaitez, des exclusions de périmètre peuvent être définies pour un périmètre en indiquant un hôte, une plage ou une définition de sous-réseau. Les adresses IP ainsi obtenues ne seront pas considérées comme faisant partie du périmètre et ne seront pas analysées.

TSA accepte trois types d'ensembles de périmètres :

1. **Ensembles de périmètres généraux** : vous permettent de découvrir les éléments individuels d'un réseau informatique. Chaque ensemble contient un ou plusieurs périmètres qui identifient l'emplacement de ces éléments de réseau en utilisant une adresse IP, une plage d'adresses IP ou un réseau ou sous-réseau.
2. **Ensembles de périmètres dynamiques HMC** : vous permettent de spécifier l'adresse IP d'une ou de plusieurs HMC IBM POWER Systems ainsi que les données d'identification associées. Les informations concernant toutes les LPAR gérées par les HMC peuvent aussi être recueillies sans qu'il soit nécessaire d'identifier leur adresse IP. Pour accéder à ces LPAR, l'ensemble de périmètres dynamiques utilise les données d'identification que vous fournissez.
3. **Ensembles de périmètres dynamiques VMware** : vous permettent de spécifier l'adresse IP d'une ou de plusieurs instances VMware vCenter Server ou ESXi ainsi que les données d'identification associées. Les informations concernant toutes les machines virtuelles gérées par les instances VMware peuvent aussi être obtenues sans qu'il soit nécessaire d'identifier leur adresse IP. Pour accéder à ces machines virtuelles, l'ensemble de périmètres dynamiques utilise les données d'identification que vous fournissez.

Pour les HMC et les instances VMware vCenter Server / ESXi, l'utilisation d'ensembles de périmètres dynamiques est recommandée. En effet, les périmètres dynamiques requièrent beaucoup moins d'effort de configuration dans TSA par rapport au travail que représentent la création et la gestion des périmètres de découverte pour les LPAR/machines virtuelles individuelles. De même, dans le cas d'environnements où les LPAR ou les machines virtuelles sont ajoutées et supprimées au fil du temps, les ensembles de périmètres dynamiques peuvent faire face sans qu'il soit nécessaire de modifier des ensembles de périmètres.

Pour des instructions détaillées sur la façon de définir des périmètres de reconnaissance sur TSA, consultez la section **Configurer des périmètres de reconnaissance** du guide d'installation.

Facteurs à prendre en compte lors de la création de périmètres

Même s'il n'y a pas de standards définis pour la configuration des périmètres, certaines considérations pratiques peuvent faire gagner du temps et des efforts :

- Lorsque cela est possible, utilisez des ensembles de périmètres dynamiques pour définir la reconnaissance des HMC et de leurs LPAR gérées, ou des instances VMware vCenter Server / ESXi et de leurs machines virtuelles gérées. Dès lors que

des ensembles de périmètres dynamiques sont utilisés, il n'y a plus lieu de définir des périmètres spécifiques pour les LPAR ou les machines virtuelles.

- Utilisez les périmètres Plages d'adresses IP ou Sous-réseau pour reconnaître plusieurs équipements au lieu d'adresses IP ou de noms d'hôte individuels. Cela limitera le nombre de définitions de périmètres et simplifiera l'administration.
- Si vous utilisez des définitions de périmètre de sous-réseau, incluez-en une seule par ensemble de périmètres. Assurez-vous que la définition du périmètre de sous-réseau fait référence à un réseau de classe C (256 adresses IP) ou moins.
- Utilisez la fonction **Importer un ensemble de périmètres généraux** pour créer un nouvel ensemble de périmètres d'après le nom indiqué et la liste d'adresses IP issues d'un fichier texte d'entrée. Pour plus d'informations, consultez la section **Périmètres de reconnaissance → Importer un ensemble de périmètres généraux** dans le guide d'installation.
- A l'heure actuelle, stocke uniquement des adresses IP, ce qui veut dire que les noms d'hôte sont résolus au moment de l'entrée et non au moment de la reconnaissance. Les meilleures pratiques suggèrent d'utiliser soit l'Adresse IP, soit la Plage d'adresses IP pour la définition du périmètre, mais pas le nom d'hôte.
- Plus il y aura d'adresses IP dans l'ensemble de périmètres, plus la reconnaissance sera longue. Pour réduire la durée d'une reconnaissance, configurez les périmètres de sorte qu'ils ciblent uniquement les éléments que vous voulez reconnaître.

Lorsque vous utilisez des ensembles de périmètres généraux, limitez le nombre total d'adresses IP auxquelles un périmètre de reconnaissance fait référence (après avoir étendu les définitions de périmètre plage d'adresse IP ou sous-réseau disponibles) à 400 ou moins. Des problèmes de performance, de serveur ou de réseau peuvent survenir lors du processus de reconnaissance si plus de 400 adresses IP sont analysées pour un seul ensemble de périmètres.

- TSA n'empêche pas les adresses IP d'être définies dans plusieurs ensembles de périmètres. En général, cette pratique est à éviter car elle augmente la durée de la reconnaissance sans toutefois collecter davantage d'informations.
- Regroupez les périmètres dans des ensembles de périmètres qui constituent un groupement logique d'équipements :

- Regroupez le même type d'équipement dans un ensemble de périmètres. Par exemple, créez un ensemble de périmètres pour les sous-systèmes de stockage IBM FlashSystem.
- Regroupez les équipements qui se trouvent dans le même lieu géographique.
- Regroupez les équipements en fonction des applications métier ou des services associés.

Données d'identification de la reconnaissance

A quelques exceptions près, les reconnaissances exigent un certain niveau d'accès pour acquérir les informations détaillées nécessaires à une parfaite compréhension de votre environnement.

Normalement les comptes de service doivent être créés sur les équipements de reconnaissance qui seront utilisés par TSA. Reportez-vous aux sections ci-dessous pour voir les droits d'accès spécifiques requis par chaque type de plateforme. Pour simplifier l'administration de ces comptes de service, utilisez le même nom d'utilisateur pour tous les équipements d'une famille de produits donnée.

La tâche de maintenance des comptes de service utilisés par TSA pour se connecter aux équipements peut être simplifiée en appliquant l'une des stratégies suivantes :

- Créer des comptes de service avec des mots de passe sans date d'expiration
- Utiliser des clés SSH pour les familles d'équipements qui acceptent leur utilisation

Pour obtenir des instructions détaillées sur la façon de définir des données d'identification d'accès sur l'appliance, voir la section **Configurer les données d'identification de la reconnaissance** du guide d'installation.

Facteurs à prendre en compte pour la configuration des données d'identification de la reconnaissance

L'appliance tente d'utiliser les données d'identification dans l'ordre où elles apparaissent dans la liste d'accès. Pour accélérer la reconnaissance, assurez-vous d'avoir les données d'identification dans l'ordre qui convient le mieux à votre environnement. Les points suivants sont à prendre en compte :

- Limiter les données d'identification à des ensembles de périmètres spécifiques si nécessaire. Cela limitera les tentatives de connexion inutiles et améliorera la performance de la reconnaissance.
- Les clés SSH peuvent être utilisées pour la reconnaissance des équipements suivants :
  - AIX

- Cisco
- Linux
- HMC
- IBM i
- IVM
- Sun SPARC (Solaris)
- SVC / V7000
- VIOS
- Fortinet
- HP-UX
- IBM FlashSystem
- F5 Big IP
- Check Point

Une seule donnée d'identification de clé SSH peut être associée à un ensemble de périmètres.

- Une bonne pratique consiste à créer des comptes de service séparés qui sont utilisés exclusivement par TSA avec les droits d'accès les plus limités possibles.

Mise en route

Cette section couvre certaines bonnes pratiques et recommandations sur la configuration de TSA.

Installation initiale et configuration de TSA

Parcourez les instructions fournies dans les sections suivantes du guide d'installation :

- Installer IBM Technical Support Appliance (TSA)
- Se connecter à Technical Support Appliance
- Accepter le contrat de licence
- Configurer Technical Support Appliance avec l'assistant d'installation

Préparer les reconnaissances

Un processus itératif est recommandé selon lequel une petite partie du réseau est d'abord configurée pour la reconnaissance, puis d'autres parties du réseau sont ajoutées à chaque itération jusqu'à obtenir la couverture du réseau souhaitée.

> Une bonne pratique consiste à faire une sauvegarde de votre configuration de TSA après avoir effectué un nombre important d'ajouts et de modifications des périmètres et/ou des données d'identification. Pour plus d'informations, consultez la section “Sauvegarde et restauration” dans le Guide de l'installation d'IBM Technical Support Appliance.

Etapes de la reconnaissance

Pour chaque itération de reconnaissance, procédez comme suit :

1. Préparez les équipements pour la reconnaissance. Pour en savoir plus sur la configuration requise pour les entités et les données d'identification nécessaires, consultez la section "Configuration de la reconnaissance des équipements", à la page 12.
2. Pour les ensembles de périmètres dynamiques HMC, effectuez les étapes suivantes :
   a. Ajoutez les adresses IP des HMC dans la page **Ensemble de périmètres dynamiques HMC**.
   b. Ajoutez les données d'identification des HMC dans la page **Ensemble de périmètres dynamiques HMC**.
   c. Sélectionnez les types de LPAR que vous voulez reconnaître. Fournissez les données d'identification pour chaque type.

   > Vous pouvez sélectionner les types de LPAR à découvrir soit au moment où vous créez l'ensemble de périmètres dynamiques, soit plus tard, en éditant l'ensemble de périmètres dynamiques.

d. (Optionnel) Utilisez la fonction Test sur la page **Ensemble de périmètres dynamiques HMC** pour vérifier que les données d'identification sont correctement définies et peuvent être utilisées pour établir une connexion aux HMC ou aux LPAR qu'elles gèrent.

3. Pour les ensembles de périmètres dynamiques VMware, effectuez les étapes suivantes :
   a. Ajoutez les adresses IP des instances VMware vCenter Server.
   b. Ajoutez les adresses IP des éventuels hôtes VMware ESXi qui ne sont pas gérés par une instance VMware vCenter Server.
   c. Ajoutez les données d'identification des instances VMware vCenter Server et ESXi dans la page **Ensemble de périmètres dynamiques VMware**.
   d. Sélectionnez les types de machines virtuelles que vous voulez reconnaître. Fournissez les données d'identification pour chaque type.

      Vous pouvez sélectionner les types de machines virtuelles à découvrir soit au moment où vous créez l'ensemble de périmètres dynamiques, soit plus tard, en éditant l'ensemble de périmètres dynamiques.

   e. (Optionnel) Utilisez la fonction Test sur la page **Ensemble de périmètres dynamiques VMware** pour vérifier que les données d'identification sont correctement définies et peuvent être utilisées pour établir une connexion aux instances VMware vCenter Server et ESXi ainsi qu'aux machines virtuelles qu'elles gèrent.

