Version 2.7.0.0

Technical Support Appliance
Guide d'installation

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Mentions légales», à la page 147.

Vingt-troisième édition (août 2020)

La présente édition s'applique à la version 2, révision 7, modification 0 d'IBM® Technical Support Appliance ainsi qu'à toutes les futures révisions et modifications jusqu'à indication contraire dans les nouvelles éditions.

Table des matières

Figures

Chapitre 1. Introduction

IBM Technical Support Appliance (TSA) est un outil facile d'emploi qui vous permet de tirer le meilleur profit 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 applications, le middleware, les serveurs et les composants réseau dans votre data center.

TSA comprend une interface utilisateur Web qui vous permet de configurer et de personnaliser l'accès à votre système et à vos données. Cette interface vous permet également de modifier vos plannings de reconnaissance et de transmission des données.

Dans le cadre du processus de reconnaissance, TSA tente avant tout de détecter les terminaux 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 les moins intrusives possibles. 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.

Les 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.

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.

Comptes d'utilisateur et groupes d'utilisateurs

L'exécution d'une fonction de TSA exige un certain niveau d'autorisation. Si un utilisateur authentifié tente d'exécuter une fonction sans avoir le niveau d'autorisation adéquat, un message d'erreur s'affiche et la fonction ne s'exécute pas.

Au sein d'une organisation, des rôles peuvent être créés pour différentes fonctions. Les droits autorisant à effectuer certaines opérations sont affectés à des rôles spécifiques. Les utilisateurs de TSA se voient affecter des rôles particuliers, qui leur donnent les droits nécessaires pour exécuter des fonctions système spécifiques. Ainsi, chaque utilisateur affecté à un rôle disposera des niveaux d'autorisation associés à ce rôle et vous pourrez facilement ajouter un utilisateur à un rôle, faire passer les utilisateurs d'un rôle à un autre ou encore supprimer certains utilisateurs d'un rôle.

Dans TSA, les rôles sont gérés avec des groupes d'utilisateurs auxquels sont associés des niveaux d'autorisation. Les utilisateurs sont gérés avec des comptes d'utilisateur. Ces comptes d'utilisateur peuvent appartenir à un ou plusieurs groupes d'utilisateurs et du fait de cette appartenance, les utilisateurs ont le niveau d'autorisation requis pour exécuter certaines fonctions.

De plus, les droits des groupes d'utilisateurs peuvent aussi être limités à certains ensembles de périmètres. Un ensemble de périmètres est un groupe d'adresses IP, de plages d'adresses ou de sous-réseaux qui identifient les éléments informatiques pouvant être reconnus par TSA. Appliquer des restrictions d'accès à un ensemble de périmètres pour un groupe d'utilisateurs est un moyen de limiter davantage les droits d'accès des membres de ce groupe d'utilisateurs. Par exemple, il est possible de créer des groupes d'utilisateurs par plateforme, comme des utilisateurs responsables de la maintenance

des systèmes Linux®, en associant à un groupe d'utilisateurs particulier une combinaison de niveau d'autorisation et de restrictions d'accès à un ensemble de périmètres.

Périmètres de reconnaissance et ensembles de périmètres

Les périmètres de reconnaissance identifient les ressources qui doivent être reconnues par TSA. Les périmètres de reconnaissance sont groupés par ensembles de périmètres de reconnaissance.

Vous pouvez indiquer des périmètres de reconnaissance en utilisant une adresse IP, une plage d'adresses IP ou un réseau ou sous-réseau pour définir les ressources qui seront accessibles durant la reconnaissance. Un périmètre de reconnaissance peut se limiter à une seule adresse IP ou au contraire couvrir une plage d'adresses IP ou un réseau.

Pour simplifier la création d'un ensemble de périmètres, un fichier peut être utilisé pour importer une liste d'adresses IP. Pour plus d'informations, voir la section «Importer un ensemble de périmètres», à la page 74.

Plus il y a d'adresses IP dans le périmètre de reconnaissance, plus la reconnaissance est longue. Vous pouvez modifier la taille de la reconnaissance en désactivant ou en activant les ensembles de périmètres de reconnaissance ou en excluant des adresses IP, des plages d'adresses IP, des réseaux ou des sous-réseaux d'un périmètre dans un ensemble de périmètres.

Remarque : Pour de meilleurs résultats, limitez le nombre cumulé d'adresses IP (adresse IP, plages, sous-réseaux et exclusions) dans un ensemble de périmètres à 400 adresses maximum.

Tâches associées

Ajouter des comptes d'utilisateur et des groupes d'utilisateurs
Vous pouvez ajouter des comptes d'utilisateur et des groupes d'utilisateurs pour contrôler l'accès aux fonctions TSA.

Données d'identification de la reconnaissance

Les données d'identification de la reconnaissance sont composées de noms d'utilisateur, de mots de passe ou clés SSH et de noms de communauté SNMP (Simple Network Management Protocol) que TSA utilise pour accéder aux ressources lors de la reconnaissance.

Vous devez configurer et tenir à jour les données d'identification de la reconnaissance pour les ressources que vous souhaitez reconnaître. Les informations d'accès que vous fournissez varient selon le type de données d'identification mais elles incluent généralement au moins un nom d'utilisateur et un mot de passe ou une clé SSH.

Les données d'identification de la reconnaissance peuvent s'appliquer à tous les ensembles de périmètres ou se limiter à un seul ensemble de périmètres. Définir des données d'identification qui s'appliquent à un seul ensemble de périmètres améliore la performance et empêche les tentatives de connexion invalides, qui peuvent entraîner le blocage du compte.

Lorsque vous accédez à une ressource, TSA utilise séquentiellement chaque jeu de données d'identification qui est associé à un périmètre particulier dans l'ordre indiqué sur la page **Données d'identification de la reconnaissance** jusqu'à ce que la ressource lui donne le droit d'y accéder. Par exemple, lorsque vous accédez à un système informatique, TSA utilise la première combinaison de nom d'utilisateur et de mot de passe qui apparaît dans la liste des données d'identification pour les systèmes informatiques et qui est associée à l'ensemble de périmètres qui la contient. Si le nom d'utilisateur et le mot de passe sont incorrects pour un système informatique particulier, TSA utilise automatiquement le nom d'utilisateur et le mot de passe suivants indiqués dans la liste des données d'identification pour les systèmes informatiques.

Conseil : Avant d'enregistrer les données d'identification, vous pouvez vérifier si vous avez indiqué des données d'identification valides pour les types de système, telles que **Système informatique**, **Système informatique (Windows)**, **SNMP** ou **SNMPV3**. En faisant ce test, vous pouvez vérifier que les données d'identification sont bien définies et valides.

Conseil :

- Utilisez un compte de service avec un mot de passe commun à tous les équipements d'un certain type, tels que AIX ou Windows. Un seul jeu de données d'identification peut alors être défini pour découvrir toutes les instances de ce type d'équipement.
- Utilisez des comptes avec des mots de passe sans date d'expiration.
- Utilisez des clés SSH si nécessaire.

Planning de reconnaissance

Les reconnaissances sont effectuées les jours et aux heures prévus afin de s'assurer que les données reconnues sont toujours valides et exactes. TSA a un planning de "reconnaissance complète" par défaut qui effectue la reconnaissance de tous les ensembles de périmètres définis. Il vous est possible de modifier ce planning par défaut selon vos besoins. Vous pouvez aussi créer des plannings dans le but d'étaler la reconnaissance des différents ensembles de périmètres dans le temps, c'est-à-dire à des dates et heures différentes. Vous pouvez aussi voir le détail, l'historique et l'état de la dernière reconnaissance effectuée.

Lorsque vous modifiez un planning de reconnaissance, vous indiquez le nom, les ensembles de périmètres, l'heure de début et la fréquence des reconnaissances. Si le planning de reconnaissance actif est le planning de reconnaissance par défaut, vous ne pouvez changer que l'heure de début et la fréquence des reconnaissances. Vous pouvez aussi effectuer des reconnaissances à la demande.

La durée de la reconnaissance dépend de différents facteurs, dont le nombre et la complexité des ressources, et peut prendre jusqu'à 72 heures.

Planning de transmission

Les données reconnues sont regroupées et transmises de façon sécurisée au support IBM les jours et aux heures prévus afin de s'assurer qu'IBM dispose des informations les plus à jour et les plus précises. TSA possède un planning de transmission par défaut que vous pouvez modifier selon vos besoins. Vous pouvez aussi effectuer des transmissions à la demande et voir l'état de la dernière transmission effectuée.

La durée d'une transmission varie en fonction de la quantité de données reconnues.

Chapitre 2. Prérequis

Pour configurer et utiliser TSA, vous devez vous assurer de respecter certains prérequis tels que les données d'identification requises pour l'environnement de reconnaissance et la configuration requise pour se connecter au support IBM.

Remarque : Tous les prérequis décrits dans les sections suivantes sont obligatoires pour TSA, à l'exception des exigences indiquées dans la section «Configuration requise pour TSA», à la page 5.

Télécharger l'image de TSA

Des images de TSA sont disponibles pour les serveurs Microsoft Hyper-V [*TSA-HYPERV-<version>*] et VMware [*TSA-VMWARE-<version>*].

Vous pouvez obtenir les instructions de téléchargement à : https://ibm.biz/TSAdemo

Configuration requise pour TSA

Avant de configurer et d'utiliser TSA, assurez-vous de respecter les prérequis suivants :

Matériel x86 64 bits
TSA doit être chargé sur des systèmes x86 64 bits.

Hyperviseur
TSA requiert VMware ESXi ou Microsoft Hyper-V.

Remarque : Il est recommandé d'utiliser une version d'ESXi ou d'Hyper-V actuellement prise en charge.

Processeur
TSA exige au minimum un processeur à quatre cœurs de 2,26 GHz.

Unité centrale
TSA exige quatre unités centrales 64 bits.

Mémoire
TSA exige 16 Go de mémoire.

Unité de stockage à accès direct (DASD)
TSA exige 150 Go de DASD.

Réseau
TSA exige une carte Ethernet 1 Gigabit.

Navigateurs web requis

Une interface utilisateur Web est utilisée pour configurer et surveiller la reconnaissance et la transmission.

TSA prend en charge les navigateurs Internet suivants :

- Mozilla Firefox V68.9.0 Extended Support Release (ESR)
- Microsoft Edge V83.0.478.54 pour Windows 10
- Google Chrome V83.0.4103.116 (64 bits)

Vous pouvez télécharger ces navigateurs à partir des sites suivants :

- Mozilla Firefox (http://www.mozilla.org/products/firefox/)

- Microsoft Edge (https://www.microsoft.com/en-us/edge)
- Google Chrome (https://support.google.com/chrome/answer/95346?hl=fr)

Configuration requise pour les connexions au support IBM

TSA peut se connecter au support IBM via une connexion directe ou via un proxy fourni par l'utilisateur qui doit être configuré pour permettre la communication avec IBM. Si vous utilisez un proxy, l'inspection TLS/SSL n'est pas prise en charge. Toutes les demandes effectuées via un proxy doivent être autorisées à parvenir directement à IBM sans terminaison TLS/SSL.

Vérifiez que votre pare-feu autorise les connexions aux adresses IP et aux noms d'hôte du serveur IBM comme expliqué dans le tableau Connexions réseau. Si votre réseau n'autorise pas l'accès aux serveurs IBM, les transactions TSA transmises au support IBM échoueront.

Tableau 1. Connexions réseau

Nom du DNS	Adresse IP	Port	Protocole
esupport.ibm.com	129.42.54.189	443	HTTPS (vers IBM)
	129.42.56.189		
	129.42.60.189		

L'environnement de serveur IBM est entièrement compatible NIST SP800-131A, prend en charge le protocole TLS 1.2, les fonctions de hachage SHA-256 ou supérieures et les clés RSA d'au moins 2048 bits.

Remarque : L'inspection SSL n'est pas supportée ; si vous l'utilisez sur le proxy, désactivez-la pour ces flux.

Dans le cas des proxies Blue Coat, désactivez "Détection de protocole" pour les serveurs IBM. Ajoutez les règles de configuration suivantes :

- url.domain=esupport.ibm.com detect_protocol (none)
- url.address=129.42.54.189 detect_protocol (none)
- url.address=129.42.56.189 detect_protocol (none)
- url.address=129.42.60.189 detect_protocol (none)

Données d'identification et configuration logicielle requises pour l'environnement de reconnaissance

Pour reconnaître les terminaux ou les ressources de votre environnement, TSA doit avoir accès à ces ressources. Il est donc recommandé de créer un compte de service sur chaque ressource que TSA pourra spécialement utiliser lorsqu'il tentera d'accéder à la ressource concernée.

Après avoir créé un compte de service sur une ressource, vous devez définir et tenir à jour les données d'identification sur TSA qui correspondent à celles définies sur la ressource pour ce compte de service. TSA utilise ces données d'identification pour accéder à la ressource. Les données d'identification requises varient selon l'environnement et le type de ressource que vous voulez reconnaître mais elles incluent généralement un nom d'utilisateur et un mot de passe ou une clé SSH. Certaines ressources requièrent également une configuration logicielle spécifique.

Type de données d'identification	Informations d'accès
Système informatique	**Nom d'utilisateur :** Nom d'utilisateur permettant d'accéder à l'équipement. **Mot de passe / phrase de passe :** Mot de passe / phrase de passe permettant d'accéder à l'équipement. **Type d'authentification :** Type d'authentification permettant d'accéder à l'équipement. • **Mot de passe** - Utilisez le mot de passe fourni. • **Infrastructure PKI** - Utilisez la clé SSH associée à l'ensemble de périmètres spécifique.
Système informatique (Windows)	**Nom d'utilisateur :** Nom d'utilisateur permettant d'accéder au système informatique Windows. **Mot de passe :** Mot de passe permettant d'accéder au système informatique Windows.
Elément réseau (SNMP)	**Nom de communauté :** Nom de communauté de l'équipement.
Elément réseau (SNMPV3)	**Nom d'utilisateur :** Nom d'utilisateur permettant d'accéder à l'équipement. **Mot de passe :** Mot de passe permettant d'accéder à l'équipement. **Mot de passe privé :** Mot de passe utilisé si le chiffrement de données est paramétré pour SNMP. **Protocole d'authentification :** Type de protocole d'authentification utilisé par le protocole SNMP. • Aucun • MD5 • SHA
Autre (équipement Cisco)	**Nom d'utilisateur :** Nom d'utilisateur permettant d'accéder à l'équipement Cisco. **Mot de passe :** Mot de passe permettant d'accéder à l'équipement Cisco. **Mot de passe d'activation :** Mot de passe d'activation de l'équipement Cisco.

Type de données d'identification	Informations d'accès
Autre (CiscoWorks)	**Nom d'utilisateur :** Nom d'utilisateur permettant d'accéder au serveur CiscoWorks. **Mot de passe :** Mot de passe permettant d'accéder au serveur CiscoWorks.

Remarque : Pour plus d'informations sur les données d'identification et la configuration logicielle requise, reportez-vous au Guide de l'Assistant de la configuration de TSA (Technical Support Appliance).

Chapitre 3. Installer IBM Technical Support Appliance (TSA)

TSA comprend des logiciels préinstallés. Il est empaqueté et distribué sous forme d'image pour les installations VMware ou sous forme d'image VHDX pour les installations Microsoft Hyper-V. Pour VMware, TSA peut être installé soit avec VMware vSphere Client, soit avec l'interface Web VMware (pour ESXi). Pour Hyper-V, TSA peut être installé avec l'Hyper-V Manager. Cette section décrit les étapes à suivre pour installer TSA avec l'une ou l'autre de ces méthodes.

Installation avec l'interface web de VMware ESXi

Avant de commencer
TSA exige de charger VMware ESXi 6.5 ou version ultérieure pour contrôler le matériel.

Pourquoi et quand exécuter cette tâche
Suivez ces étapes pour installer l'image de TSA.

Procédure

1. Connectez-vous au système ESXi via l'interface web VMware ESXi.
2. Cliquez sur **Create/Register VM**. L'assistant **New virtual machine** s'affiche.

Figure 1. Création / enregistrement d'une machine virtuelle

3. Sur l'écran **Select creation type**, sélectionnez l'option **Déployer une machine virtuelle à partir d'un fichier OVF ou OVA** et cliquez sur **Suivant**.

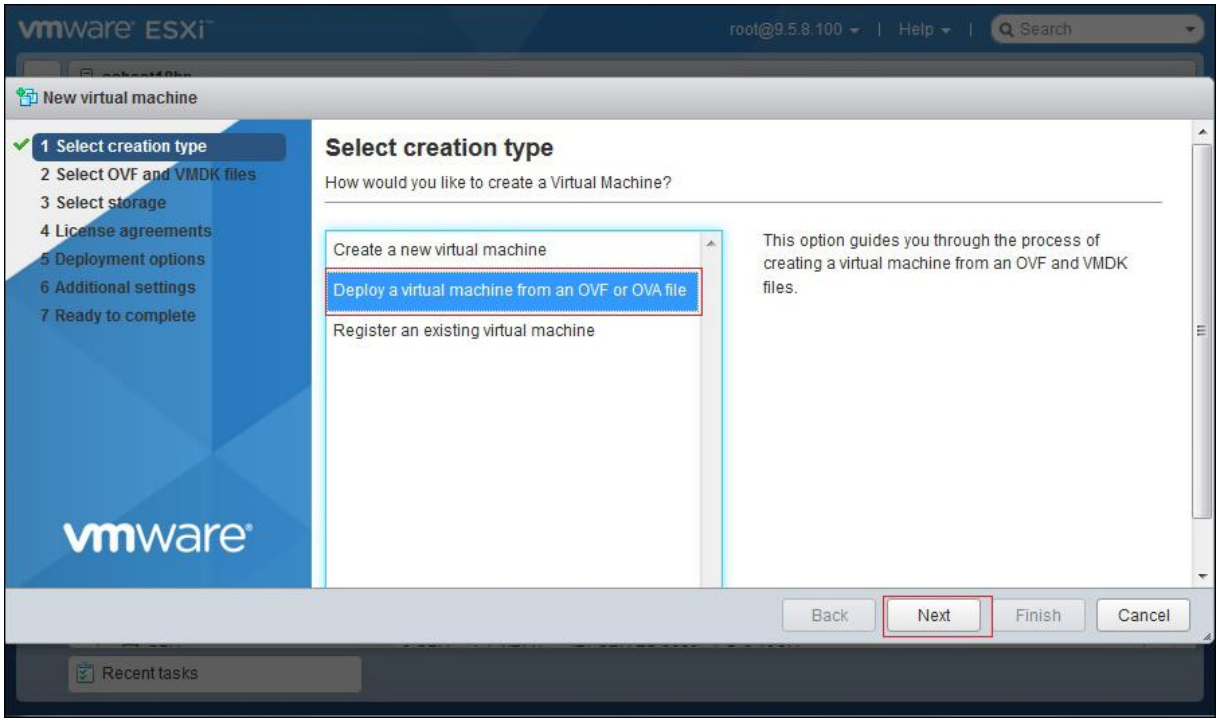

Figure 2. Sélection du type de création

4. Sur l'écran **Select OVF and VMDK files**, entrez un nom pour votre machine virtuelle ou utilisez la valeur par défaut.

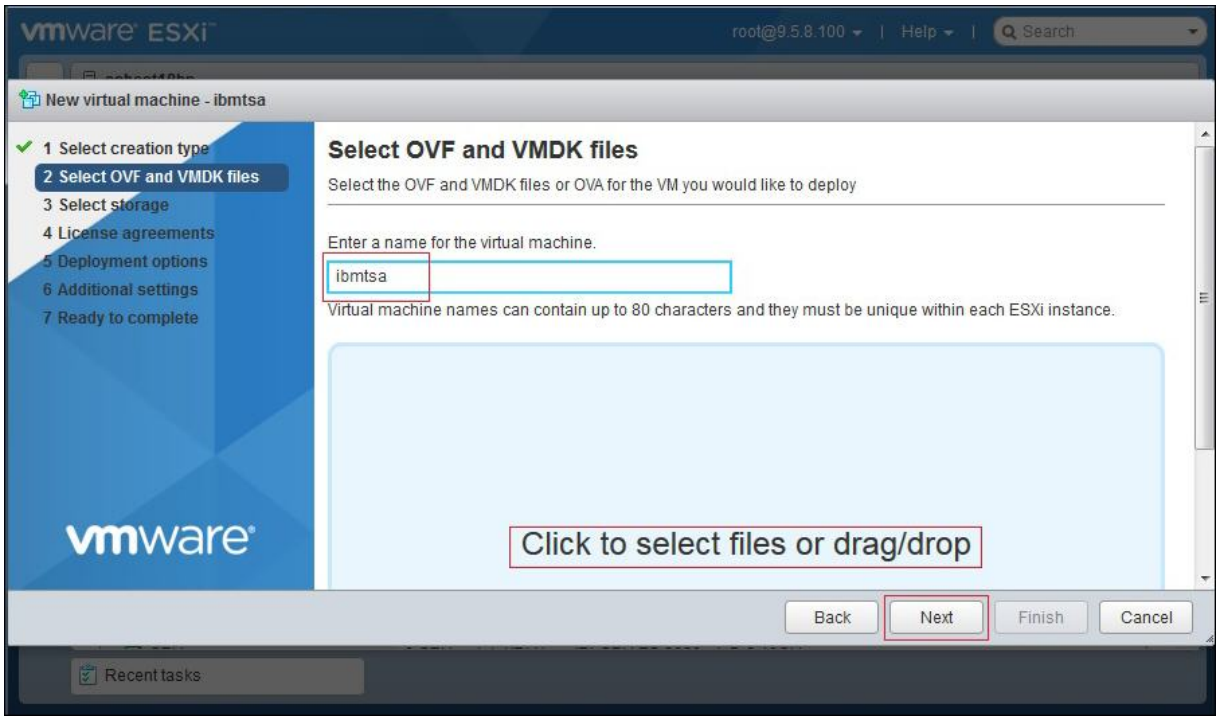

Figure 3. Sélection des fichiers OVF et VMDK

5. Cliquez dans la zone **Cliquez pour sélectionner les fichiers ou faites glisser/déposer** et sélectionnez le fichier image que vous avez téléchargé depuis Fix Central, puis cliquez sur **Suivant**.
6. Dans la liste qui s'affiche sur l'écran **Select storage**, sélectionnez un magasin de données où stocker la configuration et les fichiers disque, puis cliquez sur **Suivant**.

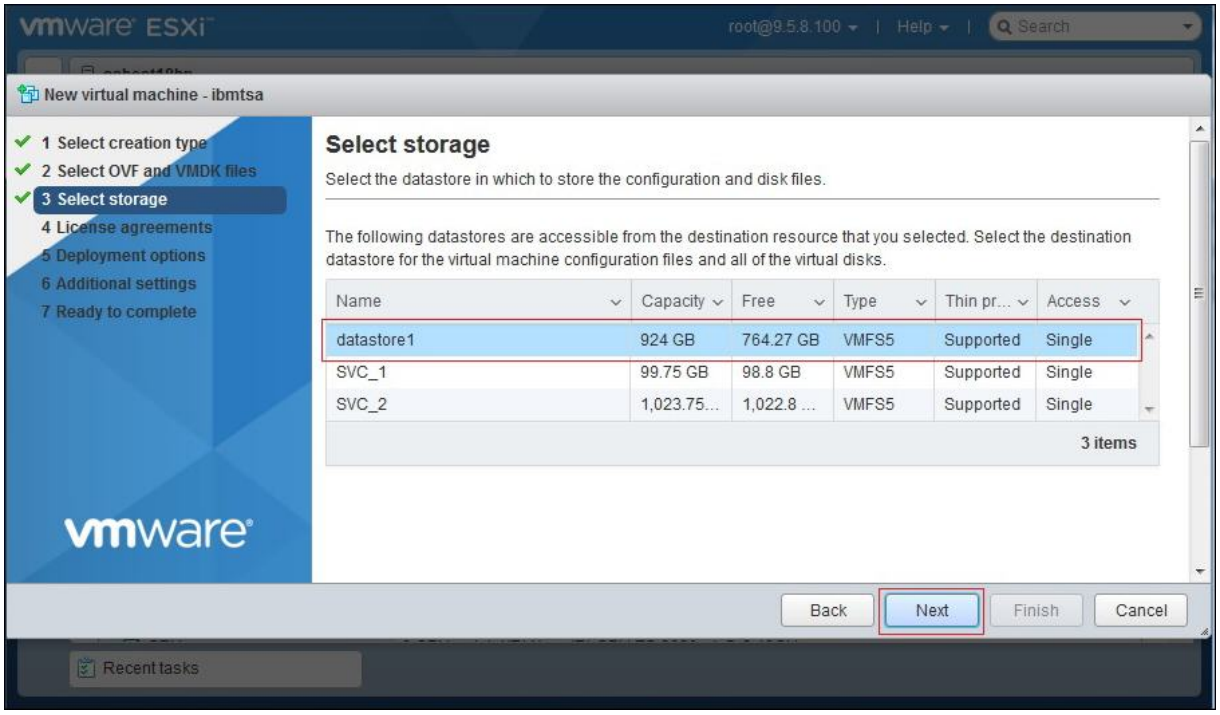

Figure 4. Sélection du stockage

7. Sur l'écran **Deployment options**, sélectionnez les mappages réseau dans la liste déroulante **Réseau de machines virtuelles**.

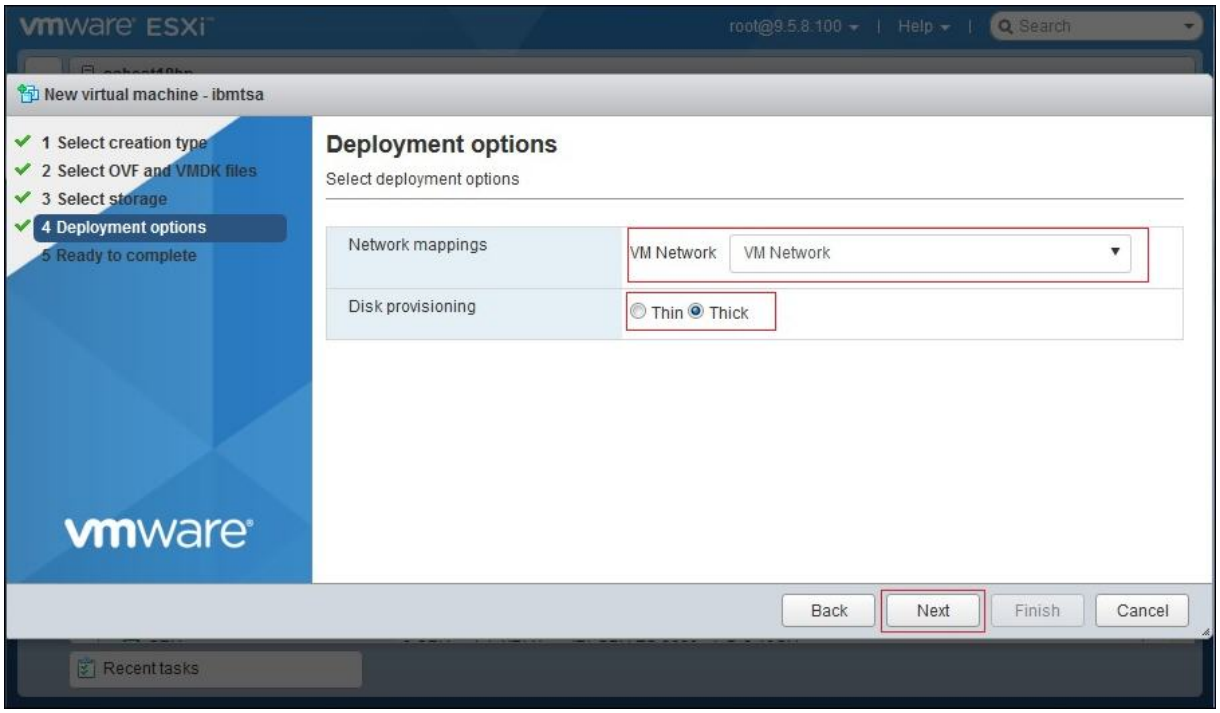

Figure 5. Options de déploiement

8. Sélectionnez l'option de provisionnement de disque **Thick**, puis cliquez sur **Suivant**.
9. Sur l'écran **Ready to complete**, passez en revue tous les paramètres que vous avez indiqués. Si vous voulez en modifier certains, cliquez sur **Précédent** et modifiez les options concernées. Si les options choisies vous conviennent, cliquez sur **Finish**.

   Important : N'actualisez pas la page de votre navigateur tandis que la machine virtuelle est en cours de déploiement.

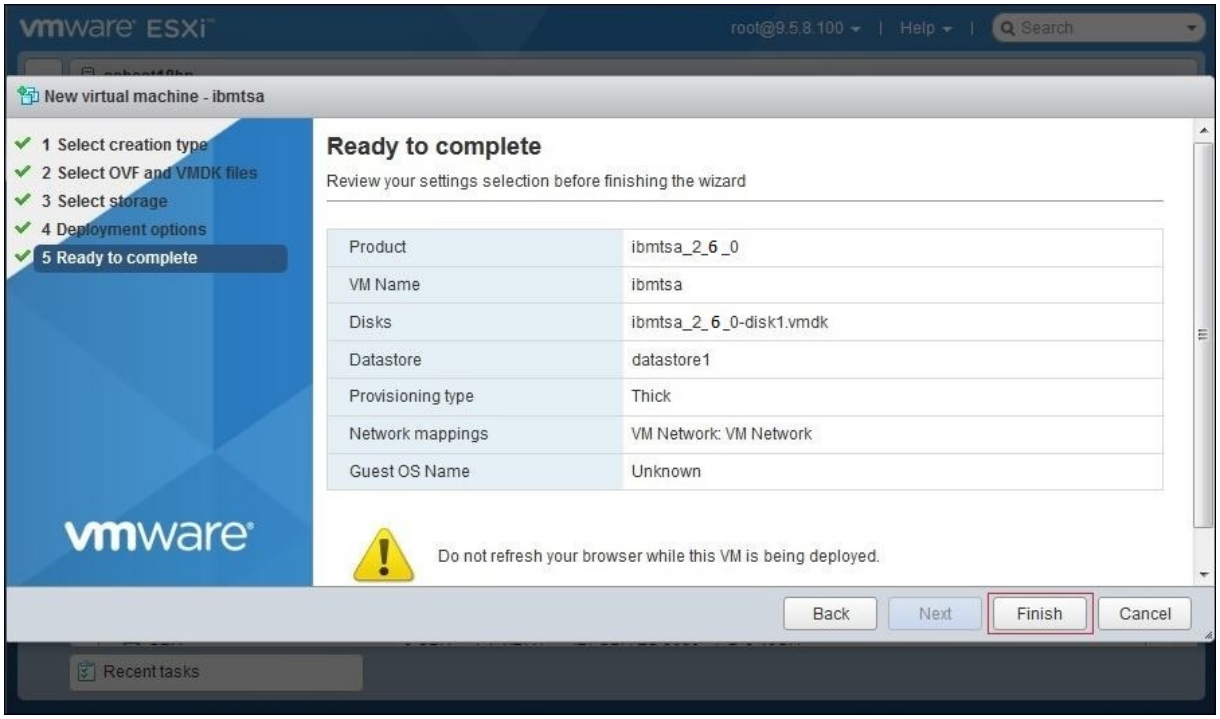

Figure 6. Revue des paramètres sélectionnés

La machine virtuelle TSA est installée sur votre système.

10. Dans la console TSA, entrez **`tsausr`** comme **identifiant de connexion IBM TSA** et **`configTsa`** comme **mot de passe**.
11. Obligatoire : pour changer le mot de passe de connexion, suivez les étapes décrites à la section «Changer le mot de passe tsausr (obligatoire)», à la page 19.
12. Pour terminer l'installation, suivez les étapes décrites à la section «Configurer les données du réseau», à la page 19.

Installer TSA sur Microsoft Hyper-V

Avant de commencer
Avant d'installer et d'utiliser TSA sur Hyper-V, assurez-vous que les conditions préalables ci-dessous sont satisfaites.

- Hyper-V Server 2012, 2016 ou 2019
- Hyper-V Manager
- Un commutateur réseau virtuel a été créé via Hyper-V Manager

Pourquoi et quand exécuter cette tâche
Suivez les étapes ci-dessous pour installer TSA sur Hyper-V.

Procédure

Pour installer TSA sur Hyper-V, procédez comme suit :

1. Après avoir téléchargé l'image de TSA, extrayez le fichier *ibmtsa_2700.vhdx* de l'archive *ibmtsa_2700.zip* et déplacez-le dans un répertoire du serveur Hyper-V.
2. Démarrez Hyper-V Manager et connectez-vous au serveur Hyper-V à partir du système client.
3. Cliquez sur **Parcourir** et sélectionnez l'image qui est enregistrée sur votre système.

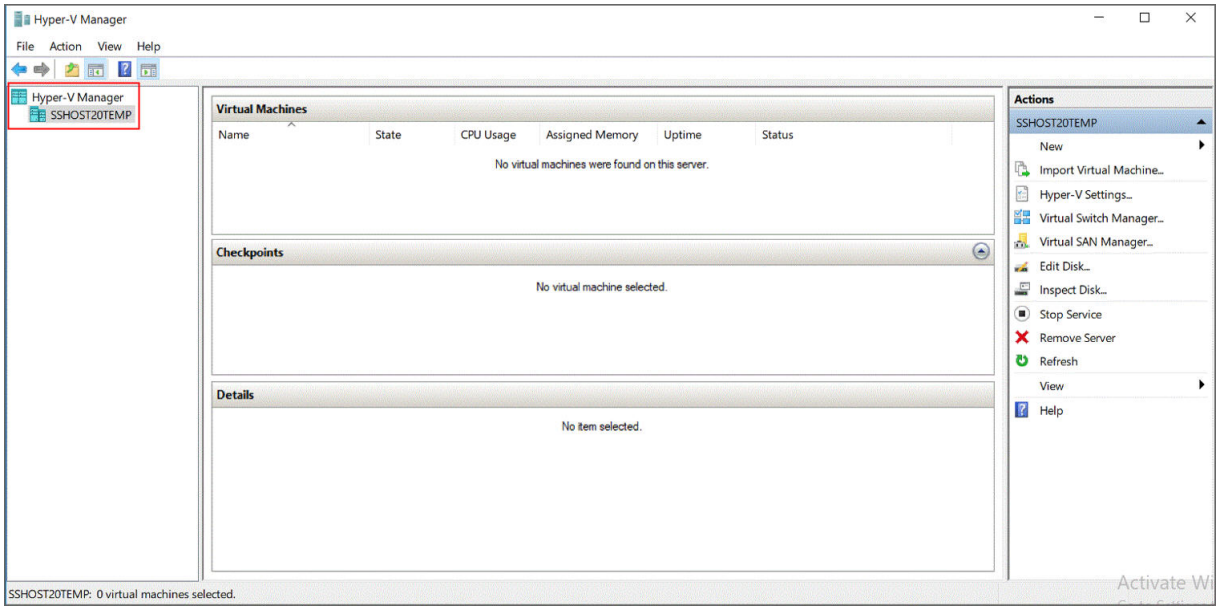

Figure 7. Hyper-V Manager

4. Dans le menu **Action**, sélectionnez **New** → **Virtual Machine**. L'assistant **New Virtual Machine Wizard** s'affiche.
5. Entrez le **Nom** de la nouvelle machine virtuelle et cliquez sur **Suivant**.