4. Pour les périmètres de reconnaissance généraux, effectuez les étapes suivantes :
   a. Ajoutez les adresses IP souhaitées dans les ensembles de périmètres / périmètres appropriés. Si des pare-feux sont installés entre l'instance TSA et les équipements concernés par la reconnaissance, assurez-vous que les ports adéquats sont ouverts dans le pare-feu afin de permettre le bon déroulement de la reconnaissance. Pour savoir quels ports doivent être accessibles pour chaque type de plateforme, consultez la section "Problématiques des pare-feux", à la page 41.
   b. Créez les données d'identification nécessaires. Utilisez la fonction Test sur le panneau **Nouveau Reconnaissance Données d'identification** pour vérifier que les données d'identification sont correctement définies et peuvent être utilisées pour établir une connexion avec un équipement cible.

5. Exécutez une reconnaissance complète pour analyser les adresses IP ajoutées pour cette itération.

6. Exécutez une transmission pour télécharger les données vers IBM.

Configuration de la reconnaissance des équipements

En plus de fournir des données d'identification, il peut y avoir d'autres prérequis spécifiques pour la configuration de la reconnaissance des équipements afin de permettre à TSA de reconnaître et de collecter des informations utiles sur les composants de manière efficace. Cette section va vous permettre d'identifier les équipements de reconnaissance de votre environnement qui vont nécessiter des configurations spécifiques. Il est recommandé de créer des comptes de service avec le minimum de droits requis. Voir aussi la section "Problématiques des pare-feux" pour en savoir plus sur les ports et les protocoles concernés.

- Pour les équipements dont les ports SSH et Telnet sont ouverts, TSA va d'abord tenter d'établir une connexion via SSH (pour des raisons de sécurité). Si cette connexion SSH échoue, TSA tentera alors la connexion en utilisant Telnet.

Systèmes d'exploitation et hôtes

Plateforme
IBM Power Systems • Hardware Management Console (HMC) • Integrated Virtualization Manager (IVM) • Virtual I/O Server (VIOS) Partitions • AIX • Linux on Power
IBM i
UNIX Systems • Solaris • Solaris via iLOM • Linux • HP-UX
VMware vCenter Server et VMware ESXi
Windows
Equipements ATM

Module de gestion
• Flex System Manager (FSM) • Chassis Management Module (CMM) • Advanced Management Module (AMM) • Serveur lame HP ProLiant via HP OnBoard Administrator • Integrated Management Module (IMM & IMM2) • Serveurs HP Integrity et HP9000 via iLO
Cliquez sur les liens ci-dessus pour plus d'informations.

IBM Power Systems

Pour IBM Power Systems, où la configuration des LPAR est gérée par une HMC ou IVM, utilisez des ensembles de périmètres dynamiques HMC. Avec ces ensembles de périmètres dynamiques HMC, vous pouvez créer une définition de périmètre pour les HMC et fournir les données d'identification HMC et LPAR associées, sans avoir à créer de périmètres pour chaque LPAR gérée. Lorsqu'une HMC est découverte, TSA détermine quelles LPAR existent à cet instant et analyse automatiquement chacune d'elles.

Pour IBM Power Systems, où la configuration des LPAR est généralement statique, une méthode alternative à l'emploi d'ensembles de périmètres dynamiques HMC est d'itérer en ajoutant des périmètres et des données d'identification pour les entités dans l'ordre suivant :

1. **Instances HMC ou IVM** : la console HMC renvoie des informations détaillées sur toutes les entités Power Systems qu'elle gère et sur les partitions logiques qu'elle contient. L'IVM renvoie quant à lui des informations similaires pour l'unique système qu'il gère.
2. **Partitions VIOS** : elles renvoient des informations sur les adaptateurs physiques et les ressources qu'elles gèrent.
3. **Partitions individuelles** : dans certains cas, une partition non-VIOS possède des adaptateurs physiques.

Hardware Management Console (HMC)

Pour découvrir des instances HMC, effectuez les étapes suivantes :

Préparer l'environnement :

- Pour permettre à TSA de recueillir des informations sur la gestion des LPAR via la console HMC, celle-ci doit être capable de communiquer avec les LPAR à l'aide

d'outils RMC. Assurez-vous que la console HMC et les LPAR sont configurés de façon à autoriser cette communication. Pour plus d'informations sur les outils RMC pour Linux, rendez-vous sur https://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/yum.html

- Pour une collecte de données sécurisée, l'exécution des commandes à distance doit être activée sur la console HMC. Pour plus d'informations, voir la section "Activation et désactivation de l'exécution des commandes à distance de la console HMC" à l'adresse suivante : https://www.ibm.com/support/knowledgecenter/fr/POWER7/p7ha1/enablinganddisablinghmcremotecommands.htm

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques HMC - Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service HMC.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service HMC.
- L'utilisateur HMC doit avoir les rôles suivants :
  - Rôle de ressource : AllSystemResources
  - Rôle de tâche (basée sur **hmcoperator** avec des tâches de ligne de commande) :
    - Système managé (lshwres, lssyscfg)
    - Partition logique (lshwres, lssyscfg, viosvrcmd)
    - Configuration HMC (lshmc)
- Un utilisateur (compte de service) disposant des droits **hmcviewer** peut être utilisé si nécessaire ; en revanche, la collecte des données ne sera que partielle.

> Lors d'une exécution avec les droits **hmcviewer**, il n'est pas possible d'obtenir des informations sur les adaptateurs détenus par les partitions VIOS. Pour les obtenir, assurez-vous que le compte de service dispose au moins des droits **hmcoperator**. Si ce n'est pas possible, ajoutez des périmètres et des données d'identification pour reconnaître les partitions VIOS directement en plus de la console HMC.

Integrated Virtualization Manager (IVM)

Pour découvrir des instances IVM, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service IVM.
- Le compte de service doit avoir des droits de consultation uniquement.

Virtual I/O Server (VIOS) Partitions

Pour découvrir des instances VIOS, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques HMC - Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service de partition VIOS.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service de partition VIOS.
- Le compte de service doit être un compte administrateur (ex. : **padmin**).
- Le compte de service doit avoir l'attribut utilisateur **rlogin=true**. Vous pouvez fixer cet attribut à l'aide de SMIT ou en éditant le fichier **/etc/security/user**.
- Le paramètre **PermitUserEnvironment** dans le fichier **/etc/ssh/sshd_config** doit être mis à **yes**.

AIX

Pour découvrir des instances AIX, effectuez les étapes suivantes :

Préparer l'environnement :

- Assurez-vous que les packages bos.perf.tools et openSSH/openSSL sont installés.
- Désactivez le blocage des tentatives de connexion invalides pour le compte de service.

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques HMC - Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service de partition AIX.

- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service AIX.
- Le compte de service peut être root ou un compte avec des droits sudo.
- Le compte de service doit avoir l'attribut utilisateur **rlogin=true**. Vous pouvez fixer cet attribut à l'aide de SMIT ou en éditant le fichier **/etc/security/user**.
- Pour activer un compte de service non-root avec les droits sudo pour AIX :
  - Installez la ressource RPM sudo (sudo-1.6.9p15-2noldap) et les ensembles de fichiers ssh (openssh.base.server, openssh.base.client sur l'instance AIX).
  - Créez un ID utilisateur non-root sur l'instance AIX cible qui peut être utilisée par TSA pour accéder au système.
  - Modifiez **/etc/sudoers** sur chaque instance AIX pour permettre à TSA d'exécuter les commandes indiquées à l'aide des droits sudo.

    # Spécification d'alias de commande Cmnd alias

    ```
    Cmnd_Alias TSA_CMDS = /usr/bin/lparstat, /usr/sbin/no,
    /usr/sbin/nfso, /usr/bin/lslicense, /usr/sbin/vmo,
    /usr/sbin/ioo, /usr/sbin/lvmo, /usr/sbin/schedo,
    /usr/bin/sysdumpdev, /usr/sbin/smtctl, /usr/sbin/emgr,
    /usr/bin/sissasraidmgr, /usr/sbin/lswpar,
    /usr/sbin/cpuextintr_ctl, /usr/sbin/lsnim, /usr/sbin/raso,
    /usr/sbin/bosdebug, /usr/sbin/chedition,
    /usr/esa/bin/esacli, /usr/sbin/bootinfo,
    /usr/bin/mpio_get_config, /usr/bin/cat /etc/objrepos/CuData,
    /usr/bin/cat /etc/objrepos/CuData.vc, /usr/bin/cat
    /var/adm/ras/bootlog, /usr/bin/cat
    /etc/lpp/diagnostics/data/diagrpt*.dat, /usr/bin/tapeutil,
    /usr/lpp/OV/bin/opcagt, /usr/DynamicLinkManager/bin/dlnkmgr
    view, /usr/sbin/powermt version, /usr/sbin/powermt display,
    /usr/bin/pcmpath query, /usr/sbin/datapath query
    ```

    # Spécification de droits utilisateur

    ```
    <Nom utilisateur> ALL = NOPASSWD: TSA_CMDS
    ```

    <Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur AIX. Cette variable <Nom utilisateur> est un utilisateur sur chaque instance AIX. Le fichier **/etc/sudoers** sur chaque instance AIX doit être mis à jour avec la spécification ci-dessus.

    Ou

    Comme alternative aux modifications de **/etc/sudoers** ci-dessus, vous pouvez utiliser la spécification de droits utilisateur suivante :

    ```
    <Nom utilisateur> ALL = NOPASSWD: ALL
    ```

- <Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur AIX. Cette spécification utilisateur permet au compte de service d'utiliser les droits sudo sur n'importe quelle commande AIX.

Linux on Power

Pour découvrir des instances Linux on Power, effectuez les étapes suivantes :

Préparer l'environnement :

- Désactivez le blocage des tentatives de connexion invalides pour le compte de service.

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques HMC - Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service de partition Linux.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service Linux.
- Pour activer un compte de service non-root avec les droits sudo pour Linux :
  - Créez un ID utilisateur non-root sur l'instance Linux cible qui peut être utilisée par TSA pour accéder au système.
  - Modifiez **/etc/sudoers** sur chaque instance Linux pour permettre à TSA d'exécuter les commandes indiquées à l'aide des droits sudo.

    # Spécification d'alias de commande Cmnd alias

    ```
    Cmnd_Alias TSA_CMDS = /usr/sbin/lsvpd, /sbin/lsvpd,
    /usr/sbin/lscfg, /sbin/lscfg, /usr/sbin/lsmcode,
    /sbin/lsmcode, /usr/sbin/lvmdiskscan, /sbin/lvmdiskscan,
    /usr/sbin/dmidecode, /usr/bin/mtlib, /usr/bin/tapeutil,
    /usr/bin/crontab, /sbin/fdisk, /bin/ls -alR /boot/*,
    /bin/cat /proc/irq/*, /bin/cat /proc/net/vlan/config,
    /bin/cat /proc/ppc64/rtas/*, /bin/cat /proc/sys/kernel/cap-
    bound, /bin/cat /proc/sys/kernel/random/entropy_avail
    ```

    # Spécification de droits utilisateur

    ```
    <Nom utilisateur> ALL = NOPASSWD: TSA_CMDS
    ```

- <Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur Linux. Cette variable <Nom utilisateur> est un utilisateur sur chaque instance Linux. Le fichier

/etc/sudoers sur chaque instance Linux doit être mis à jour avec la spécification ci-dessus.