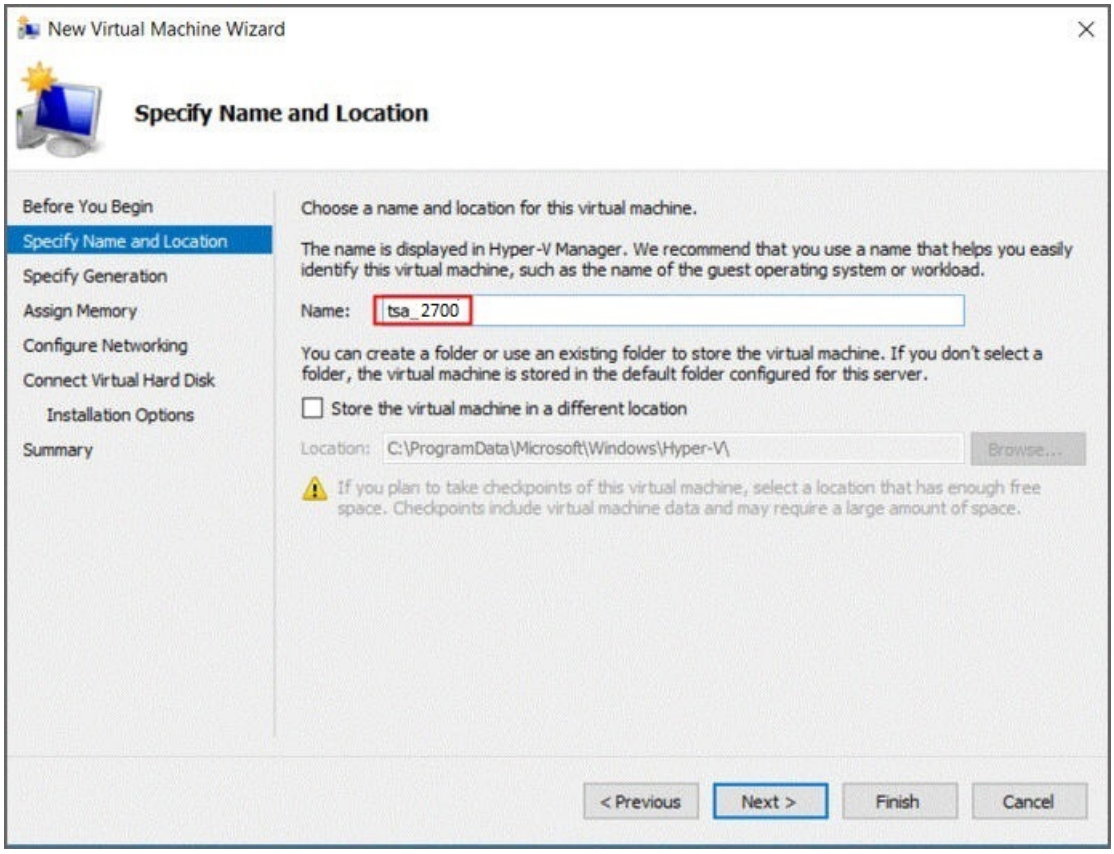

Figure 8. Nom de la machine virtuelle

6. Sélectionnez **Generation 1** comme génération de la machine virtuelle et cliquez sur **Suivant**.

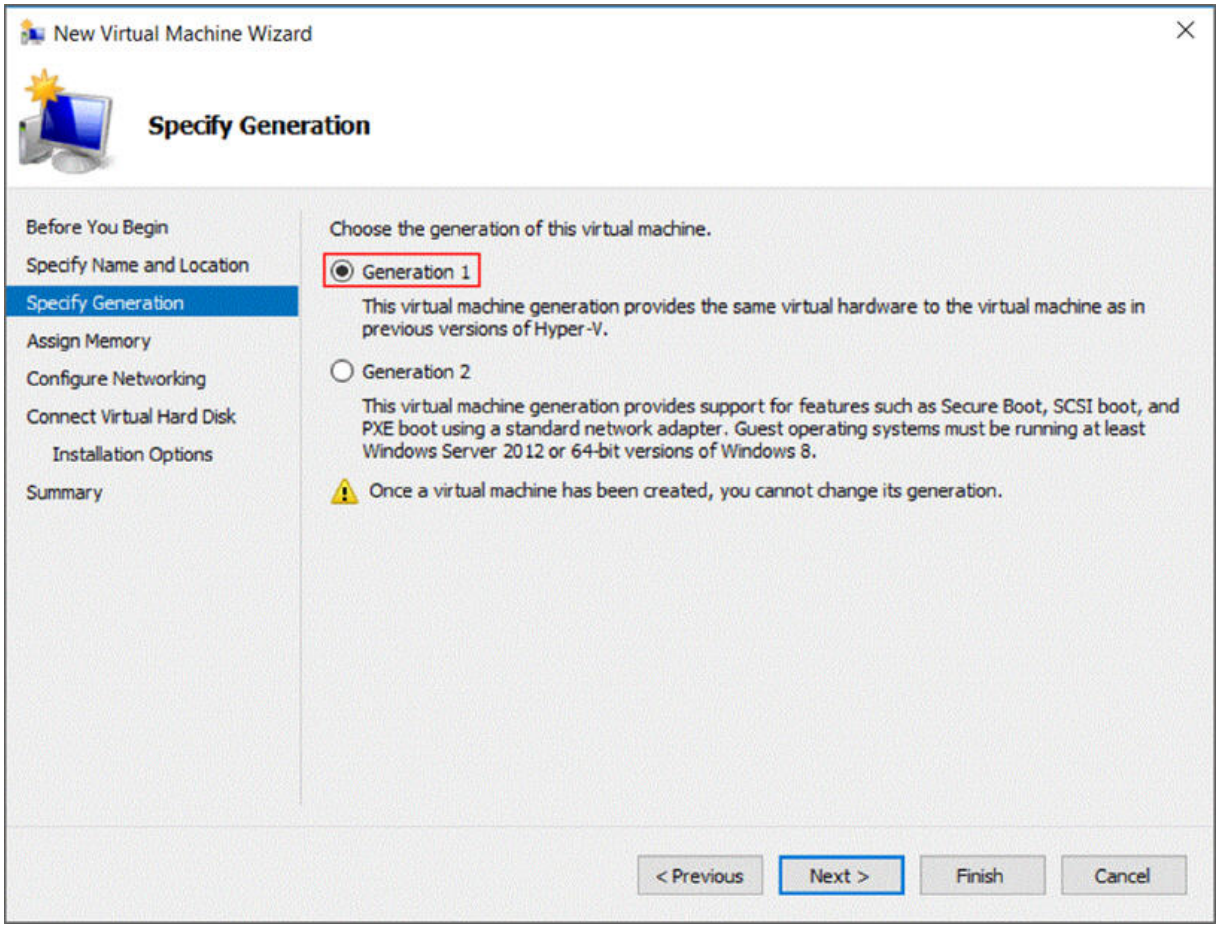

Figure 9. Indication de la génération

7. Entrez *16384* Mo comme **Mémoire au démarrage** et cliquez sur **Suivant**.

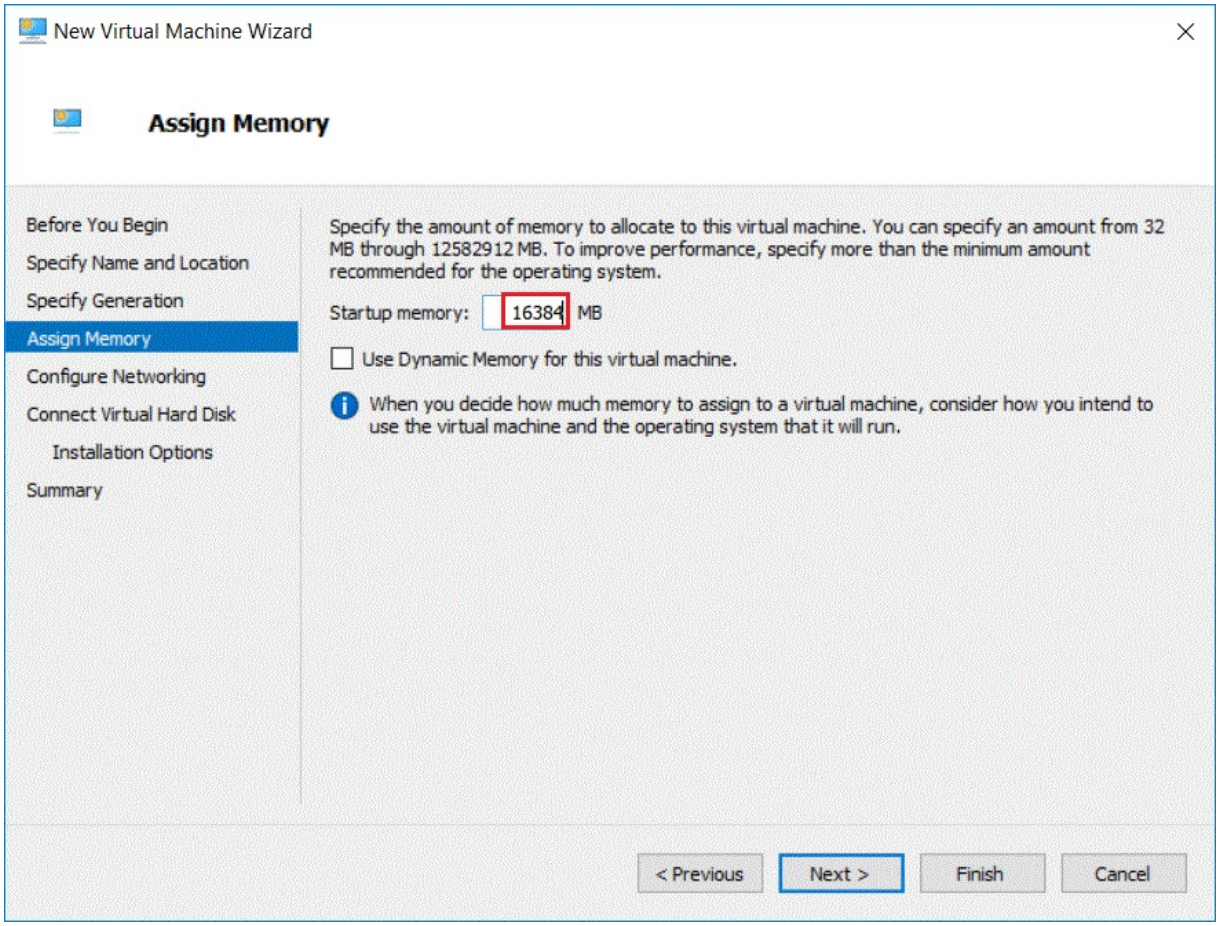

Figure 10. Mémoire au démarrage

8. Sélectionnez un commutateur virtuel préconfiguré et cliquez sur **Suivant**.

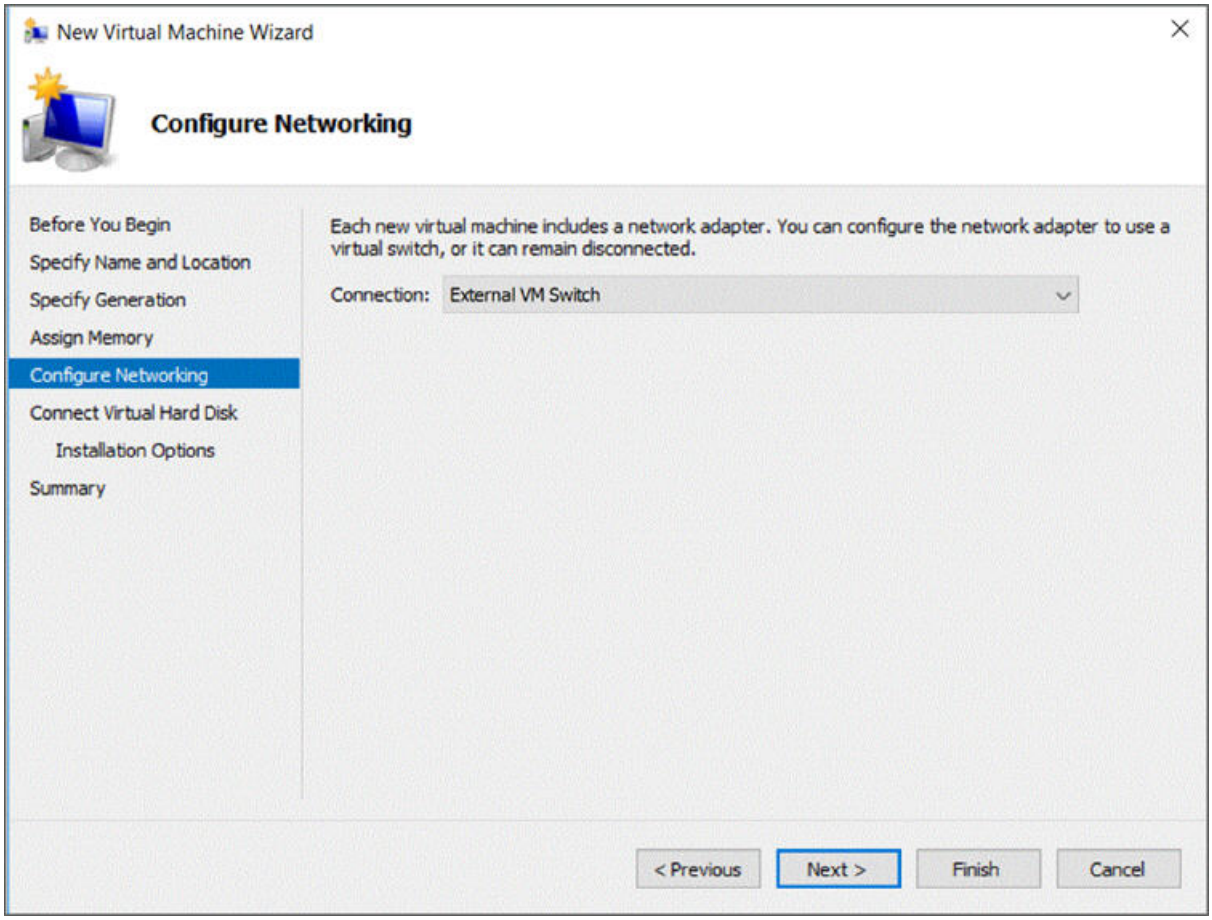

Figure 11. Configuration de la mise en réseau

9. Sélectionnez l'option **Utiliser un disque dur virtuel existant** et recherchez le fichier *ibmtsa_2700.vhdx* que vous avez copié sur le serveur Hyper-V à l'étape 2, puis cliquez sur **Suivant**.

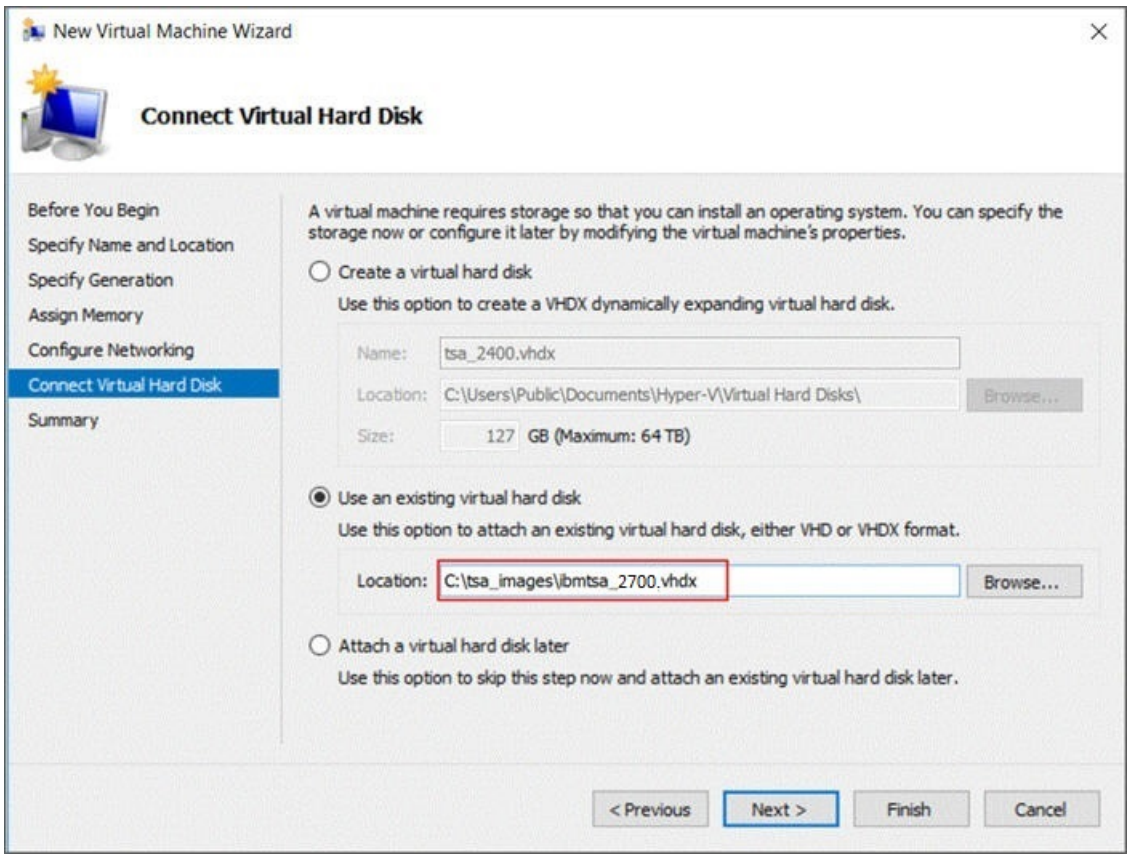

Figure 12. Connexion d'un disque dur virtuel

10. Sur la page **Récapitulatif**, passez en revue les paramètres puis cliquez sur **Finish**.

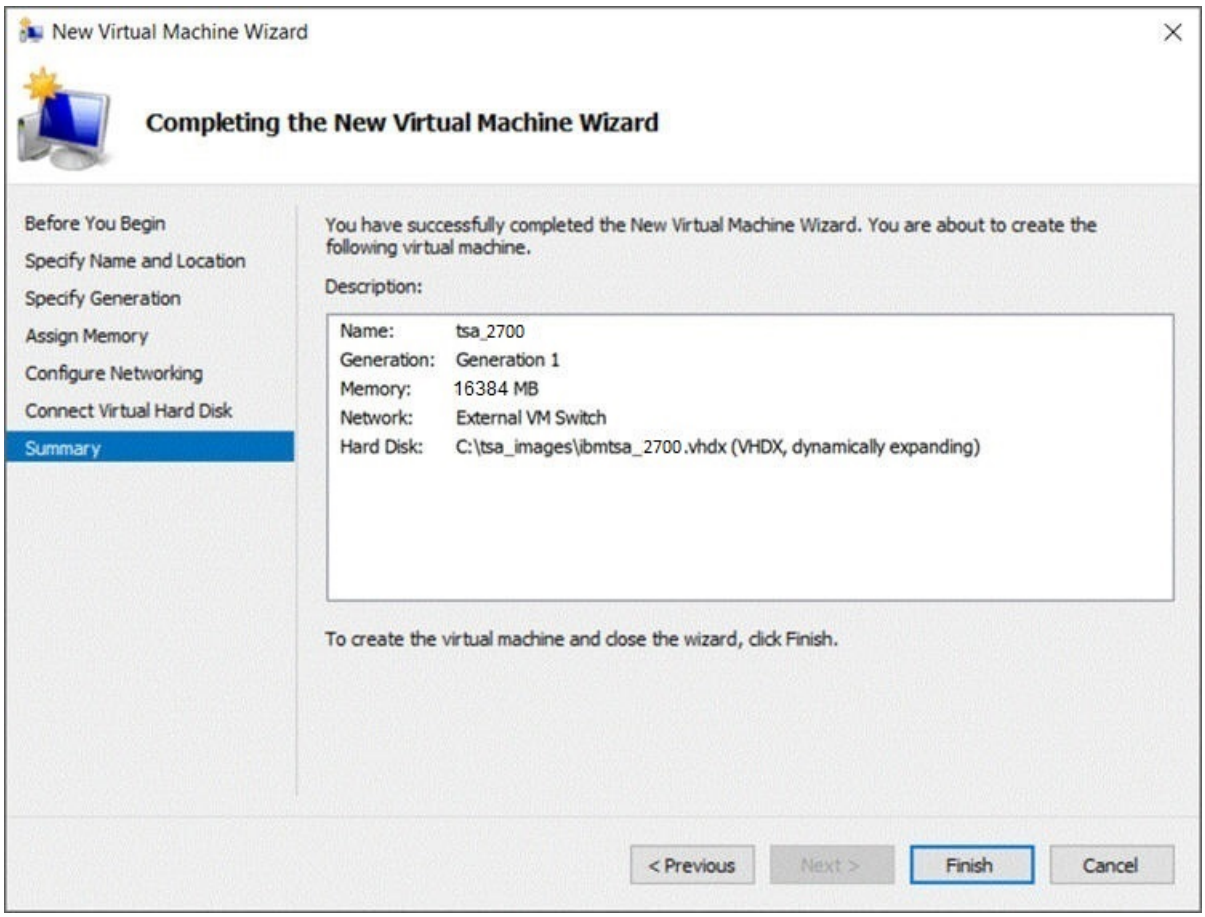

Figure 13. Récapitulatif

11. La nouvelle machine virtuelle est ajoutée sous Hyper-V Manager. Sélectionnez la machine virtuelle, allez dans le menu **Action** puis cliquez sur **Start**.

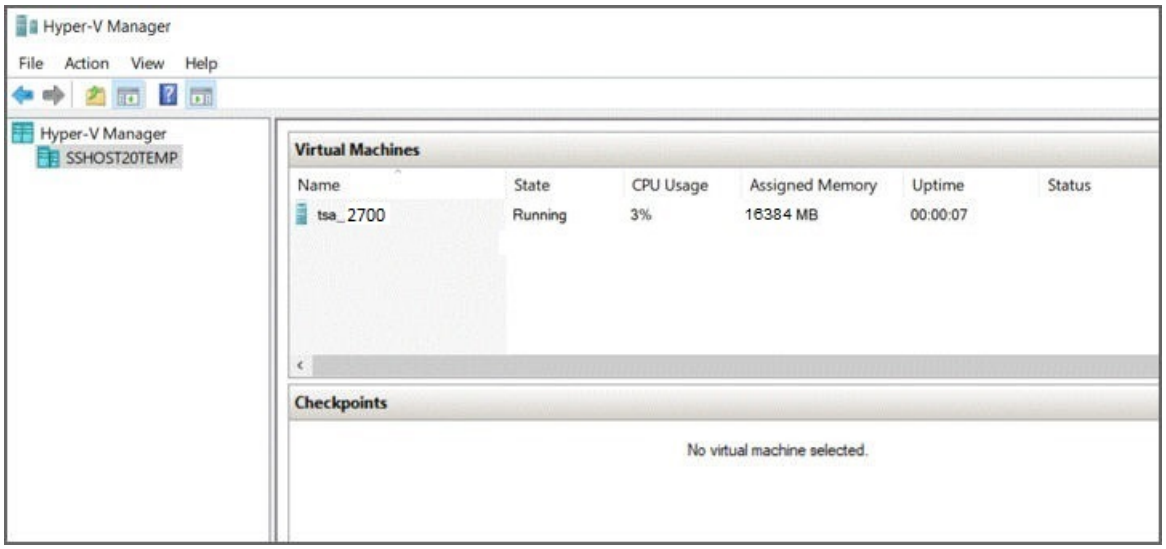

Figure 14. Hyper-V Manager

12. Dans le menu **Action**, sélectionnez l'option **Connect** pour démarrer une session de console. Dans la console TSA, entrez **`tsausr`** comme **identifiant de connexion IBM TSA** et **`configTsa`** comme **mot de passe**.
13. Obligatoire : pour changer le mot de passe de connexion, suivez les étapes décrites à la section «Changer le mot de passe tsausr (obligatoire)», à la page 19.

14. Pour terminer l'installation, suivez les étapes décrites à la section «Configurer les données du réseau», à la page 19.

Changer le mot de passe *tsausr* (obligatoire)

Pour des raisons de sécurité, il est recommandé de changer la valeur initiale du mot de passe *tsausr*. Pour changer le mot de passe *tsausr*, procédez comme suit.

Procédure

1. Sélectionnez l'option **2) Changer le mot de passe tsausr** dans le **Menu de configuration de TSA**.

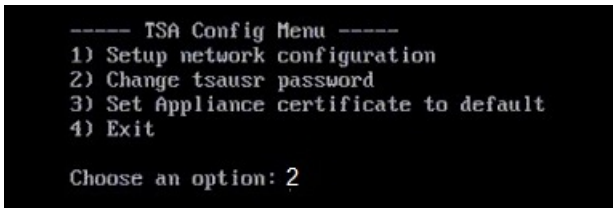

Figure 15. Modification du mot de passe

2. Entrez le nouveau mot de passe à l'invite **Nouveau mot de passe**. Entrez le même mot de passe à l'invite **Retaper le nouveau mot de passe**. Le nouveau mot de passe doit comporter au moins 7 caractères.

Figure 16. Nouveau mot de passe

Configurer les données du réseau

Procédure

1. Sélectionnez l'option **1) Paramétrer la configuration réseau** dans le **Menu de configuration de TSA**.

Figure 17. Paramétrer la configuration réseau

2. Entrez les données de configuration réseau suivantes.

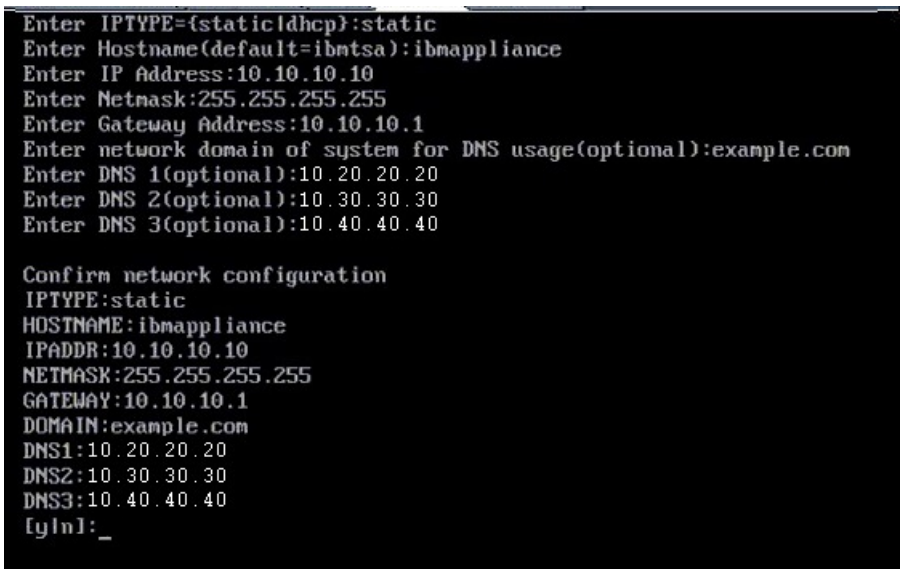

Figure 18. Configuration réseau

a) **Entrez TYPEIP = {statique|dhcp}**. Entrez `statique` ou `dhcp`. Si vous avez entré `statique`, suivez les étapes ci-dessous, sinon suivez les étapes de configuration `dhcp` à la section Annexe C, «Configurer les données du réseau DHCP», à la page 135

TYPEIP : statique

Entrer nom d'hôte(valeur par défaut=ibmtsa). Vous pouvez modifier le nom d'hôte par défaut. Assurez-vous que le nom d'hôte utilisé est unique.

Entrer l'adresse IP.

Entrer le masque de réseau et **Entrer la passerelle**.

Entrer le domaine de réseau du système pour utilisation DNS (facultatif).

Entrer DNS 1(facultatif), **Entrer DNS 2(facultatif)** et **Entrer DNS 3 (facultatif)**.

Les données de configuration réseau indiquées s'affichent pour confirmation.

b) Entrer **[o|n]** pour confirmer ou annuler la configuration réseau. Si vous entrez **o**, la configuration réseau est enregistrée et le système redémarre automatiquement.

Remarque : Si une configuration est incorrecte, vous pouvez en modifier les données. Entrez **n** pour ignorer les paramètres actuels et recommencez la configuration à partir de l'étape «2.a», à la page 20

c) Le système redémarre 15 secondes après afin que la nouvelle configuration réseau soit prise en compte.

d) Accédez à TSA depuis le navigateur en utilisant une connexion HTTP sécurisée avec le nom d'hôte ou l'adresse IP entré(e) ci-dessus.
Exemple : `https://<nom d'hôte | adresse IP>.`

Remarque : Lors de la première connexion, il se peut que votre navigateur affiche une exception de sécurité. Vous devez accepter le certificat de sécurité et poursuivre la procédure de connexion à TSA.

Remarque : Pour modifier les paramètres réseau de base de TSA via l'interface utilisateur, suivez les étapes de la section «Configurer les paramètres réseau de base», à la page 36. Pour configurer les paramètres réseau avancés, suivez les étapes de la section «Configurer les paramètres réseau avancés», à la page 37.

3. Configurez Technical Support Appliance en suivant les étapes décrites dans Chapitre 4, «Configurer Technical Support Appliance», à la page 23

Résultats

Une fois la configuration de TSA terminée, rendez-vous au Chapitre 5, «Configurer la découverte et la transmission à IBM», à la page 51

Chapitre 4. Configurer Technical Support Appliance

Pourquoi et quand exécuter cette tâche
Suivez les étapes ci-dessous pour une prise en main rapide de TSA. Si vous ne l'avez pas encore fait, consultez le Chapitre 2, «Prérequis», à la page 5.

Procédure

1. «Se connecter à Technical Support Appliance», à la page 23
2. «Accepter le contrat de licence», à la page 26
3. «Utiliser l'Assistant de configuration pour la configuration initiale», à la page 27
   a) «Mise en place de la Connectivité IBM», à la page 28
   b) «Enregistrer Technical Support Appliance», à la page 30
   c) «Régler l'horloge», à la page 32
   d) «Mise en place du planning de transmission», à la page 33
   e) «Mettre à jour Technical Support Appliance», à la page 34
4. «Configurer les paramètres réseau», à la page 35
5. «Mise en place des certificats», à la page 43.
6. Facultatif : Annexe D, «Comptes d'utilisateur et groupes d'utilisateurs», à la page 137

Que faire ensuite
Lorsque vous avez fini de configurer TSA, reportez-vous au Chapitre 5, «Configurer la découverte et la transmission à IBM», à la page 51 pour découvrir comment exécuter d'autres tâches.

Se connecter à Technical Support Appliance

Procédure

1. Ouvrez un navigateur Internet depuis un système disposant d'un accès réseau à TSA.
   Pour plus d'informations, voir la section «Navigateurs web requis», à la page 5.
2. Entrez l'adresse URL suivante dans la barre d'adresse du navigateur :

   ```
   https://<nom d'hôte ou adresse IP>
   ```

   Remarque : Si le `<nom d'hôte>` ne fonctionne pas, essayez l'adresse IP affectée de TSA.
3. Lorsque vous y êtes invité, entrez les informations suivantes :

   ID utilisateur :
   Entrez `admin`

   Mot de passe :
   Entrez le mot de passe administrateur de TSA.

   Le mot de passe initial est `passw0rd`. Vous devez le modifier après vous être connecté à TSA.

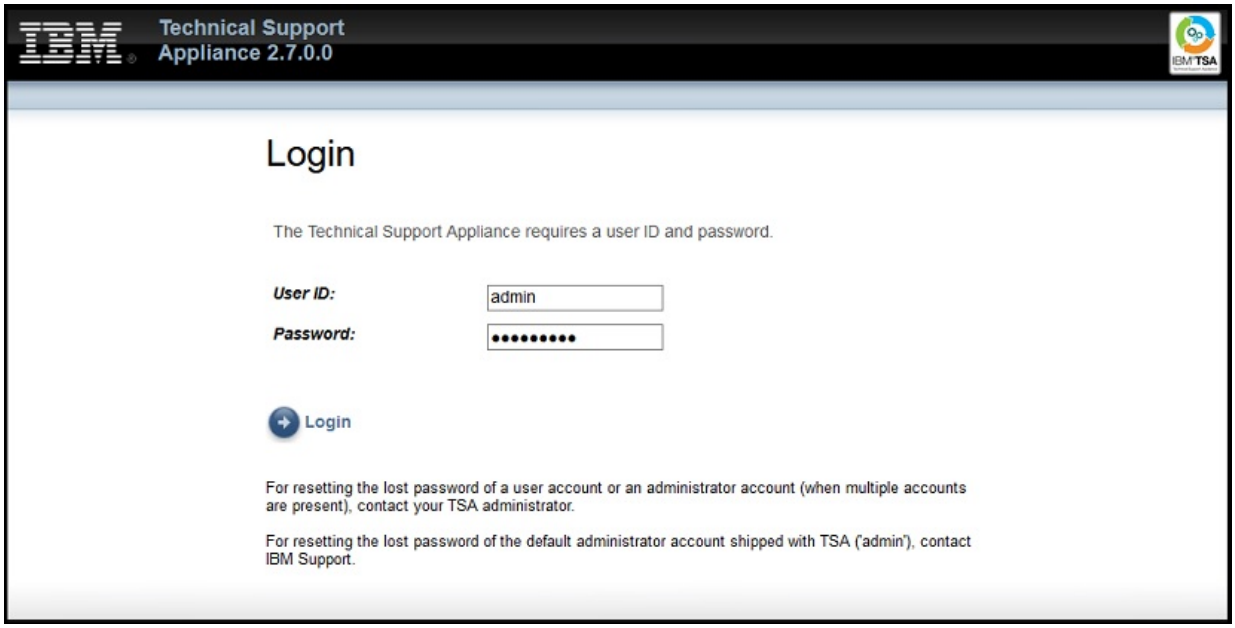

Figure 19. Connexion

La page **Changer le mot de passe** s'affiche lors de votre première connexion.

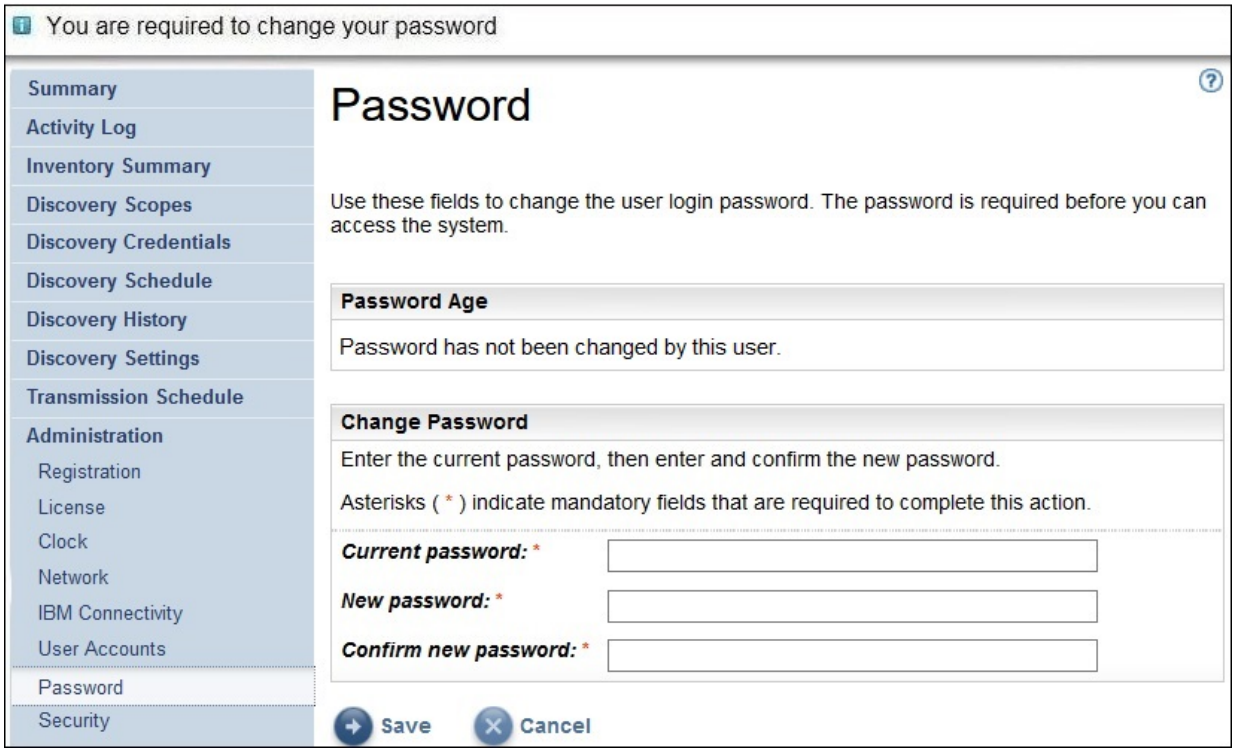

Figure 20. Modification du mot de passe

Pour changer le mot de passe initial, procédez comme suit :

a) Entrez un nouveau mot de passe.

Le mot de passe doit respecter les règles suivantes :

- 8 caractères minimum
- Au moins un caractère alphabétique et un caractère non alphabétique
- Ne doit pas contenir le nom de l'utilisateur

- Doit être différent des huit mots de passe précédents
- Doit être modifié au moins une fois tous les 90 jours, mais pas plus d'une fois par jour.

b) Entrez à nouveau le nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe**.

Avant que le mot de passe ne soit enregistré, les deux saisies sont comparées afin de vérifier qu'elles sont bien identiques.

c) Enregistrez le nouveau mot de passe pour référence ultérieure.

Important : Il n'est pas possible de récupérer un mot de passe donc si vous avez perdu ou oublié votre mot de passe, vous ne pouvez pas vous connecter à TSA pour modifier les données d'identification. Si vous perdez ou oubliez votre mot de passe pour un compte d'utilisateur ou un compte administrateur (si vous avez plusieurs comptes), contactez votre administrateur TSA. Si vous perdez ou oubliez votre mot de passe pour le compte administrateur par défaut (fourni avec TSA), contactez le support IBM.

d) Cliquez sur **Enregistrer**. Lors de la première connexion, la page **Contrat de licence** s'affiche.

Accepter le contrat de licence

Lisez et acceptez le contrat de licence pour continuer.

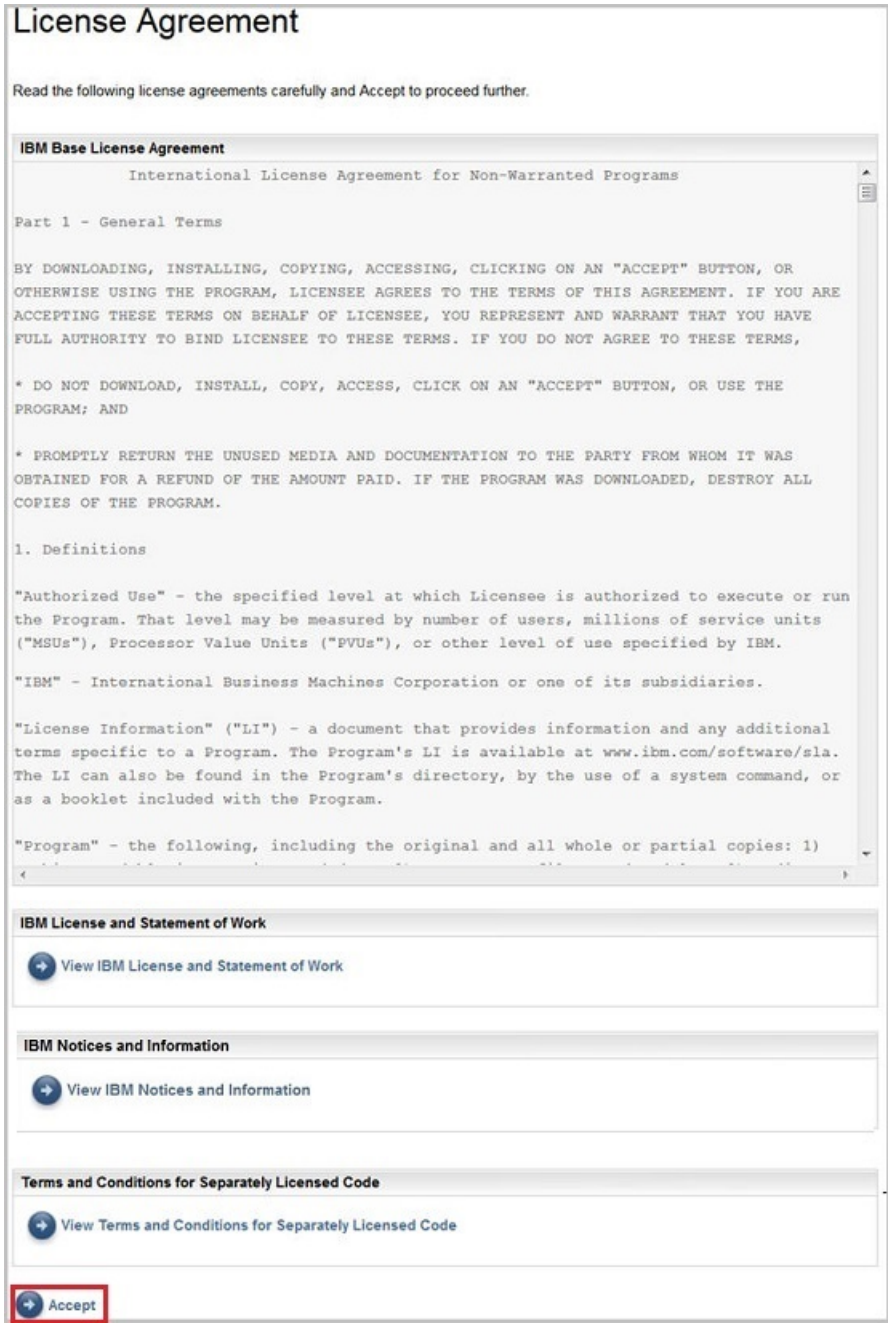

Figure 21. Contrat de licence

Le Contrat de licence comprend les éléments suivants :

- **Contrat de licence de base IBM** : affiche le contrat de licence de base IBM.
- **Licence IBM et Descriptif des prestations** : cliquez sur **Voir la licence IBM et le Descriptif des prestations** pour afficher les documents correspondants.

  Remarque : TSA est conforme au RGPD [UE/2016/679]. Vous pouvez consulter les informations de conformité au RGPD dans la section **Licence IBM et Descriptif des prestations**.
- **Avis et informations d'IBM** : cliquez sur **Voir les avis et les informations d'IBM** pour afficher les informations correspondantes.

- **Dispositions relatives au code à licence distincte** : cliquez sur **Voir les dispositions relatives au code à une licence distincte** pour afficher les dispositions correspondantes.

Cliquez sur **Accepter** pour accepter le contrat. Dès que vous avez accepté le contrat de licence, l'**Assistant de configuration** apparaît pour vous permettre de configurer TSA. Vous pouvez soit l'utiliser pour configurer TSA soit le quitter et configurer les réglages de TSA selon vos besoins.

Remarque : Dans le panneau de navigation, cliquez sur **Administration** > **Licence** pour afficher le dernier contrat de licence que vous avez accepté.

Concepts associés

«Utiliser l'Assistant de configuration pour la configuration initiale», à la page 27
Utilisez l'**Assistant de configuration** pour créer la configuration initiale du TSA.

«Configurer Technical Support Appliance», à la page 125
Si vous omettez de configurer des réglages dans l'**Assistant de configuration**, vous pouvez toujours revenir dessus dans le menu de navigation de gauche de TSA.

Utiliser l'Assistant de configuration pour la configuration initiale

Utilisez l'**Assistant de configuration** pour créer la configuration initiale du TSA.

Une fois que vous avez accepté le contrat de licence, l'**Assistant de configuration** s'affiche automatiquement.

Remarque : Pour démarrer l'**Assistant de configuration**, dans le panneau de navigation, cliquez sur **Outils** > **Assistant de configuration** > **Démarrer l'assistant de configuration**.

Figure 22. Assistant de configuration

L'**Assistant de configuration** vous fait passer par les étapes suivantes :

- «Mise en place de la Connectivité IBM», à la page 28
- «Enregistrer Technical Support Appliance», à la page 30
- «Régler l'horloge», à la page 32
- «Mise en place du planning de transmission», à la page 33
- «Mettre à jour Technical Support Appliance», à la page 34

Remarque : Si vous quitter l'**Assistant de configuration** ou omettez d'y configurer des réglages, vous pouvez toujours revenir dessus dans le menu de navigation de TSA. Pour plus d'informations sur la configuration de ces réglages, consultez Annexe B, «Configurer Technical Support Appliance», à la page 125.

Mise en place de la Connectivité IBM

Procédure

Vous pouvez voir, changer et tester la configuration que TSA utilise pour se connecter à IBM.

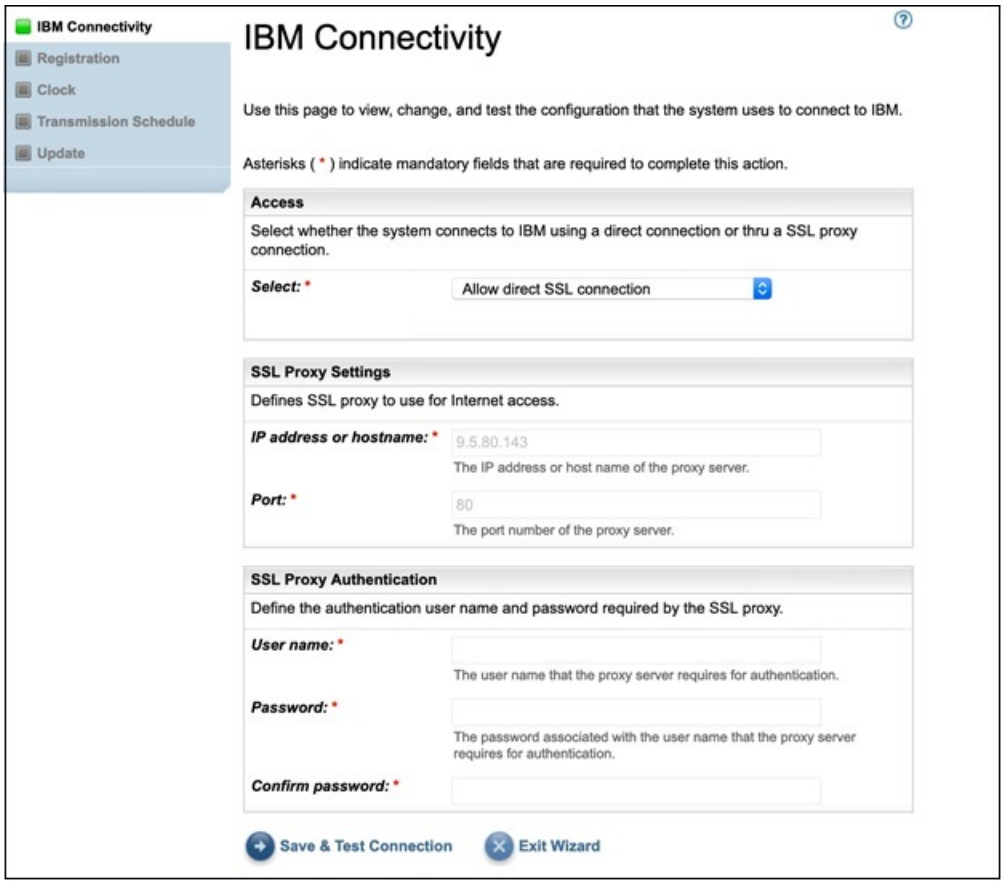

Figure 23. Connectivité IBM

1. Dans le panneau **Accès**, sélectionnez l'un des types d'accès Internet suivants :

   Autoriser une connexion SSL directe
   TSA se connecte à IBM via une connexion directe.

   Utiliser une connexion proxy SSL
   TSA se connecte à IBM via une connexion proxy SSL.

   Utiliser une connexion proxy SSL d'authentification
   TSA se connecte à IBM via une connexion proxy SSL qui nécessite une authentification.

2. Si vous avez sélectionné **Utiliser une connexion proxy SSL** ou **Utiliser une connexion proxy SSL d'authentification**, spécifiez les informations suivantes pour le serveur proxy.

   Adresse IP ou nom d'hôte
   Adresse IP ou nom d'hôte du serveur proxy.

   Remarque : Le nom d'hôte saisi ne doit pas contenir de trait de soulignement ("_").

   Port
   Numéro de port du serveur proxy.

3. Si vous avez sélectionné **Utiliser une connexion proxy SSL d'authentification**, spécifiez les informations suivantes pour le serveur proxy :

   Nom d'utilisateur
   Nom d'utilisateur requis par le serveur proxy pour l'authentification.

Mot de passe
Mot de passe associé au nom d'utilisateur requis par le serveur proxy pour l'authentification.

Confirmer le mot de passe
Entrez à nouveau le mot de passe. Les deux mots de passe saisis sont comparés afin de vérifier qu'ils correspondent avant que le mot de passe soit enregistré.

Que faire ensuite

- Cliquez sur **Enregistrer et tester la connexion** pour sauvegarder et tester la connexion spécifiée. Si la connexion réussit, le bouton **Continuer** apparaît.
- Cliquez sur **Continuer** pour aller à la page **Enregistrement**.

  -ou-
- Cliquez sur **Quitter l'assistant** pour quitter l'**Assistant de configuration** et aller à la page **Récapitulatif**.

Enregistrer Technical Support Appliance

Vous pouvez voir et changer le contact responsable de la maintenance et l'emplacement physique du système.

Procédure

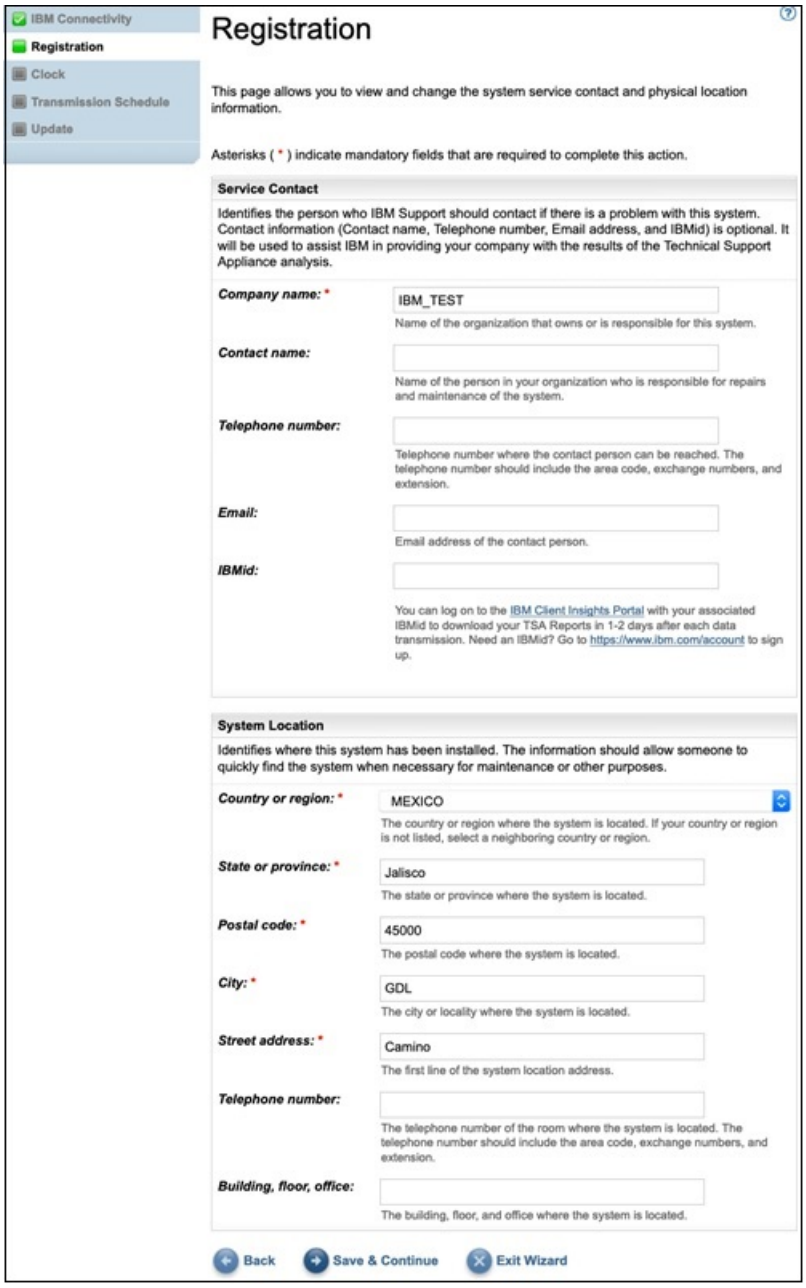

Figure 24. Enregistrement

1. Indiquez les coordonnées du contact pour la maintenance dans les champs suivants :

   Nom de l'entreprise
   Nom de l'entreprise qui utilise TSA.

   Nom du contact
   (Facultatif) Nom de la personne responsable de TSA dans l'entreprise.

Numéro de téléphone
(Facultatif) Numéro de téléphone auquel la personne responsable du système peut être contactée. Il doit comprendre l'indicatif pays, le préfixe national, le numéro national et le numéro de poste. N'utilisez pas de parenthèses dans le numéro de téléphone.

Adresse e-mail
(Facultatif) Adresse e-mail de la personne à contacter.

IBMid
(Facultatif) IBMid de la personne que vous autorisez à consulter les rapports sur IBM Client Insights Portal.

Remarque : Vous pouvez vous connecter à https://clientinsightsportal.ibm.com/ avec votre IBMid correspondant pour télécharger vos rapports TSA un ou deux jours après chaque transmission de données. Pour demander un IBMid, rendez-vous sur la page https://www.ibm.com/account.

Remarque : Le contact pour la maintenance permet d'identifier la personne que le support IBM doit contacter en cas de problème sur le système. Ces coordonnées vont permettre à IBM de fournir à votre entreprise les résultats de l'analyse de Technical Support Appliance.

2. Indiquez les informations sur l'emplacement de TSA dans les champs suivants :

Pays ou région
Pays ou région où TSA est installé.

État ou province
État ou province où TSA est installé. Si vous n'en êtes pas sûr, tapez *Inconnu*.

Code postal
Code postal du lieu où TSA est installé.

Ville
Ville ou localité où TSA est installé.

Adresse
Adresse de TSA.

Numéro de téléphone
(Facultatif) Numéro de téléphone de la pièce où TSA est installé. Il doit comprendre l'indicatif pays, le préfixe national, le numéro national et le numéro de poste. N'utilisez pas de parenthèses dans le numéro de téléphone.

Bâtiment, étage, bureau
(Facultatif) Bâtiment, étage et bureau où TSA est installé.

Que faire ensuite

- Cliquez sur **Enregistrer et continuer** pour enregistrer les données d'enregistrement et passer à la page **Horloge**.
- Cliquez sur **Précédent** pour revenir à la page **Connectivité IBM**.

-ou-

- Cliquez sur **Quitter l'assistant** pour quitter l'**Assistant de configuration** et aller à la page **Récapitulatif**.

Régler l'horloge

Vous pouvez régler l'heure système, la date et le fuseau horaire local de TSA lors de la configuration.

Procédure

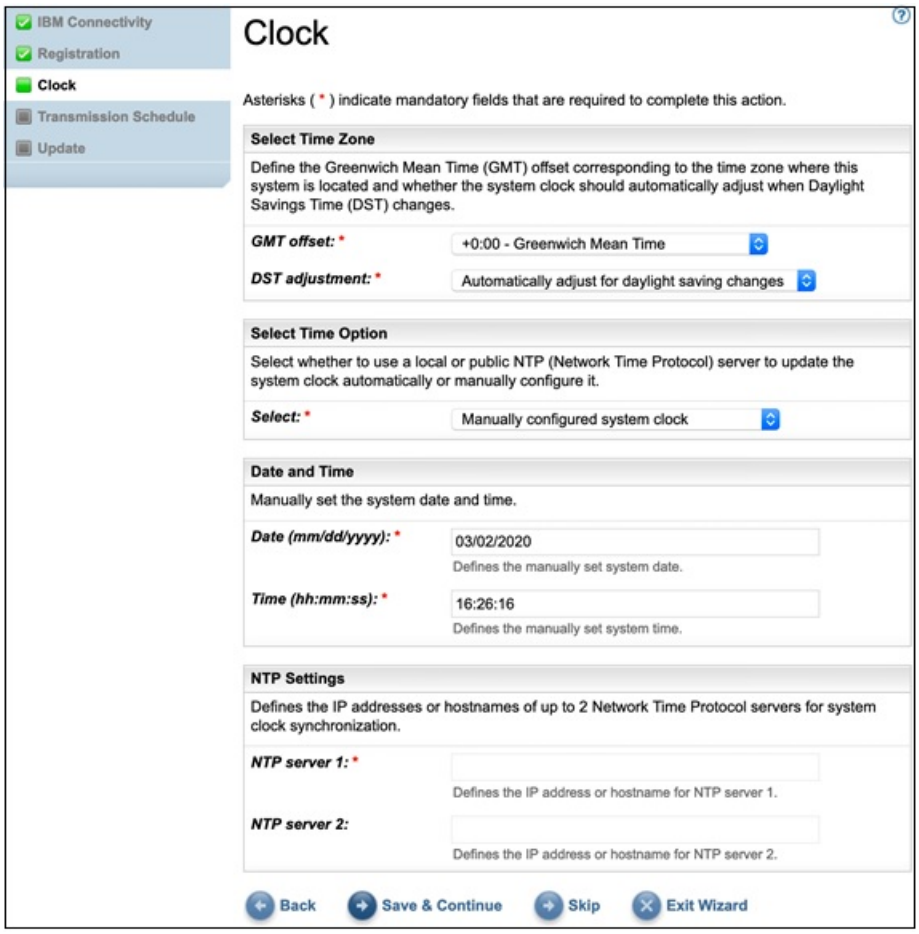

Figure 25. Horloge

1. Sélectionnez votre fuseau horaire local dans la liste déroulante **Décalage par rapport à l'heure GMT**.
2. Sélectionnez l'option d'ajustement lors des changements d'heure dans la liste déroulante **Ajustement lors des changements d'heure**.

   Remarque : Tous les fuseaux horaires n'ont pas de changement d'heure. Si cette option est sélectionnée pour un fuseau horaire où il n'y a pas de changement d'heure, une erreur se produit.
3. Sélectionnez une méthode pour mettre à jour l'horloge système dans la liste déroulante **Sélectionner l'option d'heure**.

   Les options disponibles sont la synchronisation de l'horloge système avec un serveur NTP pour une mise à jour automatique de l'horloge système, ou la configuration manuelle de l'horloge système.

   a) Si vous avez choisi de configurer l'horloge système manuellement, vous devez définir l'heure et la date système. Entrez la date et l'heure dans les champs **Date** et **Heure** correspondants.

   b) Si vous avez choisi de synchroniser l'horloge système avec un serveur NTP afin de mettre à jour automatiquement l'horloge système, vous devez indiquer l'adresse IP et le nom d'hôte de chaque serveur NTP. Tapez l'adresse IP ou le nom d'hôte pour un maximum de deux serveurs dans les champs **Serveur NTP** correspondants.

   Remarque : Assurez-vous que le serveur NTP est accessible via le réseau à TSA.

Que faire ensuite

- Cliquez sur **Enregistrer et continuer** pour enregistrer les données d'horloge et passer à la page **Planning de transmission**.

  -ou-

- Cliquez sur **Ignorer** pour omettre cette étape et passer directement à la page **Planning de transmission**.

Pour modifier des choix à l'étape précédente de l'assistant

- Cliquez sur **Précédent** pour revenir à la page **Enregistrement**.

Pour quitter l'assistant

- Cliquez sur **Quitter l'assistant** pour quitter l'**Assistant de configuration** et aller à la page **Récapitulatif**.

Mise en place du planning de transmission

TSA fournit un planning par défaut pour que le processus de transmission s'exécute à un moment précis. Vous pouvez modifier ce planning selon vos besoins.

Procédure

1. Sélectionnez une nouvelle heure à l'aide des listes déroulantes **Heure** et **Minute**.
2. Sélectionnez le **Mode de sélection du jour**.

Hebdomadaire par jour(s) (dimanche au samedi)

Pour planifier la transmission un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)**.

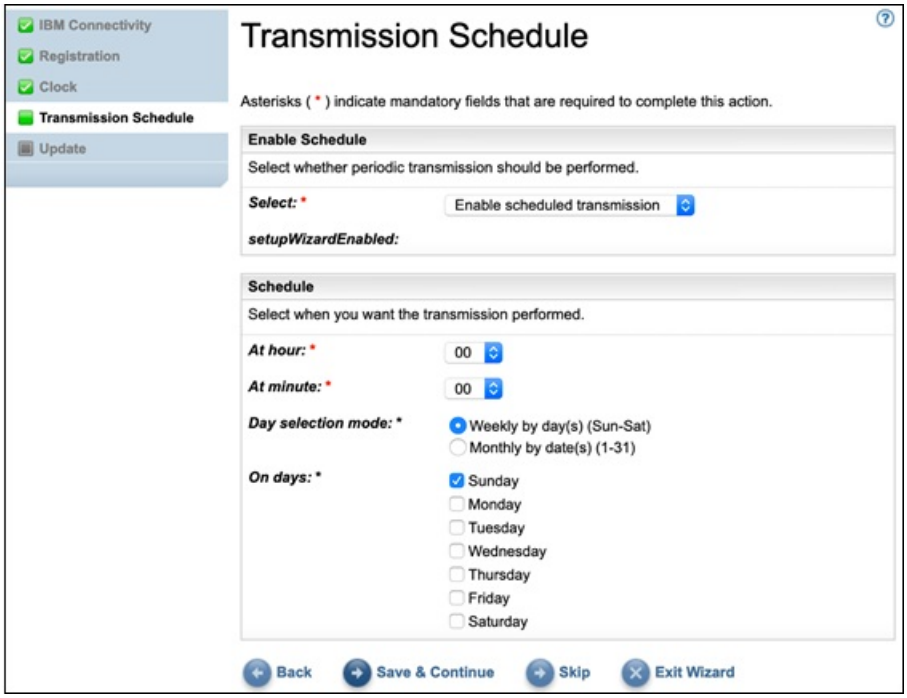

Figure 26. Hebdomadaire par jour(s) (dimanche au samedi)

Pour le champ **Jours**, cochez la ou les cases appropriées pour sélectionner un ou plusieurs jours de la semaine.

Mensuel par date(s) (1-31)

Pour planifier la transmission un ou plusieurs jours précis du mois, sélectionnez l'option **Mensuel par date(s) (1-31)**.

Pour le champ **Jours**, cochez la ou les cases appropriées pour sélectionner un ou plusieurs jours du mois.

Remarque : Si les jours sélectionnés vont au-delà de la fin d'un mois (par exemple, un mois se terminant le 30 alors que vous avez sélectionné le 31), le travail sera déclenché le dernier jour de ce mois.

Remarque : Assurez-vous que l'heure de début de la découverte précède l'heure de la transmission, afin d'éviter tout retard dans la transmission des nouvelles données collectées.

Que faire ensuite

- Cliquez sur **Enregistrer et continuer** pour enregistrer le planning de transmission et passer à la page **Mise à jour**.

  -ou-

- Cliquez sur **Ignorer** pour omettre cette étape et passer directement à la page **Mise à jour**.

Pour modifier des choix à l'étape précédente de l'assistant

- Cliquez sur **Précédent** pour revenir à la page **Horloge**.

Pour quitter l'assistant

- Cliquez sur **Quitter l'assistant** pour quitter l'**Assistant de configuration** et aller à la page **Récapitulatif**.

Mettre à jour Technical Support Appliance

Vous pouvez mettre à jour TSA pour le passer à la version la plus récente.

Si une mise à jour est disponible, la page **Mise à jour** suivante est affichée.

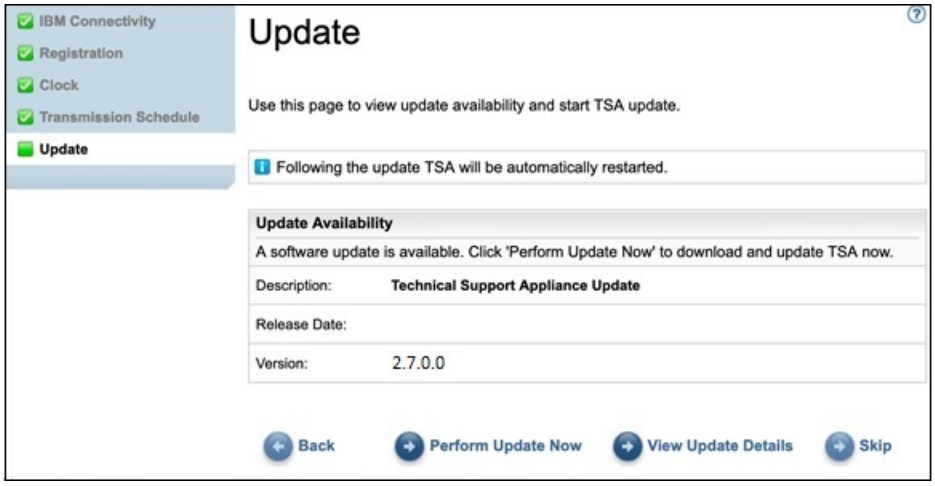

Figure 27. Mises à jour disponibles

- Cliquez sur **Exécuter la mise à jour** pour installer la mise à jour et terminer l'**Assistant de configuration**.

  -ou-

- Cliquez sur **Voir les détails de la mise à jour** pour simplement obtenir des informations sur le contenu de la mise à jour.

Pour modifier des choix à l'étape précédente de l'assistant

- Cliquez sur **Précédent** pour revenir à la page **Planning de transmission**.

Pour terminer l'assistant

- Cliquez sur **Ignorer** pour terminer l'**Assistant de configuration** sans appliquer la mise à jour.

Si aucune mise à jour n'est disponible, la page **Mise à jour** suivante est affichée.

Figure 28. Aucune mise à jour n'est disponible

- Cliquez sur **Terminer l'assistant** pour terminer l'**Assistant de configuration**. La page **L'assistant de configuration a terminé** s'affiche.

  -ou-

- Cliquez sur **Précédent** pour revenir à la page **Planning de transmission**.

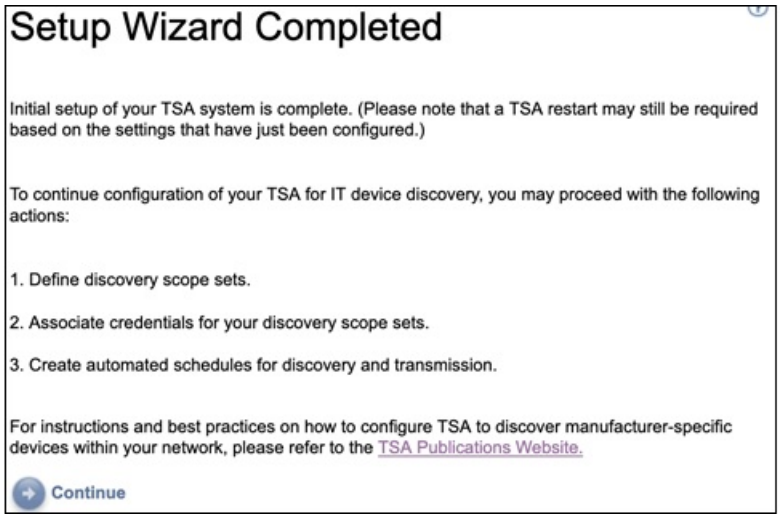

Figure 29. L'assistant de configuration a terminé.

- Cliquez sur **Continuer** pour aller à la page **Récapitulatif**.

  Remarque : Pour prendre effet, certains changements dans la page **Horloge** peuvent nécessiter un redémarrage du système. C'est le cas notamment si vous réglez la date et l'heure ou si vous passez d'une configuration manuelle à une configuration avec serveur NTP.

  – Cliquez sur **OK** pour terminer l'**Assistant de configuration** et retourner à la page **Récapitulatif**. La page **Récapitulatif** s'affiche et le système redémarre.

Remarque : Si vous quitter l'**Assistant de configuration** ou omettez d'y configurer des réglages, vous pouvez toujours revenir dessus dans le menu de navigation de TSA. Pour plus d'informations sur la configuration de ces réglages, consultez Annexe B, «Configurer Technical Support Appliance», à la page 125.

Configurer les paramètres réseau

L'installation de TSA nécessite de configurer les réglages réseau de base. Si ces réglages sont déjà adaptés à votre réseau informatique, vous pouvez passer cette section.

Avant de commencer

Utilisez la page **Réseau** pour :

- Changer les réglages réseau de base initiaux

- Configurer TSA pour l'accès à plusieurs réseaux

Pour configurer les paramètres réseau de base via la console, suivez les étapes décrites à la section «Configurer les données du réseau», à la page 19.

Configurer les paramètres réseau de base

Utilisez la page **Réseau** pour agir sur les réglages réseau initiaux.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Réseau**.
   La page **Réseau** s'affiche.

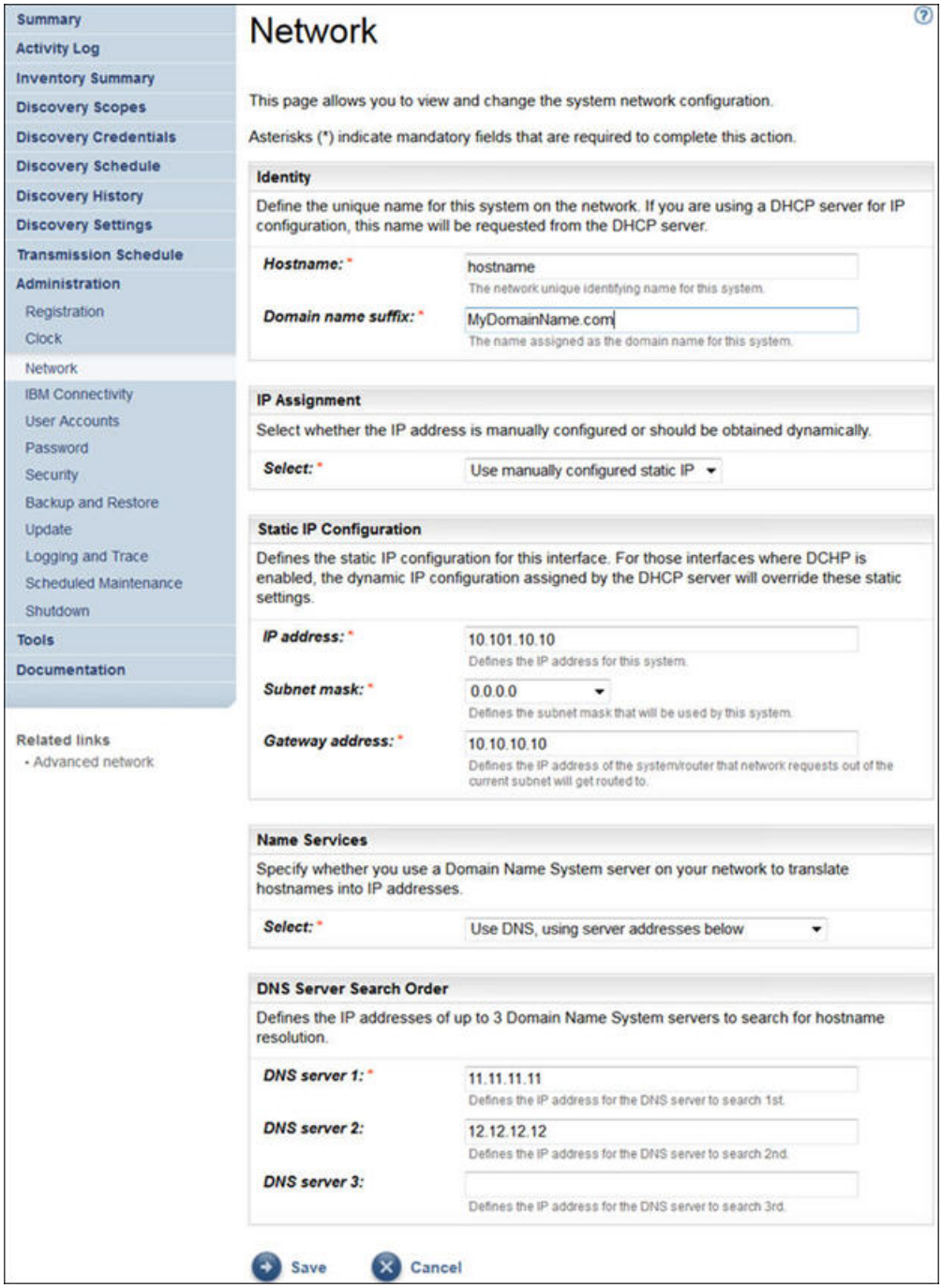

Figure 30. Réseau

2. Dans le champ **Nom d'hôte**, indiquez le nom unique de ce système sur le réseau local.

3. Dans le champ **Suffixe du nom de domaine**, indiquez le nom qui est utilisé comme nom de domaine de ce système sur le réseau local.
4. Sélectionnez **Utiliser une adresse IP statique configurée manuellement** dans le panneau *Attribution d'adresse IP*. Pour l'attribution d'une adresse DHCP, voir la section Annexe C, «Configurer les données du réseau DHCP», à la page 135.
5. Configurez l'adresse IP statique :
   a) Dans le champ **Adresse IP**, entrez l'adresse IP de ce système.
   b) Dans la liste déroulante **Masque de sous-réseau**, sélectionnez le masque de sous-réseau qui sera utilisé par ce système.
   c) Dans le champ **Adresse de passerelle**, sélectionnez l'adresse IP du système ou du routeur qui va traiter les demandes sortant du sous-réseau en cours.
6. Spécifiez les **Services annuaire** en fonction de la méthode d'affectation d'adresse IP.
   a) Pour une IP statique configurée manuellement, sélectionnez l'option **Utiliser un DNS, en utilisant les adresses de serveurs ci-dessous**.
   b) Pour une affectation d'adresse IP par DHCP, sélectionnez l'option **Utiliser un DNS mais obtenir les adresses de serveurs via DHCP**.
7. Entrez jusqu'à trois adresses IP pour les serveurs de noms de domaine (DNS) qui seront utilisées pour la résolution des noms d'hôte.

   TSA recherche les serveurs dans l'ordre où ils apparaissent.
8. Cliquez sur **Enregistrer** pour enregistrer les paramètres réseau.

   Vous êtes invité à redémarrer le système.

   ATTENTION : Soyez prudent lorsque vous modifiez les paramètres réseau. Si vous faites une erreur dans la configuration réseau, l'interface utilisateur de TSA pourrait ne plus être accessible. Dans ce cas, la console TSA devra être utilisée pour réparer la configuration réseau.
   - Pour VMware, utilisez l'interface web VMware ESXi ou VMware vSphere Client
   - Pour Microsoft Hyper-V, utilisez Hyper-V Manager.
9. Cliquez sur **Annuler** pour quitter la page **Réseau** sans enregistrer les paramètres.

Configurer les paramètres réseau avancés

Si vous voulez configurer TSA de façon à accéder à plusieurs réseaux, utilisez la page **Réseau (avancé)** pour indiquer ces paramètres réseau.

Pour configurer les paramètres réseau avancés, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Réseau**.
2. Dans le panneau de navigation inférieur, sous **Liens connexes**, cliquez sur **Réseau avancé**.

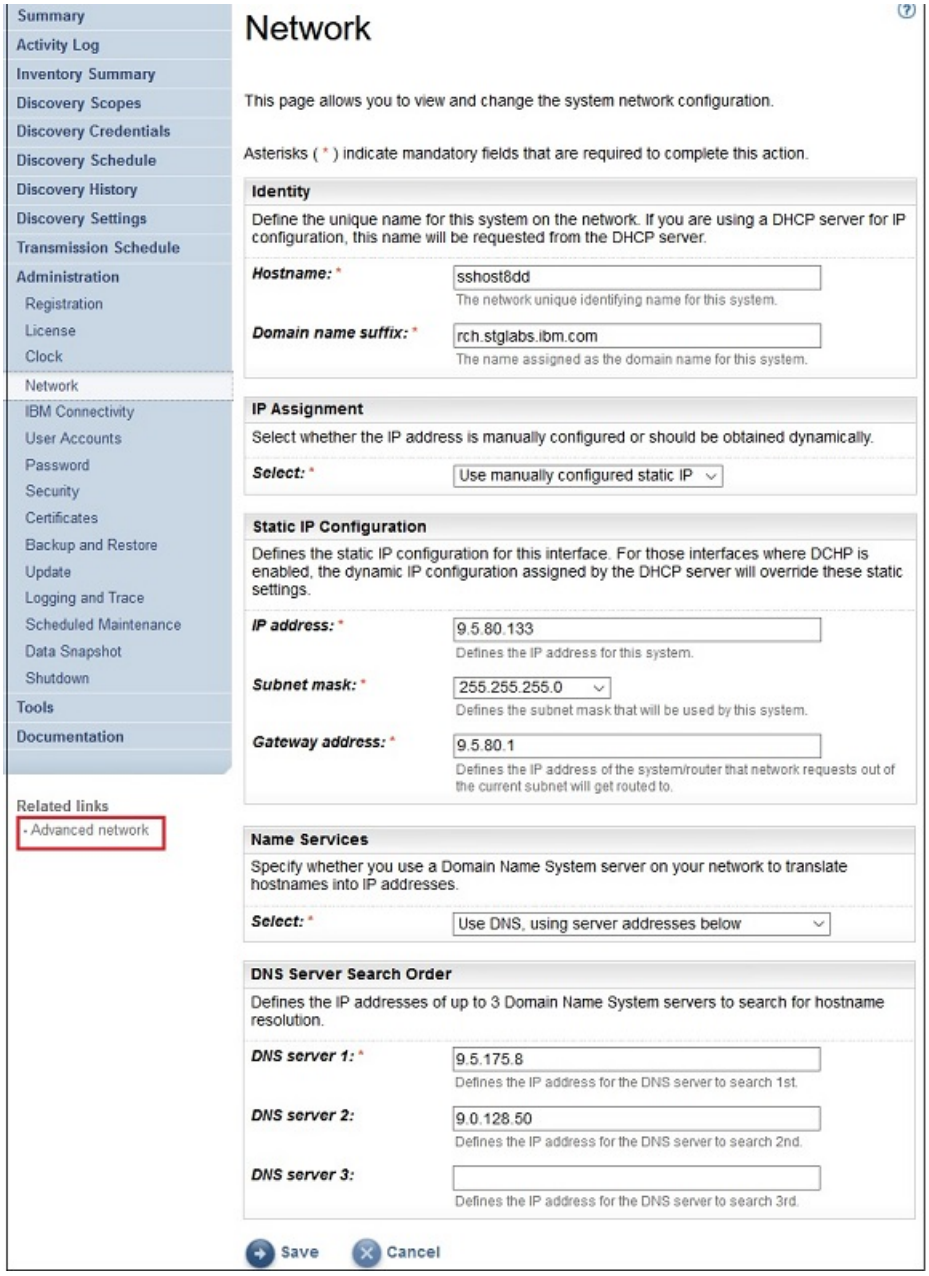

Figure 31. Accès à la page Réseau (avancé)

La page **Réseau (avancé)** s'affiche.

La page **Réseau (avancé)** comporte plusieurs pages d'onglet :

- Globaux
- Interfaces réseau
- Paramètres DNS
- Routes de réseau

Pour accéder à chacune de ces pages, cliquez sur l'onglet correspondant.

Important : vous devez cliquer sur **Enregistrer** avant de quitter une page pour enregistrer les modifications effectuées dans les champs de cette page. Vous êtes invité à redémarrer le système pour que les modifications prennent effet.

Globaux

Utilisez cette page pour voir et modifier les paramètres réseau globaux :

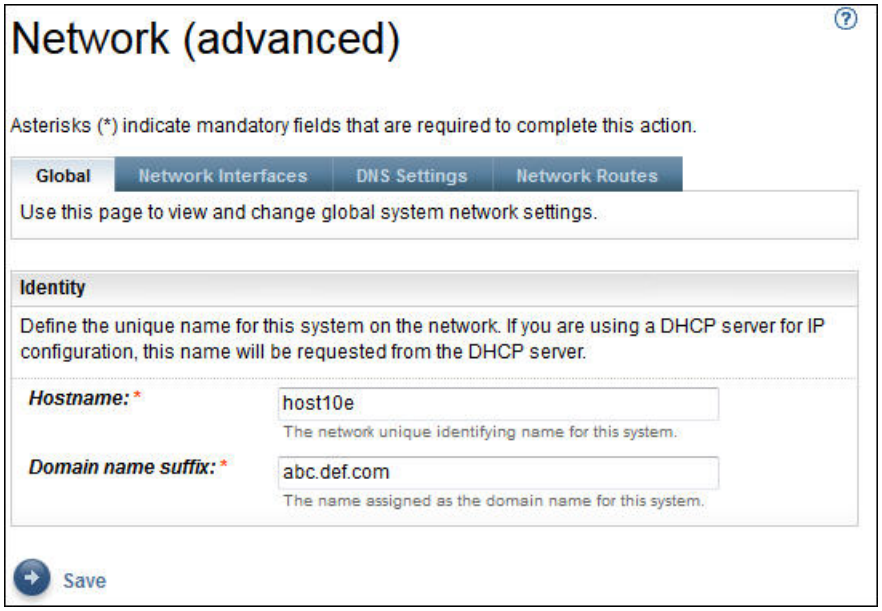

Figure 32. Réseau (avancé) - Globaux

Identité

Définissez l'identité de ce système sur le réseau.

1. Dans le champ **Nom d'hôte**, indiquez le nom unique de ce système.
2. Dans le champ **Suffixe du nom de domaine**, indiquez le nom utilisé comme nom de domaine de ce système.

Interfaces réseau

TSA est configuré pour avoir deux contrôleurs d'interface réseau (NIC) - eth0 et eth1. Utilisez cette page pour afficher et modifier les paramètres actuels de l'interface réseau sélectionnée.

1. Cliquez sur **eth0** pour sélectionner l'interface réseau eth0.
2. Cliquez sur **eth1** pour sélectionner l'interface réseau eth1.

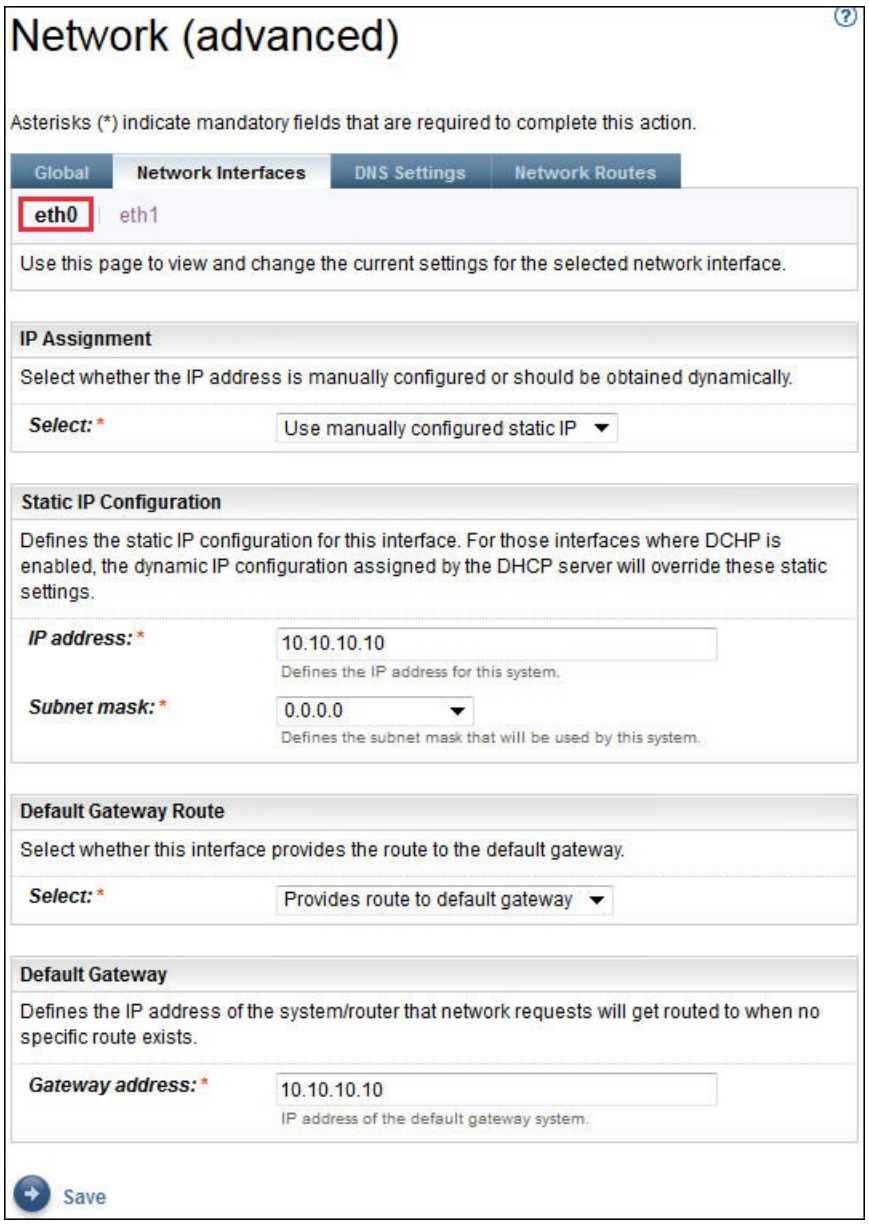

Figure 33. Réseau (avancé) - Interfaces réseau

Attribution d'adresse IP

Sélectionnez une méthode d'affectation d'adresse IP pour ce système. Vous avez le choix entre obtenir l'adresse IP de façon dynamique depuis un serveur DHCP ou utiliser une adresse IP statique configurée manuellement. Si vous choisissez d'utiliser une adresse IP statique configurée manuellement, vous devez configurer l'adresse IP du système sur cette page.

Configuration IP statique

Si vous avez choisi de configurer manuellement une adresse IP statique, indiquez les informations IP de cette interface réseau comme suit :

1. Dans le champ **Adresse IP**, indiquez l'adresse IP de ce système.
2. Dans la liste déroulante **Masque de sous-réseau**, sélectionnez le masque de sous-réseau qui sera utilisé par ce système.

Route de passerelle par défaut

Indiquez si cette interface réseau fournit une route vers la passerelle par défaut.

Passerelle par défaut

Dans le champ **Adresse de passerelle**, indiquez l'adresse IP de la passerelle par défaut ce système.

Paramètres DNS

Utilisez cette page pour afficher et modifier les paramètres DNS.

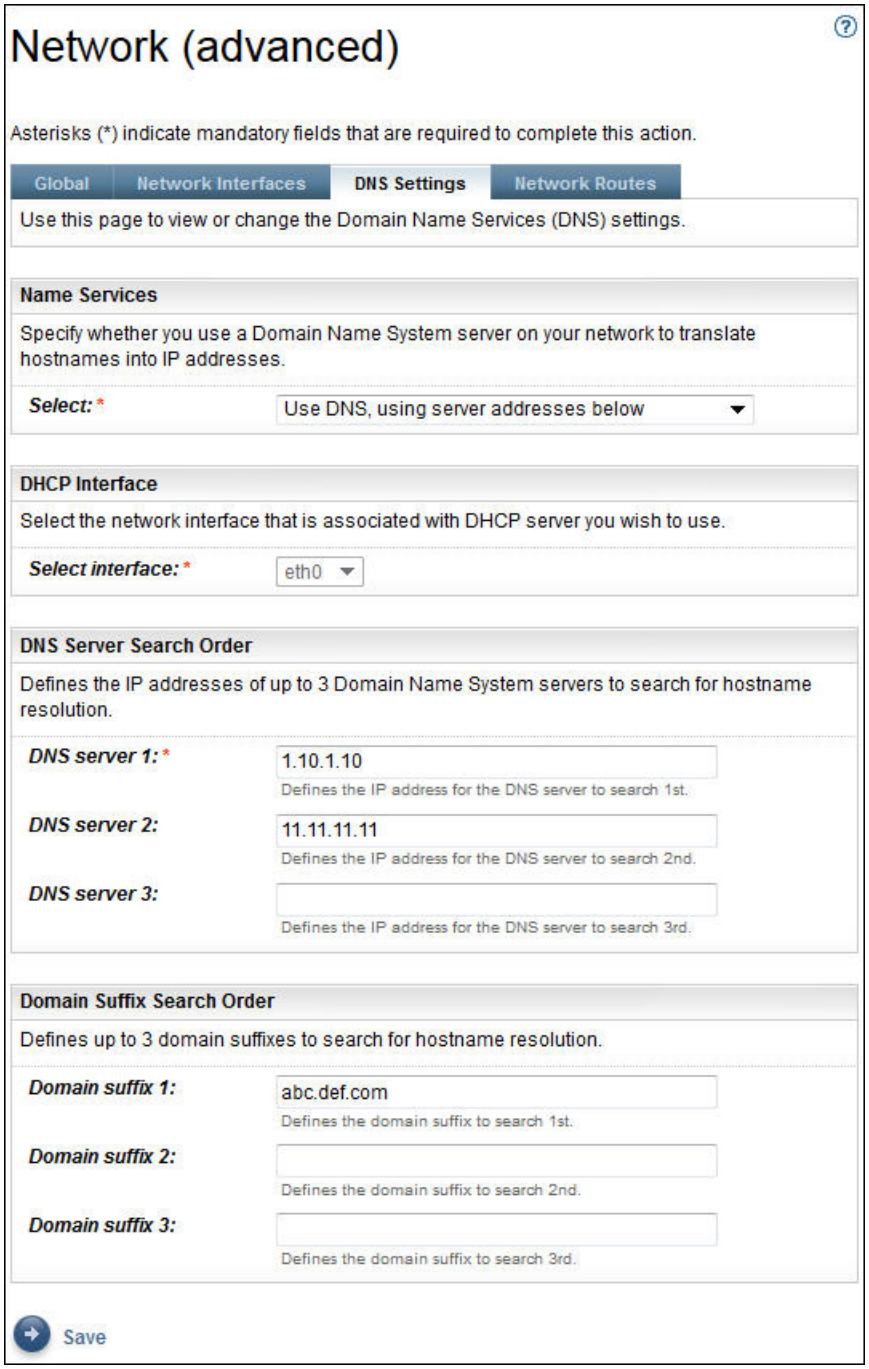

Figure 34. Réseau (avancé) - Paramètres DNS

Services annuaire

Spécifiez un serveur DNS (système de noms de domaine) sur votre réseau pour convertir les noms d'hôte en adresses IP. Vous avez le choix entre les options suivantes :

- Utiliser un DNS mais obtenir les adresses de serveurs via DHCP

Si vous choisissez cette option, vous devez sélectionner l'interface réseau qui est associée au serveur DHCP que vous voulez utiliser.

- Utiliser un DNS avec des adresses de serveurs que vous indiquez

  Si vous choisissez cette option, vous devez indiquer au moins un serveur DNS sur cette page.

Interface DHCP
Sélectionnez l'interface réseau qui est associée au serveur DHCP que vous voulez utiliser.

Ordre de recherche des serveurs DNS
Si vous choisissez d'utiliser un DNS avec des adresses de serveurs que vous indiquez, entrez jusqu'à trois adresses IP pour les serveurs de noms de domaine (DNS) qui seront utilisées pour la résolution des noms d'hôte. TSA recherche les serveurs dans l'ordre où ils apparaissent.

Ordre de recherche des suffixes de domaine
Si vous choisissez d'utiliser un DNS avec des adresses de serveurs que vous indiquez, entrez jusqu'à trois suffixes de nom de domaine à utiliser pour la résolution des noms d'hôte. TSA recherche ces suffixes de nom de domaine dans l'ordre où ils apparaissent.

Routes de réseau

Utilisez cette page pour afficher, ajouter, modifier ou supprimer des entrées de routage statique.

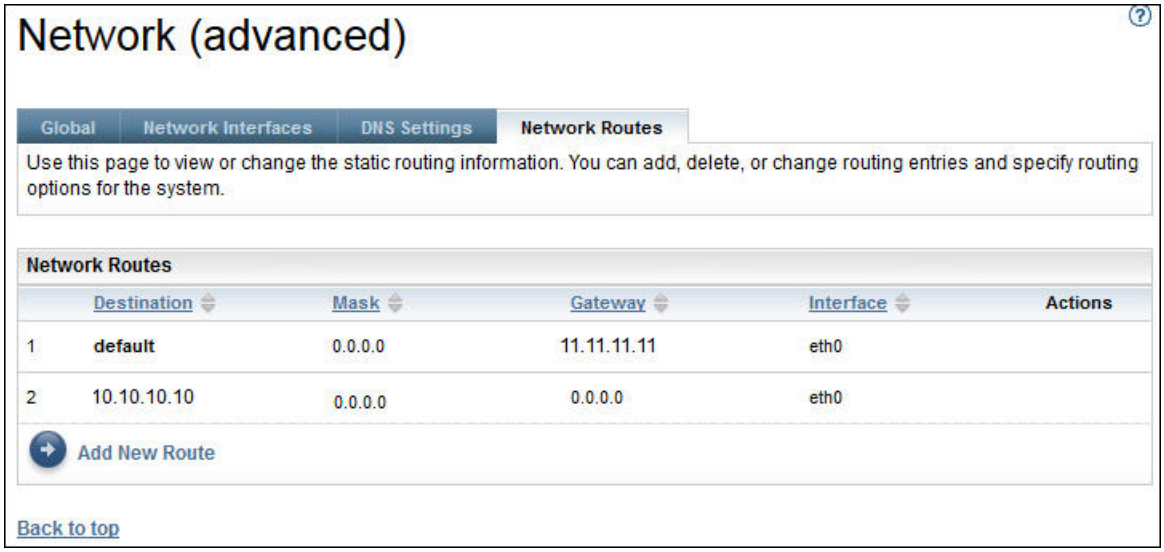

Figure 35. Réseau (avancé) - Routes de réseau

Les informations suivantes s'affichent pour chaque route de réseau :

Destination

Indique l'adresse de sous-réseau ou le nom d'hôte du réseau de destination TCP/IP.