Ou

Comme alternative aux modifications de **/etc/sudoers** ci-dessus, vous pouvez utiliser la spécification de droits utilisateur suivante :

```
<Nom utilisateur> ALL = NOPASSWD: ALL
```

<Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur Linux. Cette spécification utilisateur permet au compte de service d'utiliser les droits sudo sur n'importe quelle commande Linux.

- Si vous utilisez le portail IBM Proweb pour AIX dans le cadre de l'offre de support dont vous bénéficiez avec IBM, vous devriez de préférence configurer TSA en utilisant des ensembles de périmètres dynamiques HMC. Comme alternative, vous pouvez configurer TSA pour la reconnaissance des HMC et des partitions logiques (dont VIOS) sur les équipements Power Systems.
- Lorsque des ensembles de périmètres dynamiques HMC sont utilisés pour les analyses, les informations de configuration du système d'exploitation obtenues pour chaque LPAR sont souvent plus détaillées qu'avec ProWeb.

Pour des informations sur l'ajout de périmètres et de données d'identification pour les environnements HMC, consultez la section **Périmètres dynamiques HMC** dans le Guide de l'installation d'IBM Technical Support Appliance.

- Niveau de données collectées pour le rapport en analysant diverses entités Power Systems :
  - En analysant uniquement les consoles HMC, vous obtiendrez toutes les informations essentielles sur les onglets Identified, HMC Topology, Power Systems Firmware, IBM i Recommendations, Linux Recommendations, HMC/VIOS/AIX et Contract, ainsi que certaines informations sur les adaptateurs.
  - En analysant les partitions VIOS directement, vous obtiendrez des informations supplémentaires sur le firmware des adaptateurs et les dispositifs de stockage connectés.

- En analysant les LPAR directement, vous obtiendrez de plus amples informations sur celles-ci, notamment les détails du système d'exploitation et les instances de logiciels spécifiques tels que PowerHA, GPFS et PowerSC.

IBM i

Les instances IBM i sont reconnues à l'aide d'une connexion SSH. Si SSH n'est pas installé ni configuré dans l'instance IBM i, effectuez les étapes suivantes :

Préparer l'environnement :

Assurez-vous que les produits/options suivants sont installés et configurés pour IBM i 7.2 :

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, option 30
- Portable Application Solutions Environment, 5770-SS1, option 33
- IBM Developer Kit for Java, 5770-JV1

Assurez-vous que les produits/options suivants sont installés et configurés pour IBM i 7.3 :

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, option 30
- Portable Application Solutions Environment, 5770-SS1, option 33
- IBM Developer Kit for Java, 5770-JV1, option 16
- Java SE 8 32 bits

Assurez-vous que les produits/options suivants sont installés et configurés pour IBM i 7.4 :

- IBM Portable Utilities for i, 5733-SC1
- Qshell, 5770-SS1, option 30
- Portable Application Solutions Environment, 5770-SS1, option 33
- IBM Developer Kit for Java, 5770-JV1, option 16
- Java SE 8 32 bits

Pour démarrer le démon SSH, exécutez la commande suivante :

```
SBMJOB CMD (CALL PGM (QP2SHELL) PARM('/QOpenSys/usr/sbin/sshd'))
```

Pour démarrer le service SSHD sur IBM i, exécutez la commande suivante :

```
STRTCPSVR SERVER(*SSHD)
```

Pour plus d'informations sur la façon de configurer SSH sur IBM i, consultez les chapitres 21 à 23 du Redbook suivant : http://www.redbooks.ibm.com/redpapers/pdfs/redp4163.pdf

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut utiliser n'importe quelle classe d'utilisateur, y compris***USER**, bien que des droits sur les objets supplémentaires soient requis pour collecter les informations PTF (ce qui se fait via la commande **DSPPTF**).
- **DSPPTF** est livré avec les limitations de droits sur les objets suivantes :
  - La commande est livrée avec les droits publics ***EXCLUDE**
  - **Les profils d'utilisateur QPGMR**, **QSYSOPR**, **QSRV** et **QSRVBAS** sont livrés avec des droits privés pour utiliser cette commande
  - Comme toujours, le profil d'utilisateur **QSECOFR** ou tout profil d'utilisateur associé à la classe d'utilisateur ***SECOFR** peut exécuter cette commande
- L'objet **QSYS/DSPPTF** du type d'objet ***CMD** peut voir ses droits modifiés pour permettre à un autre utilisateur d'exécuter cette commande.
- Si un nouveau compte de service est créé pour TSA, les recommandations suivantes s'appliquent :
  - Créez le profil d'utilisateur avec la classe d'utilisateur ***USER**
  - Utilisez la commande **GRTOBJAUT** pour autoriser ce profil d'utilisateur à exécuter la commande **DSPPTF** ; l'objet est **QSYS/DSPPTF**, du type d'objet ***CMD**.

Systèmes UNIX

Solaris

Pour reconnaître les équipements Solaris, procédez comme suit :

Préparer l'environnement :

- Sur les systèmes Solaris, assurez-vous que le package SUNWscpu (Source Compatibility) est installé.
- Sur certains systèmes Solaris, SNEEP doit être installé et configuré pour obtenir les numéros de série.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Le compte de service peut avoir des droits non-root.

Solaris via Oracle iLOM

Pour reconnaître les équipements Solaris via Oracle iLOM, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut avoir soit les privilèges **Opérateur**, soit les privilèges **Administrateur**.

Linux

Si l'instance Linux fonctionne sur un IBM Power System, reportez-vous à la section Linux on Power, page 17, sous IBM Power Systems.

Pour découvrir des instances Linux on x86, effectuez les étapes suivantes :

Préparer l'environnement :

- Assurez-vous que le package pciutils est installé. La commande `lspci` qu'il contient sert à collecter des informations sur les adaptateurs et les connexions avec des équipements de stockage externes.

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques VMware - Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service de machine virtuelle Linux.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service Linux.
- Désignez `/bin/sh` comme shell pour ce compte.
- Pour Linux (x86), le compte de service peut être root ou un compte avec des droits `sudo`.
- Pour effectuer la reconnaissance à l'aide d'un compte de service non-root, ajoutez les éléments suivants au fichier **/etc/sudoers** sur le système Linux.

  # Spécification d'alias de commande Cmnd alias

  ```
  Cmnd_Alias TSA_CMDS = /usr/sbin/dmidecode
  ```

  # Spécification de droits utilisateur

  ```
  <Nom utilisateur> ALL = NOPASSWD: TSA_CMDS
  ```

  <Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur Linux. Cette variable <Nom utilisateur> est

un utilisateur sur chaque instance Linux. Le fichier **/etc/sudoers** sur chaque instance Linux doit être mis à jour avec la spécification ci-dessus.

Ou

Comme alternative aux modifications de **/etc/sudoers** ci-dessus, vous pouvez utiliser la spécification de droits utilisateur suivante :

```
<Nom utilisateur> ALL = NOPASSWD: ALL
```

<Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur Linux. Cette spécification utilisateur permet au compte de service d'utiliser les droits sudo sur n'importe quelle commande Linux.

HP-UX

Pour reconnaître les équipements HP-UX, procédez comme suit :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Pour activer un compte de service non-root avec les droits sudo pour HP-UX :
  - Modifiez **/usr/local/etc/sudoers** sur chaque instance HP-UX pour permettre à TSA d'exécuter les commandes indiquées à l'aide des droits sudo.

```
# Spécification d'alias de commande Cmnd alias
Cmnd_Alias TSA_CMDS
=/usr/sbin/diskinfo,/opt/hpvm/bin/hpvmstatus

# Spécification de droits utilisateur
<Nom utilisateur> ALL=(ALL) NOPASSWD:TSA_CMDS
```

<Nom utilisateur> est le compte de service non-root utilisé par TSA pour collecter des informations sur HP-UX.

VMware vCenter Server et VMware ESXi

Pour les environnements VMware, utilisez des ensembles de périmètres dynamiques VMware. Avec ces ensembles de périmètres dynamiques VMware, vous pouvez créer une définition de périmètre pour les instances VMware vCenter Server / ESXi et fournir les données d'identification VMware et des machines virtuelles associées, sans avoir à créer de périmètres pour chaque machine virtuelle gérée. Lorsqu'une instance VMware vCenter Server / ESXi est

découverte, TSA détermine quelles machines virtuelles existent à cet instant et analyse automatiquement chacune d'elles.

Pour les environnements VMware, où la configuration des machines virtuelles est généralement statique, une méthode alternative à l'emploi d'ensembles de périmètres dynamiques VMware est d'itérer en ajoutant des périmètres et des données d'identification pour les entités dans l'ordre suivant :

1. **Instances vCenter Server** : elles renvoient des informations détaillées sur les hôtes ESXi qu'elles gèrent et sur les invités de machine virtuelle qu'elles contiennent.
2. **Hôtes ESXi** : ajoutez les hôtes ESXi qui ne sont pas gérés par un serveur vCenter.
3. **Invités de machine virtuelle individuels** : ils permettent de collecter des informations plus détaillées sur le système d'exploitation.

Lorsque vous configurez TSA pour les environnements VMware, les actions suivantes sont recommandées :

1. Configurez TSA pour découvrir les serveurs VMware vCenter. Lorsque TSA découvre un serveur VMware vCenter, il recueille des informations sur tous les hôtes VMware ESXi que le serveur vCenter gère. Aucune information de configuration à propos des hôtes ESXi n'est nécessaire.
2. Configurez TSA pour découvrir les hôtes VMware ESXi seulement lorsque ceux-ci ne sont pas gérés par un serveur VMware vCenter.
3. Installez les outils VMware sur chaque machine virtuelle hébergée sur les hôtes ESXi. Si les outils VMware ne sont pas installés, certaines données d'inventaire telles que l'adresse IP ou le système d'exploitation installé ne seront pas accessibles.
4. Configurez chaque hôte VMware ESXi pour que son interface CIM soit active. L'interface CIM permet à TSA de recueillir des informations détaillées sur les adaptateurs équipant l'hôte ESXi. Pour plus d'informations sur le fournisseur CIM, consultez l'"Annexe C", page 44.

Pour découvrir les instances de serveur vCenter et recueillir des informations sur les serveurs ESXi qu'elles gèrent, effectuez les étapes suivantes :

Préparer l'environnement :

- Installez les outils VMware sur chaque machine virtuelle hébergée sur les hôtes ESXi.
- Configurez chaque hôte VMware ESXi pour que son interface CIM soit active.
- Pour une reconnaissance complète, le port CIM (5989) doit être joignable depuis le TSA (il ne doit pas être bloqué par un pare-feu).

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques VMware - Nom d'utilisateur / mot de passe pour le compte de service VMware vCenter Server.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe pour le compte de service VMware vCenter Server.
- Le compte de service doit avoir les droits **Administrateur** ou au moins les droits associés à un rôle en lecture seule personnalisé avec les droits complémentaires suivants :
  - Global → Licenses
  - Global → Settings
  - Host → CIM
  - Host → Configuration → Change settings
  - Host → CIM→ CIM Interaction

Pour reconnaître les équipements ESXi directement, procédez comme suit :

Préparer l'environnement :

- Installez les outils VMware sur chaque machine virtuelle hébergée sur les hôtes ESXi.
- Configurez chaque hôte VMware ESXi pour que son interface CIM soit active.