Masque
Indique le masque de sous-réseau à utiliser comme masque de réseau lorsque vous ajoutez une route. C'est l'adresse de sous-réseau pour la portion hôte de l'adresse IP. Les interfaces réseau peuvent utiliser différents masques de sous-réseau, offrant ainsi la possibilité d'ajouter des routes en sélectionnant un masque de sous-réseau (routes de sous-réseau variables). Vous pouvez sélectionner un masque de sous-réseau lorsque vous ajoutez une route, en notation décimale à point 32 bits.

Passerelle
Indique l'adresse de passerelle TCP/IP pour le routage des paquets IP.

Interface
Sélectionnez l'adaptateur dans le menu. C'est le nom de l'adaptateur de réseau qui est associé à l'entrée du tableau.

Actions
Cliquez sur l'icône **Supprimer** pour supprimer la route.

Remarque : Les deux routes qui apparaissent sur la figure ne peuvent être ni modifiées, ni supprimées.

Cliquez sur **Ajouter une nouvelle route** pour définir une nouvelle route de réseau statique. La page **Route de réseau** s'affiche.

Ajouter des routes de réseau

Vous pouvez ajouter des routes de réseau statique.

Procédure

Pour ajouter une route de réseau, procédez comme suit :

1. Sur la page **Réseau (avancé) - Routes de réseau**, cliquez sur **Ajouter une nouvelle route**. La page **Route de réseau** s'affiche.

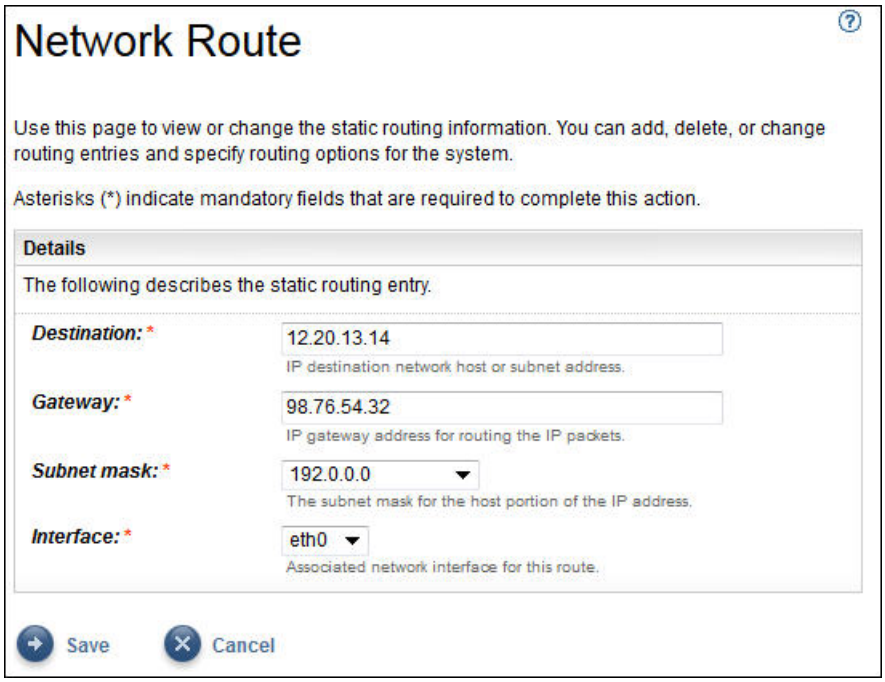

Figure 36. Nouvelle route de réseau

2. Dans le champ **Destination**, entrez l'adresse IP pour le sous-réseau ou l'hôte du réseau de destination TCP/IP.
3. Dans le champ **Passerelle**, entrez l'adresse de passerelle TCP/IP pour le routage de l'information. L'adresse doit en notation décimale à point 32 bits. Exemple : `xxx.xxx.xxx.xxx`.
4. Dans la liste déroulante **Masque de sous-réseau**, sélectionnez le masque de sous-réseau à utiliser comme masque de réseau pour cette route.
5. Dans la liste déroulante **Interface**, sélectionnez l'adaptateur de réseau à associer à cette route.
6. Cliquez sur **Enregistrer** pour enregistrer cette route de réseau.

Mise en place des certificats

La page **Certificats** vous permet d'afficher les informations sur les signatures de certificat, de générer et d'installer des certificats ou d'importer des certificats. Il s'agit des certificats de serveur que TSA présente à un navigateur Web en cas d'accès à l'interface utilisateur.

Dans la configuration par défaut de TSA, un certificat de serveur SSL autosigné générique est implémenté pour faciliter l'installation. Pour plus de sécurité, il est recommandé de remplacer le certificat par défaut une fois les premières étapes de déploiement et de configuration terminées. Vous pouvez utiliser TSA pour générer et installer un certificat de serveur SSL autosigné qui soit propre à ce TSA, pour générer et installer un certificat personnalisé qui soit signé par l'autorité de certification de votre choix ou pour remonter votre propre fichier magasin de clés Java contenant un certificat de serveur SSL personnalisé.

Vous pouvez installer un certificat personnalisé de l'une des manières suivantes :

- «Installer un certificat personnalisé (avec des signataires)», à la page 45
- «Installer un certificat personnalisé (autre méthode) », à la page 46

Afficher l'état du certificat de serveur SSL

La configuration de TSA installe le certificat TSA par défaut qui est fourni avec Technical Support Appliance.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Certificats**.
   La page **Certificats** s'affiche.

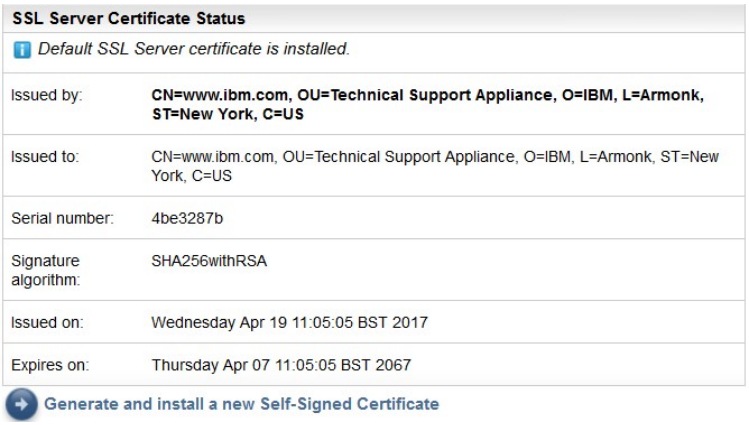

   Figure 37. État du certificat de serveur SSL

   La section **État du certificat de serveur SSL** affiche les informations suivantes sur le certificat de serveur SSL qui est installé dans TSA : *Émetteur*, *Destinataire*, *Date d'émission*, *Date d'expiration*, *Numéro de série* et *Algorithme de signature*.
2. Cliquez sur **Générer et installer un nouveau certificat autosigné** pour installer un certificat autosigné propre à cette version de TSA. Un message d'avertissement indique que l'appliance redémarrera automatiquement une fois que vous aurez généré et installé un certificat autosigné.

   Remarque : Le bouton **Générer et installer un nouveau certificat autosigné** est visible uniquement si le certificat par défaut est installé sur TSA.

Générer et télécharger la demande de signature de certificat (CSR)

Pour demander un certificat SSL certifié par une autorité de certification, vous devez fournir les informations suivantes pour générer et télécharger le fichier de demande de signature de certificat (CSR).

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Certificats**.
   La page **Certificats** s'affiche.

Figure 38. Demande de signature de certificat

2. Entrez le nom de système hôte qualifié complet (FQDN) de TSA dans le champ **Nom usuel**. Il doit comporter entre 1 et 64 caractères.
3. Indiquez le nom de l'organisation, qui doit distinguer les différentes divisions de l'organisation, dans le champ **Unité organisationnelle**.
4. Indiquez le nom de l'entreprise, du "limited partnership", de l'université ou de l'agence gouvernementale dans le champ **Organisation**.
5. Dans le champ **Ville**, spécifiez le nom de la ville ou de la localité où le TSA est exploité.
6. Dans le champ **Etat**, spécifiez le nom de l'Etat ou de la Province où le TSA est exploité. Si vous n'en êtes pas sûr, ou si cette donnée est sans objet pour votre pays, tapez *Inconnu*.
7. Dans la liste déroulante **Pays**, sélectionnez le nom du pays où le TSA est exploité.
8. Indiquez le nombre de jours de validité du certificat, à compter de la date de création du certificat, dans le champ **Nombre de jours jusqu'à expiration**.
9. Cliquez sur **Générer et télécharger le fichier de demande de signature de certificat (CSR)** pour créer et télécharger le fichier CSR avec les informations indiquées.

   Remarque : Pour restaurer le certificat par défaut livré avec TSA, consultez la section «Restaurer le certificat par défaut», à la page 47.

Installer un certificat personnalisé (avec des signataires)

Utilisez cette fonctionnalité pour installer un certificat personnalisé. Vous avez besoin du certificat de serveur qui est généré par une autorité de certification, du certificat racine pour l'autorité de certification et de tous les certificats intermédiaires éventuels pour l'autorité de certification.

Avant de commencer

Assurez-vous que les fichiers de certificat (certificat racine, intermédiaire et serveur) sont dans l'un des formats suivants :

- *.crt*
- *.der*
- *.pem*

Procédure

Pour télécharger et installer les certificats sur TSA, effectuez les étapes suivantes :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Certificats**.

   La page **Certificats** s'affiche.

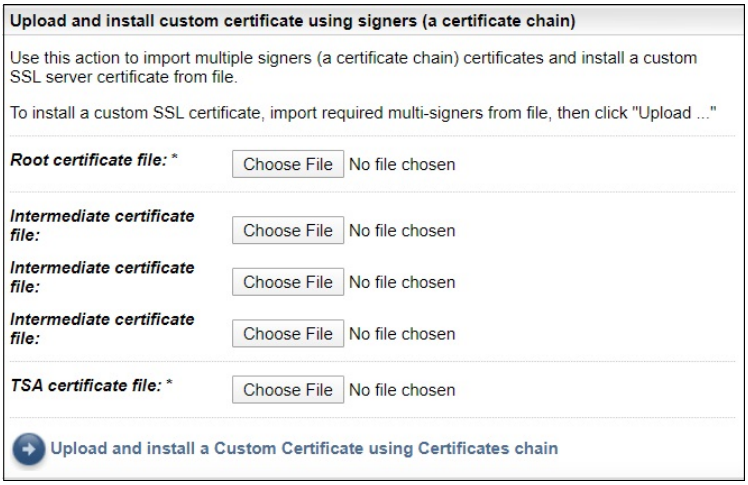

Figure 39. Installer un certificat personnalisé

2. Dans le champ **Fichier de certificat racine**, indiquez l'emplacement du fichier de certificat racine que vous voulez installer sur TSA.
3. Dans le champ **Fichier de certificat intermédiaire**, indiquez l'emplacement du fichier de certificat intermédiaire que vous voulez installer sur TSA.

   Remarque : Il peut y avoir plusieurs fichiers de certificat intermédiaire (3 maximum) en fonction du nombre de signataires importés.
4. Dans le champ **Fichier de certificat de TSA**, indiquez l'emplacement du fichier de certificat de serveur de TSA que vous voulez installer sur TSA.
5. Cliquez sur **Télécharger et installer un certificat personnalisé avec une chaîne de certificats** pour télécharger tous les fichiers (*fichier de certificat racine*, *fichier de certificat intermédiaire*, *fichier de certificat TSA*) que vous avez indiqués et installer un certificat personnalisé à l'aide de la chaîne de certificats.

   Remarque : Pour restaurer le certificat par défaut livré avec TSA, consultez la section «Restaurer le certificat par défaut», à la page 47.

Installer un certificat personnalisé (autre méthode)

Utilisez cette fonctionnalité pour installer un certificat personnalisé. Vous pouvez l'utiliser pour déployer un fichier magasin de clés Java (jks) complet et déjà construit.

Avant de commencer

Il est recommandé d'utiliser les fonctions **Demande de signature de l'autorité de certification** et **Télécharger et installer un certificat personnalisé avec des signataires (une chaîne de certificats)** de la page **Certificats** pour déployer un certificat personnalisé. Toutefois, si vous avez déjà créé indépendamment un fichier de magasin de clés Java (jks) complet (contenant les clés, le certificat personnalisé et les certificats appropriés de l'autorité de certification), vous pouvez utiliser cette fonction pour le déployer. Vous devez indiquer l'emplacement du fichier du magasin de clés et son mot de passe d'accès.

Remarque : Lorsque vous créez le fichier du magasin de clés, assurez-vous que le mot de passe d'entrée de clé et le mot de passe protégeant le magasin de clés lui-même soient identiques.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Certificats**.

   La page **Certificats** s'affiche.

Figure 40. Installation d'un certificat personnalisé

2. Pour installer un certificat personnalisé, procédez comme suit :
   a) Entrez le mot de passe du certificat dans le champ **Mot de passe du certificat**.
   b) Entrez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.

      Avant que le mot de passe ne soit enregistré, les deux saisies sont comparées afin de vérifier qu'elles sont bien identiques.
   c) Dans le champ **Fichier de certificat personnalisé**, entrez l'emplacement du fichier du magasin de clés Java.
   d) Cliquez sur **Télécharger et installer un fichier JKS complet** pour télécharger le fichier du magasin de clés Java que vous avez indiqué et installer un certificat personnalisé. Le fichier du magasin de clés Java doit inclure le certificat personnalisé et tous les certificats intermédiaires et racines d'autorité de certification pertinents. TSA redémarrera pour activer l'utilisation du nouveau certificat.

Remarque : Pour restaurer le certificat par défaut livré avec TSA, consultez la section «Restaurer le certificat par défaut», à la page 47.

Résultats

Une fois le nouveau certificat installé, TSA redémarre automatiquement. Lorsque le redémarrage est terminé, votre navigateur peut afficher une invite de sécurité demandant si le nouveau certificat est fiable.

Restaurer le certificat par défaut

Pour restaurer le certificat par défaut livré avec TSA, utilisez la console de TSA et sélectionnez l'option **Définir le certificat d'appliance comme certificat par défaut**.

Procédure

1. Lancez la console TSA.
2. Sélectionnez l'option **3) Définir le certificat d'appliance comme certificat par défaut** dans le **Menu de configuration de TSA**.

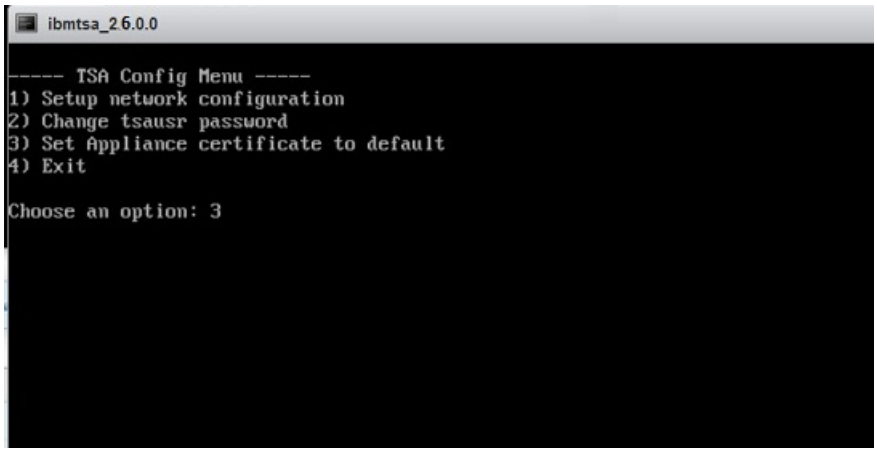

Figure 41. Définir le certificat d'appliance comme certificat par défaut

3. **Confirmer que le certificat de l'appliance est défini comme certificat par défaut [o|n] :** entrez **o** pour confirmer le paramétrage du certificat TSA comme certificat par défaut.

Résultats

Une fois le certificat par défaut installé, TSA redémarre automatiquement au bout de 5 secondes. Lorsque le redémarrage est terminé, votre navigateur peut afficher une invite de sécurité demandant si le certificat par défaut est fiable.

Planifier le nettoyage des données d'inventaire

Vous pouvez planifier ou exécuter manuellement une tâche de nettoyage pour toutes les données d'inventaire collectées sur les ressources à compter du moment où elles sont reconnues.

Pourquoi et quand exécuter cette tâche

Avertissement : Il est recommandé d'exécuter la tâche de nettoyage une fois par semaine pour la plupart des installations.

Pour afficher le planning actuel de la tâche de nettoyage d'inventaire, sélectionnez **Récapitulatif de l'inventaire** > **Planning du nettoyage d'inventaire**.

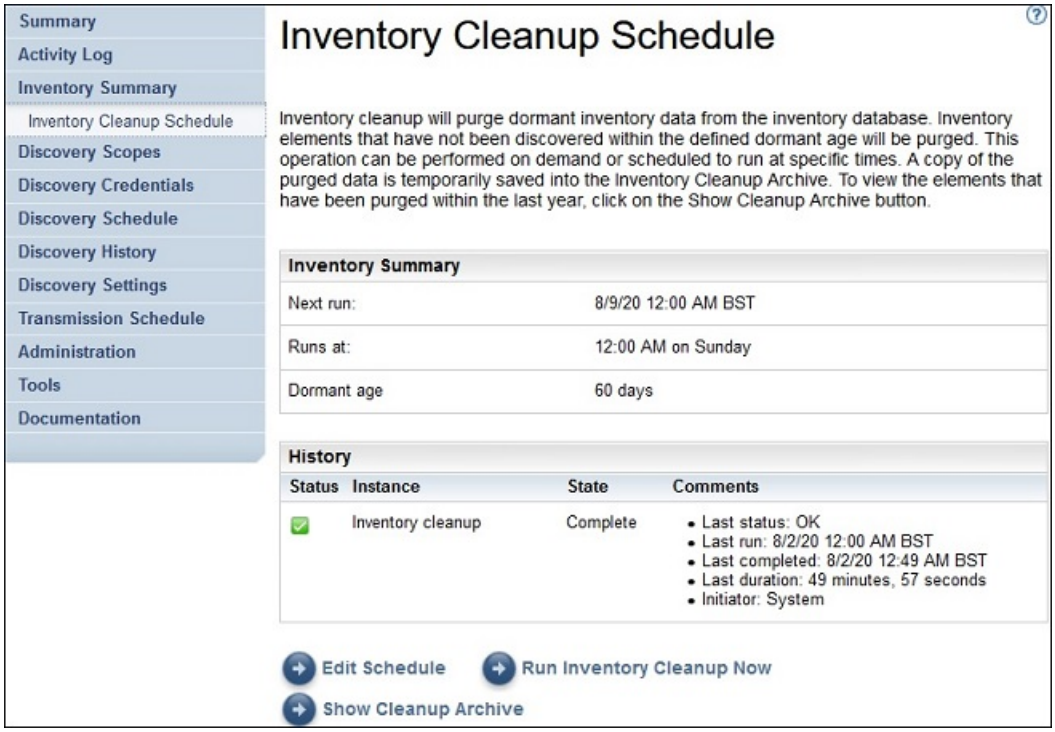

Figure 42. Planning du nettoyage d'inventaire

Pour exécuter le nettoyage d'inventaire manuellement, cliquez sur **Exécuter le nettoyage d'inventaire**.

Pour modifier, activer ou désactiver le planning de nettoyage d'inventaire actuel, procédez comme suit :

Procédure

1. Sur la page **Planning du nettoyage d'inventaire**, cliquez sur **Modifier le planning**.
2. Sur la page **Paramètres de l'inventaire**, sélectionnez **Activer le nettoyage d'inventaire planifié** pour activer la tâche de nettoyage d'inventaire ou **Désactiver le nettoyage d'inventaire planifié** pour désactiver la tâche de nettoyage d'inventaire.
3. Si vous choisissez d'activer la tâche de nettoyage d'inventaire, procédez comme suit :
   a) Sélectionnez une nouvelle heure à l'aide des listes déroulantes **Heure** et **Minute**.

b) Sélectionnez le **Mode de sélection du jour**. Pour planifier le nettoyage d'inventaire un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)** ou pour planifier le nettoyage d'inventaire à une ou plusieurs dates précises du mois, sélectionnez l'option **Mensuelle par date(s) (1-31)**.

c) Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner des jours différents ou des jours supplémentaires de la semaine ou du mois.

Remarque : Si vous sélectionnez des jours au-delà de la fin d'un mois spécifique, le travail sera déclenché le dernier jour de ce mois.

4. Sélectionnez la période durant laquelle vous souhaitez conserver les données d'inventaire dans la liste **Durée d'inactivité**.
5. Cliquez sur **Enregistrer**.

Chapitre 5. Configurer la découverte et la transmission à IBM

Une fois l'installation de TSA terminée, vous pouvez utiliser différentes fonctions d'administration pour gérer la reconnaissance, la transmission et les travaux.

Périmètres de reconnaissance

Un périmètre de reconnaissance indique l'adresse IP, la plage d'adresses IP ou le réseau à utiliser pour découvrir des éléments informatiques. Les périmètres de reconnaissance sont groupés pour former des ensembles de périmètres de reconnaissance.

TSA fournit plusieurs types de périmètres de reconnaissance :

- Ensembles de périmètres dynamiques HMC : pour découvrir des HMC ainsi que toutes les partitions qu'elles gèrent.
- Ensembles de périmètres dynamiques VMware : pour découvrir des hôtes VMware vCenter ou ESXi ainsi que toutes les machines virtuelles sur les hôtes ESXi.
- Périmètres de reconnaissance généraux : pour découvrir toutes les autres ressources qui ne le sont pas avec un ensemble de périmètres dynamiques. Les adresses IP, plages d'adresses IP ou réseaux peuvent être entrés manuellement, ou bien la liste des adresses IP peut être importé d'un fichier dans TSA.

Périmètres dynamiques HMC

Vous pouvez définir des périmètres dynamiques HMC afin de dresser un inventaire détaillé des HMC, des systèmes IBM Power qu'elles gèrent et des LPAR VIOS, AIX et Linux sur ces systèmes.

Pourquoi et quand exécuter cette tâche

En plus de récupérer les informations d'inventaire à partir des HMC définies, TSA interroge les LPAR gérées dynamiquement par ces HMC, sans que les utilisateurs soient obligés de créer et gérer plusieurs définitions de périmètres. Vous devez définir un périmètre pour les HMC et sélectionner quels types de LPAR (AIX, VIOS et Linux) vous souhaiteriez voir analyser automatiquement lorsque ces HMC sont découvertes. L'avantage est que même si les LPAR changent, vous n'avez pas à reconfigurer TSA.

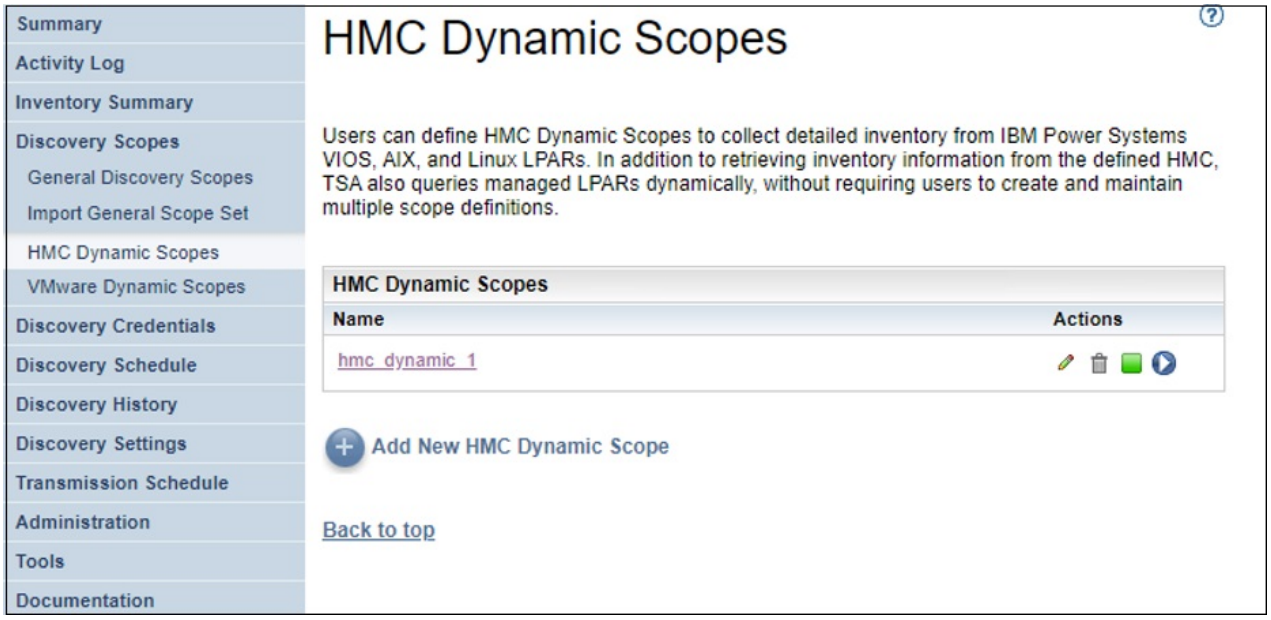

Figure 43. Périmètres dynamiques HMC

Afficher des périmètres dynamiques HMC
Vous pouvez afficher les périmètres dynamiques HMC existants.

Pourquoi et quand exécuter cette tâche

Pour afficher les périmètres dynamiques HMC existants, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC** dans le panneau de navigation. La page **Périmètres dynamiques HMC** s'affiche. Le panneau **Périmètres dynamiques HMC** contient la liste des périmètres dynamiques HMC.

Pour afficher les périmètres et les données d'identification associés à un ensemble de périmètres dynamique spécifique, cliquez sur le nom de celui-ci dans la colonne **Nom**. La page **Ensemble de périmètres dynamiques HMC** s'affiche.

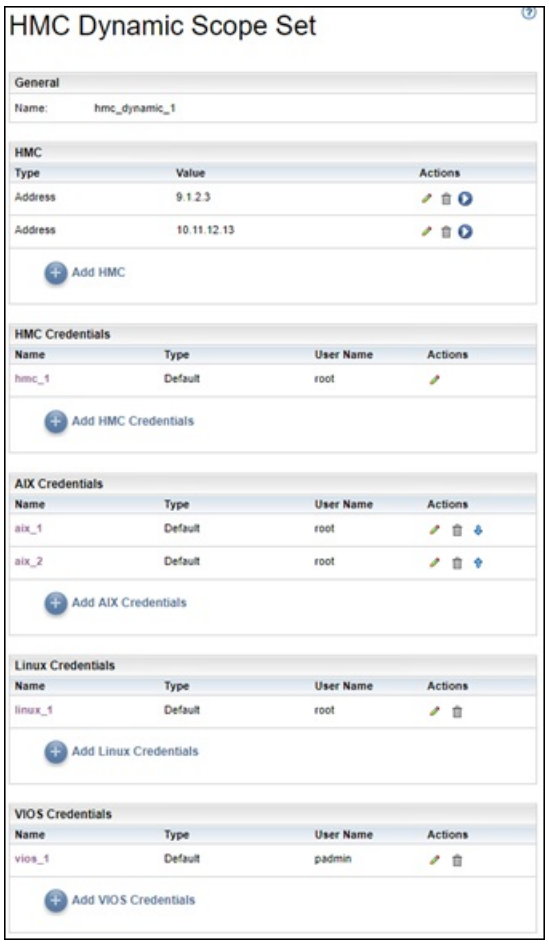

Figure 44. Vue d'un ensemble de périmètres dynamiques HMC

Le panneau **HMC** affiche la liste des adresses IP des HMC découvertes par l'ensemble de périmètres dynamiques. Les différents panneaux de données d'identification, tels que **Données d'identification AIX**, affichent la liste des données d'identification configurées dans l'ensemble de périmètres.

Ajouter des périmètres dynamiques HMC
Pour ajouter un ensemble de périmètres dynamiques HMC, indiquez l'adresse IP d'une unique console HMC ainsi qu'un unique jeu de données d'identification permettant d'accéder à cette console. Au besoin, vous pouvez spécifier les données d'identification pour AIX, Linux et VIOS afin d'autoriser la découverte des partitions logiques des systèmes IBM Power gérés par la console HMC. Une fois l'ensemble de périmètres dynamiques HMC créé, vous pouvez l'éditer pour définir des adresses IP HMC supplémentaires. Il est aussi possible d'éditer un ensemble de périmètres dynamiques HMC afin de rendre les consoles accessibles avec plusieurs jeux de données d'identification ainsi que pour rendre les partitions logiques accessibles avec plusieurs jeux de données d'identification.

Pourquoi et quand exécuter cette tâche
Pour ajouter un ensemble de périmètres, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche.
2. Pour définir un nouvel ensemble de périmètres dynamiques HMC, cliquez sur **Ajouter un nouveau périmètre dynamique de la console HMC**.

   La page **Ensemble de périmètres dynamiques HMC** s'affiche.

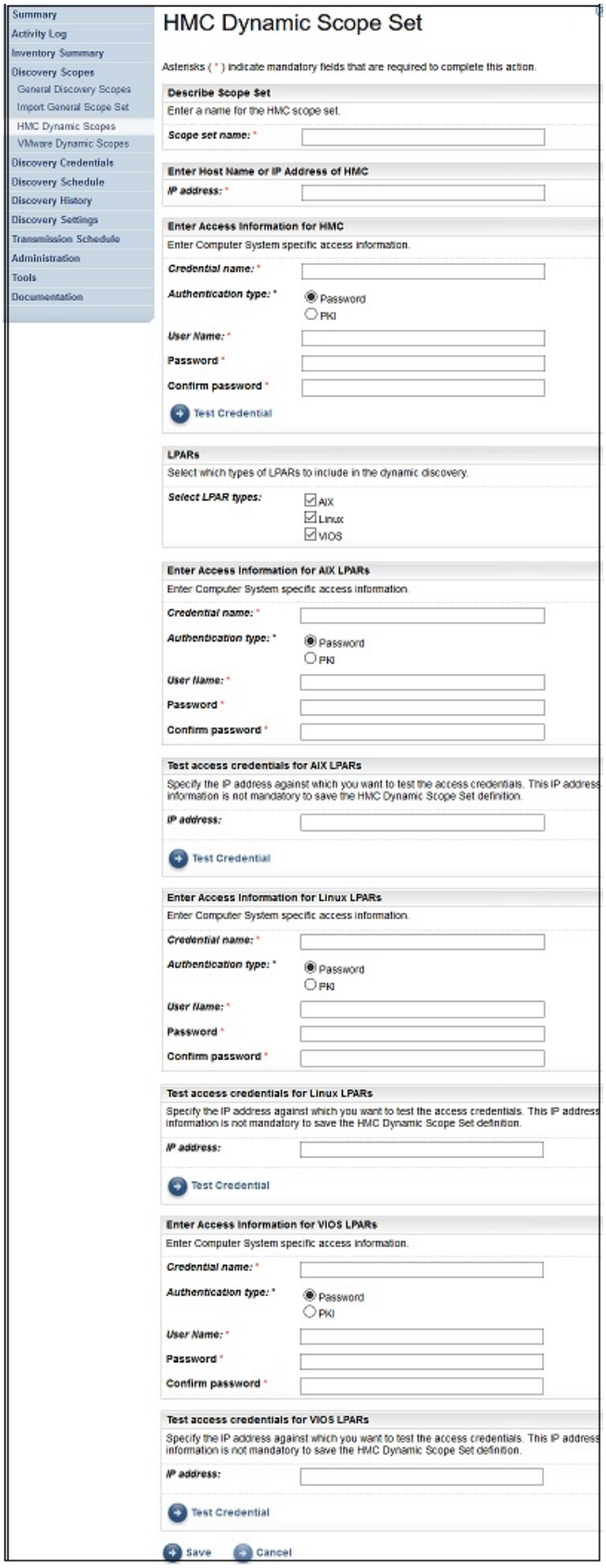

Figure 45. Ajouter un ensemble de périmètres dynamiques HMC

3. Dans le panneau **Décrire l'ensemble de périmètres**, entrez un nom unique dans le champ **Nom de l'ensemble de périmètres**.

4. Dans le panneau **Entrer le nom d'hôte ou l'adresse IP de la console HMC**, entrez l'adresse IP ou le nom d'hôte de la console HMC.
5. Dans le panneau **Entrer les informations d'accès pour HMC**, entrez les détails suivants :
   a) Entrez le **Nom des données d'identification**.
   b) Sélectionnez le **Type d'authentification** :
      - **Mot de passe** - utilise le mot de passe fourni.
      - **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.
   c) Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de la console HMC.
   d) Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.
   e) Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.
   f) Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur la HMC.
   g) Facultatif : Cliquez sur **Tester les données d'identification** pour tester les données d'identification de la console HMC cible.
6. Dans le panneau **Partitions logiques (LPAR)**, sélectionnez les types de LPAR (AIX, LINUX ou VIOS) à inclure dans la reconnaissance dynamique.
7. Si vous sélectionnez un type de LPAR (AIX, Linux, VIOS), vous devez entrer les informations d'accès associées.

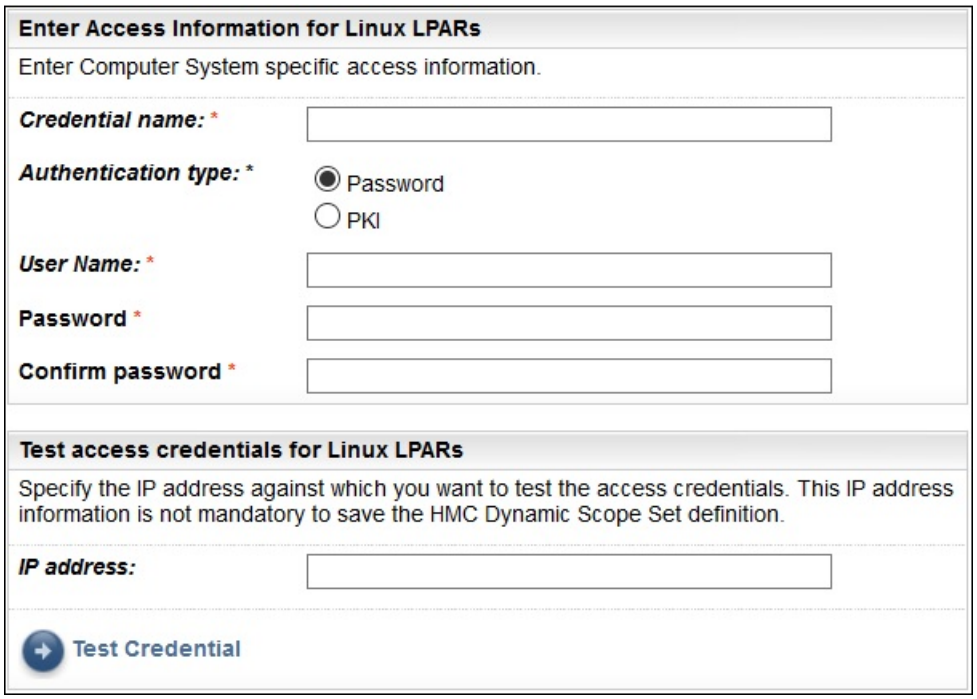

Figure 46. Exemple : Entrer les informations d'accès pour les partitions logiques LINUX

   a) Entrez le **Nom des données d'identification**.
   b) Sélectionnez le **Type d'authentification** :
      - **Mot de passe** - utilise le mot de passe fourni.
      - **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.
   c) Entrez le **Nom d'utilisateur** qui permet de vous authentifier lors de la connexion à la partition logique concernée.

d) Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

e) Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

f) Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur chaque LPAR.

g) Facultatif : Entrez l'**Adresse IP** d'une LPAR gérée par cette HMC et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la LPAR cible.

8. Cliquez sur **Enregistrer** pour enregistrer l'ensemble de périmètres dynamiques HMC.

Modifier des périmètres dynamiques HMC - Adresses IP HMC
Vous pouvez modifier la liste des adresses IP HMC associées à un ensemble de périmètres dynamiques HMC existant.

Pourquoi et quand exécuter cette tâche
Pour modifier la liste des adresses IP HMC, suivez ces étapes.

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.
   La page **Périmètres dynamiques HMC** s'affiche.
2. Pour éditer l'ensemble de périmètres, cliquez sur l'icône .
   La page **Ensemble de périmètres dynamiques HMC** s'affiche.
   - Pour ajouter une adresse IP HMC à l'ensemble de périmètres, suivez ces étapes :
     a. Dans le panneau **HMC**, cliquez sur **Ajouter une HMC**. La page **Périmètres dynamiques HMC** s'affiche.
     b. Entrez l'**Adresse IP** de la HMC dans le panneau **Décrire l'adresse ou l'hôte**.
     c. Cliquez sur **Enregistrer** pour enregistrer la HMC.
   - Pour éditer une adresse IP HMC existante dans l'ensemble de périmètres, suivez ces étapes :
     a. Dans le panneau **HMC**, cliquez sur l'icône . La page **Périmètres dynamiques HMC** s'affiche.
     b. Modifiez l'**Adresse IP** de la HMC dans le panneau **Décrire l'adresse ou l'hôte**.
     c. Cliquez sur **Enregistrer** pour modifier la HMC.
   - Pour supprimer une adresse IP HMC existante dans l'ensemble de périmètres, suivez ces étapes :
     a. Dans le panneau **HMC**, cliquez sur l'icône .
     b. Dans la boîte de dialogue, cliquez sur **OK** pour confirmer la suppression.

        Remarque : Un ensemble de périmètres dynamiques HMC doit toujours avoir au moins une adresse IP HMC de définie. TSA n'autorise pas la suppression de toutes les adresses IP HMC.

Modifier des périmètres dynamiques HMC - Données d'identification
Vous pouvez modifier la liste des données d'identification associées à un ensemble de périmètres dynamiques HMC existant.

Pourquoi et quand exécuter cette tâche
Un ensemble de périmètres dynamiques HMC doit toujours avoir au moins un jeu de données d'identification HMC de défini. TSA n'autorise pas la suppression de toutes les données d'identification HMC. S'il n'existe aucun jeu de données d'identification pour un type de LPAR AIX, Linux ou VIOS, TSA ne recueillera aucune information détaillée concernant ce type de LPAR.

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche.

2. Pour éditer l'ensemble de périmètres, cliquez sur l'icône .

   La page **Ensemble de périmètres dynamiques HMC** s'affiche.

   - Pour ajouter un jeu de données d'identification pour HMC, AIX, Linux ou VIOS, suivez ces étapes :

     a. Dans le panneau **Données d'identification** approprié, cliquez sur **Ajouter des données d'identification**. Par exemple, pour ajouter un jeu de données d'identification HMC, cliquez sur **Ajouter des données d'identification HMC** dans le panneau **Données d'identification HMC**. La page **Nouvelles données d'identification de reconnaissance HMC** apparaît.

     b. Entrez le **Nom des données d'identification**.

     c. Sélectionnez le **Type d'authentification** :

        – **Mot de passe** - utilise le mot de passe fourni.

        – **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.

     d. Entrez le **Nom d'utilisateur** qui servira à s'authentifier auprès de la HMC ou de la LPAR concernée.

     e. Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

     f. Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

     g. Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur les HMC ou les LPAR.

     h. **Optionnel :** Entrez l'**Adresse IP** de la HMC ou LPAR et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la LPAR cible.

     i. Cliquez sur **Enregistrer** pour enregistrer le jeu de données d'identification de l'ensemble de périmètres dynamiques HMC.

   - Pour éditer un jeu de données d'identification pour HMC, AIX, Linux ou VIOS, suivez ces étapes :

     a. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône du jeu de données d'identification que vous voulez modifier. Par exemple, pour éditer un jeu de données d'identification HMC, dans le panneau **Données d'identification HMC**, cliquez sur l'icône du jeu de données à modifier. La page **Modifier les données d'identification de reconnaissance HMC** apparaît.

     b. Dans le panneau **Entrer les informations d'accès**, vous pouvez modifier les détails suivants :

        1) Entrez le **Nom d'utilisateur** qui servira à s'authentifier auprès de la HMC ou de la LPAR concernée.

        2) Sélectionnez le **Type d'authentification** :

           – **Mot de passe** - utilise le mot de passe fourni.

           – **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.

        3) Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

        4) Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

5) Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur chaque HMC ou LPAR.

c. **Optionnel :** Entrez l'**Adresse IP** de la HMC ou LPAR et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la LPAR cible.

d. Cliquez sur **Enregistrer** pour enregistrer les modifications des données d'identification concernées.

- Pour supprimer un jeu de données d'identification pour HMC, AIX, Linux ou VIOS, suivez ces étapes :

  a. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône **Supprimer** du jeu de données d'identification concerné. Par exemple, pour supprimer un jeu de données d'identification HMC, dans le panneau **Données d'identification HMC**, cliquez sur l'icône du jeu de données à supprimer. Un message de confirmation s'affiche.

  b. Cliquez sur **OK** pour supprimer les données d'identification concernées.

- Pour changer l'ordre d'apparition d'un jeu de données d'identification pour HMC, AIX, Linux ou VIOS, suivez ces étapes :

  a. S'il existe plusieurs jeux de données d'identification pour HMC, AIX, Linux ou VIOS, il est possible de changer leur ordre pour les HMC ou les LPAR. Lorsqu'il n'existe qu'un seul jeu de données d'identification, les flèches vers le haut et vers le bas n'apparaissent pas dans la colonne **Actions** du panneau des données d'identification.

  b. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône ou pour changer la position du jeu de données d'identification par rapport aux autres.

Activer ou désactiver des ensembles de périmètres dynamiques
Vous pouvez activer ou désactiver un ensemble de périmètres dynamiques HMC.

Pourquoi et quand exécuter cette tâche

Un ensemble de périmètres désactivé est ignoré lors d'une découverte programmée.

Remarque : Il est toujours possible d'effectuer une découverte manuel, quel que soit l'état de l'ensemble de périmètres.

Désactiver des ensembles de périmètres dynamiques

Procédure

Pour désactiver un ensemble de périmètres dynamiques HMC, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.
   La page **Périmètres dynamiques HMC** s'affiche.
2. Cliquez sur l'icône **Activer** à côté de l'ensemble de périmètres que vous voulez désactiver.

Activer des ensembles de périmètres dynamiques

Procédure

Pour activer un ensemble de périmètres dynamiques HMC, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.
   La page **Périmètres dynamiques HMC** s'affiche.
2. Cliquez sur l'icône **Désactiver** à côté de l'ensemble de périmètres que vous voulez activer.

Découvrir une HMC
Vous pouvez lancer vous-même la découverte d'une HMC particulière au sein d'un ensemble de périmètres dynamiques HMC. Des informations seront collectées à propos de cette HMC ainsi que sur ses LPAR associées.

Procédure

Pour lancer la découverte d'une HMC, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche.
2. Cliquez sur l'icône de l'ensemble de périmètres dynamiques HMC voulu. La page **Ensemble de périmètres dynamiques HMC** s'affiche.
3. Cliquez sur l'icône à côté de l'adresse IP de la HMC que vous voulez découvrir.

Découvrir des ensembles de périmètres dynamiques
Vous pouvez lancer vous-même la découverte d'un ensemble de périmètres dynamiques HMC. Des informations seront collectées à propos de toutes les HMC définies à l'ensemble de périmètres, ainsi que sur ses LPAR associées.