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques VMware - Nom d'utilisateur / mot de passe pour le compte de service VMware ESXi.
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique : Nom d'utilisateur / mot de passe pour le compte de service VMware ESXi.
- Le compte de service doit avoir les droits **Administrateur**.

Windows

TSA prend en charge la reconnaissance des instances Windows avec les méthodes suivantes :

- WINRM
- SMB1

Windows via WINRM est privilégié car c'est l'interface la plus sécurisée.

Windows via WINRM

Pour reconnaître les équipements Windows via WINRM, procédez comme suit :

Préparer l'environnement :

La façon la plus courante de préparer l'environnement est d'utiliser un certificat de serveur généré par une autorité de certification qui est installée sur le serveur Windows cible. Le certificat doit remplir les conditions suivantes :

- Les certificats racines et intermédiaires de l'autorité de certification se trouvent dans Certificats > Autorités de certification racines de confiance.
- Le certificat de serveur est installé dans Certificats > Personnel.
- Le certificat de serveur doit indiquer qu'il est émis pour le nom d'hôte complet du serveur.
- Le certificat de serveur doit inclure la clé privée de ce serveur.

La commande suivante configure WINRM pour les connexions HTTPS distantes :

```
winrm quickconfig -transport:https
```

Cette commande permet d'exécuter les actions suivantes :

- Active WINRM s'il n'est pas actuellement actif
- Modifie le service WINRM afin que WINRM démarre automatiquement lors des redémarrages
- Configure le programme d'écoute WINRM HTTPS
- Modifie les règles de pare-feu Windows pour autoriser les connexions HTTPS distantes

La commande produit la sortie suivante. Entrez **y** pour confirmer les modifications.

```
Le service WinRM est déjà en cours d'exécution sur cet ordinateur.
WinRM n'est pas configuré pour la gestion à distance de cet
ordinateur.
Les modifications suivantes doivent être effectuées :

Créez un écouteur WinRM sur HTTPS://* pour accepter les demandes
de la gestion des services Web sur toutes les adresses IP de cet
ordinateur.
Configurez le paramètre d'empreinte de certificat pour le service,
à utiliser pour l'authentification CredSSP.
Configurez LocalAccountTokenFilterPolicy pour attribuer des
droits d'administration à distance à des utilisateurs locaux.

Effectuer ces modifications [y/n] ? y

WinRM a été mis à jour pour la gestion à distance.
```

```
Écouteur WinRM créé sur HTTPS://* pour accepter les demandes de
la gestion des services Web sur toutes les adresses IP de cet
ordinateur.
Paramètres requis configurés pour le service.
LocalAccountTokenFilterPolicy configuré pour attribuer des droits
d'administration à distance à des utilisateurs locaux.
```

Enfin, pour permettre l'authentification par ID utilisateur / mot de passe via HTTPS, exécutez la commande suivante :

```
winrm set winrm/config/service/auth @{Basic="true"}
```

Une autre solution consiste à utiliser un certificat autosigné. Les instructions concernant cette configuration se trouvent dans l'Annexe D : Windows avec WINRM, page 53.

Données d'identification pour la liste d'accès :

- Pour les ensembles de périmètres dynamiques VMware : Nom d'utilisateur / mot de passe pour le compte de service.
- Pour les ensembles de périmètres de reconnaissance généraux : Système informatique (Windows) : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit faire partie de l'un des groupes suivants :
  - Administrateurs
  - WinRMRemoteWMIUsers__

Pour ajouter un utilisateur au groupe WinRMRemoteWMIUsers__, utilisez la commande suivante :

```
net localgroup WinRMRemoteWMIUsers__ [user_id] /add
```

Windows via SMB1

Pour reconnaître les équipements Windows, procédez comme suit :

Préparer l'environnement :

- Assurez-vous que Windows Scripting Host (WSH) ou le service Windows Management Instrumentation (WMI) et VBScript sont activés sur l'équipement cible.
- Assurez-vous que le port 445 n'est pas bloqué par un pare-feu ou par des règles de sécurité IP car TSA a besoin du protocole Server Message Block (SMBv1) sur TCP/IP.
- Pour appliquer les règles de sécurité, allez dans **Démarrer → Panneau de configuration → Outils d'administration**, puis choisissez la navigation suivante selon que vos règles sont stockées localement ou dans l'Active Directory :

- Règles stockées localement : **Outils d'administration → Stratégie de sécurité locale → Stratégies de sécurité IP** sur ordinateur local
- Règles stockées dans l'Active Directory : **Outils d'administration → Paramètres de sécurité du domaine par défaut → Stratégies de sécurité IP** sur l'Active Directory ou **Outils d'administration → Paramètres de sécurité du contrôleur de domaine par défaut → Stratégies de sécurité IP** sur l'Active Directory

- TSA a besoin d'accéder au disque d'administration distant masqué en partage pour accéder au répertoire %TEMP% et aux autres répertoires du système. L'accès au partage Interprocess Communications (IPC$) est également requis pour que TSA ait accès aux registres à distance. Assurez-vous que le service de Serveur du partage Interprocess Communication est démarré. Pour démarrer le service de Serveur, allez dans **Panneau de configuration → Outils d'administration → Services → Serveur**.
- Assurez-vous que le service Registre à distance est actif. C'est obligatoire pour que TSA puisse établir une session avec l'équipement Windows.

Données d'identification pour la liste d'accès :

Windows 2012 R2 et versions ultérieures :

- Pour les ensembles de périmètres dynamiques VMware - Compte / mot de passe d'administrateur de base. Ce compte fonctionnera quels que soient les paramètres de contrôle de compte utilisateur (UAC).
- Pour les ensembles de périmètres de reconnaissance généraux - Système informatique (Windows) : compte / mot de passe d'administrateur de base. Ce compte fonctionnera quels que soient les paramètres de contrôle de compte utilisateur (UAC).

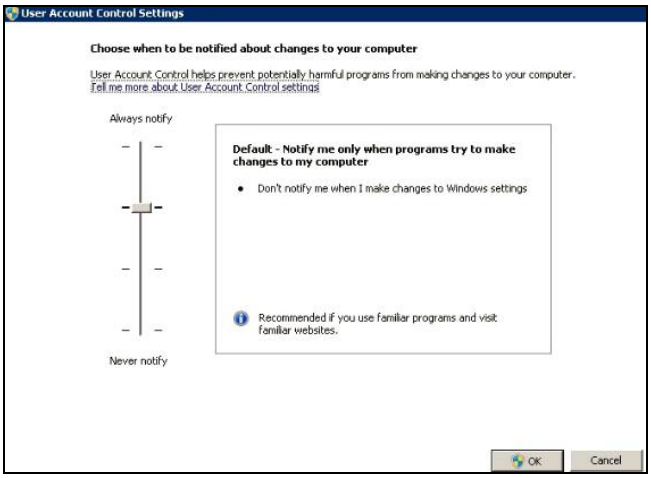
Il est possible d'utiliser un compte autre que le compte Administrateur de base si certaines conditions sont réunies. Le compte doit être un compte administrateur local ou de domaine et les paramètres UAC doivent répondre à certaines exigences. Reportez-vous au tableau ci-dessous pour connaître les combinaisons type de compte / paramètres UAC prises en

charge. Reportez-vous à la documentation Microsoft Windows pour plus d'informations sur les paramètres UAC.

	Paramètres de contrôle de compte utilisateur			
	Toujours prévenir	**Me prévenir uniquement lorsque les programmes tentent d'apporter des modifications à mon ordinateur (paramètre par défaut)**	**Me prévenir uniquement lorsque les programmes tentent d'apporter des modifications à mon ordinateur (ne pas estomper mon bureau)**	**Ne jamais prévenir**
Administrateur de base	**Oui**	**Oui**	**Oui**	**Oui**
Utilisateur dans le groupe d'administrateurs de domaine	**Non**	**Oui**	**Oui**	**Oui**
Utilisateur dans le groupe d'administrateurs locaux	**Non**	**Oui**	**Oui**	**Oui**
Compte non administrateur (domaine ou local)	**Non**	**Non**	**Non**	**Non**

- Pour accéder aux paramètres UAC, cliquez sur **Démarrer**, puis cliquez sur **Panneau de configuration**. Tapez **uac** dans la zone de recherche puis cliquez sur **Modifier les paramètres de contrôle du compte d'utilisateur**.

Le réglage par défaut est le suivant :



Equipements ATM

Certains modèles d'équipements ATM peuvent être reconnus. Pour reconnaître les équipements ATM, y compris les informations de base sur leurs composants, procédez comme suit :

Préparer l'environnement :

- Modèles Wincor Nixdorf - suivre les instructions du paragraphe Windows via SMB.

Module de gestion

Pour IBM Flex Systems, le mieux est d'itérer en ajoutant des périmètres et des données d'identification pour les entités dans l'ordre suivant :

1. **Flex System Manager (FSM) :** renvoi d'informations détaillées sur les systèmes Flex System Manager et les châssis qu'ils gèrent ainsi que sur les nœuds de traitement associés.

   Si aucun FSM n'est présent, il est recommandé d'analyser les équipements CMM et toutes les consoles HMC gérant des nœuds de traitement POWER sur des systèmes Flex.

2. **Chassis Management Module (CMM) :** pour les châssis non gérés par un FSM, pointez vers chaque CMM pour récupérer des informations détaillées sur chaque châssis et ses nœuds associés.

3. **Nœuds de traitement :** renvoie des informations détaillées sur le système d'exploitation.

Equipements du Flex System Manager (FSM)

Pour découvrir les équipements FSM, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir les droits **SMAdmin**.

Equipements du module de gestion des châssis (CMM)

Pour découvrir les équipements CMM, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit au moins avoir les droits **opérateur**.

Equipements du module de gestion avancée (AMM)

Pour découvrir les équipements AMM, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit au moins avoir les droits **opérateur**.

Serveur lame HP Proliant via HP OnBoard Administrator

Pour les serveurs Hewlett Packard (HP) ProLiant, le mieux est d'ajouter des périmètres et des données d'identification pour les entités de HP OnBoard Administrator (HP OBA). Vous obtiendrez ainsi des informations détaillées sur HP OnBoard Administrator, le boîtier qu'il gère et les nœuds de traitement contenus dans le boîtier.

Pour reconnaître un serveur lame HP Proliant via HP OnBoard Administrator (OBA), procédez comme suit :

Préparer l'environnement :

- HP OBA doit être en mode actif.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir les **droits Administrateur OA**, **Opérateur OA** ou **Utilisateur OA** sur HP Onboard Administrator. Le rôle **Droits d'utilisateur OA** est recommandé.

> TSA collecte des informations auprès d'administrateurs HP OnBoard qui sont à l'état actif seulement. Aucune information n'est collectée auprès d'administrateurs HP OnBoard à l'état de veille.

Equipements des modules de gestion intégrés (IMM et IMM2)

Pour découvrir les équipements IMM & IMM2, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.

- Le compte de service peut utiliser n'importe quels droits valides.