Procédure

Pour lancer la découverte d'un ensemble de périmètres dynamiques HMC, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche.
2. Cliquez sur l'icône **Exécuter** à côté de l'ensemble de périmètres que vous voulez découvrir.

Supprimer des périmètres dynamiques HMC
Vous pouvez supprimer un ensemble de périmètres dynamiques HMC existant.

Procédure

Pour supprimer un ensemble de périmètres dynamiques HMC, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche.
2. Cliquez sur l'icône **Supprimer** en regard de l'ensemble de périmètres à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression de l'ensemble de périmètres dynamiques HMC.

   Remarque : Lorsque vous confirmez la suppression d'un ensemble de périmètres dynamiques HMC, les informations d'accès aux LPAR AIX, Linux ou VIOS associées sont également supprimées.

Périmètres dynamiques VMware

Vous pouvez définir des périmètres dynamiques VMware afin de dresser un inventaire détaillé des instances VMware vCenter Servers et ESXi. Les périmètres dynamiques VMware recueille aussi des informations sur les serveurs x86 gérés par une instance VMware vCenter Server ou ESXi, ainsi que sur les machines virtuelles Linux et Windows présentes sur ces systèmes.

TSA obtient des informations d'inventaire auprès des instances VMware vCenter Server et ESXi définies. Il se renseigne aussi dynamiquement sur les machines virtuelles gérées par ces instances VMware sans qu'il soit nécessaire de créer et de tenir à jour plusieurs définitions de périmètres. Vous devez définir un périmètre pour les instances VMware et sélectionner quels types de machines virtuelles (Linux et Windows) vous souhaiteriez voir analyser automatiquement lorsque ces instances VMware sont découvertes. L'avantage est que même si les machines virtuelles changent, vous n'avez pas à reconfigurer TSA.

Lorsqu'une instance VMware vCenter Server est découverte, toutes les instances VMware ESXi qu'elle gère sont trouvées, ce qui élimine la nécessité de les découvrir directement. Les instances VMware ESXi qui ne sont pas gérées par une instance VMware vCenter Server peuvent être découvertes directement par TSA à condition qu'elles soient définies dans le périmètre dynamique VMware.

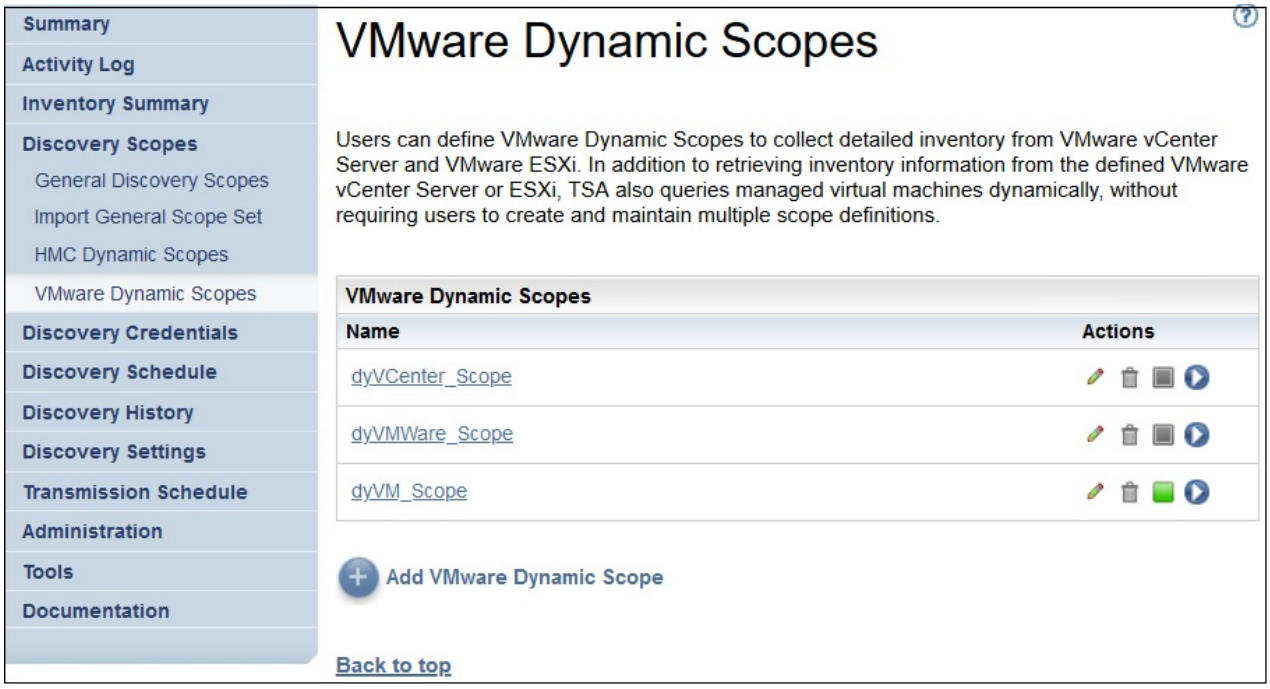

Figure 47. Périmètres dynamiques VMware

Afficher des périmètres dynamiques VMware, des ensembles de périmètres et leurs données d'identification

Vous pouvez afficher les périmètres et les ensembles de périmètres dynamiques VMware existants.

Pourquoi et quand exécuter cette tâche

Pour afficher les ensembles de périmètres dynamiques VMware existants, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware** dans le panneau de navigation. La page **Périmètres dynamiques VMware** s'affiche. Le panneau **Périmètres dynamiques VMware** contient la liste des périmètres dynamiques VMware.

Pour afficher les périmètres et les données d'identification associés à un ensemble de périmètres dynamique spécifique, cliquez sur le nom de celui-ci dans la colonne **Nom**. La page **Ensemble de périmètres dynamiques VMware** s'affiche.

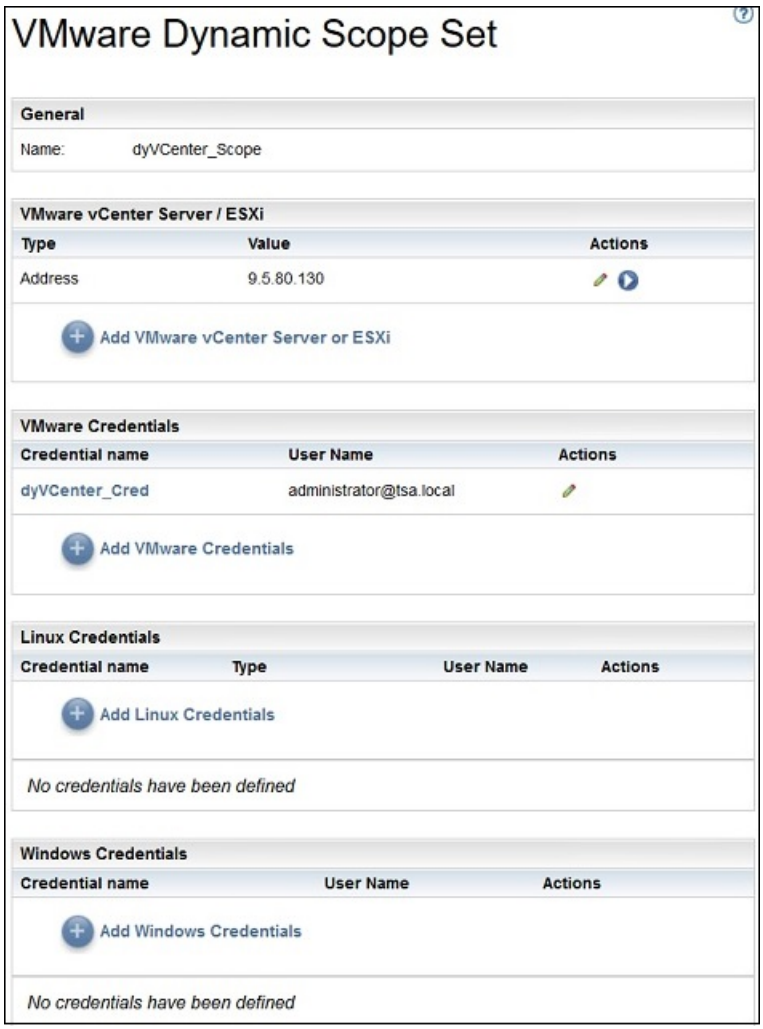

Figure 48. Vue d'un ensemble de périmètres dynamiques VMware

Le panneau **VMware vCenter Server / ESXi** affiche la liste des adresses IP des instances VMware vCenter Server et ESXi découvertes par l'ensemble de périmètres dynamiques. Les différents panneaux de données d'identification, tels que **Données d'identification Linux**, affichent la liste des données d'identification configurées dans l'ensemble de périmètres.

Ajout de périmètres dynamiques VMware

Pour ajouter un ensemble de périmètres dynamiques VMware, indiquez l'adresse IP d'une unique instance VMware vCenter Server ou ESXi ainsi qu'un unique jeu de données d'identification permettant d'accéder à l'instance VMware. Au besoin, vous pouvez spécifier les données d'identification pour Linux et Windows afin d'autoriser la découverte des machines virtuelles des serveurs x86 gérés par l'instance VMware. Une fois l'ensemble de périmètres dynamiques VMware créé, vous pouvez l'éditer pour définir des adresses IP VMware vCenter Server ou ESXi supplémentaires. Il est aussi possible d'éditer un ensemble de périmètres dynamiques VMware afin de rendre l'instance VMware accessible avec plusieurs jeux de données d'identification ainsi que pour accéder aux machines virtuelles.

Pourquoi et quand exécuter cette tâche

Pour ajouter un ensemble de périmètres dynamiques VMware, suivez ces étapes :

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.

La page **Périmètres dynamiques VMware** s'affiche.

2. Pour définir un nouvel ensemble de périmètres dynamiques VMware, cliquez sur **Ajouter un périmètre dynamique VMware**.

   La page **Ensemble de périmètres dynamiques VMware** s'affiche.

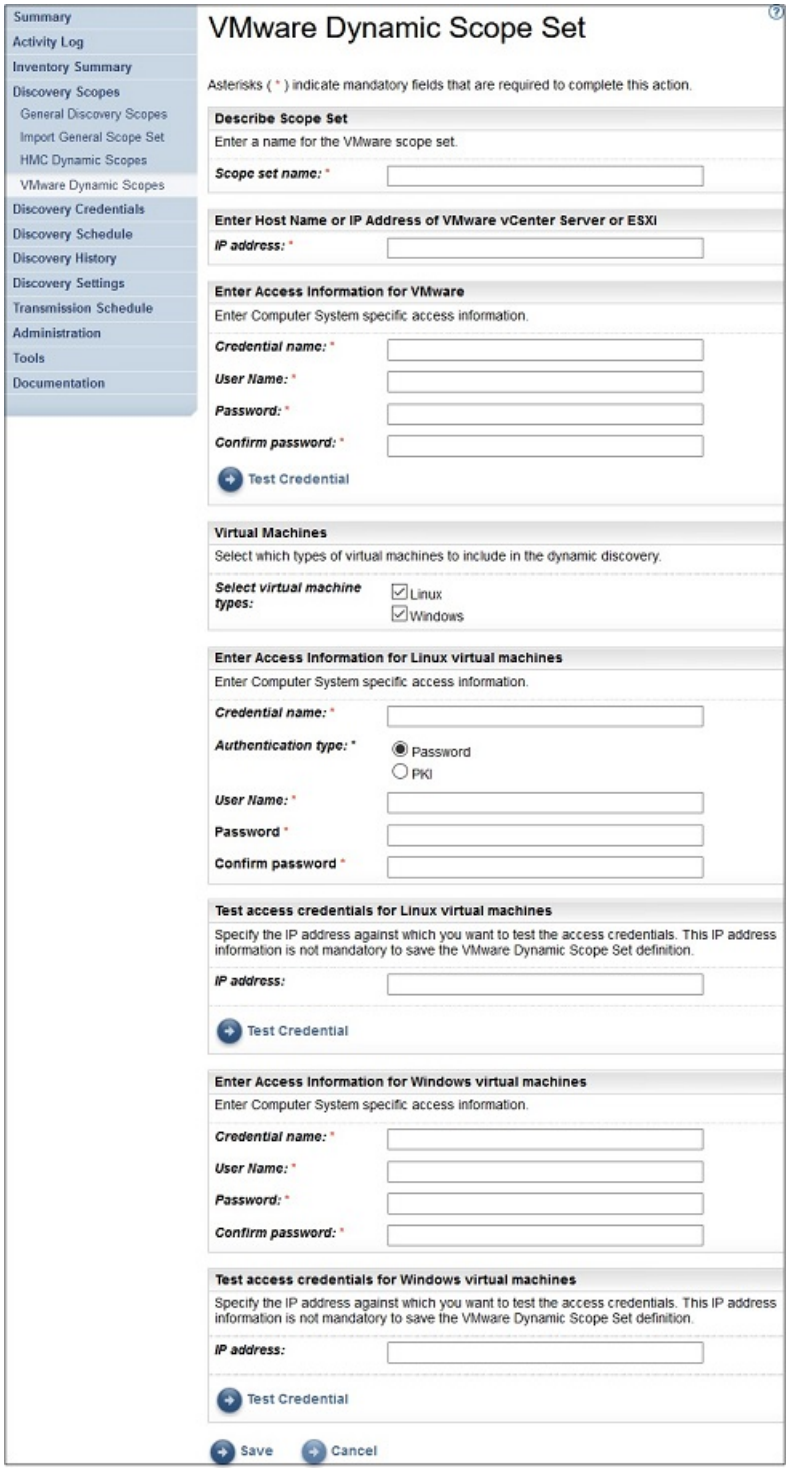

Figure 49. Ajouter un ensemble de périmètres dynamiques VMware

3. Dans le panneau **Décrire l'ensemble de périmètres**, entrez un nom unique dans le champ **Nom de l'ensemble de périmètres**.
4. Dans le panneau **Entrer le nom d'hôte ou l'adresse IP de VMware vCenter Server ou ESXi**, entrez l'adresse IP ou le nom d'hôte de l'instance VMware vCenter Server ou ESXi.
5. Dans le panneau **Entrer les informations d'accès pour VMware**, entrez les détails suivants :

a) Entrez le **Nom des données d'identification**.

b) Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de l'instance VMware vCenter Server ou ESXi

c) Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

d) Facultatif : Cliquez sur **Tester les données d'identification** pour tester les données d'identification de l'instance VMware vCenter Server ou ESXi cible.

6. Dans le panneau **Machines virtuelles**, sélectionnez les types de machines virtuelles (Linux, Windows) à inclure dans la découverte dynamique.
7. Si vous sélectionnez Machine virtuelle Linux, entrez les informations d'accès correspondantes.

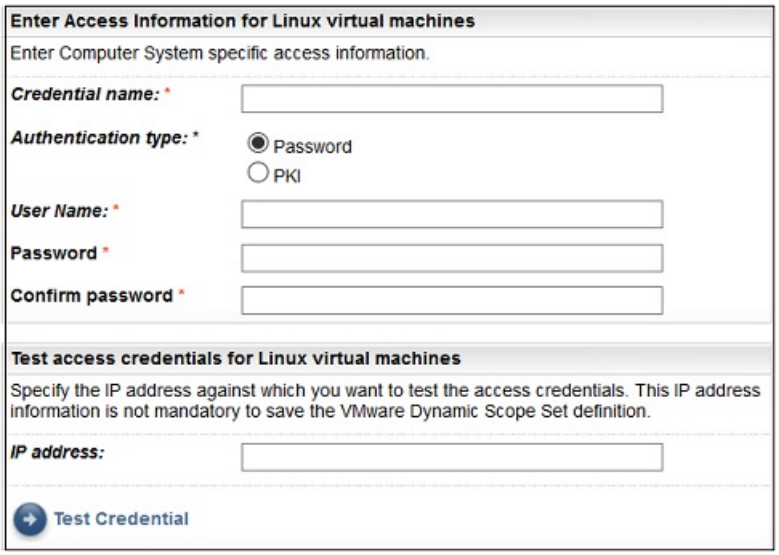

Figure 50. Entrer les informations d'accès pour une machine virtuelle Linux

a) Entrez le **Nom des données d'identification**.

b) Sélectionnez le **Type d'authentification** :

- **Mot de passe** - utilise le mot de passe fourni.
- **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.

c) Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de la machine virtuelle concernée.

d) Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

e) Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

f) Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur chaque machine virtuelle.

g) Facultatif : Entrez l'**Adresse IP** de la machine virtuelle et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la machine virtuelle cible.

8. Si vous sélectionnez Machine virtuelle Windows, entrez les informations d'accès correspondantes.

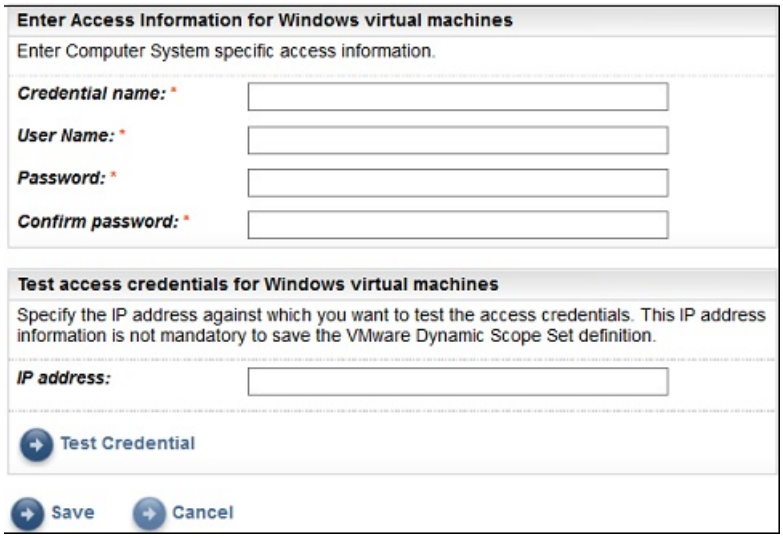

Figure 51. Entrer les informations d'accès pour une machine virtuelle Windows

a) Entrez le **Nom des données d'identification**.

b) Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de la machine virtuelle concernée.

c) Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

d) Facultatif : Entrez l'**Adresse IP** de la machine virtuelle et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la machine virtuelle cible.

9. Cliquez sur **Enregistrer** pour enregistrer l'ensemble de périmètres dynamiques VMware.

Modifier des périmètres dynamiques VMware - Adresses IP VMware vCenter Server ou ESXi
Vous pouvez modifier la liste des adresses IP VMware vCenter Server ou ESXi associée à un ensemble de périmètres dynamiques VMware existant.

Pourquoi et quand exécuter cette tâche
Pour modifier la liste des adresses IP VMware vCenter Server ou ESXi, suivez ces étapes.

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.
   La page **Périmètres dynamiques VMware** s'affiche.
2. Pour éditer l'ensemble de périmètres, cliquez sur l'icône .
   La page **Ensemble de périmètres dynamiques VMware** s'affiche.
   - Pour ajouter une adresse IP VMware vCenter Server ou ESXi à l'ensemble de périmètres, suivez ces étapes :
     a. Dans le panneau **VMware vCenter Server / ESXi**, cliquez sur **Ajouter un système VMware vCenter Server ou ESXi**. La page **Périmètres dynamiques VMware** s'affiche.
     b. Entrez l'**adresse IP** du système VMware vCenter Server ou ESXi dans le panneau **Décrire l'adresse ou l'hôte**.
     c. Cliquez sur **Enregistrer** pour ajouter l'instance VMware vCenter Server ou ESXi.
   - Pour éditer une adresse IP VMware vCenter Server ou ESXi existante dans l'ensemble de périmètres, suivez ces étapes :
     a. Dans le panneau **VMware vCenter Server/ESXi**, cliquez sur l'icône . La page **Périmètres dynamiques VMware** s'affiche.

b. Modifiez l'**adresse IP** de l'instance VMware vCenter Server ou ESXi dans le panneau **Décrire l'adresse ou l'hôte**.

c. Cliquez sur **Enregistrer**.

- Pour supprimer une adresse IP VMware vCenter Server ou ESXi existante dans l'ensemble de périmètres, suivez ces étapes :

  a. Dans le panneau **VMware vCenter Server/ESXi**, cliquez sur l'icône .

  b. Dans la boîte de dialogue, cliquez sur **OK** pour confirmer la suppression.

  Remarque : Un ensemble de périmètres dynamiques VMware doit toujours avoir au moins une adresse IP VMware vCenter Server ou ESXi de définie. TSA n'autorise pas la suppression de toutes les adresses IP VMware.

Modifier des périmètres dynamiques VMware - Données d'identification
Vous pouvez modifier la liste des données d'identification associées à un ensemble de périmètres dynamiques VMware existant.

Pourquoi et quand exécuter cette tâche
Un ensemble de périmètres dynamiques VMware doit toujours avoir au moins un jeu de données d'identification VMware de défini. TSA n'autorise pas la suppression de toutes les données d'identification VMware. S'il n'existe aucun jeu de données d'identification pour un type de machine virtuelle (Linux ou Windows), TSA ne recueillera aucune information détaillée concernant ce type de machine virtuelle.

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.
   La page **Périmètres dynamiques VMware** s'affiche.
2. Pour éditer l'ensemble de périmètres, cliquez sur l'icône .
   La page **Ensemble de périmètres dynamiques VMware** s'affiche.
   - Pour ajouter un jeu de données d'identification pour VMware ou Windows, suivez ces étapes :

     a. Dans le panneau **Données d'identification** approprié, cliquez sur **Ajouter des données d'identification**. Par exemple, pour ajouter un jeu de données d'identification VMware, cliquez sur **Ajouter des données d'identification VMware** dans le panneau **Données d'identification VMware**. La page **Nouvelles données d'identification de reconnaissance VMware** apparaît.

     b. Entrez le **Nom des données d'identification**.

     c. Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de l'instance VMware vCenter Server ou ESXi ou des machines virtuelles Windows.

     d. Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

     e. **Optionnel :** Entrez l'**Adresse IP** de l'instance VMware vCenter Server ou ESXi ou de la machine virtuelle Windows et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la cible.

     f. Cliquez sur **Enregistrer** pour enregistrer le jeu de données d'identification associé.
   - Pour ajouter un jeu de données d'identification pour Linux, suivez ces étapes :

     a. Dans le panneau **Données d'identification Linux**, cliquez sur **Ajouter des données d'identification Linux**. La page **Nouvelles données d'identification de reconnaissance VMware** apparaît.

     b. Entrez le **Nom des données d'identification**.

     c. Sélectionnez le **Type d'authentification** :

        – **Mot de passe** - utilise le mot de passe fourni.

        – **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.

d. Entrez le **Nom d'utilisateur** servant à s'authentifier auprès des machines virtuelles Linux.

e. Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

f. Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

g. Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur les machines virtuelles Linux.

h. **Optionnel :** Entrez l'**Adresse IP** de la machine virtuelle Linux et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la machine virtuelle Linux cible.

i. Cliquez sur **Enregistrer** pour enregistrer le jeu de données d'identification Linux.

- Pour éditer un jeu de données d'identification pour VMware ou Windows, suivez ces étapes :

  a. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône du jeu de données d'identification que vous voulez modifier. Par exemple, pour éditer un jeu de données d'identification VMware, dans le panneau **Données d'identification VMware**, cliquez sur l'icône du jeu de données à modifier. La page **Modifier les données d'identification de reconnaissance VMware** apparaît.

  b. Dans le panneau **Entrer les informations d'accès**, vous pouvez modifier les détails suivants :

     1) Entrez le **Nom d'utilisateur** servant à s'authentifier lors de la connexion aux instances VMware vCenter Server ou ESXi ou aux machines virtuelles Windows.

     2) Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

  c. **Optionnel :** Entrez l'**Adresse IP** de l'instance VMware vCenter Server ou ESXi ou de la machine virtuelle Windows et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la cible.

  d. Cliquez sur **Enregistrer** pour enregistrer les modifications des données d'identification concernées.

- Pour éditer un jeu de données d'identification pour Linux, suivez ces étapes :

  a. Dans le panneau **Données d'identification Linux**, cliquez sur l'icône du jeu de données d'identification que vous voulez modifier. La page **Modifier les données d'identification de reconnaissance VMware** apparaît.

  b. Dans le panneau **Entrer les informations d'accès**, vous pouvez modifier les détails suivants :

     1) Sélectionnez le **Type d'authentification** :

        – **Mot de passe** - utilise le mot de passe fourni.

        – **Infrastructure PKI** - utilise la clé SSH associée à l'ensemble de périmètres spécifique.

     2) Entrez le **Nom d'utilisateur** servant à s'authentifier auprès de la machine virtuelle Linux.

     3) Lorsque **Type d'authentification** est **Mot de passe**, Entrez le **Mot de passe** et cliquez sur **Confirmer le mot de passe**.

     4) Lorsque **Type d'authentification** est **Infrastructure PKI**, entrez la **Phrase de passe** et **Confirmez la phrase de passe** si la SSH est chiffrée. Si la clé SSH n'est pas chiffrée, n'entrez rien dans ces champs.

     5) Si **Type d'authentification** est **Infrastructure PKI**, cliquez sur **Choisir un fichier** et remontez la clé privée vers TSA. Vous devez déployer la clé publique à l'extérieur sur les machines virtuelles Linux.

     6) **Optionnel :** Entrez l'**Adresse IP** de la machine virtuelle et cliquez sur **Tester les données d'identification** pour tester les données d'identification de la machine virtuelle Linux cible.

c. Cliquez sur **Enregistrer** pour enregistrer les modifications des données d'identification concernées.

- Pour supprimer un jeu de données d'identification pour VMware, Linux ou Windows, suivez ces étapes :

  a. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône **Supprimer** du jeu de données d'identification concerné. Par exemple, pour supprimer un jeu de données d'identification VMware, dans le panneau **Données d'identification VMware**, cliquez sur l'icône du jeu de données à supprimer. Un message de confirmation s'affiche.

  b. Cliquez sur **OK** pour supprimer les données d'identification concernées.

- Pour changer l'ordre d'apparition d'un jeu de données d'identification pour VMware, Linux ou Windows, suivez ces étapes :

  a. S'il existe plusieurs jeux de données d'identification pour VMware, Linux ou Windows, il est possible de changer leur ordre pour les instances VMware ou les machines virtuelles. Lorsqu'il n'existe qu'un seul jeu de données d'identification, les flèches vers le haut et vers le bas n'apparaissent pas dans la colonne **Actions** du panneau des données d'identification.

  b. Dans le panneau **Données d'identification** approprié, cliquez sur l'icône ou pour changer la position du jeu de données d'identification par rapport aux autres.

Activer ou désactiver des ensembles de périmètres dynamiques
Vous pouvez activer ou désactiver un ensemble de périmètres dynamiques VMware.

Pourquoi et quand exécuter cette tâche

Un ensemble de périmètres désactivé est ignoré lors d'une découverte programmée.

Remarque : Il est toujours possible d'effectuer une découverte manuel, quel que soit l'état de l'ensemble de périmètres.

Désactiver des ensembles de périmètres dynamiques

Procédure

Pour désactiver un ensemble de périmètres dynamiques VMware, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.

   La page **Périmètres dynamiques VMware** s'affiche.
2. Cliquez sur l'icône **Activer** à côté de l'ensemble de périmètres que vous voulez désactiver.

Activer des ensembles de périmètres dynamiques

Procédure

Pour activer un ensemble de périmètres dynamiques VMware, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.

   La page **Périmètres dynamiques VMware** s'affiche.
2. Cliquez sur l'icône **Désactiver** à côté de l'ensemble de périmètres que vous voulez activer.

Découvrir un VMware vCenter ou ESXi
Vous pouvez lancer vous-même la découverte d'une instance particulière de VMware vCenter Server ou ESXi au sein d'un ensemble de périmètres dynamiques VMware. Des informations seront collectées à propos de cette instance VMware ainsi que sur ses machines virtuelles associées.

Procédure

Pour lancer la découverte d'un VMware vCenter Server ou ESXi, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.
   La page **Périmètres dynamiques VMware** s'affiche.
2. Cliquez sur l'icône de l'ensemble de périmètres dynamiques VMware voulu. La page **Ensemble de périmètres dynamiques VMware** s'affiche.
3. Cliquez sur l'icône à côté de l'adresse IP du VMware vCenter Server ou ESXi que vous voulez découvrir.

Découvrir des ensembles de périmètres dynamiques
Vous pouvez lancer vous-même la découverte d'un ensemble de périmètres dynamiques VMware. Des informations seront collectées à propos de toutes les instances VMware vCenter Server ou ESXi définies à l'ensemble de périmètres, ainsi que sur leurs machines virtuelles associées.

Procédure

Pour lancer la découverte d'un ensemble de périmètres dynamiques VMware, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**.
   La page **Périmètres dynamiques VMware** s'affiche.
2. Cliquez sur l'icône **Exécuter** à côté de l'ensemble de périmètres que vous voulez découvrir.

Suppression de périmètres dynamiques VMware
Vous pouvez supprimer un ensemble de périmètres dynamiques VMware existant.

Procédure

Pour supprimer un ensemble de périmètres dynamiques VMware, suivez ces étapes :

1. Dans le panneau de navigation, cliquez sur **Périmètres dynamiques VMware**.
   La page **Périmètres dynamiques VMware** s'affiche.
2. Cliquez sur l'icône **Supprimer** en regard de l'ensemble de périmètres à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression de l'ensemble de périmètres dynamiques VMware.

   Remarque : Lorsque vous confirmez la suppression d'un ensemble de périmètres dynamiques VMware, les informations d'accès aux machines virtuelles Linux ou Windows associées sont également supprimées.

Périmètres de reconnaissance généraux

Le processus de reconnaissance recherche des éléments informatiques dans votre infrastructure. Un périmètre de reconnaissance définit une adresse IP ou une plage d'adresses IP qui seront explorées lors du processus de reconnaissance. Les périmètres de reconnaissance sont groupés en ensembles de périmètres dont le nom est défini par l'utilisateur.

Afficher des périmètres et des ensembles de périmètres de reconnaissance

Vous pouvez afficher les périmètres et les ensembles de périmètres de reconnaissance existants.

Pourquoi et quand exécuter cette tâche

Pour afficher les ensembles de périmètres de reconnaissance existants, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux** dans le panneau de navigation. La page **Périmètres de reconnaissance généraux** s'affiche. Le panneau **Périmètres de reconnaissance généraux** contient la liste des ensembles de périmètres.

Pour afficher les périmètres contenus dans un ensemble de périmètres, cliquez sur l'ensemble de périmètres concerné. La page **Ensemble de périmètres de reconnaissance** s'affiche.

- Le panneau **Général** affiche le nom de l'ensemble de périmètres.
- Le panneau **Nombre d'adresses IP** affiche le nombre total d'adresses IP dans l'ensemble de périmètres.
- Le panneau **Périmètres** affiche le détail des périmètres contenus dans cet ensemble de périmètres.

Ajouter des périmètres de reconnaissance

Vous pouvez ajouter un ensemble de périmètres et un nouveau périmètre à cet ensemble, ajouter un périmètre à un ensemble de périmètres existant ou déplacer des périmètres vers d'autres ensembles de périmètres. Pour ajouter un périmètre, indiquez une adresse IP valide, une plage d'adresses IP, un réseau ou un sous-réseau.

Pourquoi et quand exécuter cette tâche

Astuces : Il y a des aspects pratiques à prendre en compte pour configurer les périmètres de reconnaissance et les ensembles de périmètres.

- Plus il y a d'adresses IP dans le périmètre de reconnaissance, plus la reconnaissance est longue. Vous pouvez modifier la taille de la reconnaissance en désactivant ou en activant des ensembles de périmètres ou en excluant des adresses IP, des plages d'adresses IP, des réseaux ou des sous-réseaux d'un périmètre dans un ensemble de périmètres.

  Pour réduire la durée d'une reconnaissance, configurez les périmètres de reconnaissance de sorte qu'ils ciblent uniquement les éléments que vous voulez reconnaître, et désactivez des ensembles de périmètres ou excluez des adresses IP, des plages d'adresses IP, des réseaux ou des sous-réseaux que vous ne voulez pas ou que vous n'avez pas besoin de reconnaître.

  Remarque : Pour de meilleures performances, limitez le nombre cumulé d'adresses IP dans un ensemble de périmètres à 400 ou moins. Pour plus d'informations sur l'importation d'un ensemble de périmètres, voir la section «Importer un ensemble de périmètres», à la page 74.
- Tous les éléments ne sont pas égaux. Par exemple, la reconnaissance d'un routeur avec des dizaines d'interfaces peut prendre plus longtemps que celle d'un hôte unique.
- Si vous utilisez l'authentification PKI pour la reconnaissance des équipements, une seule clé SSH peut être associée à chaque ensemble de périmètres.

Pour plus d'informations sur les bonnes pratiques en matière de configuration des périmètres de reconnaissance, reportez-vous au Guide de l'Assistant de la configuration de TSA (Technical Support Appliance).

Pour ajouter un ensemble de périmètres et un périmètre, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.

   La page **Périmètres de reconnaissance généraux** s'affiche.
2. Pour définir un nouvel ensemble de périmètres de reconnaissance, cliquez sur **Ajouter un nouvel ensemble de périmètres**.

La page **Ensemble de périmètres de reconnaissance** s'affiche.

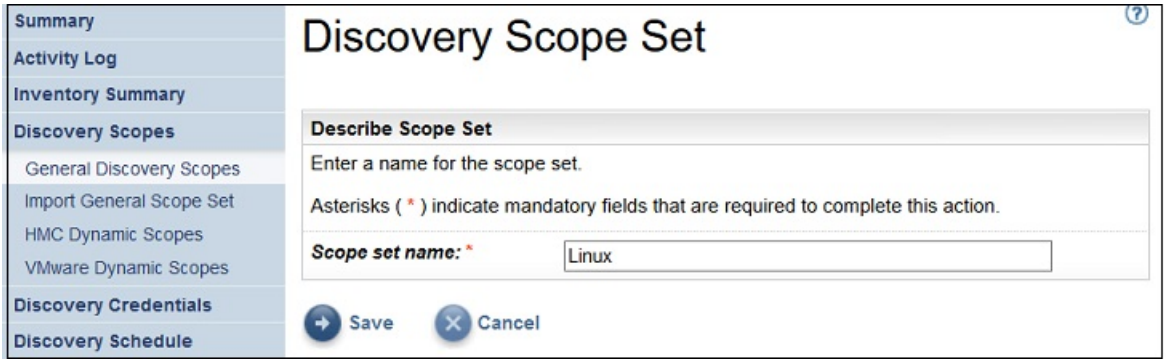

Figure 52. Ensemble de périmètres de reconnaissance

a) Entrez un nom d'ensemble de périmètres unique dans le champ **Ensemble de périmètres**.

b) Cliquez sur **Enregistrer**.

Le nouvel ensemble de périmètres est créé et la page **Périmètres de reconnaissance généraux** s'affiche.

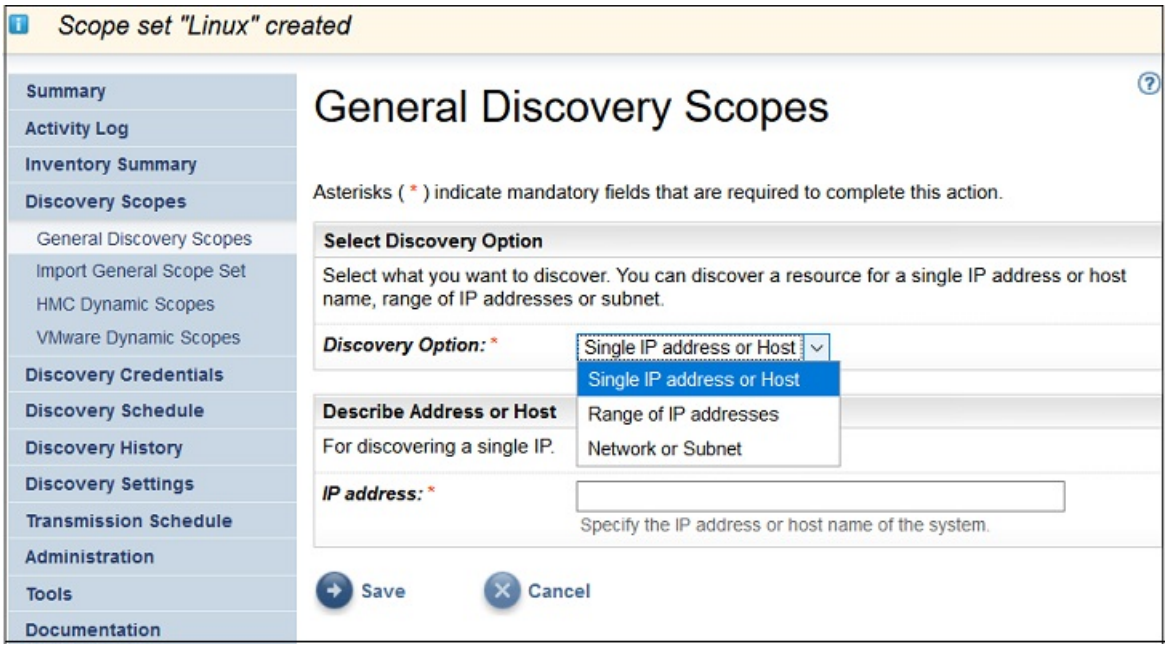

Figure 53. Périmètres de reconnaissance généraux

3. Dans le panneau **Sélectionner l'option de reconnaissance**, sélectionnez l'une des options suivantes.
   - `Adresse IP ou hôte unique`

     Dans la section **Décrire l'adresse ou l'hôte**, entrez l'adresse IP ou le nom d'hôte.
   - `Plage d'adresses IP`

     Dans la section **Décrire la plage d'adresses**, entrez l'adresse IP de début, l'adresse IP de fin et éventuellement une description dans les champs proposés.
   - `Réseau ou sous-réseau`

     Dans la section **Décrire le réseau ou le sous-réseau**, entrez l'adresse IP, le masque et éventuellement une description dans les champs proposés.
4. Si vous voulez exclure des hôtes, des adresses IP, des plages d'adresses IP ou des sous-réseaux de la reconnaissance, cliquez sur **Ajouter une exclusion** et procédez comme suit :

   a) Sélectionnez **Hôte**, **Plage** ou **Sous-réseau**.

   b) Indiquez l'adresse IP, la plage d'adresses IP ou le sous-réseau à exclure de la reconnaissance.

c) Facultatif : Entrez une description pour l'adresse IP, la plage d'adresses IP ou le sous-réseau que vous êtes en train d'exclure de la reconnaissance.

Remarque : Les exclusions ne peuvent s'appliquer qu'à un périmètre défini avec une plage d'adresses IP ou un sous-réseau.

Remarque : Vous ne pouvez pas réutiliser une adresse IP, une plage d'adresses IP, des sous-réseaux ou une description dans les périmètres ou les exclusions d'un ensemble de périmètres.

d) Pour ajouter d'autres exclusions, cliquez sur **Ajouter une exclusion** et suivez les étapes ci-dessus pour définir davantage d'exclusions.

5. Cliquez sur **Enregistrer** pour enregistrer le périmètre et les exclusions. La page **Ensemble de périmètres de reconnaissance** s'affiche avec le nouveau périmètre dans la liste.
6. Pour ajouter d'autres périmètres à cet ensemble de périmètres, cliquez sur **Ajouter un nouveau périmètre** et suivez les étapes précédentes pour définir d'autres périmètres.

Remarque : Pour de meilleures performances, limitez le nombre cumulé d'adresses IP dans un ensemble de périmètres à 400 ou moins.

Ajouter un périmètre de reconnaissance à un ensemble de périmètres existant

Vous pouvez ajouter un périmètre à un ensemble de périmètres existant.

Procédure

Pour ajouter un périmètre à un ensemble de périmètres existant, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.

   La page **Périmètres de reconnaissance généraux** s'affiche.
2. Dans le panneau **Périmètres de reconnaissance généraux**, cliquez sur l'ensemble de périmètres auquel vous voulez ajouter un périmètre.

   La page **Ensemble de périmètres de reconnaissance** s'affiche.
3. Cliquez sur **Ajouter un nouveau périmètre**.

   La page **Périmètres de reconnaissance généraux** s'affiche.
4. Dans le panneau **Sélectionner l'option de reconnaissance**, sélectionnez l'une des options suivantes.

   - `Adresse IP ou hôte unique`

     Dans la section **Décrire l'adresse ou l'hôte**, entrez l'adresse IP ou le nom d'hôte.
   - `Plage d'adresses IP`

     Dans la section **Décrire la plage d'adresses**, entrez l'adresse IP de début, l'adresse IP de fin et éventuellement une description dans les champs proposés.
   - `Réseau ou sous-réseau`

     Dans la section **Décrire le réseau ou le sous-réseau**, entrez l'adresse IP, le masque et éventuellement une description dans les champs proposés.
5. Si vous voulez exclure des hôtes, des adresses IP, des plages d'adresses IP ou des sous-réseaux de la reconnaissance, cliquez sur **Ajouter une exclusion** et procédez comme suit :

   a) Sélectionnez **Hôte**, **Plage** ou **Sous-réseau**.

   b) Indiquez l'adresse IP, la plage d'adresses IP ou le sous-réseau à exclure de la reconnaissance.

   c) Facultatif : Entrez une description pour l'adresse IP, la plage d'adresses IP ou le sous-réseau que vous êtes en train d'exclure de la reconnaissance.

   Remarque : Les exclusions ne peuvent s'appliquer qu'à un périmètre défini avec une plage d'adresses IP ou un sous-réseau.

   Remarque : Vous ne pouvez pas réutiliser une adresse IP, une plage d'adresses IP, des sous-réseaux ou une description dans les périmètres ou les exclusions d'un ensemble de périmètres.

d) Pour ajouter d'autres exclusions, cliquez sur **Ajouter une exclusion** et suivez les étapes ci-dessus pour définir davantage d'exclusions.

6. Cliquez sur **Enregistrer** pour enregistrer le périmètre et les exclusions.

   La page **Ensemble de périmètres de reconnaissance** s'affiche avec le nouveau périmètre dans la liste.

Modifier un ensemble de périmètres de reconnaissance

Vous pouvez modifier un ensemble de périmètres de reconnaissance existant en modifiant les paramètres de l'ensemble de périmètres.

Pourquoi et quand exécuter cette tâche

Pour modifier un ensemble de périmètres de reconnaissance existant, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.

   La page **Périmètres de reconnaissance généraux** s'affiche.

2. Pour modifier l'ensemble de périmètres, cliquez sur l'icône **Modifier** en regard de l'ensemble de périmètres.

   La page **Ensemble de périmètres de reconnaissance** s'affiche. Vous pouvez modifier l'ensemble de périmètres en modifiant ou en ajoutant un périmètre, en déplaçant un périmètre vers un autre ensemble de périmètres ou en supprimant un périmètre.

   - Pour ajouter un périmètre, procédez comme suit :

     a. Cliquez sur **Ajouter un nouveau périmètre**.

     b. Dans le panneau **Sélectionner l'option de reconnaissance**, sélectionnez l'une des options suivantes :

     – `Adresse IP ou hôte unique`

       Dans la section **Décrire l'adresse ou l'hôte**, entrez l'adresse IP ou le nom d'hôte.