Serveurs HP Integrity et HP9000 via iLO

iLO est une carte processeur séparée intégrée à un serveur HP Integrity ou HP9000 et qui fournit des informations matérielles de base sur le serveur. iLO est active dès que le serveur est branché, même si celui-ci n'a pas encore été mis sous tension.

Pour reconnaître les informations d'inventaire au niveau Récapitulatif via iLO pour les serveurs HP Integrity et HP9000, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut utiliser n'importe quels droits valides. Les droits **Utilisateur** sont recommandés.

Equipements réseau

Cette section donne des informations détaillées sur les types d'équipement réseau suivants :

Plateforme
Commutateurs BNT
Commutateurs Brocade
Check Point
Commutateurs Cisco
F5 Big-IP (TMOS)
Fortinet (FortiOS)
Commutateurs IBM SAN de type b
Commutateurs Juniper
Palo Alto Networks (PAN-OS)
Commutateurs QLogic

Cliquez sur les liens ci-dessus pour plus d'informations.

Commutateurs BNT

Pour découvrir les commutateurs BNT, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.

- Le compte de service doit avoir les droits **admin**.

Brocade

Pour découvrir les équipements Brocade, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Mode Virtual Fabric désactivé : le compte de service peut utiliser n'importe quel type de droits valides. Les droits **Utilisateur** sont recommandés.
- Mode Virtual Fabric activé : le compte de service a besoin des droits **Admin** sur Fabric OS.

Check Point

Pour découvrir les systèmes Check Point, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Le compte de service doit avoir des droits administrateur (**adminRole**).
- Le compte de service doit avoir un accès SSH pour exécuter les commandes CLI.

Cisco

Pour reconnaître les équipements Cisco, vous pouvez utiliser les données d'identification de système informatique ou SNMP suivantes :

Données d'identification pour la liste d'accès :

- Système informatique ou autre (Equipement Cisco) ou autre (CiscoWorks) : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / clé SSH pour le compte de service.
- Le compte de service doit avoir des droits **network-admin** (administrateur réseau).
- SNMP : entrez le nom de communauté (pour SNMPv1 et SNMPv2).
- SNMP (SNMPv3) :
  - Entrez :
    - le nom d'utilisateur
    - le mot de passe
    - le mot de passe privé (facultatif)
  - Sélectionnez le protocole d'authentification : aucun, MD5, SHA

Il est important qu'un seul nom de communauté soit disponible pour TSA et dispose d'un accès en lecture seule à TOUS les équipements réseau entrant dans le périmètre.

F5 Big-IP (TMOS)

Pour reconnaître les systèmes F5 Big-IP qui exécutent TMOS, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Le compte de service doit avoir des droits administrateur F5.
- Le compte de service doit avoir un accès SSH pour exécuter les commandes CLI de TMSH.

Fortinet (FortiOS)

Pour reconnaître les équipements Fortinet qui exécutent FortiOS, procédez comme suit :

Préparer l'environnement :

- Assurez-vous que la console système est configurée de façon à afficher le résultat complet de la commande :

```
config system console
set output standard
end
```

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Le compte de service doit au moins avoir des droits d'accès en lecture seule.

Commutateurs IBM SAN de type b

Pour reconnaître les équipements IBM SAN de type b, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Mode Virtual Fabric désactivé : le compte de service peut utiliser n'importe quel type de droits valides. Les droits **Utilisateur** sont recommandés.
- Mode Virtual Fabric activé : le compte de service a besoin des droits **Admin** sur Fabric OS.

Juniper

Pour découvrir les équipements Juniper, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Remarque : la reconnaissance des informations sur la taille de mémoire nécessite d'installer Junos® version 12.1 ou une version ultérieure sur l'équipement.

Palo Alto Networks (PAN-OS)

Pour reconnaître les systèmes Palo Alto Networks qui exécutent PAN-OS, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits Superutilisateur ou Superutilisateur (en lecture seule)
- Le compte de service doit avoir accès aux API REST (port 443).

Commutateurs QLogic

Pour découvrir les commutateurs QLogic, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Equipements de stockage

Cette section donne des informations détaillées sur les types d'équipements de stockage et à bande :

Plateforme
Stockage EMC Corporation
HP StorageWorks P2000 Modular Smart Array
IBM DS3xxx, DS4xxx ou DS5xxx
IBM DS6xxx ou DS8xxx
IBM FlashSystem, v9000
IBM ProtecTier
IBM SVC ou V7000/V3700
Bandothèque IBM TS3100
Bandothèque IBM TS3200
Bandothèque IBM TS3310

Plateforme
Bandothèques IBM TS3494, TS3953
Bandothèques IBM TS3500, TS3584
Bandothèque IBM TS4500
Bandothèque IBM TS7700
IBM V7000 Unified
IBM XIV
nSeries ou NetApp

Cliquez sur les liens ci-dessus pour plus d'informations.

Stockage EMC Corporation

EMC CLARiiON / VNX / VMAX

Pour reconnaître les équipements EMC CLARiiON / VNX / VMAX, procédez comme suit :

Préparer l'environnement :

- Assurez-vous qu'une instance du produit EMC SMI-S Provider est installée sur un système Windows ou Linux. Par défaut, TSA suit la recommandation EMC SMI-S invitant à reconnaître l'emplacement du fournisseur à l'aide du protocole SLP. Si vos règles de sécurité réseau bloquent le trafic réseau SLP, TSA peut être configuré de façon à accéder directement à EMC SMI-S Provider sans utiliser le protocole SLP.
- Si vos règles de sécurité réseau n'autorisent pas le trafic réseau SLP, utilisez la page **Paramètres de reconnaissance → Paramètres de connexion** pour fournir des informations sur les ports que les EMC SMI-S Providers écoutent pour les demandes de requête.
- Assurez-vous qu'au moins une des adresses IP utilisées par le SMI-S Provider est définie dans un ensemble de périmètres. TSA se connectera au SMI-S Provider pour récupérer des informations sur les équipements EMC qu'il gère. Il n'est pas nécessaire de placer les adresses IP de chaque équipement EMC dans un ensemble de périmètres. TSA tente de se connecter à SMI-S Provider à l'aide du protocole HTTPS, s'il est disponible ; sinon, c'est le protocole HTTP qui est utilisé.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut utiliser n'importe quel rôle valide. Le rôle **monitor** est recommandé.

Seules les données d'identification du fournisseur SMI-S doivent être entrées dans TSA. Aucune donnée d'identification pour les équipements EMC n'a besoin d'être saisie.

EMC Data Domain

Pour reconnaître les équipements EMC Data Domain, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut avoir le minimum de droits requis.

HP StorageWorks P2000 Modular Smart Array

Pour reconnaître les systèmes HP Storage, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut avoir le minimum de droits requis.

Stockage IBM DS3xxx, DS4xxx ou DS5xxx

Pour reconnaître les équipements IBM DS3xxx, DS4xxx ou DS5xxx, procédez comme suit :

Préparer l'environnement :

- Assurez-vous que le gestionnaire de stockage permet d'utiliser les commandes distantes **smcli**.

Données d'identification pour la liste d'accès :

- Pour les équipements de stockage non sécurisés, aucune donnée d'identification n'est requise.
- Pour les équipements de stockage sécurisés, effectuez les étapes suivantes :
  - Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
  - Le compte de service peut avoir le rôle **admin** ou **monitor**. Le rôle **monitor** est recommandé.

Stockage IBM DS6xxx / DS8xxx

Pour reconnaître les équipements IBM DS6xxx / DS8xxx, procédez comme suit :

Préparer l'environnement :

- Assurez-vous que le gestionnaire de stockage permet d'utiliser les commandes distantes **dscli**.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir le rôle **monitor**.

IBM FlashSystem, v9000

Pour reconnaître les équipements IBM FlashSystem, procédez comme suit :

Préparer l'environnement :

- Pour les anciens modèles, le MCP (Management Control Port) doit être à l'état actif pour réaliser la reconnaissance du système avec succès.
  - Pour vérifier si un système est à l'état actif, exécutez la commande `system status`.
  - Sur les deux adresses IP, si l'une tombe, le système passe à l'état passif. Pour rendre l'autre port Ethernet actif, exécutez la commande `sync activate`.
  - Le système découvert doit être celui qui a l'adresse IP de gestion et/ou le noeud de configuration.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / authentification par clé SSH pour le compte de service.
- Le compte de service peut utiliser n'importe quel rôle valide. Le rôle **monitor** est recommandé.

IBM ProtecTIER

Pour découvrir les équipements ProtecTIER, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Stockage IBM SVC, V7000/V3700

Pour reconnaître les équipements SVC et V7000/V3700, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe ou Nom d'utilisateur / clé SSH pour l'authentification.

- Le compte de service peut utiliser n'importe quel rôle valide. Le rôle **monitor** est recommandé.

Bandotèque IBM TS3100

Pour reconnaître les bandothèques TS3100, procédez comme suit :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Bandothèque IBM TS3200

Pour reconnaître les bandothèques TS3200, procédez comme suit :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Bandothèque IBM TS3310

Pour reconnaître les bandothèques TS3310, procédez comme suit :

Préparer l'environnement :

- Le service Web est toujours configuré en mode sécurisé.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Bandothèques IBM TS3494, TS3953

Pour reconnaître les bandothèques TS3494 et TS3953, procédez comme suit :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut avoir le minimum de droits requis.

IBM TS3500, TS3584

Les prérequis sont les suivants :

- La bandothèque TS3500 doit être au niveau de microprogramme 8xxx (ou supérieur).
- Le système ALMS (Advanced Library Management System) doit être installé et activé.

Les connexions SSL et non-SSL sont prises en charge.

Pour reconnaître les bandothèques TS35xx, procédez comme suit :

Préparer l'environnement :

- L'interface web TS3500 peut être configurée sur **Sans protection par mot de passe** ou **Protection par mot de passe**.
  - Si l'option **Protection par mot de passe** est activée, créez un jeu de données d'identification en suivant les instructions de la section **Données d'identification pour la liste d'accès** ci-dessous.
  - Si l'option **Protection par mot de passe** est désactivée, aucun jeu de données d'identification n'est nécessaire.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir des droits administrateur.

Bandothèque IBM TS4500

Les prérequis sont les suivants :

- La bandothèque TS4500 doit être au niveau de microprogramme 1.4.1.2 ou supérieur (jusqu'à 1.7.0.0).
- Le système ALMS (Advanced Library Management System) doit être installé et activé.


Les connexions SSL et non-SSL sont prises en charge.

Pour reconnaître les bandothèques TS4500, procédez comme suit :

Préparer l'environnement :

- L'interface web TS4500 peut être configurée uniquement sur **Protection par mot de passe**.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit être mappé au rôle **Service**.

Bandothèque IBM TS7700

Pour reconnaître les bandothèques TS7700, procédez comme suit :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service a seulement besoin de droits **en lecture seule**.

Stockage IBM V7000 Unified

Pour reconnaître les équipements V7000 Unified, effectuez les étapes suivantes :

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut utiliser n'importe quel rôle valide. Le rôle **monitor** est recommandé.

IBM XIV

Pour reconnaître les équipements XIV, procédez comme suit :

Préparer l'environnement :

- Assurez-vous que le gestionnaire de stockage permet d'utiliser les commandes distantes **xcli**.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service doit avoir le rôle d'utilisateur **read-only**.
- Notez que les systèmes XIV peuvent avoir un seuil bas pour les tentatives de connexion non valides avant de générer des alertes. Si vous utilisez un ensemble de données d'identification étendu, vous risquez de dépasser cette limite et de générer des problèmes inutiles. Essayez de regrouper les équipements XIV dans un seul ensemble de périmètres et de limiter leurs données d'identification de compte de service à cet ensemble de périmètres.

Stockage nSeries ou NetApp

Pour reconnaître les équipements nSeries ou NetApp, procédez comme suit :

Préparer l'environnement :

- La collecte de données est prise en charge pour les systèmes configurés avec les interfaces CLI Data ONTAP, RLM et SP. En revanche, l'interface CLI BMC n'est pas prise en charge.
- L'option **telnet.distinct.enable** doit être activée.

Données d'identification pour la liste d'accès :

- Système informatique : Nom d'utilisateur / mot de passe pour le compte de service.
- Le compte de service peut avoir le minimum de droits requis.

Problématiques des pare-feux

Tout pare-feu installé entre l'appliance et les équipements de reconnaissance peut empêcher la réalisation d'une reconnaissance complète et réussie.

Dans les cas où il est nécessaire de traverser un pare-feu, des ports devront potentiellement être ouverts dans le pare-feu, suivant le type d'équipement que l'utilisateur voudra reconnaître. En général, ce sont les ports 22 (SSH) et 161 (SNMP) qui doivent être ouverts, suivis des ports appropriés indiqués dans le tableau suivant, suivant les équipements pris en charge.

Terminal de reconnaissance	**Ports**	**Interface / Protocole**
Plusieurs	161	SNMP
Equipements de stockage		
DS6000 / DS8000	1750 (HTTP) ou 1751 (HTTPS)	DSCLI
DS3000 / DS4000 / DS5000	2463	SMCLI
XIV	7778	XCLI
nSeries ou NetApp	22 / 23	SSH ou Telnet
SVC ou V7000/V3700	22	SSH
V7000 Unified	22	SSH
IBM TS3500	443 / 80	HTTPS ou HTTP
IBM TS4500	443 / 80	HTTPS ou HTTP
IBM TS7700	443 / 80	HTTPS ou HTTP
IBM TS3100 / TS3200 / TS3310	80	HTTP
IBM TS3494, TS3953	23	Telnet
IBM ProtecTier	22	SSH
HP Storage	22 / 23	SSH ou Telnet
IBM Flash System, v9000	22	SSH

Terminal de reconnaissance	Ports	Interface / Protocole
Stockage EMC Corporation - CLARiion/VNX/VMAX	427 - (valeur par défaut) lorsque la reconnaissance SLP est autorisée ; sinon, si la reconnaissance SLP est désactivée, ce port n'est pas utilisé. Ports HTTPS / HTTP configurés par EMC SMI-S Provider ; les valeurs par défaut sont 5989 / 5988	SLP, HTTPS / HTTP
	Vous pouvez activer l'option de reconnaissance SLP pour reconnaître les équipements de stockage EMC via les EMC SMI-S Providers.	
Stockage EMC Corporation – EMC Data Domain	22	SSH*
Systèmes d'exploitation et hôtes		
FSM	22 / 23	SSH ou Telnet
CMM	22 / 23	SSH ou Telnet
AMM	22 / 23	SSH ou Telnet
Serveur lame HP Proliant via HP OnBoard Administrator	22 / 23	SSH ou Telnet
IMM et IMM2	22 / 23	SSH ou Telnet
HP iLO pour les serveurs HP Integrity / HP 9000	22 / 23	SSH* ou Telnet
Equipements réseau		
Brocade	161 / 22 /23	SNMP, SSH, Telnet
Commutateurs IBM SAN de type b	22 /23	SSH, Telnet
Cisco	161 / 22 / 23	SNMP, SSH, Telnet
BNT	22 / 23	SSH ou Telnet
Juniper	22 / 23	SSH ou Telnet
QLogic	22 / 23	SSH* ou Telnet

Terminal de reconnaissance	Ports	Interface / Protocole
Fortinet (FortiOS)	22 / 23	SSH ou Telnet
Palo Alto Networks (PAN-OS)	443	HTTPS
F5 Big-IP (TMOS)	22 / 23	SSH ou Telnet
Check Point	22 / 23	SSH ou Telnet
Systèmes d'exploitation / plateformes de serveur		
HMC	22	SSH
VIOS	22	SSH
AIX	22	SSH
Linux	22	SSH
Windows	445	SMBv1
VMware vCenter	443	HTTPS
VMware ESXi	443, 5989	HTTPS
IVM	22 / 23	SSH ou Telnet
IBM i	22	SSH
SUN	22	SSH

- TSA prend en charge uniquement SSH v1 pour les équipements qui sont marqués par SSH*.

Problèmes de reconnaissance

La plupart des problèmes de reconnaissance sont dus à des problèmes d'accès ou d'autorisation.

Les problèmes d'accès les plus courants sont dus aux pare-feux qui bloquent l'accès aux ports nécessaires sur l'équipement. Les ports qui doivent être ouverts et atteignables varient selon le type d'équipement. Pour déterminer quels ports sont concernés, consultez la section "Problématiques des pare-feux", à la page 41.

Les problèmes d'autorisation les plus courants sont les suivants :

- **Aucune donnée d'identification définie**. Assurez-vous que les données d'identification des équipements sont définies dans TSA et que les comptes de service appropriés sont créés sur les équipements.
- **Nom d'utilisateur ou mot de passe incorrect**. Lorsque vous créez ou éditez un jeu de données d'identification, utilisez la fonction **Test** pour vérifier la validité des données.
- **Le mot de passe a expiré**.
- **Les données d'identification n'ont pas les droits nécessaires sur l'équipement**. Pour déterminer les données d'identification requises pour un équipement cible, consultez la section Configuration de la reconnaissance des équipements, page 12. .
- **Utiliser un type de données d'identification valide**. Pour les équipements Windows, créez une donnée d'identification "Système informatique (Windows)" et non "Système informatique".

Consultez la page **État d'authentification (Outils → État d'authentification)** pour voir si le mot de passe de certaines données d'identification de compte de service a expiré ou si ces données ont cessé de fonctionner.

Problématiques courantes

Une fois que les portions du réseau souhaitées ont été définies dans TSA et analysées avec succès, TSA peut commencer à exécuter des reconnaissances et des transmissions périodiques sur les plannings souhaités.

Voici quelques-unes des activités courantes attendues :

- Examinez régulièrement les rapports générés par TSA avec votre représentant IBM.
- Effectuez une sauvegarde régulière via l'interface utilisateur de TSA afin d'enregistrer une copie de la configuration de TSA.

> Cette opération ne sauvegarde pas les données collectées par TSA. Elle sauvegarde uniquement les informations de configuration.

- Consultez régulièrement le panneau **État d'authentification (Outils → État d'authentification)** pour voir si le mot de passe de certaines données d'identification de compte de service a expiré ou si ces données ont cessé de fonctionner.
- Lorsque les mots de passe sont mis à jour pour les comptes de service sur les équipements, assurez-vous de mettre également à jour les mots de passe dans TSA afin de maintenir la définition des données d'identification dans TSA synchronisée avec les données d'identification sur l'équipement cible.
- Si les règles de sécurité vous y autorisent, pensez à configurer les comptes de service avec des mots de passe sans date d'expiration ou utilisez des clés SSH. Ainsi, vous n'aurez pas à mettre à jour les mots de passe dans l'interface utilisateur de TSA et de façon périodique sur les équipements.

Identification et résolution des problèmes

Session active pour la reconnaissance AMM

Les équipements AMM ont un réglage qui limite le nombre de sessions actives simultanées (20 maximum). Si ce réglage n'est pas suffisamment haut pour permettre à TSA de créer une session, l'équipement AMM ne peut pas être reconnu.

Pour changer le nombre limite de sessions actives d'un équipement AMM, suivez ces étapes :

1. Connectez-vous à l'interface web AMM en tapant l'adresse IP de l'équipement AMM dans un navigateur web.
2. Allez dans **MM Control → Login Profiles**.
3. Cliquez sur l'ID de connexion utilisée par TSA pour reconnaître l'équipement.
4. Augmentez la valeur du paramètre **Maximum simultaneous active sessions**.
5. Cliquez sur **Save** en bas à droite de la page.

Annexe A : Termes et définitions

On suppose que le lecteur possède une connaissance approfondie des réseaux et des protocoles IP (Internet Protocol).

Terme	**Définition**
Equipement de reconnaissance	Fait référence aux composants d'infrastructure informatique déployés qui peuvent être reconnus par TSA. Les équipements types sont notamment les serveurs, les systèmes informatiques (IBM, Dell, HP, etc.), les éléments de stockage et les éléments réseau (commutateurs, ponts, routeurs, etc.).

Annexe B : Eléments divers

Fonctions de téléchargement de l'interface utilisateur

Dans certains cas, lorsque vous utilisez un navigateur Web, le téléchargement de tous les journaux (depuis la page **Journal d'activité**), le téléchargement des fichiers (depuis la page **Historique de la reconnaissance**) ou le téléchargement de documentation (depuis la page **Documentation**) ne s'exécutent pas correctement. Pour résoudre ce problème, essayez de passer sur un autre navigateur web pris en charge, comme indiqué dans le Guide de l'installation d'IBM Technical Support Appliance. Si ce n'est pas possible, essayez de redéfinir les propriétés de votre navigateur avec les paramètres par défaut.

Annexe C : Fournisseur CIM pour VMware ESXi

Un fournisseur CIM est un ensemble de plug-ins VMware ESXi qui peuvent collecter des informations matérielles et de firmware supplémentaires sur le serveur sur lequel s'exécute VMware ESXi. TSA et le VMware vCenter peuvent tous deux tirer profit de ces informations supplémentaires.