     – `Plage d'adresses IP`

       Dans la section **Décrire la plage d'adresses**, tapez dans les champs prévus l'adresse IP de début, l'adresse IP de fin et éventuellement une description.

     – `Réseau ou sous-réseau`

       Dans la section **Décrire le réseau ou le sous-réseau**, entrez dans les champs prévus l'adresse IP, le masque et éventuellement une description.

     Remarque : Indiquez un nom unique dans le champ **Description**. Si vous spécifiez une description qui existe déjà pour un autre périmètre du même ensemble, TSA ne vous autorisera pas à créer le nouveau périmètre. Si le champ **Description** reste vide, TSA crée automatiquement la description à l'aide de la plage d'adresses IP et du masque de sous-réseau indiqués.

     c. Si vous voulez exclure des hôtes, des adresses IP ou des sous-réseaux de la reconnaissance, cliquez sur **Ajouter une exclusion** et procédez comme suit :

     1) Sélectionnez **Hôte**, **Plage** ou **Sous-réseau**.

     2) Indiquez l'adresse IP, la plage d'adresses IP ou le sous-réseau à exclure de la reconnaissance.

     3) Pour ajouter d'autres exclusions, cliquez sur **Ajouter une exclusion** et suivez les étapes ci-dessus pour définir davantage d'exclusions.

     d. Cliquez sur **Enregistrer** pour enregistrer le périmètre et les exclusions. La page **Ensemble de périmètres de reconnaissance** s'affiche avec le nouveau périmètre dans la liste.

- Pour déplacer un périmètre vers un autre ensemble de périmètres, procédez comme suit :
  a. Cliquez sur **Déplacer les périmètres**.
  b. Sur la page **Déplacer des périmètres d'un ensemble vers un autre**, sélectionnez les périmètres que vous voulez déplacer dans la liste **Périmètres**.
  c. Dans la liste **Ensemble de périmètres de destination**, sélectionnez l'ensemble de périmètres vers lequel vous voulez déplacer les périmètres sélectionnés.
  d. Cliquez sur **Déplacer**.
- Pour modifier un périmètre, procédez comme suit :
  a. Cliquez sur l'icône **Modifier** d'un périmètre donné.
  b. Vous pouvez modifier les champs **Option de reconnaissance**, **Adresses IP**, **Exclusions**, etc.
  c. Cliquez sur **Enregistrer** pour enregistrer le périmètre et les exclusions. La page **Ensemble de périmètres de reconnaissance** s'affiche avec le nouveau périmètre dans la liste.
- Pour supprimer un périmètre, procédez comme suit :
  a. Cliquez sur l'icône **Supprimer** en regard du périmètre à supprimer.
  b. Cliquez sur **OK** pour confirmer la suppression du périmètre de reconnaissance.

Supprimer des périmètres de reconnaissance
Vous pouvez supprimer des périmètres de reconnaissance existants dans un ensemble de périmètres ou supprimer des ensembles de périmètres entiers.

Pourquoi et quand exécuter cette tâche

Procédure

Pour supprimer un périmètre de reconnaissance, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.
   La page **Périmètres de reconnaissance généraux** s'affiche.
2. Modifiez l'ensemble de périmètres qui contient le périmètre de reconnaissance que vous voulez supprimer en cliquant sur l'icône **Modifier** en regard de l'ensemble de périmètres.
   La page **Ensemble de périmètres de reconnaissance** s'affiche.
3. Cliquez sur l'icône **Supprimer** en regard du périmètre à supprimer.
4. Cliquez sur **OK** pour confirmer la suppression du périmètre de reconnaissance.

Supprimer des ensembles de périmètres de reconnaissance
Vous pouvez supprimer des ensembles de périmètres de reconnaissance existants.

Procédure

Remarque : Pour supprimer un ensemble de périmètres, vous devez d'abord supprimer toutes les données d'identification associées à cet ensemble de périmètres.

Pour supprimer un ensemble de périmètres de reconnaissance, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.
   La page **Périmètres de reconnaissance généraux** s'affiche.
2. Cliquez sur l'icône **Supprimer** en regard de l'ensemble de périmètres à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression de l'ensemble de périmètres de reconnaissance.

Importer un ensemble de périmètres

Vous pouvez importer une liste d'adresses IP afin de définir un nouvel ensemble de périmètres.

Pourquoi et quand exécuter cette tâche

Un nouvel ensemble de périmètres est créé d'après le nom indiqué et la liste d'adresses IP issues du fichier d'entrée. Lors de l'importation d'un ensemble de périmètres, TSA effectue les validations suivantes :

- Vérifie si le nom de l'ensemble de périmètres existe déjà.
- Valide chaque ligne du fichier afin de vérifier si l'adresse IP est valide ou non.
- Ignore les espaces de début et de fin lors de la validation de l'adresse IP.
- Ignore les doublons d'adresse IP.

Procédure

Pour importer les adresses IP, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Importer un ensemble de périmètres généraux**.

   La page **Importer un ensemble de périmètres généraux** s'affiche.
2. Entrez le **Nouveau nom de l'ensemble de périmètres**.

   Remarque : Entrez un nom unique qui n'est pas utilisé par les ensembles de périmètres existants. Si le nom de l'ensemble de périmètres existe déjà, le message d'erreur suivant apparaît : `Le nom de l'ensemble de périmètres existe déjà.`
3. Cliquez sur **Choisir un fichier** pour sélectionner le fichier texte.

   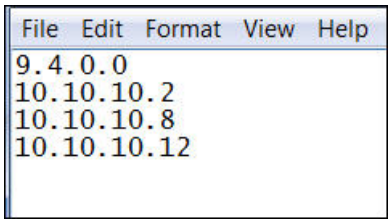

   Figure 54. Importer un ensemble de périmètres

   Remarque : Le fichier texte doit comporter une seule colonne dont chaque ligne contient une seule adresse IP et aucune autre donnée.
4. Cliquez sur **Importer le fichier de l'ensemble de périmètres** pour importer l'ensemble de périmètres. Le message d'état suivant s'affiche lorsque l'import a réussi : **`L'ensemble de périmètres a bien été importé`**.

   Remarque : Si le fichier de l'ensemble de périmètres comprend plus de 400 adresses IP, le message d'avertissement suivant s'affiche : **`L'ensemble de périmètres a bien été importé mais le nombre d'éléments de périmètre dépasse le nombre recommandé ; il doit être limité à 400 pour une performance optimale.`**
5. Après avoir importé l'ensemble de périmètres, vous pouvez l'éditer dans la section **Périmètres de reconnaissance généraux** de l'interface utilisateur et associer des données d'identification dans la section **Données d'identification de la reconnaissance**.

Paramètres de reconnaissance

Utilisez la page **Paramètres de reconnaissance** pour ajuster les paramètres de reconnaissance avancés.

Configurer les paramètres de connexion

Utilisez la page **Paramètres de connexion** pour configurer la reconnaissance SLP et reconnaître les équipements de stockage EMC via les fournisseurs EMC SMI-S.

Pourquoi et quand exécuter cette tâche

Par défaut, un travail de reconnaissance tente de trouver des fournisseurs EMC SMI-S en exécutant une requête SLP pour identifier leur adresse IP et leur numéro de port. Si le protocole SLP n'est pas disponible dans votre réseau (par exemple, si des règles de sécurité bloquent les messages SLP), la reconnaissance des unités de stockage EMC peut quand même être effectuée en désactivant la Reconnaissance SLP et en configurant les ports qu'EMC SMI-S Provider écoute pour détecter les demandes de requête.

Procédure

1. Sélectionnez l'option **Activer** ou **Désactiver** pour activer ou désactiver la reconnaissance SLP.

   Remarque : Par défaut, la reconnaissance SLP est activée.
2. Si vous désactivez la reconnaissance SLP, vous devez définir un ou plusieurs port(s) de connexion EMC SMI-S Provider.
   a) **Port(s) HTTPS EMC SMI-S :** 5989 est le port HTTPS par défaut sur lequel EMC SMI-S Provider écoute les demandes de requête. Si vous indiquez plusieurs ports, séparez-les par des virgules. EMC SMI-S écoute ces ports pour détecter les demandes de connexion (comme celles provenant de TSA). TSA doit connaître ce port pour établir la connexion.
   b) **Port(s) HTTP EMC SMI-S :** 5988 est le port HTTP par défaut sur lequel EMC SMI-S Provider écoute les demandes de requête. TSA fait d'abord une tentative de connexion HTTPS (si elle est configurée) et en cas d'échec, tente de se connecter via les ports HTTP qui sont définis. Si vous préférez éviter les connexions HTTP, ne définissez pas de ports HTTP. Si vous indiquez plusieurs ports HTTP, séparez-les par des virgules. EMC SMI-S écoute ces ports pour détecter les demandes de connexion (comme celles provenant de TSA). TSA doit connaître ce port pour établir la connexion.
3. Cliquez sur **Enregistrer** pour enregistrer les paramètres de connexion. Le message suivant apparaît : *Les paramètres de connexion de la reconnaissance ont été enregistrés avec succès.*

Données d'identification de la reconnaissance

Les données d'identification de la reconnaissance sont les noms d'utilisateur, les mots de passe ou clés SSH et les noms de communauté SNMP (Simple Network Management Protocol) que TSA utilise pour accéder aux ressources configurées dans **Périmètres de reconnaissance généraux** lors de la reconnaissance.

Afficher des données d'identification

Le processus de reconnaissance a besoin de données d'identification telles que des ID utilisateur et des mots de passe pour accéder aux ressources.

Pourquoi et quand exécuter cette tâche

Important : les informations d'accès que vous indiquez doivent correspondre aux informations d'accès à la ressource cible de reconnaissance. Si vous modifiez certaines informations d'accès comme le mot de passe sur la ressource cible, assurez-vous de modifier également les informations d'accès à Technical Support Appliance associées.

Vous pouvez afficher les données d'identification existantes en cliquant sur **Données d'identification de la reconnaissance** dans le panneau de navigation. La page **Données d'identification de la reconnaissance** s'affiche.

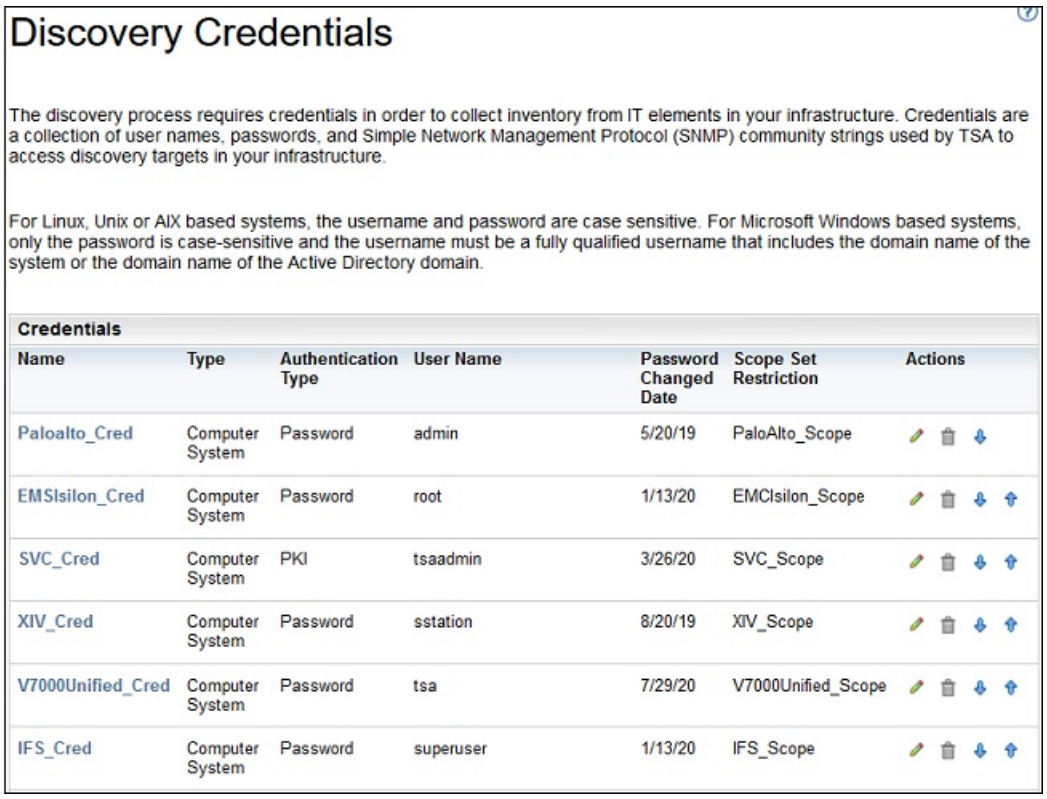

Figure 55. Nouvelles données d'identification de la reconnaissance

Afficher le détail des données d'identification

Vous pouvez afficher des informations détaillées sur jeu de données d'identification de la reconnaissance spécifique.

Pourquoi et quand exécuter cette tâche

Pour voir les détails d'un jeu de données d'identification, suivez ces étapes :

Procédure

1. Dans le panneau de navigation, cliquez sur **Données d'identification de la reconnaissance**.

   La page **Données d'identification de la reconnaissance** s'affiche avec toutes les données d'identification existantes.
2. Pour voir les détails d'un jeu de données d'identification spécifique, cliquez sur son nom.

   La page **Données d'identification de la reconnaissance** s'affiche avec des informations sur le jeu de données d'identification sélectionné.

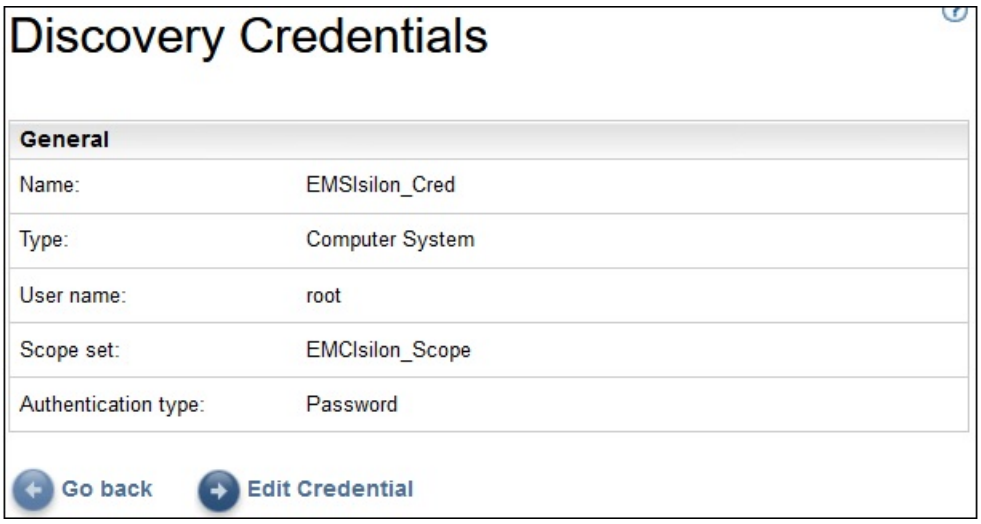

Figure 56. Détail des données d'identification de la reconnaissance

Tâches associées

Modifier les données d'identification

Vous pouvez modifier des données d'identification existantes pour proposer un contrôle d'accès pour le processus de reconnaissance.

Ajouter des données d'identification

Ajoutez des données d'identification pour proposer un contrôle d'accès pour le processus de reconnaissance.

Pourquoi et quand exécuter cette tâche

Pour ajouter des données d'identification, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Données d'identification de la reconnaissance**.
   La page **Données d'identification de la reconnaissance** s'affiche.
2. Pour créer un jeu de données d'identification, cliquez sur **Ajouter de nouvelles données d'identification**.
   La page **Nouvelles données d'identification de la reconnaissance** s'affiche.

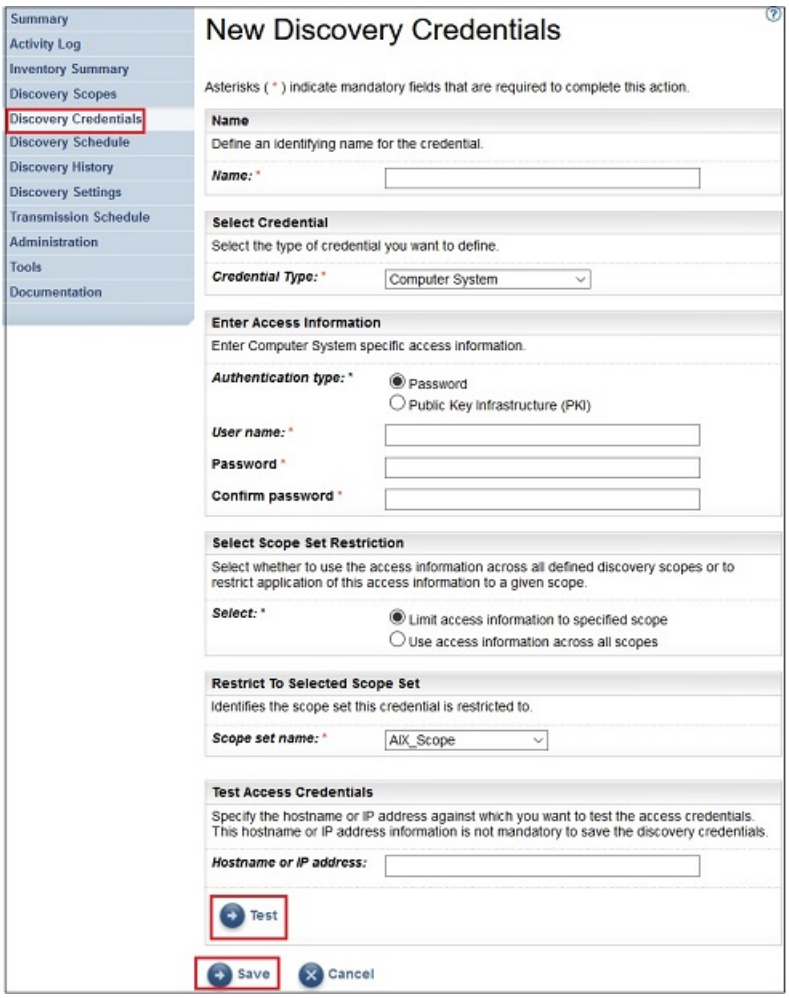

Figure 57. Nouvelles données d'identification de la reconnaissance

a) Dans le champ **Nom**, entrez un nom pour le jeu de données d'identification.

b) Dans la liste déroulante **Type de données d'identification**, sélectionnez le type de données d'identification que vous voulez créer.

c) Dans le panneau **Entrer les informations d'accès**, indiquez les informations suivantes pour le type de données d'identification sélectionné :

   Les informations requises dépendent du type de données d'identification. Pour plus d'informations sur les informations d'accès requises pour chaque type de données d'identification, voir la section «Données d'identification et configuration logicielle requises pour l'environnement de reconnaissance », à la page 6.

   Important : Les informations d'accès que vous indiquez doivent correspondre aux informations d'accès à la ressource cible de reconnaissance. Si vous modifiez certaines informations d'accès à la ressource cible, assurez-vous de modifier également les informations d'accès à TSA associées. Pour plus d'informations, référez-vous au Guide de l'Assistant de la configuration d'IBM Technical Support Appliance.

   Conseil : La page **Données d'identification de la reconnaissance** affiche la date du dernier changement du mot de passe. Si vous changez régulièrement le mot de passe sur la ressource cible, vous pouvez vous servir de cette information pour vérifier que vous avez aussi changé le mot de passe sur TSA de façon qu'il corresponde au nouveau mot de passe de la ressource cible. Pour plus d'informations sur l'affichage des données d'identification de la reconnaissance, voir la section «Afficher des données d'identification», à la page 75.

d) Le panneau **Sélectionner une restriction d'accès à l'ensemble de périmètres** sert à spécifier si un jeu de données d'identification est limité à un ensemble de périmètres en particulier ou s'il

s'applique à tous les ensembles de périmètres. Il n'est pas affiché si le **Type des données d'identification** est **Système informatique** et que le **Type d'authentification** est **Infrastructure PKI**. Les données d'identification PKI doivent toujours être limitées à un unique ensemble de périmètres.

Conseil : Créer des données d'identification qui sont limitées à un ensemble de périmètres spécifique peut améliorer les performances en réduisant le nombre de données d'identification qui sont essayées pour les ressources en cours de reconnaissance.

e) Le panneau **Limiter à l'ensemble de périmètres sélectionné** sert à limiter un jeu de données d'identification à un ensemble de périmètres spécifique. Il est visible dans les deux cas suivants.

- L'option **Limiter les informations d'accès au périmètre indiqué** est sélectionnée dans le panneau **Sélectionner une restriction d'accès à l'ensemble de périmètres** ou
- Le **Type des données d'identification** est **Système informatique** et le **Type d'authentification** est **Infrastructure PKI**.

Le jeu de données d'identification n'est utilisé que pour la reconnaissance de l'ensemble de périmètres sélectionné. Il n'est pas utilisé lors de la reconnaissance avec un autre ensemble de périmètres. Cette méthode empêche les tentatives de connexion invalides qui peuvent entraîner le blocage de l'accès à votre compte.

f) Si votre type de données d'identification est **Système informatique**, **Système informatique (Windows)**, **SNMP** ou **SNMPV3**, vous pouvez vérifier si les données d'identification sont correctes. La fonction **Test** pour le type de données d'identification **Système informatique** prend en charge les équipements suivants :

- Equipements utilisant une authentification basée sur SSH ou Telnet
- XIV
- DS6000 & DS8000
- VMware ESXi
- VMware vCenter Server
- EMC CLARiiON / VNX / VMAX via EMC SMI-S
- IBM TS3100 / TS3200
- IBM TS3310
- IBM TS3500
- IBM TS4500
- IBM TS7700
- IBM DS3000, DS4000 et DS5000 si protégé par mot de passe
- Windows
- Palo Alto Networks (PAN-OS)

Pour tester les données d'identification, entrez une adresse IP ou un nom d'hôte pour l'équipement cible sur lequel vous voulez tester les données d'identification, puis cliquez sur **Tester**.

Remarque :

- Le nom d'hôte saisi ne doit pas contenir de trait de soulignement ("_").
- Pour exécuter une reconnaissance ou tester des données d'identification sur des systèmes qui tournent sur des systèmes d'exploitation Linux, AIX, IBM i ou HP-UX, activez SSH.

g) Cliquez sur **Enregistrer**.

Les nouvelles données d'identification s'affichent sur la page **Données d'identification de la reconnaissance**.

Remarque : Il est recommandé de sauvegarder la configuration de TSA lorsque vous créez ou modifiez des données d'identification de la reconnaissance.

3. Pour modifier l'ordre dans lequel TSA utilise un jeu de données d'identification pour accéder à une ressource, cliquez soit sur l'icône **Flèche haut** , soit sur l'icône **Flèche bas** en regard du jeu de données d'identification concerné pour le faire remonter ou redescendre dans la liste.

   Pour plus d'informations sur l'utilisation de l'ordre de priorité, voir la section «Données d'identification de la reconnaissance», à la page 2.

   La page **Données d'identification de la reconnaissance** s'affiche à nouveau avec le nouvel ordre.

Modifier les données d'identification

Vous pouvez modifier des données d'identification existantes pour proposer un contrôle d'accès pour le processus de reconnaissance.

Pourquoi et quand exécuter cette tâche

Pour modifier des données d'identification, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Données d'identification de la reconnaissance**.

   La page **Données d'identification de la reconnaissance** s'affiche avec toutes les données d'identification existantes.

2. Editez le jeu de données d'identification en cliquant sur son icône **Modifier** .

   La page **Modifier les données d'identification de la reconnaissance** s'affiche.

   a) Dans le panneau **Modifier les informations d'accès**, vous pouvez changer les informations d'accès de ce jeu de données d'identification.

   Important : Les informations d'accès que vous indiquez doivent correspondre aux informations d'accès à la ressource cible de reconnaissance. Si vous modifiez certaines informations d'accès à la ressource cible, assurez-vous de modifier également les informations d'accès à TSA associées. Pour plus d'informations, référez-vous au Guide de l'Assistant de la configuration d'IBM Technical Support Appliance.

   Conseil : La page **Données d'identification de la reconnaissance** affiche la date du dernier changement du mot de passe. Si vous changez régulièrement le mot de passe sur la ressource cible, vous pouvez vous servir de cette information pour vérifier que vous avez aussi changé le mot de passe sur TSA de façon qu'il corresponde au nouveau mot de passe de la ressource cible. Pour plus d'informations sur l'affichage des données d'identification de la reconnaissance, voir la section «Afficher des données d'identification», à la page 75.

   b) Le panneau **Sélectionner une restriction d'accès à l'ensemble de périmètres** sert à spécifier si un jeu de données d'identification est limité à un ensemble de périmètres en particulier ou s'il s'applique à tous les ensembles de périmètres. Il n'est pas affiché si le **Type des données d'identification** est **Système informatique** et que le **Type d'authentification** est **Infrastructure PKI**. Les données d'identification PKI doivent toujours être limitées à un unique ensemble de périmètres.

   Conseil : Créer des données d'identification qui sont limitées à un ensemble de périmètres spécifique peut améliorer les performances en réduisant le nombre de données d'identification qui sont essayées pour les ressources en cours de reconnaissance.

   c) Le panneau **Limiter à l'ensemble de périmètres sélectionné** sert à limiter un jeu de données d'identification à un ensemble de périmètres spécifique. Il est visible dans les deux cas suivants :

   - L'option **Limiter les informations d'accès au périmètre indiqué** est sélectionnée dans le panneau **Sélectionner une restriction d'accès à l'ensemble de périmètres** ou
   - Le **Type des données d'identification** est **Système informatique** et le **Type d'authentification** est **Infrastructure PKI**.

   Le jeu de données d'identification n'est utilisé que lors de la reconnaissance de l'ensemble de périmètres sélectionné. Ce jeu de données n'est utilisé avec aucun autre ensemble de périmètres.

Cette méthode empêche les tentatives de connexion invalides qui peuvent entraîner le blocage du compte de l'utilisateur.

d) Si votre type de données d'identification est **Système informatique**, **Système informatique (Windows)**, **SNMP** ou **SNMPV3**, vous pouvez vérifier si les données d'identification sont correctes. Pour tester ces données d'identification, entrez une adresse IP ou un nom d'hôte pour la cible avec laquelle vous voulez effectuer ce test, puis cliquez sur **Tester**.

Remarque : Le nom d'hôte saisi ne doit pas contenir de trait de soulignement ("_").

e) Cliquez sur **Enregistrer**.

Les données d'identification modifiées s'affichent sur la page **Données d'identification de la reconnaissance**.

3. Pour modifier l'ordre de priorité dans lequel TSA utilise un jeu de données d'identification pour accéder à une ressource, cliquez soit sur l'icône **Flèche haut**, soit sur l'icône **Flèche bas** en regard du jeu de données d'identification concerné pour le faire remonter ou redescendre dans la liste.

Pour plus d'informations sur l'utilisation de l'ordre de priorité, voir la section «Données d'identification de la reconnaissance», à la page 2.

La page **Données d'identification de la reconnaissance** s'affiche à nouveau avec le nouvel ordre.

Concepts associés

Données d'identification de la reconnaissance
Les données d'identification de la reconnaissance sont composées de noms d'utilisateur, de mots de passe ou clés SSH et de noms de communauté SNMP (Simple Network Management Protocol) que TSA utilise pour accéder aux ressources lors de la reconnaissance.

Données d'identification et configuration logicielle requises pour l'environnement de reconnaissance
Pour reconnaître les terminaux ou les ressources de votre environnement, TSA doit avoir accès à ces ressources. Il est donc recommandé de créer un compte de service sur chaque ressource que TSA pourra spécialement utiliser lorsqu'il tentera d'accéder à la ressource concernée.

Supprimer des données d'identification

Vous pouvez supprimer des données d'identification que TSA utilise pour accéder à vos ressources.

Pourquoi et quand exécuter cette tâche

Pour supprimer un jeu de données d'identification, suivez ces étapes :

Procédure

1. Dans le panneau de navigation, cliquez sur **Données d'identification de la reconnaissance**.
   La page **Données d'identification de la reconnaissance** s'affiche.
2. Cliquez sur l'icône **Supprimer** à côté du jeu de données d'identification à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression du jeu de données d'identification.

Planning de reconnaissance

Les reconnaissances sont planifiées afin de s'assurer que les données reconnues sont toujours valides et exactes. Vous pouvez afficher le planning de reconnaissance et le détail des dernières reconnaissances, modifier les plannings de reconnaissance et désactiver des plannings de reconnaissance. Vous pouvez aussi effectuer une reconnaissance lorsque vous le souhaitez.

Avant de commencer

Par défaut, TSA utilise le planning Reconnaissance complète pour découvrir tous les éléments informatiques définis dans les périmètres dynamiques HMC et VMware ainsi que dans les périmètres de reconnaissance généraux. TSA étale automatiquement la détection des éléments informatiques pendant le processus de découverte afin de minimiser l'impact.

Une autre solution est de créer plusieurs plannings définis par l'utilisateur. Cela permet d'étaler la découverte de périmètres spécifiques en la programmant à différentes dates et heures choisies lorsque l'impact sur votre réseau et les éléments informatiques est minimal (ou idéal). Il faut dans ce cas penser à désactiver le planning de reconnaissance complète pour laisser la place aux plannings définis par l'utilisateur.

Au début d'une reconnaissance planifiée, l'appliance exécute le travail de maintenance pré-reconnaissance durant lequel certaines fonctions telles que Récapitulatif de l'inventaire, Périmètres de reconnaissance, Planning de reconnaissance et Données d'identification sont indisponibles. Durant ce travail de maintenance pré-reconnaissance, l'état du **Gestionnaire de la reconnaissance** sur la page **Récapitulatif** est défini par le symbole d'avertissement (). De plus, un message d'avertissement s'affiche sur les écrans de TSA, indiquant que certaines fonctions sont temporairement indisponibles : `Dans le cadre de la maintenance pré-reconnaissance, le Gestionnaire de la reconnaissance est temporairement désactivé. Certaines fonctions d'interface liées à la reconnaissance ou à l'inventaire peuvent n'afficher qu'une partie des informations ou aucune information pendant la durée de cette opération (en général 10 minutes maximum).`

Une fois la maintenance pré-reconnaissance réalisée avec succès, l'état du **Gestionnaire de la reconnaissance** passe à *OK*() sur la page **Récapitulatif** et reprend l'activité de reconnaissance dans son ensemble (dans les 10 minutes).

Afficher le planning de reconnaissance

Vous pouvez afficher des informations récapitulatives sur un planning de reconnaissance.

Pourquoi et quand exécuter cette tâche

Pour afficher le planning de reconnaissance, procédez comme suit :

Procédure

Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**.

La page **Planning de reconnaissance** s'affiche.

Le panneau **Planifier** affiche le nom du planning, la prochaine exécution planifiée, le planning des exécutions et les actions (Modifier (), Supprimer (), Activer / désactiver (), Exécuter ) pour chaque planning.

Cliquez sur l'icône  pour afficher tous les ensembles de périmètres qui sont affectés au planning. Pour le planning de reconnaissance complète, l'icône liste tous les ensembles de périmètres qui sont définis dans TSA et affectés au planning par défaut.

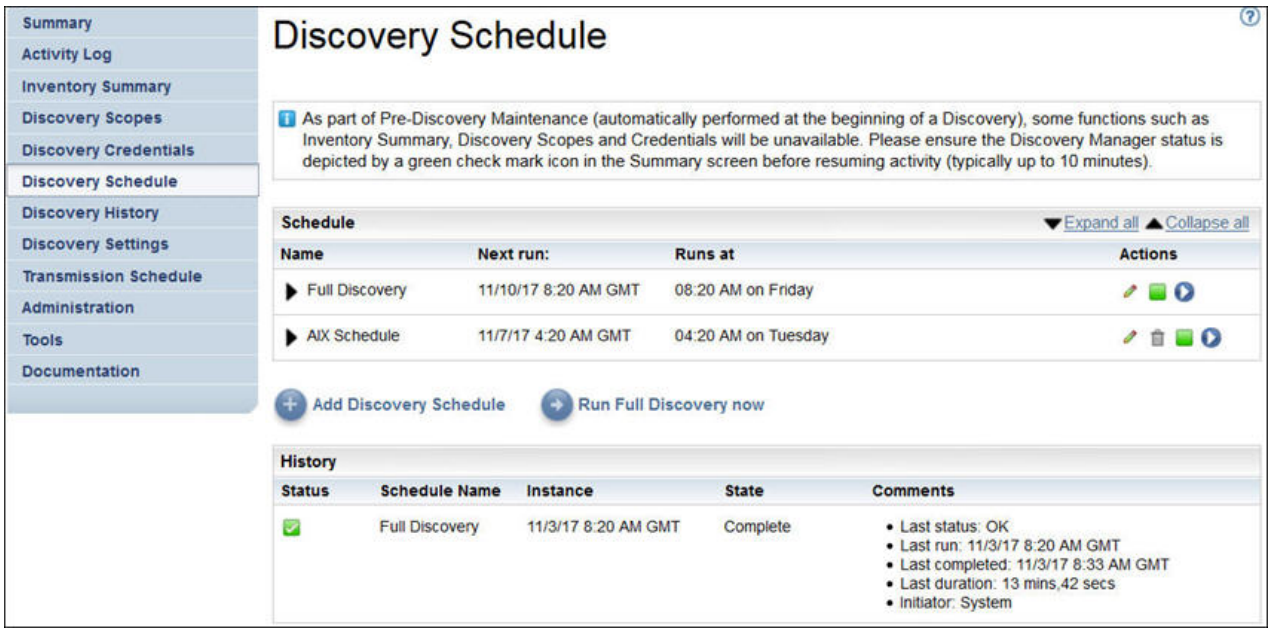

Figure 58. Planning de reconnaissance

Remarque : Si vous avez une version de TSA qui vient d'être installée, migrée ou mise à niveau avec la dernière version, la nouvelle console TSA disposera d'un planning de reconnaissance nommé **Reconnaissance complète** qui aura été créé avec la date par défaut (02:15 le mardi). Le planning Reconnaissance complète peut être édité ou désactivé, mais il n'est pas possible de le supprimer. Si vous aviez des plannings de reconnaissance prédéfinis (activés / désactivés), les mêmes valeurs seront restaurées après la migration.

Le panneau **Historique** affiche l'état, le nom du planning et d'autres informations sur les travaux de reconnaissance en cours d'exécution et ceux réalisés précédemment.

Ajouter un planning de reconnaissance

Vous pouvez ajouter de nouveaux plannings pour exécuter le processus de reconnaissance à un moment précis. Les nouveaux plannings permettent à TSA de découvrir un sous-ensemble de vos éléments informatiques à la date et à l'heure prévues.

Procédure

1. Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**.
   La page **Planning de reconnaissance** s'affiche.
2. Cliquez sur **Ajouter un planning de reconnaissance**. La page **Ajouter un planning de reconnaissance** s'affiche.

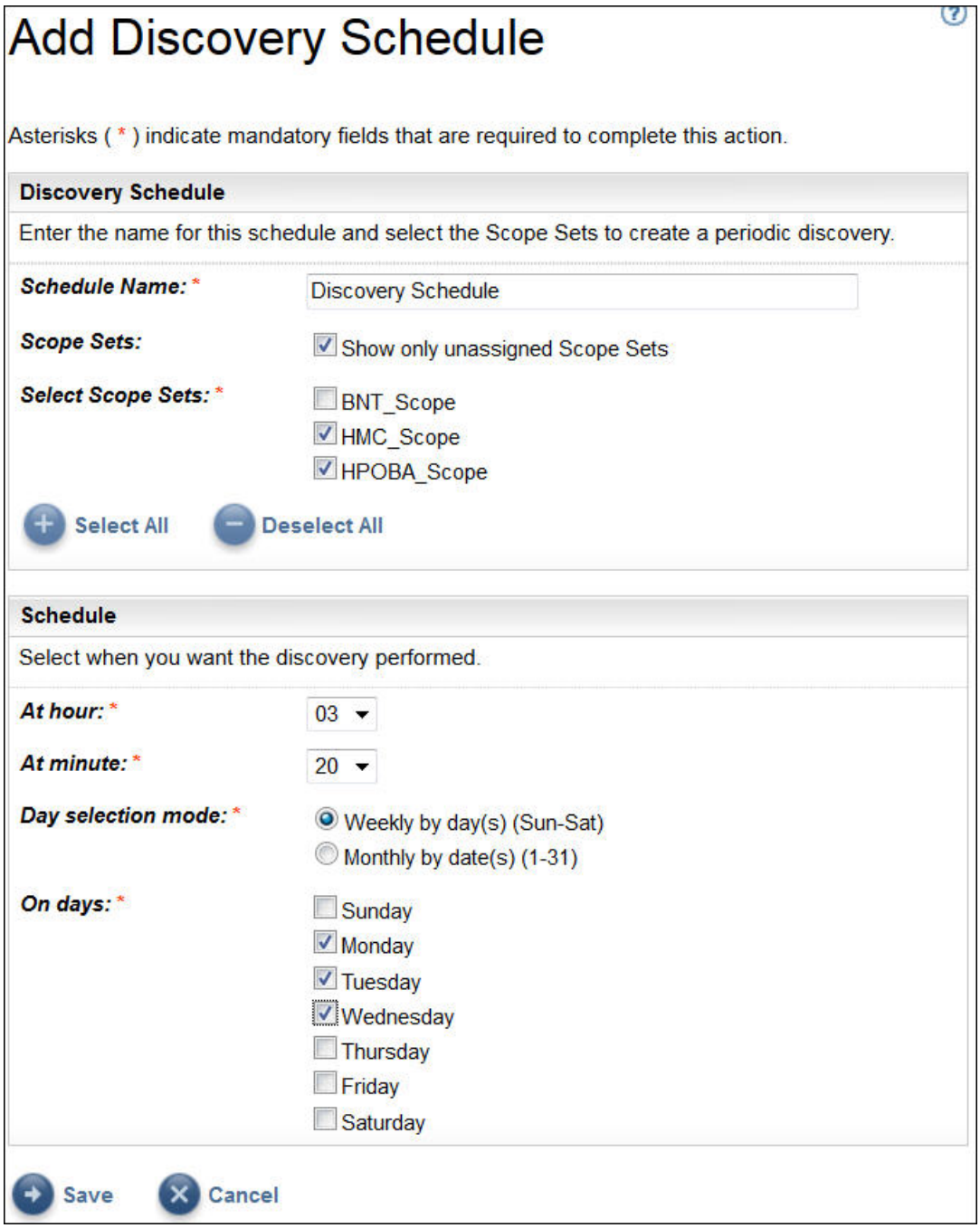

Figure 59. Ajouter un planning de reconnaissance

3. Dans le champ **Nom de planning**, entrez un nom d'identification pour le planning.
4. Sélectionnez l'option **Afficher uniquement les ensembles de périmètres non affectés** pour ne voir que les ensembles de périmètres qui ne sont affectés à aucun autre planning de reconnaissance défini par l'utilisateur.
5. Sélectionnez les ensembles de périmètres souhaités dans la liste **Sélectionner les ensembles de périmètres**.

   Vous pouvez utiliser l'option **Sélectionner tout** ou **Désélectionner tout** pour sélectionner la totalité ou aucun des ensembles de périmètres.
6. Sélectionnez une nouvelle heure à l'aide des listes **Heure** et **Minute**.
7. Sélectionnez le **Mode de sélection du jour**.

Hebdomadaire par jour(s) (dimanche au samedi)

Pour planifier la reconnaissance un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)**.

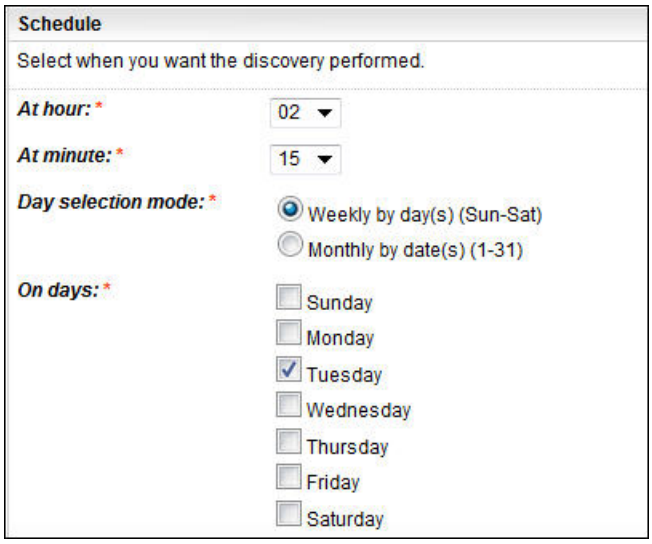

Figure 60. Hebdomadaire par jour(s) (dimanche au samedi)

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours de la semaine.

Mensuel par date(s) (1-31)

Pour planifier la reconnaissance un ou plusieurs jours précis du mois, sélectionnez l'option **Mensuel par date(s) (1-31)**.

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours du mois.

Remarque : Si vous sélectionnez des jours au-delà de la fin d'un mois spécifique, le travail sera déclenché le dernier jour de ce mois.

8. Cliquez sur **Enregistrer**.

   La page **Planning de reconnaissance** s'affiche à nouveau avec le nouveau planning.

Modifier le planning de reconnaissance

TSA fournit un planning par défaut pour que le processus de reconnaissance s'exécute à un moment précis. Vous pouvez le modifier selon vos besoins, tout comme vous pouvez utiliser les plannings personnalisés.

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**.

   La page **Planning de reconnaissance** s'affiche.

2. Cliquez sur l'icône **Modifier le planning** ( ).

   La page **Modifier un planning de reconnaissance** s'affiche.

   a) Modifiez les options **Nom de planning**, **Ensembles de périmètres** et **Sélectionner les ensembles de périmètres** selon vos besoins dans le panneau **Planning de reconnaissance**.

   Remarque : Vous ne pouvez pas modifier ces champs pour la reconnaissance complète par défaut.

   b) Modifiez les options **Heure**, **Minute**, **Mode de sélection du jour** et **Jours** selon vos besoins dans le panneau **Planifier**.

3. Cliquez sur **Enregistrer**.
   La page **Planning de reconnaissance** s'affiche à nouveau avec le planning modifié.

Désactiver le planning de reconnaissance

Vous pouvez désactiver des reconnaissances planifiées.

Avant de commencer

Remarque : Si des plannings de reconnaissance personnalisés ont été configurés, il est conseillé de désactiver le planning **Reconnaissance complète** afin d'éviter qu'une même élément informatique ne soit découvert plusieurs fois.

Procédure

Pour désactiver des reconnaissances planifiées, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**.
   La page **Planning de reconnaissance** s'affiche.
2. Cliquez sur l'icône / en regard du planning de reconnaissance à désactiver / activer.

Supprimer le planning de reconnaissance

Vous pouvez supprimer des reconnaissances planifiées.

Procédure

Pour supprimer des reconnaissances planifiées, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**.
   La page **Planning de reconnaissance** s'affiche.
2. Cliquez sur l'icône en regard du planning à supprimer.

   Remarque : Vous ne pouvez pas supprimer le planning de reconnaissance complète par défaut mais vous pouvez le désactiver si nécessaire.