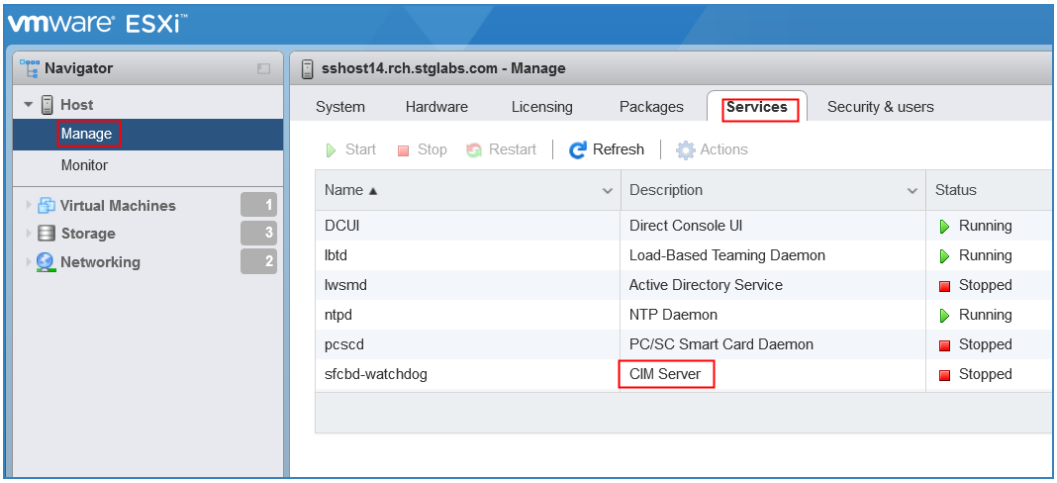
Les plug-ins du fournisseur CIM sont déployés par les fabricants du serveur et des composants. Pour vous assurer que les plug-ins du fournisseur CIM sont inclus dans ESXi, utilisez une image d'installation personnalisée où les plug-ins du fournisseur CIM sont inclus. Pour les instances VMware ESXi existantes sur lesquelles le fournisseur CIM n'est pas installé, obtenez les plug-ins nécessaires auprès des fabricants du serveur et des composants et installez-les dans ESXi. VMware fournit une liste des différents plug-ins qui sont fournis par les fabricants.

Pour plus d'informations, voir https://www.vmware.com/resources/compatibility/pdf/vi_cim_guide.pdf.

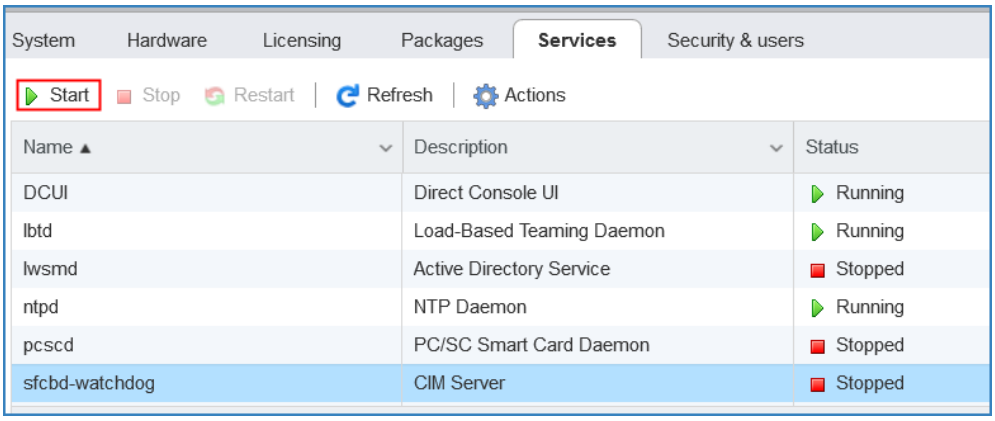
Pour déterminer si le fournisseur CIM est actif et pour le mettre sous tension s'il n'est pas actif, procédez comme suit :

Sur le client Web VMware vSphere

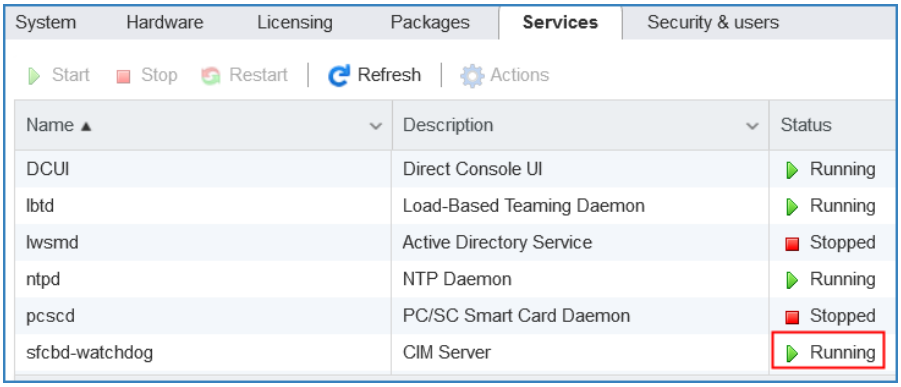
- Connectez-vous au client web VMware vSphere.
- Cliquez sur **Host → Manage** dans la fenêtre de navigation de gauche et sélectionnez l'onglet **Services** dans le panneau de droite.
- Un ensemble de services dont **CIM Server** s'affiche.



- Si **CIM Server** est à l'état **Stopped**, sélectionnez-le et cliquez sur **Start**.

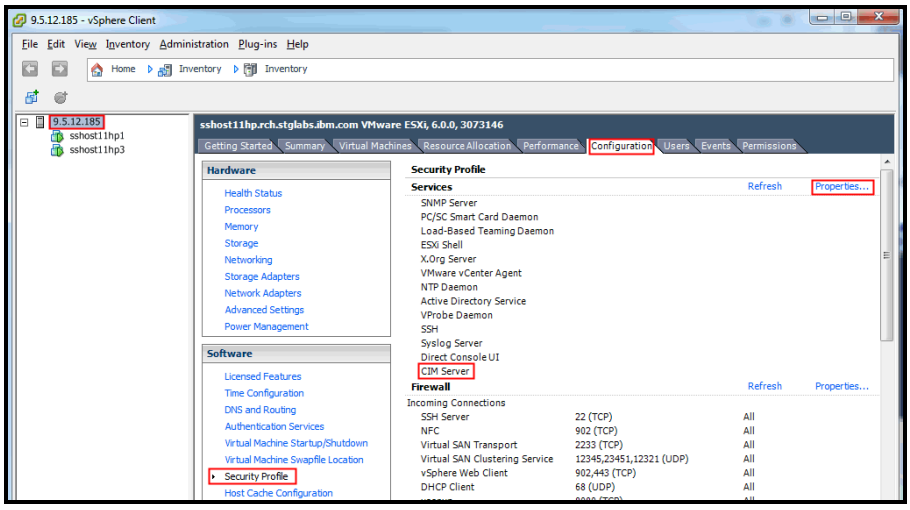


- Le service CIM Server démarre et son état devient **Running**.

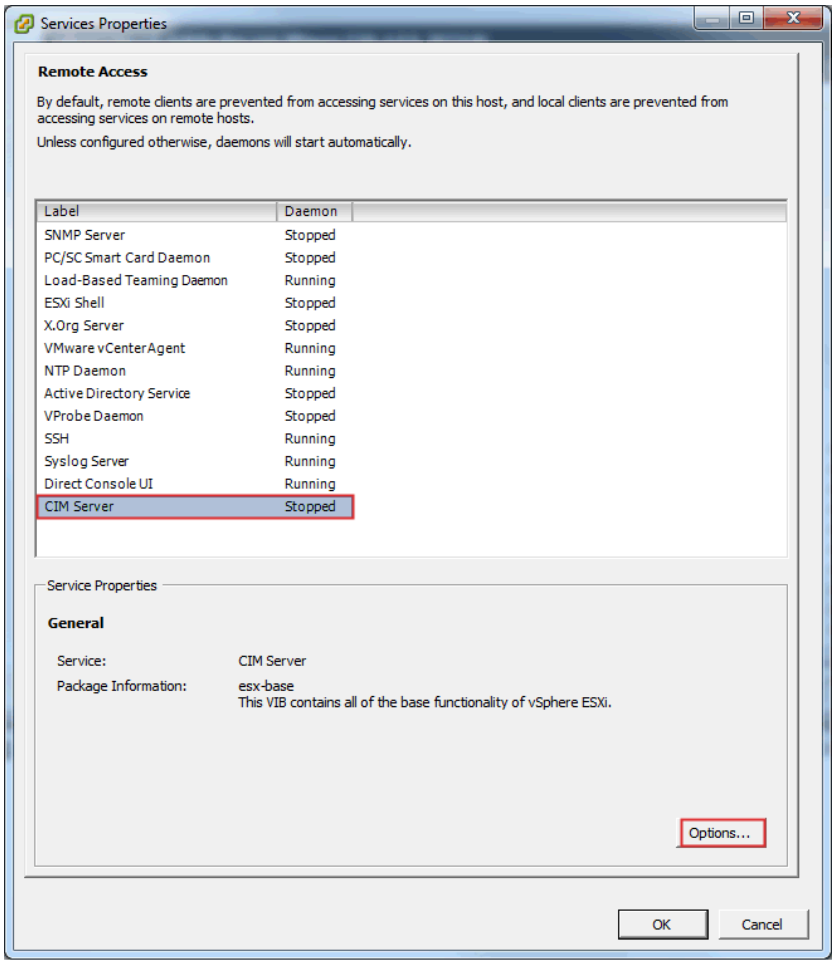


Sur le client VMware vSphere

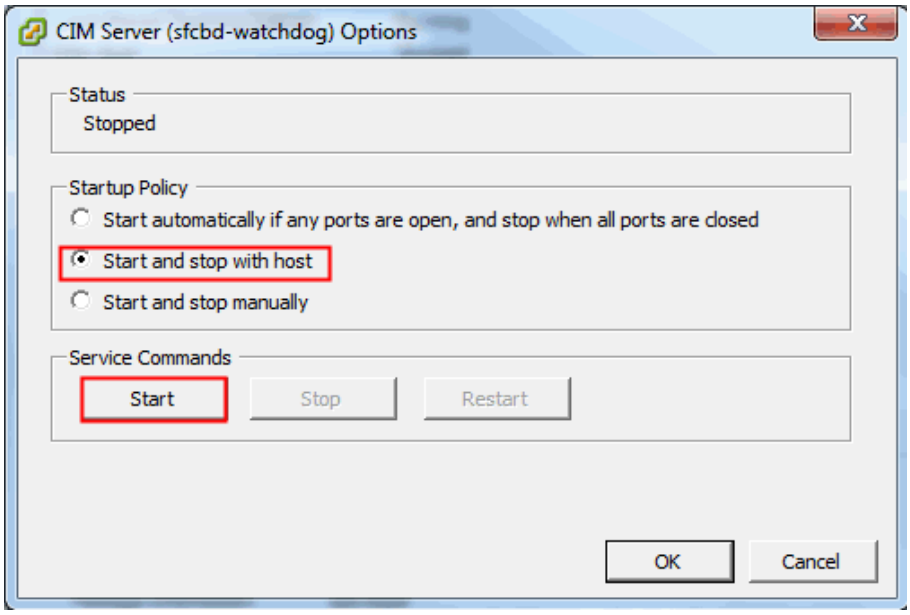
- Démarrez VMware vSphere Client.
- Cliquez sur l'adresse IP du serveur ESXi dans la fenêtre de navigation de gauche et sélectionnez l'onglet **Configuration** dans le panneau de droite.
- Sélectionnez **Security Profile** dans le menu de sélection **Software** dans le panneau de droite. Un ensemble de services dont **CIM Server** s'affiche dans la section **Services**.



- Sélectionnez l'option **Properties...** dans la section **Services**.



- Si **CIM Server** est à l'état **Stopped**, sélectionnez-le puis cliquez sur **Options...**. La boîte de dialogue suivante s'affiche.



- Sélectionnez l'option **Startup Policy (Start and stop with host**) et cliquez sur **Start** pour activer le serveur CIM.

Annexe D : Windows avec WINRM

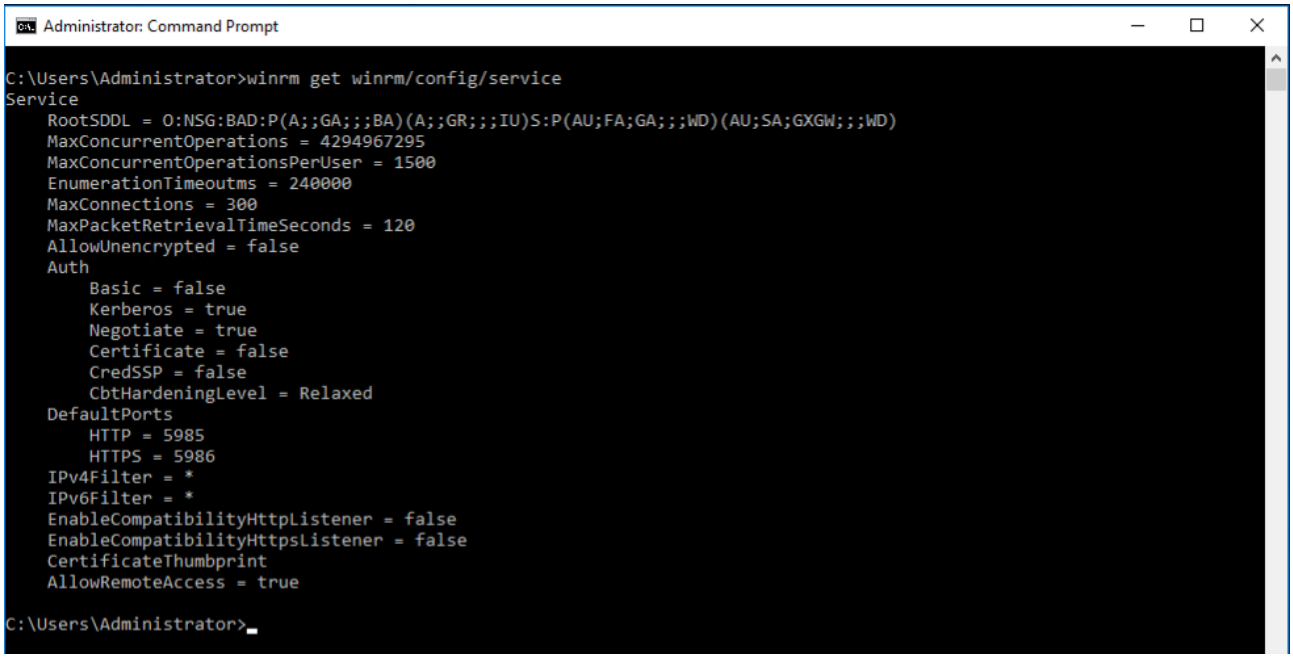
Pour Windows 2012 et 2016 Server, le service WINRM est démarré automatiquement. En revanche, la gestion à distance n'est pas activée par défaut. Voici une brève présentation des conditions requises pour activer WINRM et permettre des connexions distantes à l'aide d'un certificat autosigné :

- Activez WINRM pour accepter les connexions HTTPS qui permettent une authentification par ID utilisateur / mot de passe.
- Associez un certificat autosigné à l'écouteur HTTPS pour WINRM qui a été activé.
- Modifiez le pare-feu Windows pour permettre des connexions entrantes via le port 5986 (le port HTTPS WINRM par défaut).

Les commandes suivantes permettent à WINRM d'autoriser les connexions distantes via HTTPS :

- Déterminez l'état actuel du service WINRM à l'aide de la commande suivante :

  winrm get winrm/config/service



- La valeur de **AllowUnencrypted** doit être *false*. Si la valeur est *true*, utilisez la commande suivante pour la remplacer par *false* :

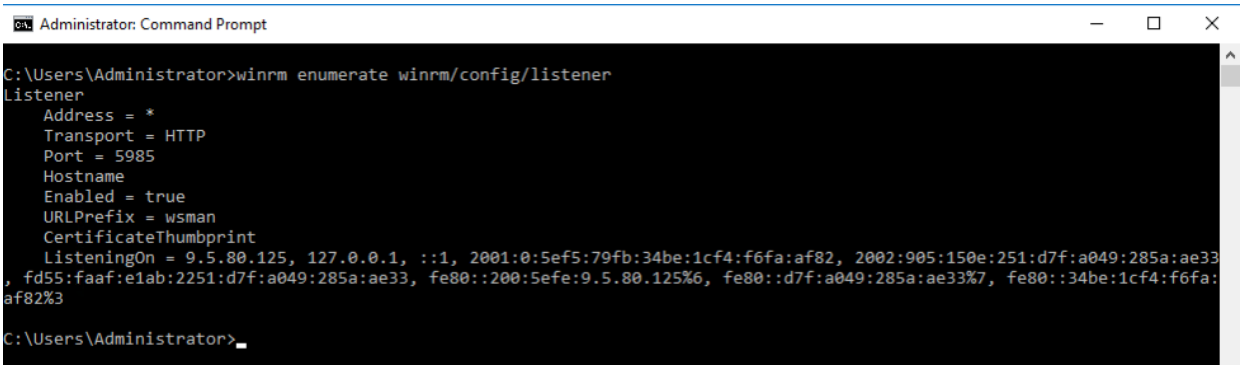
  winrm set winrm/config/service @{AllowUnencrypted="false"}

- La valeur de **Basic** doit être *true*. Si la valeur est *false*, utilisez la commande suivante pour la remplacer par *true* :

  winrm set winrm/config/service/auth @{Basic="true"}

- Déterminez si WINRM a un écouteur HTTPS à l'aide de la commande suivante :

  winrm enumerate winrm/config/listener

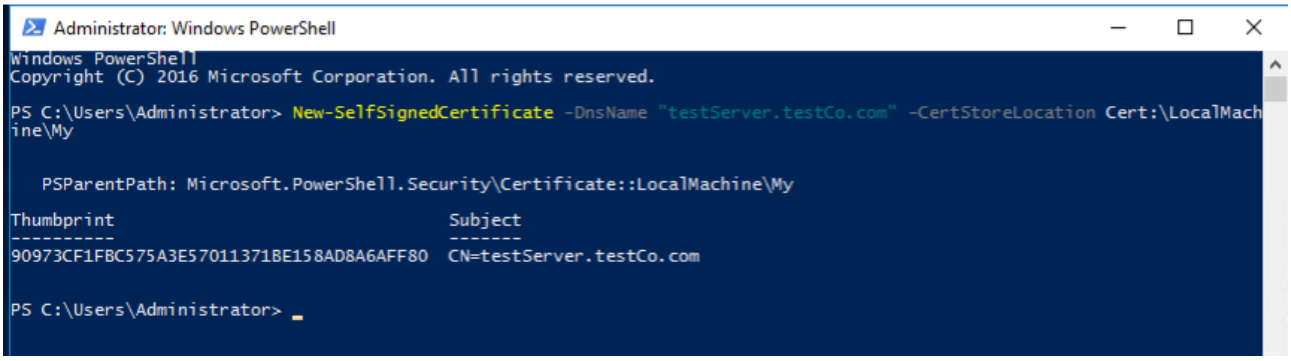


- Dans l'exemple de commande ci-dessus, il n'existe qu'un écouteur HTTP ; il faut donc configurer un écouteur HTTPS. Pour activer l'écouteur HTTPS, s'il n'est pas configuré :
  - A l'aide de PowerShell, créez un certificat autosigné :

    New-SelfSignedCertificate -DnsName "myHost@myBusiness.com" -CertStoreLocation Cert:\LocalMachine\My

    > Remplacez le DnsName **(myHost@myBusiness.com)** dans l'exemple ci-dessus par le nom de domaine complet Windows pour le serveur Windows.

  - Enregistrez l'empreinte de certificat pour la prochaine étape.



- Créez l'écouteur HTTPS :

  winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="myHost@myBusiness.com"; CertificateThumbprint="[COPIED_CERTIFICATE_THUMBPRINT]"}

- Vérifiez que l'écouteur HTTPS est désormais bien configuré :

  winrm enumerate winrm/config/listener

- Modifiez le pare-feu Windows pour permettre des connexions entrantes distantes avec WINRM :

- Allez dans **Panneau de configuration → Système et sécurité → Pare-feu Windows**
- Cliquez sur **Paramètres avancés.** La fenêtre **Pare-feu Windows avec fonctions avancées de sécurité** s'affiche.
- Cliquez sur **Règles de trafic entrant**.
- Sélectionnez le menu **Actions** puis cliquez sur **Nouvelle règle**. L'**Assistant Nouvelle règle de trafic entrant** s'affiche**.**
- Sélectionnez **Port** puis cliquez sur **Suivant.**
- Sélectionnez **TCP → Ports locaux spécifiques :** puis indiquez 5986. Cliquez sur **Suivant.**
- Sélectionnez l'option **Autoriser la connexion** puis cliquez sur **Suivant**.
- Cochez les cases **Domaine**, **Privé** et **Public** si elles ne le sont pas déjà puis cliquez sur **Suivant.**
- Donnez un nom à la nouvelle règle (ex. : Windows Remote Management (HTTPS-In)) puis cliquez sur **Terminer**.

Mentions légales

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589
Produit aux États-Unis
Août 2020.

Ce document a été élaboré pour les produits et/ou services offerts aux États-Unis. IBM peut ne pas proposer les produits, fonctionnalités ou services décrits dans ce document dans d'autres pays.

Ces informations peuvent être modifiées sans préavis. Consultez votre interlocuteur IBM local pour obtenir des informations sur les produits, fonctionnalités et services disponibles dans votre région.

Toutes les déclarations concernant les orientations et intentions futures d'IBM peuvent être modifiées ou retirées sans préavis et ne représentent que des buts et des objectifs.

IBM, le logo IBM, POWER, System I, System p et i5/OS sont des marques ou des marques déposées d'International Business Machines Corporation aux Etats-Unis et/ou dans d'autres pays. La liste complète des marques détenues par IBM aux États-Unis se trouve à l'adresse http://www.ibm.com/legal/copytrade.shtml.

Les autres noms de sociétés, de produits et de services peuvent être des marques de commerce ou des marques de service de tiers.

Les produits matériels IBM sont fabriqués à partir de pièces neuves ou de pièces neuves et de seconde main. Quel que soit le cas, nos conditions de garantie s'appliquent.

Cet équipement est soumis aux règles de la Federal Communications Commission (FCC). Il se conformera aux règles de la FCC avant la livraison finale à l'acheteur.

Les informations concernant les produits non IBM ont été obtenues auprès des fournisseurs de ces produits.

Les questions sur les capacités des produits non IBM doivent être adressées aux fournisseurs.

La page d'accueil d'IBM sur Internet se trouve à l'adresse http://www.ibm.com.

La page d'accueil d'IBM System p sur Internet se trouve à l'adresse http://www.ibm.com/systems/p.

La page d'accueil d'IBM System I sur Internet se trouve à l'adresse http://www.ibm.com/systems/i.

PSW03007-FRFR-00