   Un message vous invitant à confirmer la suppression du planning de reconnaissance sélectionné s'affiche.
3. Cliquez sur **OK** pour confirmer la suppression du planning.

Exécuter la reconnaissance

Vous pouvez exécuter une reconnaissance à la demande au lieu d'attendre la prochaine reconnaissance planifiée. Vous pouvez exécuter une reconnaissance sur tous les périmètres de reconnaissance définis, sur un planning de reconnaissance spécifique ou sur des périmètres ou des ensembles de périmètres de reconnaissance spécifiques."

Procédure

Pour exécuter une reconnaissance sur tous les périmètres définis, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Planning de reconnaissance**. La page **Planning de reconnaissance** s'affiche.
2. Cliquez sur **Exécuter la reconnaissance complète**. La section Historique est mise à jour et indique que la reconnaissance est en cours.

   Remarque : TSA tente de limiter au maximum les impacts sur l'environnement réseau. Par conséquent, le processus de reconnaissance utilise une approche itérative et mesurée qui peut faire durer une reconnaissance complète jusqu'à 72 heures. Vous pouvez surveiller le processus de reconnaissance dans la section **Récapitulatif des travaux** sur la page **Récapitulatif**.

3. Pour exécuter une reconnaissance sur un périmètre spécifique, cliquez sur l'icône **Exécuter** associée à ce périmètre.
4. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des ensembles de périmètres généraux

Procédure

Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**.

   La page **Périmètres de reconnaissance généraux** s'affiche. Cette page affiche une liste de tous les ensembles de périmètres définis pour TSA.

Figure 61. Exécuter la reconnaissance sur des périmètres spécifiques

2. Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, cliquez sur l'icône **Exécuter** associée à cet ensemble de périmètres.
3. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des ensembles de périmètres dynamiques HMC

Procédure

Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**.

   La page **Périmètres dynamiques HMC** s'affiche. Cette page affiche une liste de tous les ensembles de périmètres définis pour TSA.

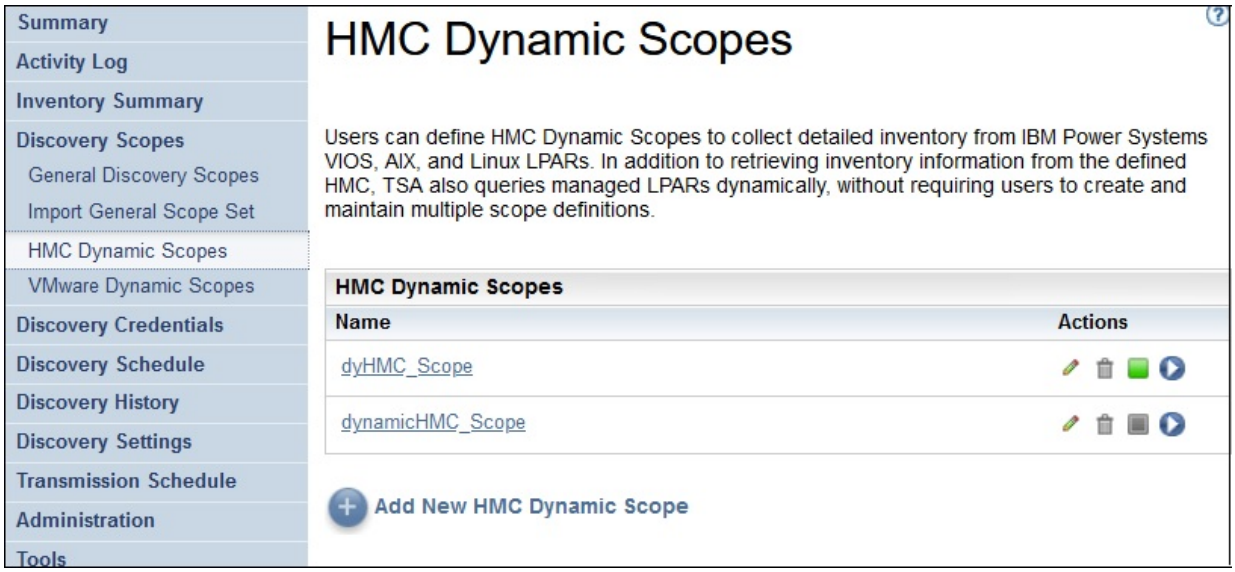

   Figure 62. Périmètres dynamiques HMC

2. Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, cliquez sur l'icône **Exécuter** associée à cet ensemble de périmètres.
3. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des ensembles de périmètres VMware

Procédure

Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Ensemble de périmètres dynamiques VMware**.

   La page **Périmètres dynamiques VMware** s'affiche. Cette page affiche la liste de tous les ensembles de périmètres définis pour ce TSA.

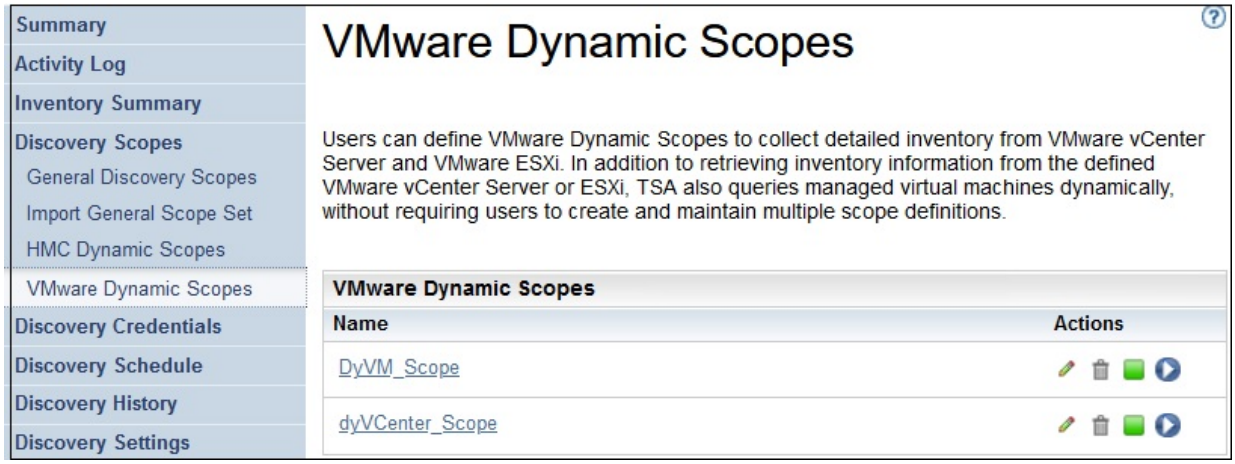

   Figure 63. Exécuter la reconnaissance sur des périmètres dynamiques VMware

2. Pour exécuter une reconnaissance sur un ensemble de périmètres spécifique, cliquez sur l'icône **Exécuter** associée à cet ensemble de périmètres.
3. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des périmètres

Vous pouvez exécuter une reconnaissance à la demande au lieu d'attendre la prochaine reconnaissance planifiée. Vous pouvez exécuter une reconnaissance sur tous les périmètres de reconnaissance définis, sur un planning de reconnaissance spécifique ou sur des périmètres ou des ensembles de périmètres de reconnaissance spécifiques."

Exécuter la reconnaissance sur des périmètres généraux

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres de reconnaissance généraux**. La page **Périmètres de reconnaissance généraux** s'affiche.

Figure 64. Périmètres de reconnaissance

2. Cliquez sur l'ensemble de périmètres qui contient le périmètre à reconnaître.

   La page **Ensemble de périmètres de reconnaissance** s'affiche. Cette page affiche tous les périmètres qui sont définis pour cet ensemble de périmètres.

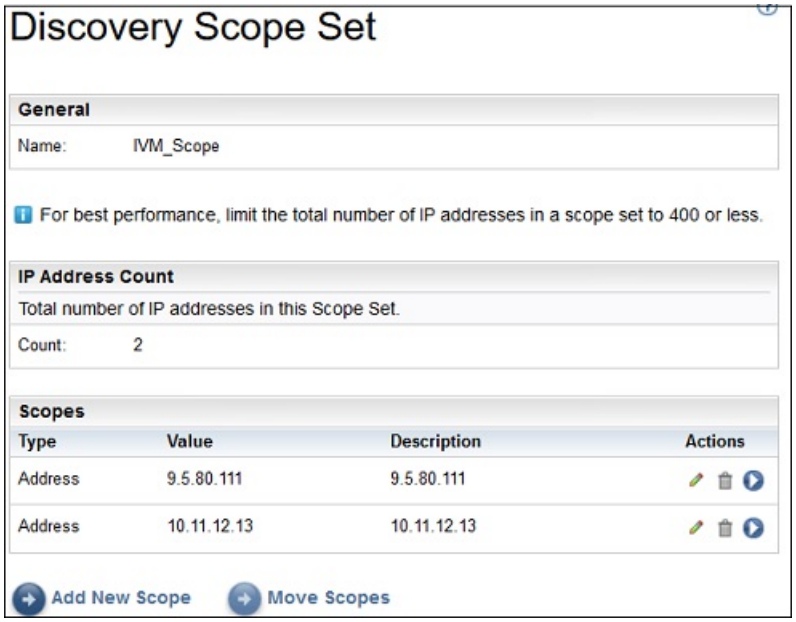

Figure 65. Exécuter la reconnaissance sur des périmètres spécifiques

3. Pour exécuter une reconnaissance sur un périmètre spécifique, cliquez sur l'icône **Exécuter** associée à ce périmètre.
4. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des périmètres dynamiques HMC

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques HMC**. La page **Périmètres dynamiques HMC** s'affiche.

Figure 66. Périmètres dynamiques HMC

2. Cliquez sur l'ensemble de périmètres qui contient le périmètre à reconnaître.

La page **Ensemble de périmètres dynamiques HMC** s'affiche. Cette page affiche tous les périmètres qui sont définis pour cet ensemble de périmètres.

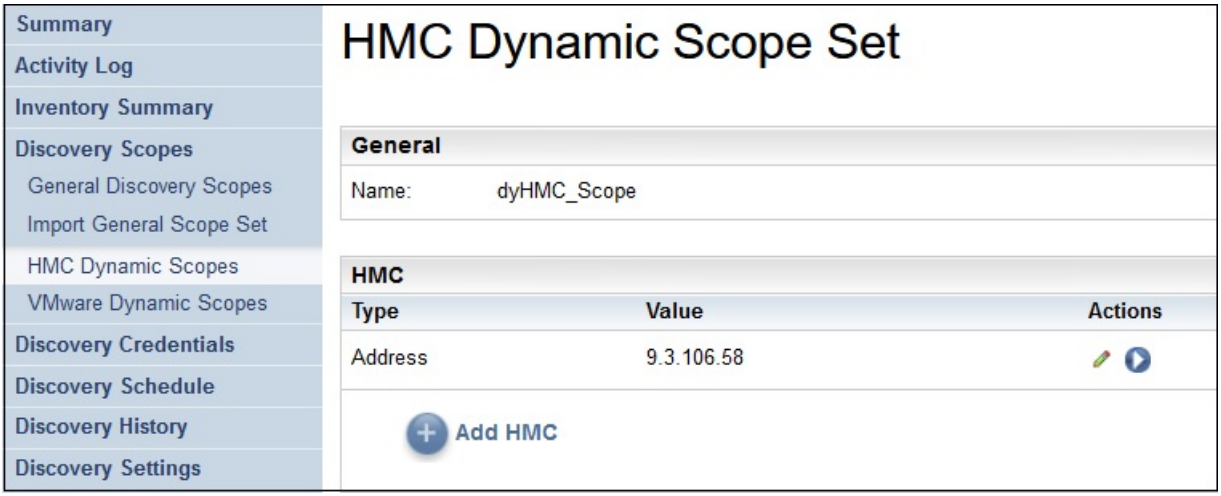

Figure 67. Exécuter la reconnaissance sur des périmètres spécifiques

3. Pour exécuter une reconnaissance sur un périmètre spécifique, cliquez sur l'icône **Exécuter** associée à ce périmètre.
4. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Exécuter la reconnaissance sur des périmètres dynamiques VMware

Procédure

1. Dans le panneau de navigation, cliquez sur **Périmètres de reconnaissance** > **Périmètres dynamiques VMware**. La page **Périmètres dynamiques VMware** s'affiche.

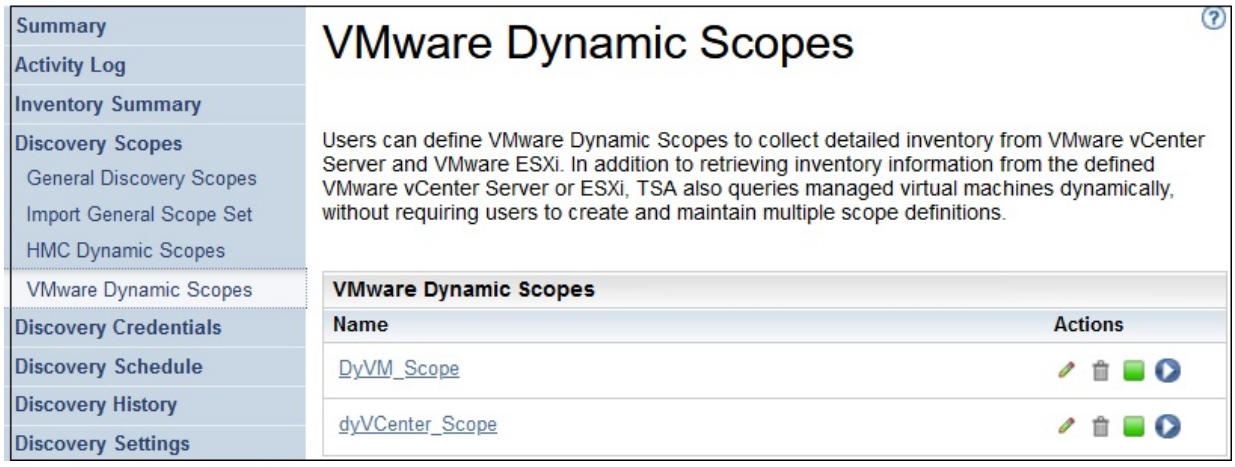

Figure 68. Périmètres dynamiques VMware

2. Cliquez sur l'ensemble de périmètres qui contient le périmètre à reconnaître.

   La page **Ensemble de périmètres dynamiques VMware** s'affiche. Cette page affiche tous les périmètres qui sont définis pour cet ensemble de périmètres.

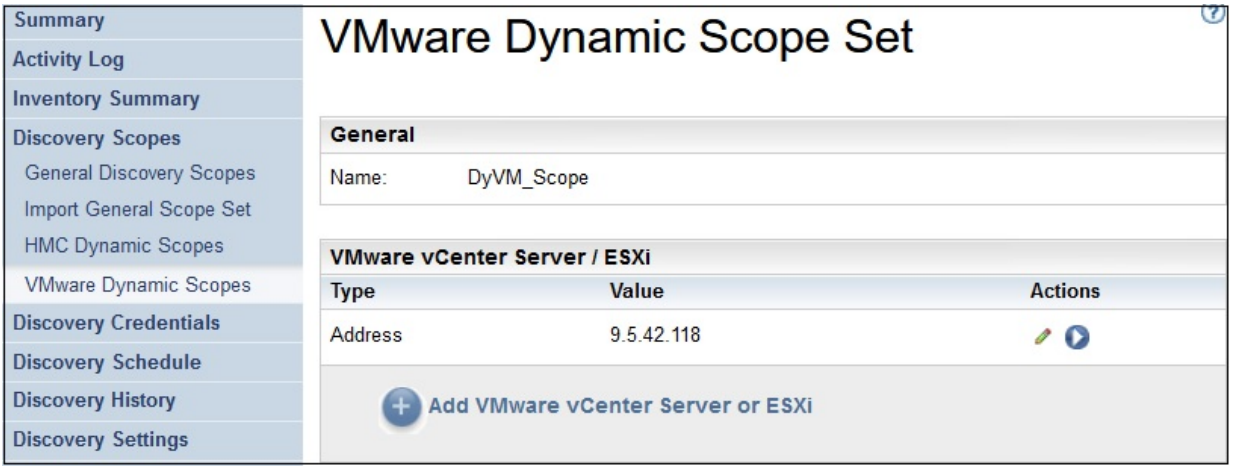

Figure 69. Exécuter la reconnaissance sur des périmètres dynamiques VMware

3. Pour exécuter une reconnaissance sur un périmètre spécifique, cliquez sur l'icône **Exécuter** associée à ce périmètre.
4. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La reconnaissance s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La reconnaissance doit se terminer sans erreur.

Historique de la reconnaissance

Vous pouvez examiner les résultats d'une reconnaissance lorsque celle-ci est terminée et télécharger le fichier journal de diagnostic de la reconnaissance.

Procédure

Pour afficher l'historique de la reconnaissance ou télécharger un fichier journal de diagnostic, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Historique de la reconnaissance**.

   La page **Historique de la reconnaissance** s'affiche. Une liste des entrées de la reconnaissance s'affiche. Chaque entrée indique l'état, le nom et l'heure de début et de fin de la reconnaissance.

   

   Figure 70. Historique de la reconnaissance
2. Pour afficher plus d'informations sur une entrée de la liste **Entrées d'historique**, cliquez sur le nom de l'entrée d'historique concernée.

   Le panneau **Informations sur l'entrée** affiche des informations sur la reconnaissance sélectionnée.
3. Pour télécharger un fichier journal de diagnostic pour une reconnaissance, cliquez sur l'icône **Télécharger** de cette reconnaissance.
4. Pour supprimer le fichier journal de diagnostic d'une reconnaissance, cliquez sur l'icône **Supprimer** de cette reconnaissance.

Planning de transmission

La transmission des données est planifiée afin de s'assurer que les données reconnues sont régulièrement envoyées au support IBM. Vous pouvez afficher le planning de transmission et le détail des

dernières transmissions, modifier le planning de transmission et désactiver les transmissions planifiées. Vous pouvez aussi envoyer les données à IBM lorsque vous le souhaitez.

Afficher le planning de transmission

Vous pouvez afficher des informations récapitulatives sur un planning de transmission.

Pourquoi et quand exécuter cette tâche

Pour afficher le planning de transmission, procédez comme suit :

Procédure

Dans le panneau de navigation, cliquez sur **Planning de transmission**.

La page **Planning de transmission** s'affiche.

Le panneau **Planifier** affiche la prochaine exécution planifiée et les heures d'exécution planifiées. Le panneau **Historique** affiche l'état et d'autres informations sur les travaux de transmission précédents et ceux en cours d'exécution.

Modifier le planning de transmission

TSA fournit un planning par défaut pour que le processus de transmission s'exécute à un moment précis. Vous pouvez modifier ce planning selon vos besoins.

Procédure

1. Dans le panneau de navigation, cliquez sur **Planning de transmission**.

   La page **Planning de transmission** s'affiche.

   Le panneau **Planifier** affiche la prochaine exécution planifiée et les heures d'exécution planifiées. Le panneau **Historique** affiche l'état et d'autres informations sur les travaux de transmission précédents et ceux en cours d'exécution.
2. Cliquez sur **Modifier le planning**.

   La page **Planning de transmission** s'affiche.

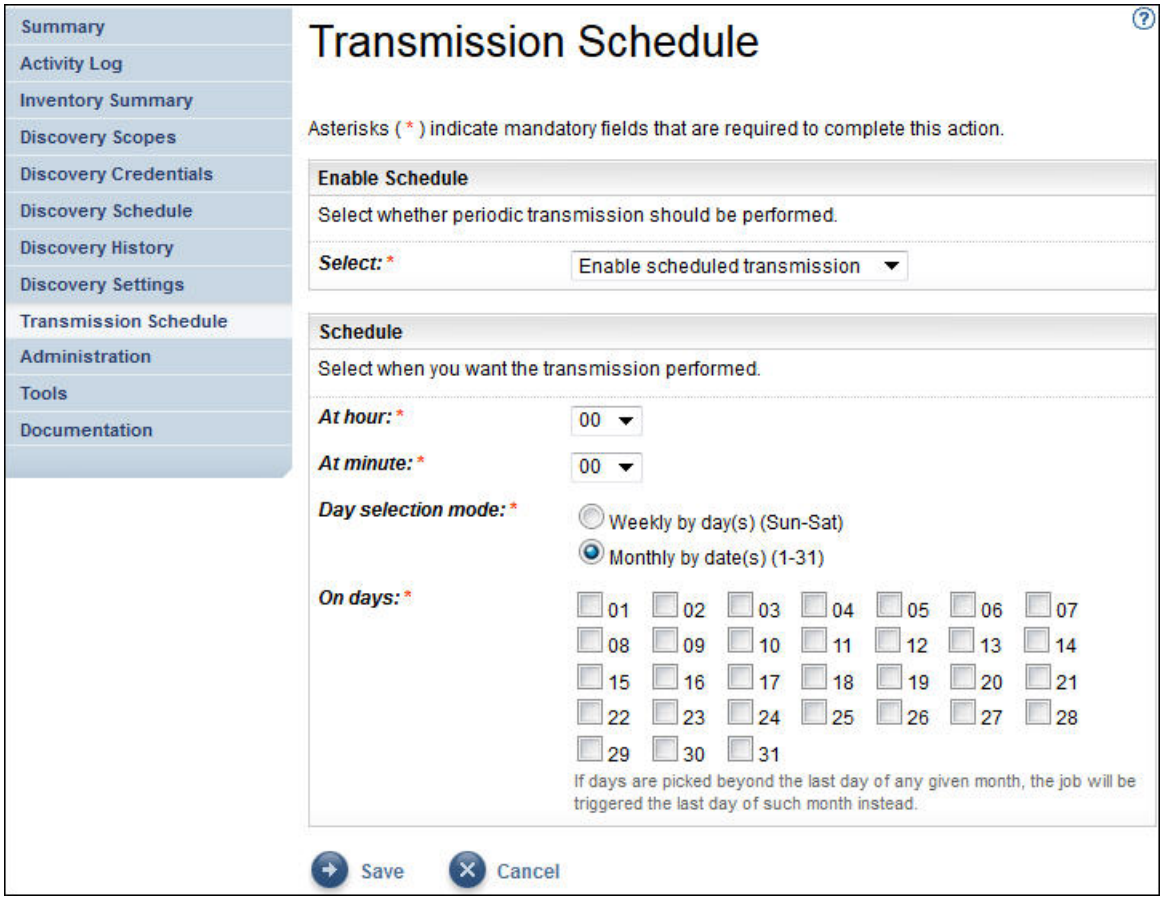

Figure 71. Modifier le planning de transmission

a) Sélectionnez une nouvelle heure à l'aide des listes déroulantes **Heure** et **Minute**.

b) Sélectionnez le **Mode de sélection du jour**.

Hebdomadaire par jour(s) (dimanche au samedi)

Pour planifier la transmission un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)**.

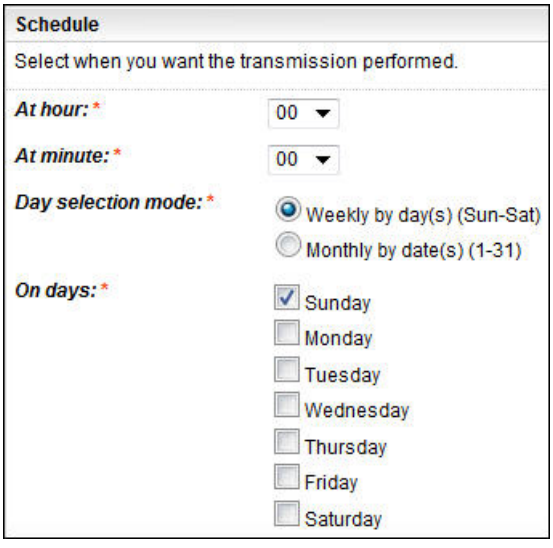

Figure 72. Hebdomadaire par jour(s) (dimanche au samedi)

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours de la semaine.

Mensuel par date(s) (1-31)

Pour planifier la transmission un ou plusieurs jours précis du mois, sélectionnez l'option **Mensuel par date(s) (1-31)**.

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours du mois.

Remarque : Si vous sélectionnez des jours au-delà de la fin d'un mois spécifique, le travail sera déclenché le dernier jour de ce mois.

3. Cliquez sur **Enregistrer**.

   La page **Planning de transmission** s'affiche à nouveau avec le nouveau planning.

Désactiver le planning de transmission

Vous pouvez désactiver des transmissions de données planifiées.

Procédure

Pour désactiver des transmissions planifiées, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Planning de transmission**.

   La page **Planning de transmission** s'affiche.

2. Cliquez sur **Modifier le planning**.

   La page **Planning de transmission** s'affiche.

3. Dans le panneau **Activer le planning**, sélectionnez **Désactiver la transmission planifiée**.
4. Cliquez sur **Enregistrer**.

   La page **Planning de reconnaissance** s'affiche et le panneau **Planifier** indique que la reconnaissance planifiée est désactivée. Vous pouvez activer les transmissions planifiées en cliquant sur **Activer la transmission planifiée**.

Exécuter la transmission

Vous pouvez exécuter une transmission à la demande au lieu d'attendre la prochaine transmission planifiée.

Procédure

1. Dans le panneau de navigation, cliquez sur **Planning de transmission**.

   La page **Planning de transmission** s'affiche.

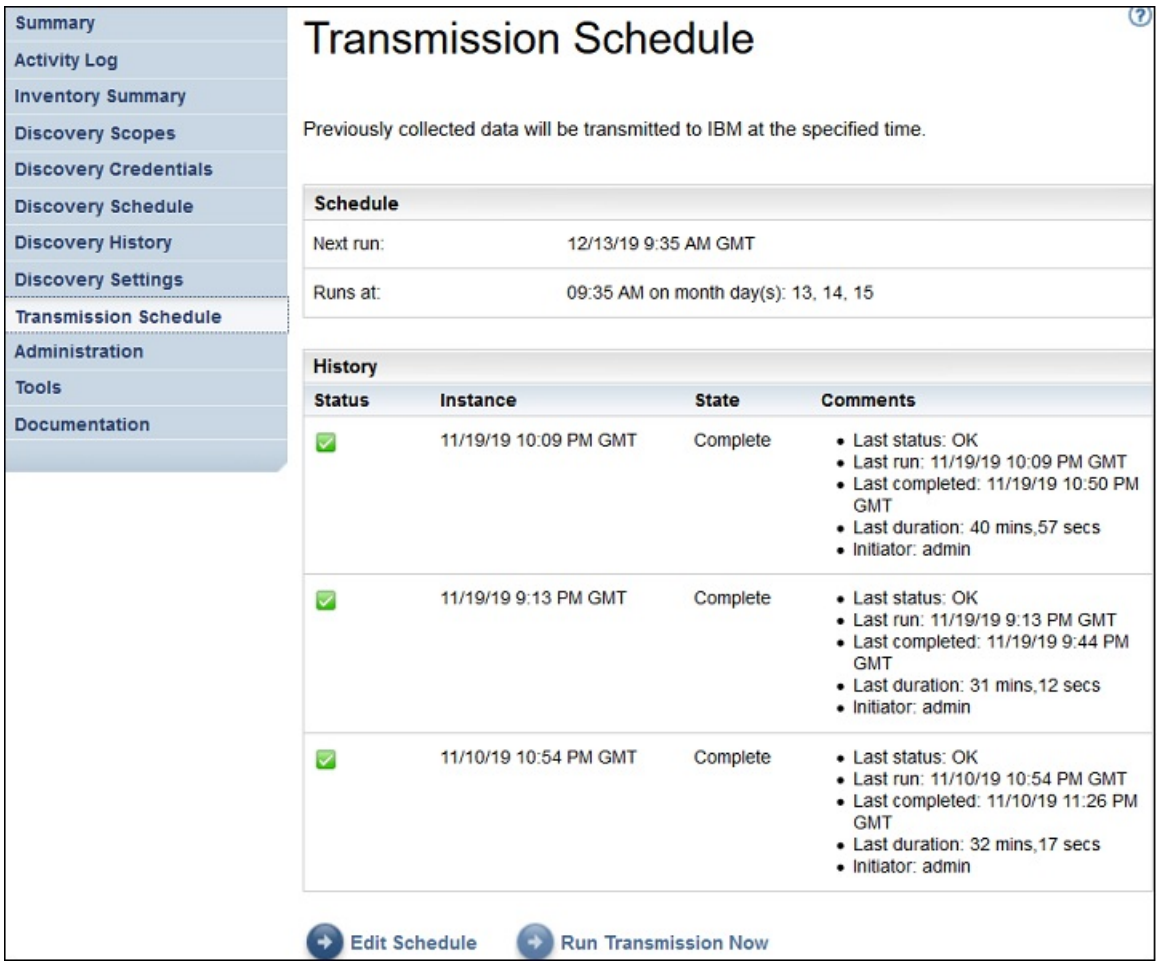

Figure 73. Exécuter la transmission

2. Cliquez sur **Exécuter la transmission**.

   Le panneau **Historique** est mis à jour et indique que la transmission est en cours.

3. Vérifiez la page **Récapitulatif** (cliquez sur **Récapitulatif** dans le panneau de navigation). La transmission s'affiche dans le panneau **Récapitulatif des travaux**. La page **Récapitulatif** s'actualise régulièrement pour afficher l'état actuel de TSA. Lorsque le travail n'est plus répertorié dans le panneau **Récapitulatif des travaux**, vérifiez le **Journal d'activité** (cliquez sur **Journal d'activité** dans le panneau de navigation). La transmission doit se terminer sans erreur.

Image instantanée de données

Vous pouvez créer et enregistrer une copie locale des données brutes non formatées collectées par TSA, sans transmettre ces données à IBM. Vous pouvez aussi voir les dernières données qui ont été transmises à IBM.

1. Dans le panneau de navigation, cliquez sur **Administration** > **Image instantanée de données**. La page **Image instantanée de données** s'affiche.

Figure 74. Image instantanée de données

Remarque : Le bouton **Télécharger la dernière image instantanée de données** n'est disponible que si une transmission a déjà eu lieu ou si une image instantanée de données existe.

2. Cliquez sur **Créer une image instantanée de données** pour collecter les dernières données reconnues par TSA et créer une image instantanée de données. Le message suivant s'affiche : `Le travail de création d'image instantanée de données est en cours. Son exécution peut prendre jusqu'à deux heures. Pour suivre son état, consultez la page Journal d'activité ou Récapitulatif.`. Pour afficher la page **Récapitulatif**, cliquez sur **Récapitulatif** dans le menu de navigation. Le panneau **Récapitulatif des travaux** affiche l'état de la collecte de l'image instantanée de données jusqu'à ce qu'elle soit terminée. Pour afficher l'état d'achèvement de la demande de création d'image instantanée de données, cliquez sur **Journal d'activité** dans le menu de navigation.
3. Si la transmission ou la création de l'image instantanée de données est terminée, la **Date de l'image instantanée de données** s'affiche.

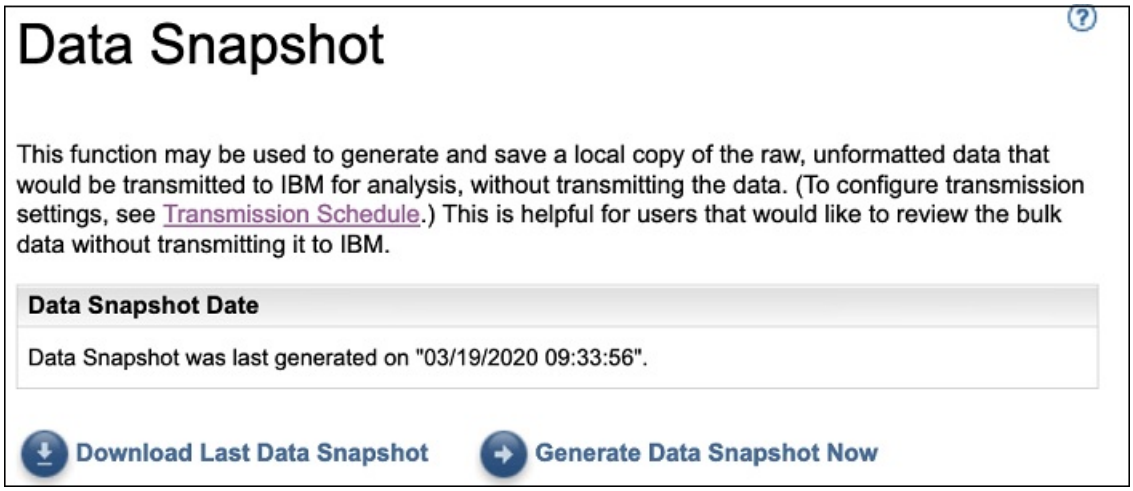

Figure 75. Date de l'image instantanée de données

4. Cliquez sur **Télécharger la dernière image instantanée de données** pour télécharger l'image instantanée de données la plus récente. Indiquez l'endroit où vous voulez enregistrer le fichier résultant (*collection.tar.xz*). Suivant la quantité de données, l'opération de téléchargement peut durer plus ou moins longtemps. Pour extraire le contenu de l'archive *.tar.xz*, utilisez l'utilitaire *tar* (pour Linux) ou l'utilitaire *7-Zip* (disponible avec Linux et Windows).

   Remarque :

   - Si un travail de transmission ou de collecte est en cours, le message suivant s'affiche : `Un travail de collecte est en cours. La dernière image instantanée de données a été créée le <<horodate>>. Voulez-vous vraiment télécharger la collection ?`.
     - Cliquez sur **OK** pour procéder au téléchargement.
     - Cliquez sur **Annuler** pour annuler le téléchargement et attendre la fin du travail de collecte en cours.

- Si aucun travail de transmission ou de collecte n'est en cours, le message suivant s'affiche : `La dernière image instantanée de données a été créée le <<horodate>>. Voulez-vous vraiment télécharger cette collection ?`. Cliquez sur **OK** pour enchaîner avec le téléchargement.

Afficher le récapitulatif de l'inventaire

Utilisez la page **Récapitulatif de l'inventaire** pour afficher le récapitulatif des éléments informatiques, tels que les systèmes informatiques, les systèmes d'exploitation et les sous-systèmes de stockage qui sont reconnus.

Cliquez sur **Récapitulatif de l'inventaire** dans le panneau de navigation pour afficher la page **Récapitulatif de l'inventaire**.

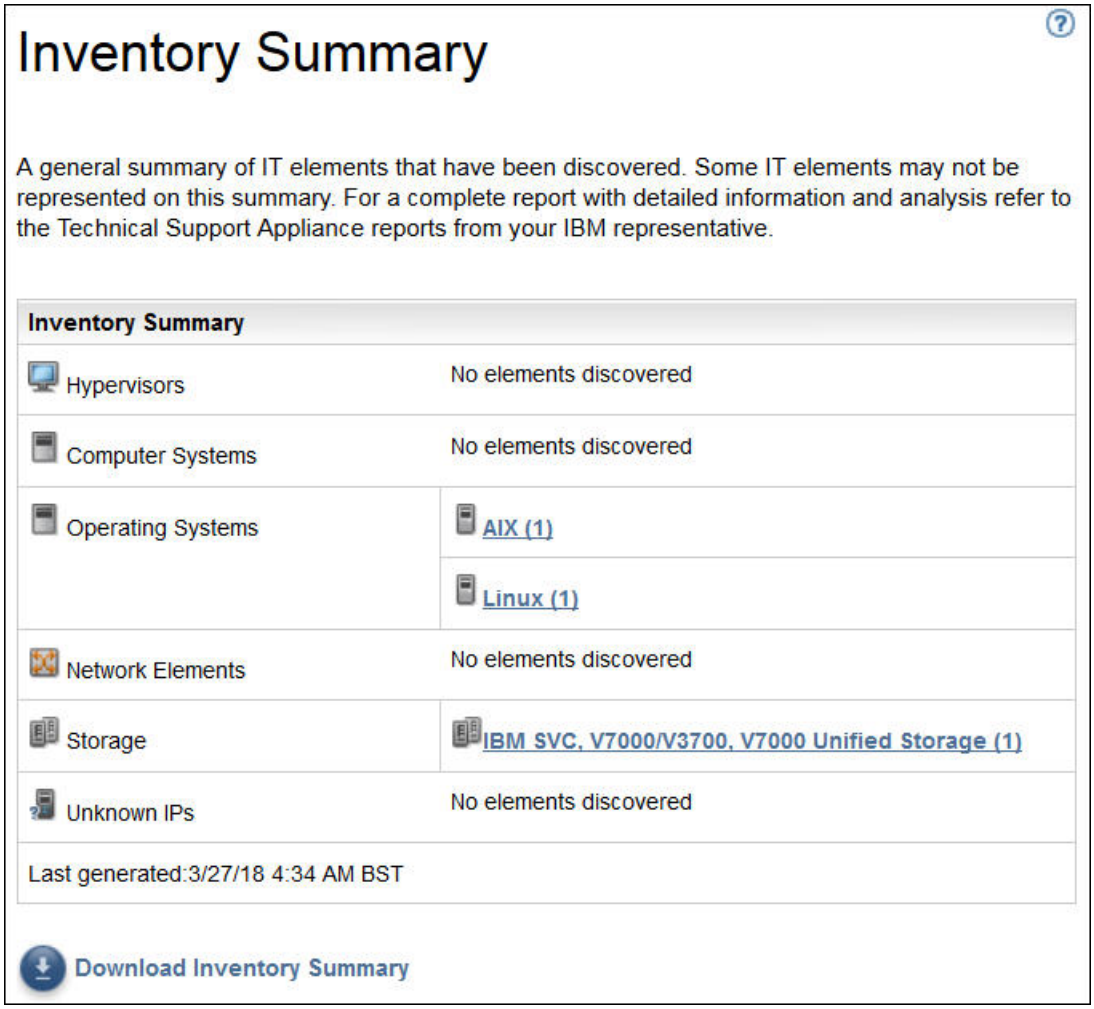

Figure 76. Récapitulatif de l'inventaire

La page Récapitulatif de l'inventaire affiche six groupes d'éléments informatiques différents.

- **Hyperviseurs** : comprend les hyperviseurs tels que HMC, IBM Flex System Manager, VMware, VIOS, etc.
- **Systèmes informatiques** : comprend les systèmes informatiques physiques.
- **Systèmes d'exploitation** : comprend les systèmes d'exploitation tels que AIX, Linux, etc. qui s'exécutent dans un environnement bare metal ou virtualisé.
- **Eléments du réseau** : comprend les commutateurs et les routeurs.

- **Stockage** : comprend les sous-systèmes de stockage tels qu'IBM XIV, IBM FlashSystem, EMC et les équipements de stockage HP. Il comprend aussi les unités de bande.
- **Adresses IP inconnues** : équipements potentiellement non classifiés pour les raisons suivantes :
  - Pare-feu bloquant l'accès à l'équipement.
  - Aucun jeu de données d'identification défini pour l'équipement. Consultez la page **État d'authentification** (**Outils** → **État d'authentification**) pour plus d'informations sur les adresses IP et les données d'identification associées.
  - Il n'existe aucun capteur pour ce type d'équipement.
- La ligne **Date de la dernière génération** indique la date à laquelle le dernier récapitulatif d'inventaire a été effectué.

Remarque : Les données de ce panneau sont affichées peu après le démarrage de TSA. Si vous accédez à cette page pendant ce temps-là, le message d'information suivant apparaît : **`La génération du récapitulatif de l'inventaire est en cours`**. Une fois les informations récapitulatives affichées, la page est actualisée toutes les 30 minutes environ. Vous pouvez l'actualiser à tout moment en cliquant sur l'icône correspondante du navigateur.

Chaque groupe affiche la liste des types d'équipement et le nombre de chaque type d'équipement.

1. Cliquez sur l'un des hyperliens des types d'équipement pour afficher la page **Détail du récapitulatif d'inventaire**.

Figure 77. Détail du récapitulatif d'inventaire

2. Sélectionnez l'un des équipements dans la liste pour afficher les **Informations sur l'élément** telles que *Adresse IP contextuelle*, *Fabricant*, *Modèle* et *Numéro de série*.

   Remarque : Dans le cas d'équipements détectés par TSA mais pour lesquels aucun jeu de données d'identification valide n'a été défini, les **Informations sur l'élément** ne sont pas fournies. Pour fournir ces détails, TSA doit en effet pouvoir se connecter à l'équipement.

Cliquez sur **Télécharger le récapitulatif de l'inventaire** pour télécharger un fichier contenant un récapitulatif des équipements reconnus.

Déboguer les problèmes de découverte

Etat d'authentification

Utilisez la page **Etat d'authentification** pour voir un récapitulatif des éléments informatiques qui sont définis dans des ensembles de périmètres et dont les données d'identification posent problème.

Pour afficher l'état d'authentification, cliquez sur **Outils** > **Etat d'authentification** dans le panneau de navigation. La page **Etat d'authentification** s'affiche.

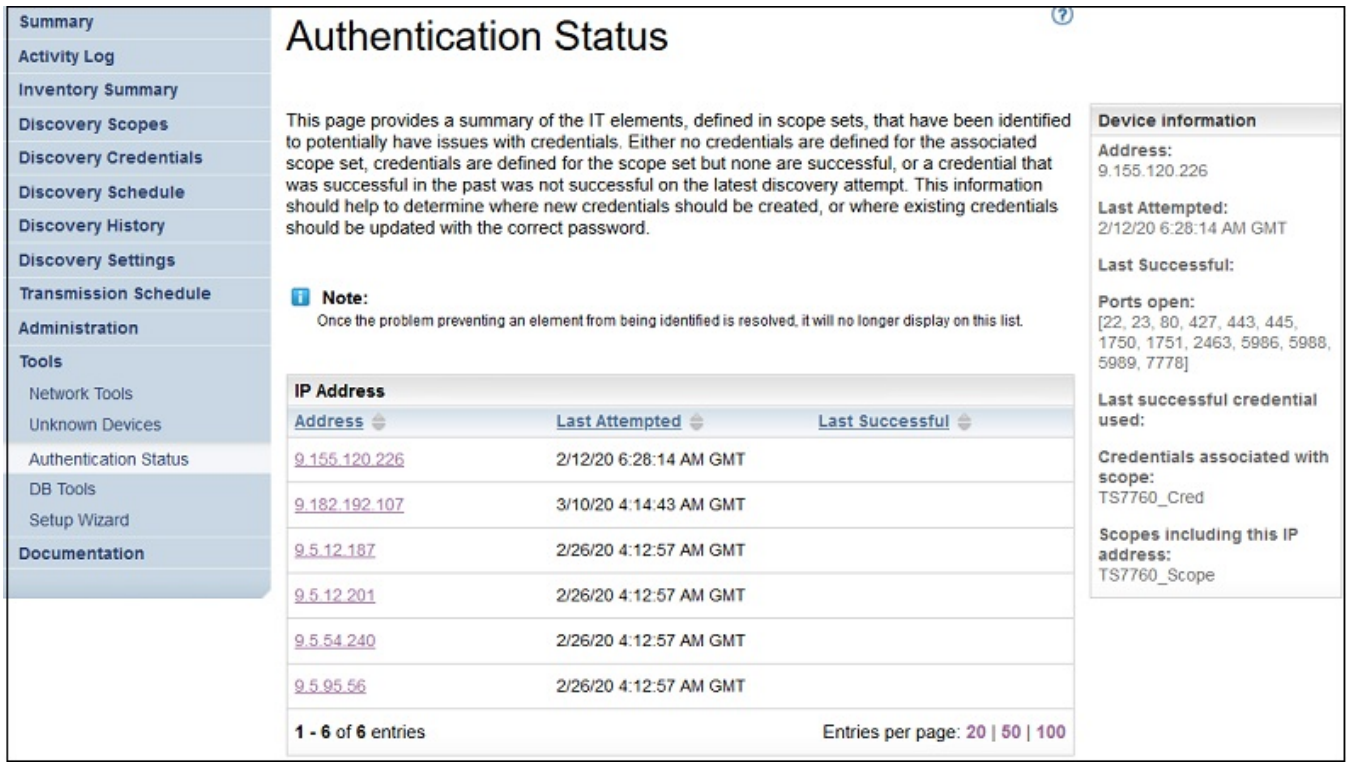

Figure 78. Etat d'authentification

La page Etat d'authentification affiche toutes les adresses IP d'équipement pour lesquelles des problèmes de données d'authentification ont été signalés. Les causes de ces problèmes peuvent être les suivantes :

- Aucun jeu de données d'identification n'est défini pour l'ensemble de périmètres associé.
- Des données d'identification sont définies pour l'ensemble de périmètres mais elles ne fonctionnent pas.
- Les données d'identification qui fonctionnaient auparavant ne fonctionnent pas avec la dernière tentative de reconnaissance.

Cliquez sur le lien de l'adresse IP concernée pour afficher des informations sur l'équipement : *Dernière tentative*, *Dernière authentification réussie*, *Ports ouverts*, *Données utilisées pour dernière authentification réussie*, *Date de la dernière modification des données d'identification*, *Données d'identification associées au périmètre* et *Périmètres incluant cette adresse IP*. Ces informations sont utiles pour déterminer où créer de nouvelles données d'identification et où mettre à jour les données d'identification existantes avec le mot de passe adéquat.

Remarque : Une fois le problème de données d'identification résolu pour un équipement, l'adresse IP de l'équipement en question n'apparaît plus dans la liste.

Equipements inconnus

Vous pouvez afficher des informations sur les équipements que TSA a reconnus mais qu'il n'est pas capable d'identifier totalement.

Pour afficher ces équipements inconnus, cliquez sur **Outils** > **Équipements inconnus** dans le panneau de navigation. La page **Équipements inconnus** s'affiche.

Vous pouvez cliquer sur n'importe quelle entrée de la liste Adresses IP inconnues pour afficher des informations supplémentaires sur ces équipements.

Chapitre 6. Configurer les tâches administratives

Informations d'état

TSA fournit des informations récapitulatives, des journaux et des rapports qui vous permettent d'obtenir rapidement des renseignements sur les travaux, l'inventaire reconnu et les informations produit.

Vous pouvez afficher un récapitulatif détaillé des travaux, de l'inventaire et des informations produit en cliquant sur **Récapitulatif** dans le panneau de navigation. La page **Récapitulatif** s'actualise régulièrement pour afficher les informations récapitulatives les plus à jour. La page **Récapitulatif** comprend les informations suivantes :

- **État système**

  Le panneau **État système** affiche l'état des services et des tâches en cours d'exécution. Vous pouvez afficher les pages correspondant aux services affichés en cliquant sur le nom du service dans le panneau **État système**.
- **Récapitulatif des travaux**

  Le panneau **Récapitulatif des travaux** affiche un récapitulatif des travaux en cours.
- **Récapitulatif de l'inventaire**

  Le panneau **Récapitulatif de l'inventaire** affiche une liste de l'inventaire reconnu.
- **Informations produit**

  Le panneau **Informations produit** affiche le nom d'hôte et l'identifiant de TSA.

Afficher le journal d'activité

Le journal d'activité affiche les messages de journal concernant les processus de reconnaissance et de transmission. Vous pouvez cliquer sur les entrées du journal d'activité pour obtenir de plus amples informations.

Pour afficher le journal d'activité, cliquez sur **Journal d'activité** dans le panneau de navigation. Une liste des entrées de journal s'affiche. Chaque entrée affiche le message, la sévérité de l'activité et l'heure à laquelle elle a eu lieu.

Figure 79. Journal d'activité

Remarque : Les reconnaissances étant exécutées sur des ensembles de périmètres spécifiques, il peut y avoir plusieurs entrées de journal pour une reconnaissance complète.

Pour plus de détails sur une entrée de journal d'activité, cliquez sur le message associé à cette entrée.

Pour enregistrer les fichiers journaux sur votre ordinateur, cliquez sur **Télécharger tous les journaux**.

Pour effacer le journal, cliquez sur **Effacer le journal**.

Afficher l'archive de nettoyage d'inventaire

Vous pouvez voir les inventaires qui sont nettoyés conformément à la durée d'inactivité (30, 60 ou 90 jours) que vous avez indiquée dans le **Planning du nettoyage d'inventaire**.

Pourquoi et quand exécuter cette tâche

Pour afficher l'inventaire supprimé, procédez comme suit :

Procédure

1. Sur la page **Planning du nettoyage d'inventaire**, cliquez sur **Afficher l'archive de nettoyage**. La page **Archive de nettoyage d'inventaire** s'affiche.

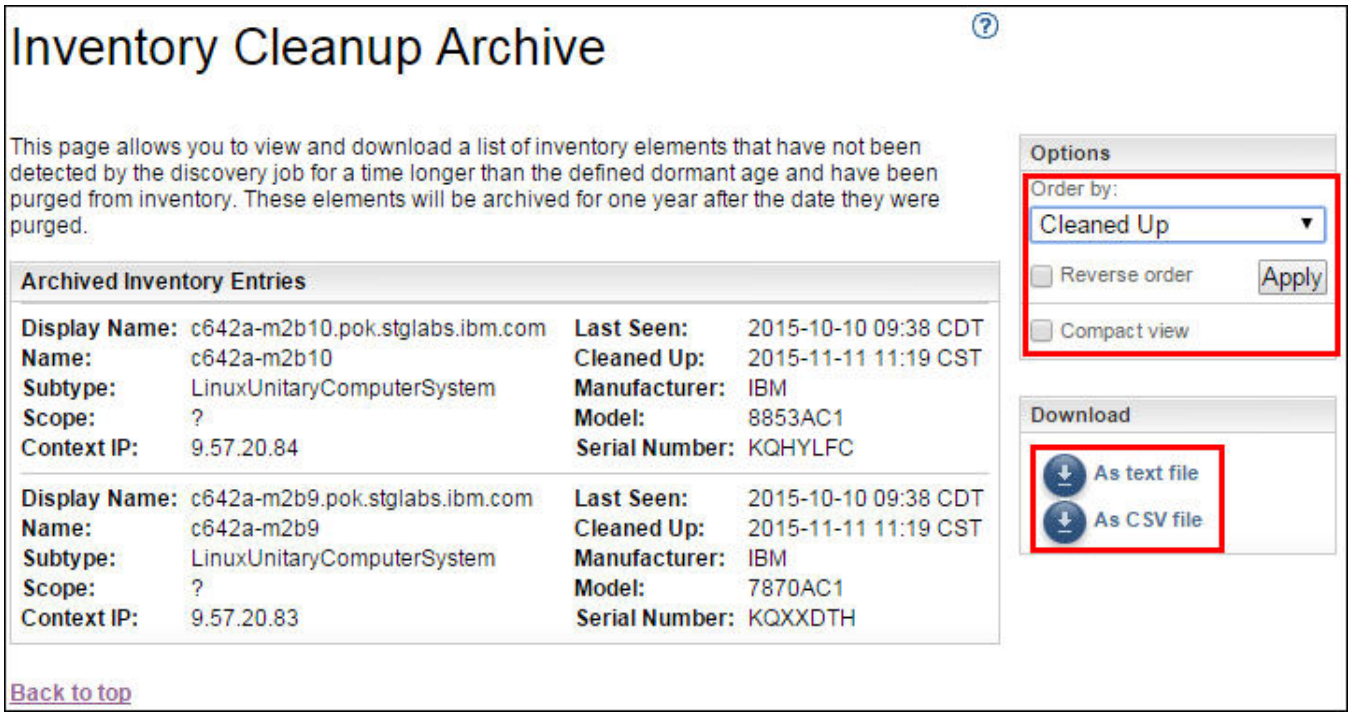

Figure 80. Archive de nettoyage d'inventaire

2. Sur la page **Archive de nettoyage d'inventaire**, vous pouvez voir les éléments qui sont purgés de l'inventaire dans le cadre du processus de nettoyage.

   Remarque :

   - Vous pouvez voir les informations d'inventaire contenues dans cette archive pendant un an seulement. Au bout d'un an, les informations d'archive sont purgées.
   - L'archive sera vide (c'est-à-dire qu'aucun objet ne sera nettoyé) si toutes les cibles définies ont été activement reconnues au cours de l'année précédente.

3. Utilisez le panneau **Options** pour retrier les données d'inventaire.
   a) Sélectionnez la propriété **Trier par** dans le panneau **Options** puis cliquez sur **Appliquer** pour trier la vue du détail de l'inventaire.
   b) Sélectionnez l'option **Inverser l'ordre** pour afficher le détail dans l'ordre inverse de la propriété sélectionnée.

c) Sélectionnez l'option **Vue compacte** pour afficher un récapitulatif de l'inventaire.

4. Cliquez sur **En tant que fichier texte** ou **En tant que fichier CSV** pour télécharger les données d'inventaire. Enregistrez les données d'inventaire pour traiter les données localement et conserver les données sur votre ordinateur pendant plus longtemps (plus d'un an). Les données conservées dans cette archive le sont pendant un an seulement, après quoi elles sont purgées.

Mots de passe

Vous utilisez des mots de passe pour sécuriser les comptes d'utilisateur TSA.

Changer votre mot de passe

Changez le mot de passe utilisateur de TSA.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Mot de passe**.
   La page **Mot de passe** s'affiche.
2. Entrez votre mot de passe actuel dans le champ **Mot de passe actuel**.
3. Entrez le nouveau mot de passe dans le champ **Nouveau mot de passe**.
   Le mot de passe doit respecter les règles suivantes :
   - 8 caractères minimum
   - Au moins un caractère alphabétique et un caractère non alphabétique
   - Ne doit pas contenir le nom de l'utilisateur
   - Doit être différent des huit mots de passe précédents
   - Doit être modifié au moins une fois tous les 90 jours, mais pas plus d'une fois par jour.
4. Entrez à nouveau le nouveau mot de passe dans le champ **Confirmer le mot de passe**.
   Les deux mots de passe saisis sont comparés afin de vérifier qu'ils correspondent avant que le mot de passe soit enregistré.
5. Cliquez sur **Enregistrer**.

Que faire ensuite

Important : Il n'est pas possible de récupérer un mot de passe donc si vous avez perdu ou oublié votre mot de passe, vous ne pouvez pas vous connecter à TSA pour modifier les données d'identification. Si vous perdez ou oubliez votre mot de passe pour un compte d'utilisateur ou un compte administrateur (si vous avez plusieurs comptes), contactez votre administrateur TSA. Si vous perdez ou oubliez votre mot de passe pour le compte administrateur par défaut (fourni avec l'appliance), contactez le support IBM. Pour plus d'informations, voir la section «Se connecter à Technical Support Appliance», à la page 23.

Sécurité

Vous pouvez accéder à des fonctions et des utilitaires de sécurité de TSA et les modifier.

La page **Sécurité** répertorie les utilitaires de sécurité disponibles. Sur cette page, vous pouvez modifier les paramètres de délai d'expiration de session ou changer l'âge maximum du mot de passe pour tous les comptes d'utilisateur.

Modifier les paramètres de délai d'expiration de session

Pour des raisons de sécurité, l'utilisateur est déconnecté de TSA au bout d'une certaine période d'inactivité. Vous pouvez empêcher TSA de déconnecter automatiquement l'utilisateur ou changer le délai au bout duquel l'utilisateur sera déconnecté s'il est inactif.

Désactiver le délai d'expiration de session

Vous pouvez empêcher TSA de déconnecter automatiquement l'utilisateur au bout d'une certaine période d'inactivité en désactivant le délai d'expiration de session.

Procédure

1. Cochez la case **Désactiver le délai d'attente de session**.
2. Cliquez sur **Modifier les paramètres de délai d'attente de session**.

Changer la valeur du délai d'expiration de session

Par défaut, l'utilisateur est déconnecté au bout de 20 minutes d'inactivité. Vous pouvez augmenter le délai au bout duquel l'utilisateur sera déconnecté en changeant sa valeur.

Procédure

1. Décochez la case **Désactiver le délai d'attente de session**.
2. Dans le champ **Délai d'attente de session**, entrez le temps en secondes au bout duquel TSA déconnectera l'utilisateur si celui-ci est inactif.

   Remarque : Ce délai d'expiration de session ne peut pas être inférieur à 20 minutes.
3. Cliquez sur **Modifier les paramètres de délai d'attente de session**.

Modifier l'âge du mot de passe

Par sécurité, chaque utilisateur a l'obligation de modifier son mot de passe de connexion à TSA au bout d'un certain nombre de jours. Par défaut, l'âge maximum d'un mot de passe est de 90 jours mais vous pouvez le modifier et le passer à 30 ou 60 jours.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Sécurité**. La page **Sécurité** s'affiche.
2. Sur la page **Sécurité**, faites défiler vers le bas jusqu'au panneau **Age maximum du mot de passe**.
3. Dans le panneau **Age maximum du mot de passe**, sélectionnez l'âge (30 jours, 60 jours ou 90 jours) dans la liste déroulante **Age maximum**.
4. Cliquez sur **Modifier l'âge maximum du mot de passe**. Le message de confirmation *L'âge maximum du mot de passe a été mis à jour.* s'affiche.

Sauvegarde et restauration

Vous pouvez sauvegarder et restaurer la configuration de TSA.

Important : Il est vivement recommandé d'effectuer une sauvegarde à intervalles réguliers. Vous devez également en effectuer une après avoir apporté des changements aux ensembles de périmètres ou aux données d'identification.

Date de sauvegarde

Affiche la date et l'heure d'exécution de la dernière sauvegarde.

Récapitulatif de la configuration

Utilisez cette option pour afficher un récapitulatif de la configuration actuelle de TSA avant de l'enregistrer.

Pour afficher le récapitulatif de la configuration de TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Sauvegarde et restauration**. La page **Sauvegarde et restauration** s'affiche.
2. Cliquez sur **Voir le récapitulatif** pour afficher un récapitulatif de la configuration actuelle de TSA. Les informations affichées montrent les configurations qui seront enregistrées par TSA si une sauvegarde est effectuée.

   Remarque : Ces informations s'affichent dans une fenêtre contextuelle. Si votre navigateur Web bloque les fenêtres contextuelles, vous devrez peut-être l'autoriser à les afficher depuis TSA.

   Sur la page **Récapitulatif**, la section **Sauvegarde** affiche les informations relatives à l'état de la sauvegarde avec les messages suivants :

   - Une icône *OK* () si la dernière sauvegarde effectuée remonte à moins de 60 jours.
   - Une icône *Avertissement* () si la dernière sauvegarde effectuée remonte entre 60 et 90 jours.
   - Une icône *Erreur* () si aucune sauvegarde n'a été effectuée depuis plus de 90 jours.

Sauvegarde

Utilisez cette option pour enregistrer une copie de la configuration de TSA.

Pour sauvegarder la configuration de TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Sauvegarde et restauration**. La page **Sauvegarde et restauration** s'affiche.

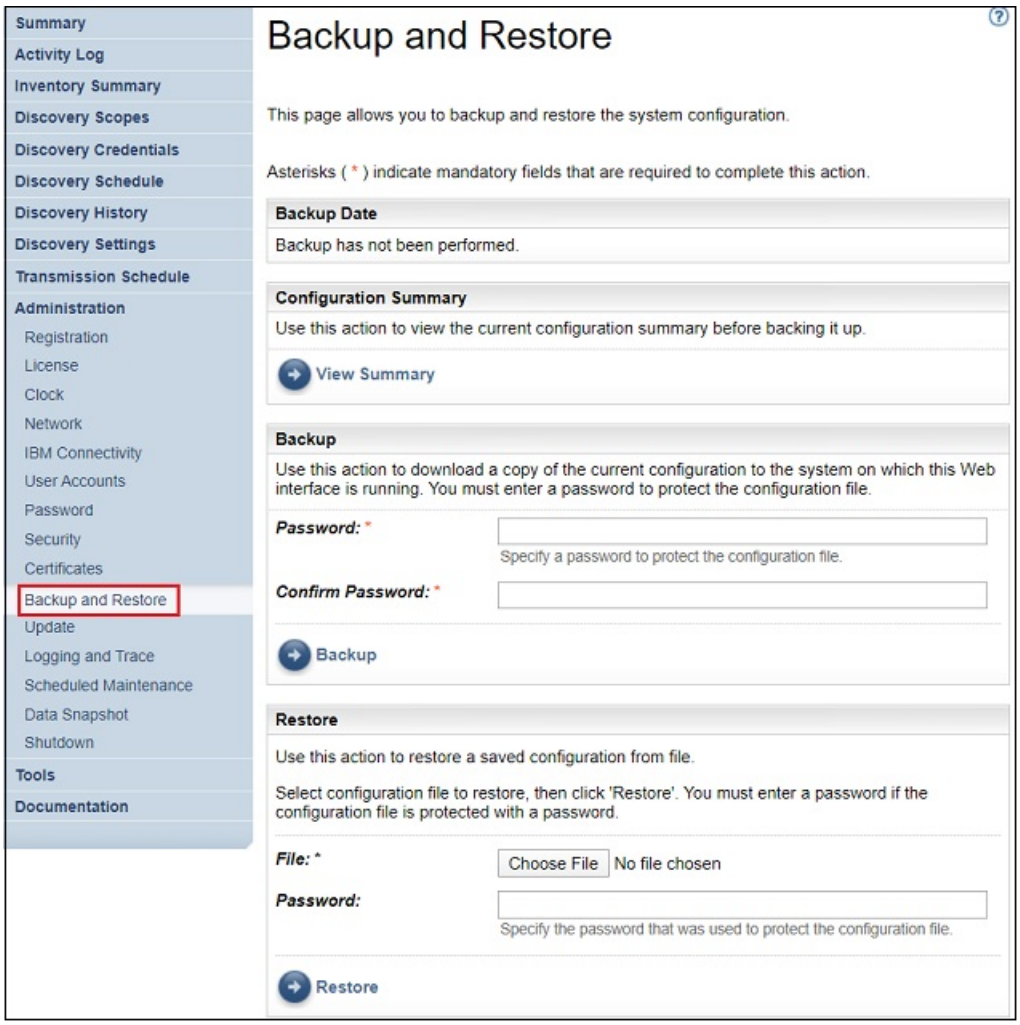

Figure 81. Sauvegarde et restauration

2. Entrez un mot de passe dans le panneau **Sauvegarde** pour protéger le fichier de configuration.
3. Entrez à nouveau le mot de passe dans le champ **Confirmer le mot de passe**. Les deux mots de passe saisis sont comparés afin de vérifier qu'ils correspondent avant que le mot de passe soit enregistré.

   Remarque : Vous devez enregistrer le mot de passe en lieu sûr car il vous sera demandé lors de la restauration.
4. Cliquez sur **Sauvegarder** et enregistrez le fichier compressé de la configuration de sauvegarde sur le système.

   Remarque : Le fichier de configuration de sauvegarde qui est généré ne peut être ouvert que par TSA.

   Remarque : Si vous avez récemment modifié votre mot de passe administrateur, effectuez une sauvegarde après avoir modifié le mot de passe et utilisez le dernière fichier de sauvegarde pour la restauration.

Restaurer

Utilisez cette option pour restaurer une copie de la configuration précédemment enregistrée.

Pour restaurer une configuration de TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Sauvegarde et restauration**. La page **Sauvegarde et restauration** s'affiche.
2. Cliquez sur **Choisir un fichier** pour localiser et sélectionner le fichier de configuration que vous voulez restaurer.

3. Entrez le mot de passe utilisé pour sauvegarder le fichier de configuration.
4. Cliquez sur **Restaurer**.

   Le travail de restauration s'affiche dans le panneau Récapitulatif des travaux de la page **Récapitulatif**. Une fois la restauration terminée, vous êtes invité à redémarrer le système.

   Remarque : Effectuer une restauration à partir d'une sauvegarde supprime les configurations existantes. Toutes les configurations, y compris les définitions de périmètre et les données d'identification, sont remplacées par celles présentes dans le fichier de sauvegarde.

Remarque : Assurez-vous que l'état du Gestionnaire de la reconnaissance est OK(✅) sur la page **Récapitulatif** lorsque vous effectuez des opérations de sauvegarde ou de restauration. Si le Gestionnaire de la reconnaissance ne s'exécute pas, vous recevrez le message suivant : `"Le Gestionnaire de la reconnaissance est inactif. Avant de reprendre l'activité, assurez-vous que le Gestionnaire de la reconnaissance est représenté par une icône verte sur la page Récapitulatif (ce qui est généralement le cas au bout de 10 minutes)."` Si, au bout de 10 minutes, le Gestionnaire de la reconnaissance est toujours inactif, contactez le support IBM.

Mettre à jour

Vous pouvez rechercher et télécharger les mises à jour de TSA.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Mise à jour**.
   La page **Mettre à jour** s'affiche.

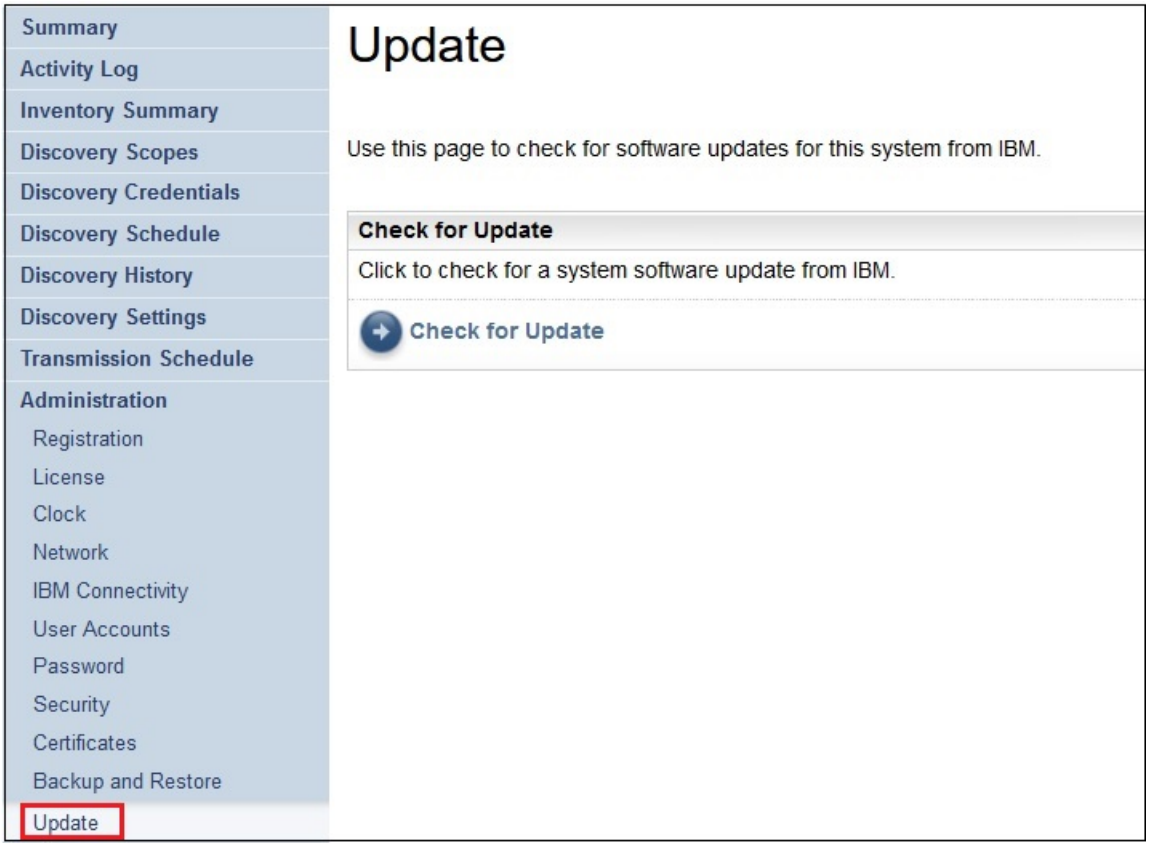

Figure 82. Mise à jour

2. Cliquez sur **Rechercher la mise à jour**.
   La page **Mises à jour disponibles** répertorie toutes les mises à jour disponibles.

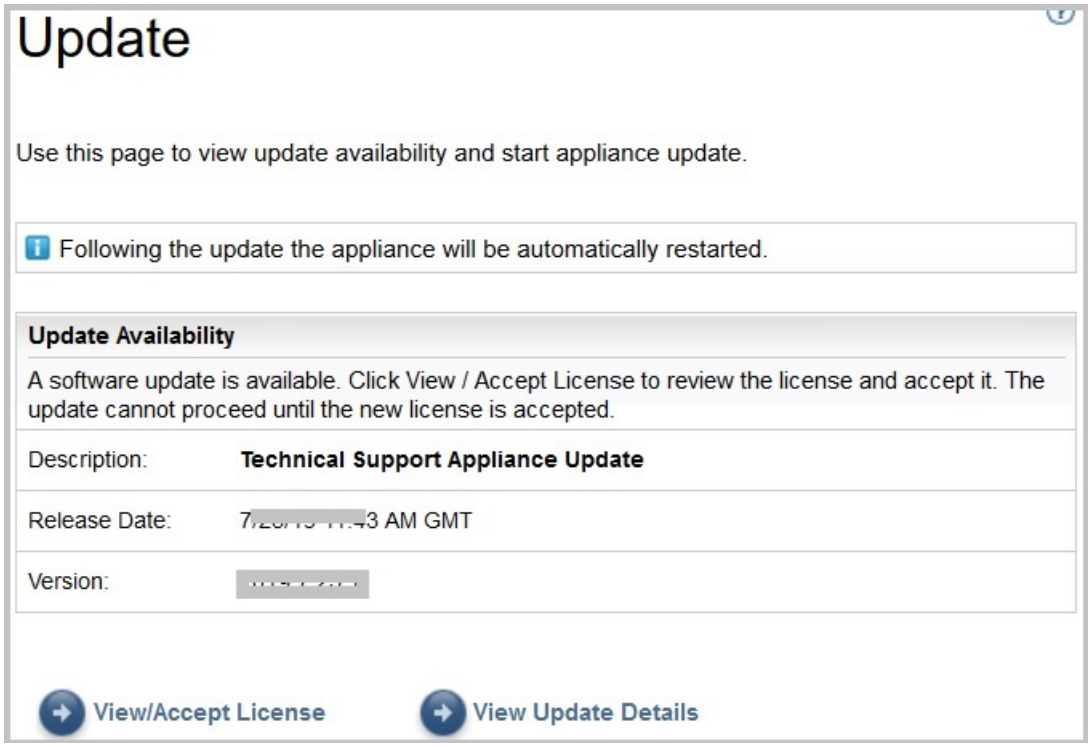

Figure 83. Mises à jour disponibles

a) Pour certaines nouvelles versions de TSA, vous devez accepter un nouveau contrat de licence avant d'effectuer la mise à jour. S'il y a une nouvelle licence, cliquez sur **Voir/accepter la licence** ; la page **Contrat de licence** s'affiche.

b) Cliquez sur le bouton **Accepter** de la page **Contrat de licence** pour accepter le nouveau contrat de licence. La page **Mise à jour** réapparaît et affiche le bouton **Exécuter la mise à jour**. S'il n'y a pas d'obligation d'accepter un nouveau contrat de licence, le bouton **Voir/accepter la licence** ne s'affiche pas et vous pouvez immédiatement cliquer sur **Exécuter la mise à jour**.

Remarque :

- Une fois que vous avez accepté la licence, le bouton **Voir/accepter la licence** n'est plus visible.
- Dans le panneau de navigation, cliquez sur **Administration** > **Licence** pour afficher le dernier contrat de licence que vous avez accepté.

c) Pour installer les mises à jour, cliquez sur **Exécuter la mise à jour**.

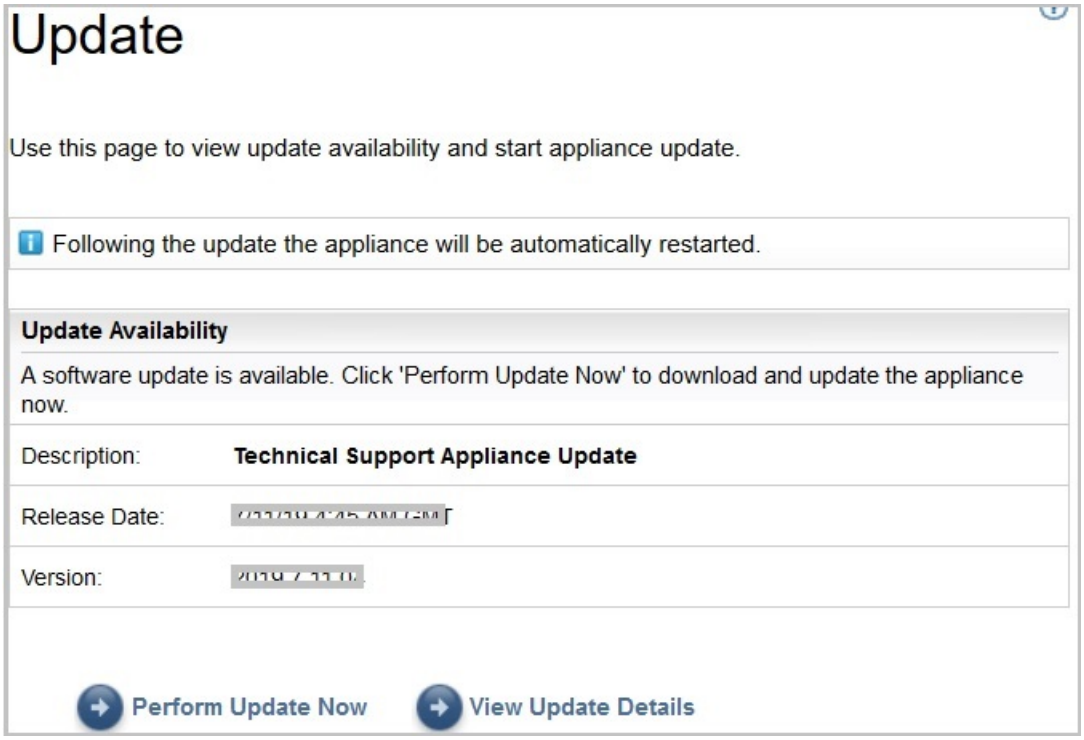

Figure 84. Exécuter la mise à jour

Lorsque la mise à jour est terminée, TSA redémarre automatiquement.

d) Pour afficher des informations sur le contenu de la mise à jour, cliquez sur **Voir les détails de la mise à jour**.

Activer la maintenance planifiée

Afin de garantir le fonctionnement optimal de TSA, il est recommandé d'activer la fonction de maintenance planifiée.

Pourquoi et quand exécuter cette tâche

Le travail de maintenance planifiée garantit le fonctionnement optimal de TSA. Vous pouvez toujours activer ou désactiver cette fonctionnalité. Si vous activez la maintenance planifiée, vous pouvez définir le jour et l'heure pour une exécution automatique de la maintenance. L'état de la maintenance planifiée s'affiche dans la section **État du système** de la page **Récapitulatif**.

Si vous planifiez le travail de maintenance, le système redémarrera automatiquement une fois l'opération terminée et vous serez notifié du redémarrage du système une heure avant. Exemple : `En raison d'une opération de maintenance planifiée, un travail de redémarrage du système sera mis en file d'attente dans 59 minute(s).`

Important : ne planifiez pas de maintenance de l'appliance dans les 30 minutes qui précèdent d'autres travaux planifiés, tels que la reconnaissance, la transmission ou le nettoyage d'inventaire. Si vous la programmez dans les 30 minutes qui précèdent d'autres travaux planifiés, TSA ne pourra pas exécuter ces travaux.

Procédure

Pour modifier le planning de maintenance, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Maintenance planifiée**.

La page **Maintenance planifiée** affiche le **planning** de la prochaine exécution l'heure d'exécution planifiée. La section **Historique** affiche l'état et d'autres informations sur les travaux de maintenance précédents et ceux en cours d'exécution.

2. Sur la page **Maintenance planifiée**, cliquez sur **Modifier le planning**.
   a) Dans le panneau **Activer le planning**, indiquez si vous souhaitez activer ou désactiver la maintenance planifiée.
   b) Si vous choisissez d'activer la tâche de maintenance planifiée, sélectionnez une nouvelle heure dans les listes déroulantes **Heure** et **Minute**.
   c) Sélectionnez le **Mode de sélection du jour**. Pour planifier la maintenance un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)** ou pour planifier la maintenance à une ou plusieurs dates précises du mois, sélectionnez l'option **Mensuelle par date(s) (1-31)**.
   d) Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner des jours différents ou des jours supplémentaires de la semaine ou du mois.

      Remarque : Si vous sélectionnez des jours au-delà de la fin d'un mois spécifique, le travail sera déclenché le dernier jour de ce mois.
3. Cliquez sur **Enregistrer**.

   La page **Maintenance planifiée** s'affiche à nouveau avec le nouveau planning.

Journalisation et trace

Vous pouvez voir et modifier les paramètres de trace de diagnostic de TSA. Vous pouvez aussi modifier les paramètres des niveaux de trace du Gestionnaire de la reconnaissance. La modification de ces paramètres pouvant affecter les performances, faites-le uniquement si le support IBM vous y invite.

1. Dans le panneau de navigation, cliquez sur **Administration** > **Journalisation et trace**. La page **Journalisation et trace** s'affiche. Le panneau **Niveau de trace de TSA** affiche les paramètres de trace actuels (Erreur, Avertissement, Information, Débogage ou Trace).

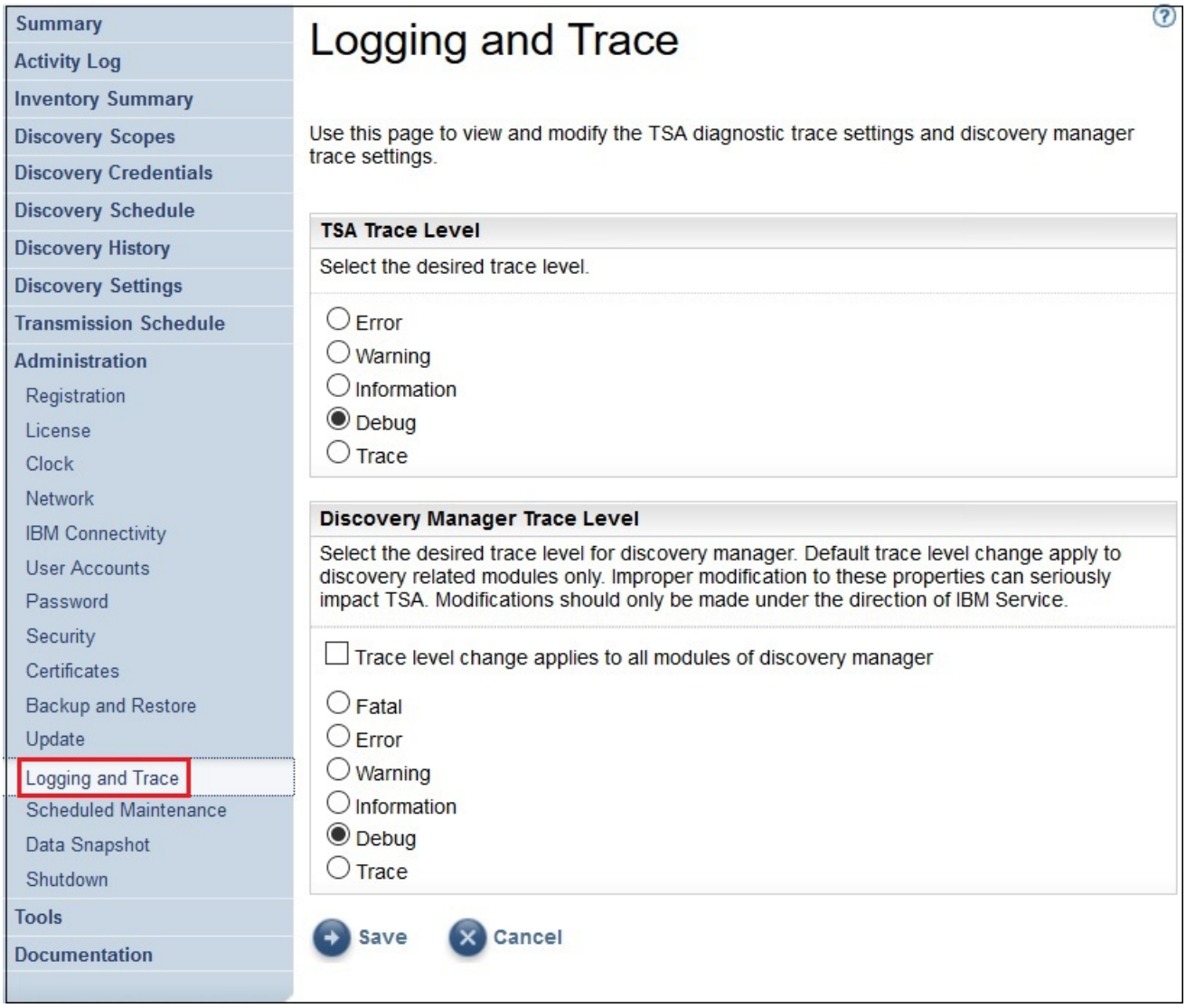

Figure 85. Journalisation et trace

2. Si nécessaire, vous pouvez changer un paramètre de trace dans le panneau **Niveau de trace de TSA** en cliquant sur le bouton d'option en regard du paramètre de trace concerné.
3. Cliquez sur **Enregistrer**.

Remarque : Par défaut, les paramètres *Niveau de trace de TSA* et *Niveau de trace du gestionnaire de reconnaissance* sont réglés sur **Débogage**.

Pour voir et modifier les réglages du **Niveau de trace du gestionnaire de reconnaissance**, suivez ces étapes :

Important : Apportez des modifications à cette section uniquement si IBM Service vous y invite.

1. Dans le panneau de navigation, cliquez sur **Administration** > **Journalisation et trace**. La page **Journalisation et trace** s'affiche, indiquant le niveau de trace en vigueur.
2. Cochez **La modification du niveau de trace s'applique à tous les modules du Gestionnaire de la reconnaissance** si vous voulez que le niveau de trace s'applique à tous les modules du Gestionnaire de la reconnaissance.
3. Sélectionnez le bouton d'option en regard du paramètre de trace concerné.
4. Cliquez sur **Enregistrer**.

Arrêt

Vous pouvez suspendre ou reprendre les opérations de TSA, ou arrêter puis redémarrer ou mettre hors tension TSA.

L'arrêt de TSA prend quelques minutes.

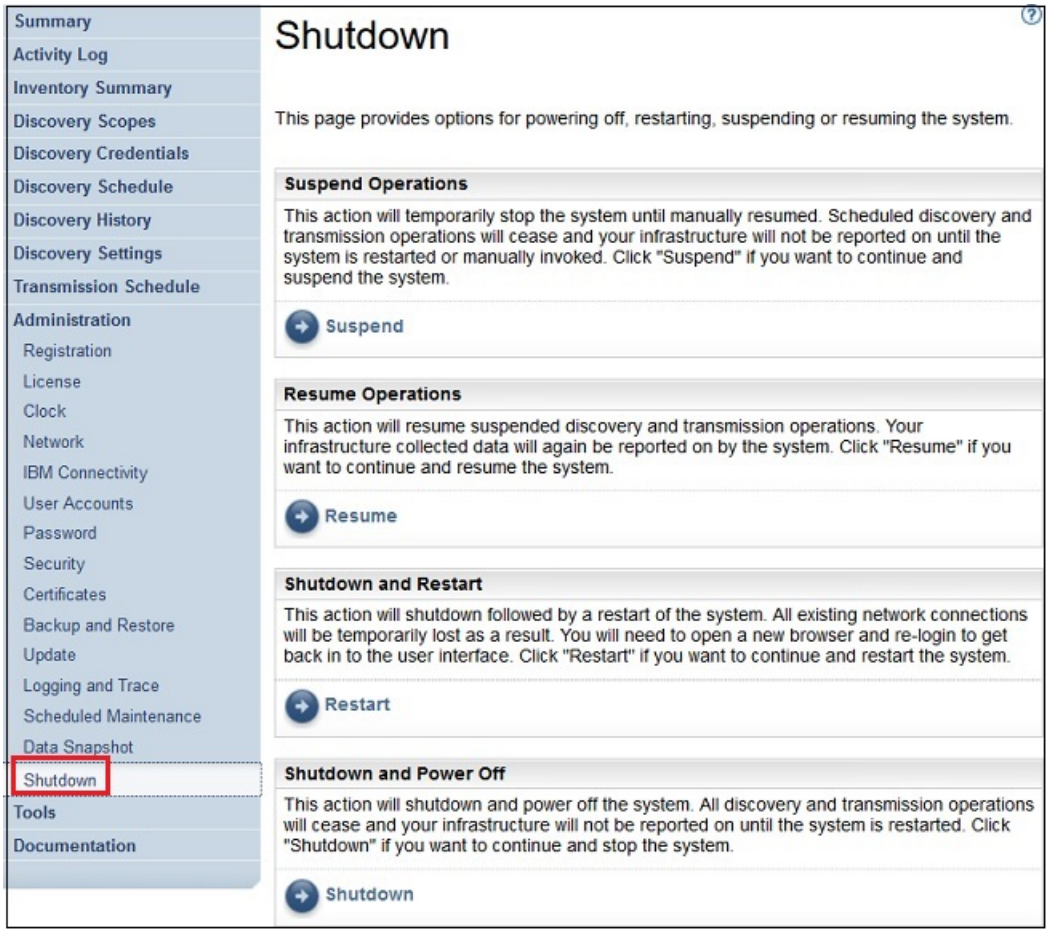

Figure 86. Arrêt

Suspendre les opérations

Cette action arrête temporairement TSA. Toutes les opérations de reconnaissance et de transmission sont suspendues et aucune information n'est transmise à IBM jusqu'à la reprise des opérations.

Pour suspendre les opérations de TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Arrêt**. La page **Arrêter** s'affiche.
2. Cliquez sur **Suspendre**.

Reprendre les opérations

Cette action relance TSA qui avait été temporairement arrêté. Toutes les opérations de reconnaissance et de transmission reprennent et des informations sont transmises à IBM comme prévu.

Pour reprendre les opérations de TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Arrêt**. La page **Arrêter** s'affiche.
2. Cliquez sur **Reprendre**.

Arrêter et redémarrer

Cette action arrête puis redémarre TSA. Toutes les connexions réseau existantes sont momentanément perdues. Vous devez ouvrir une nouvelle fenêtre de navigateur et vous reconnecter à TSA.

Pour arrêter et redémarrer TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Arrêt**. La page **Arrêter** s'affiche.
2. Cliquez sur **Redémarrer**.

Arrêter et mettre hors tension

Cette action arrête et met hors tension TSA. Toutes les opérations de reconnaissance et de transmission cessent et aucun rapport concernant votre infrastructure n'est créé tant que TSA n'a pas redémarré.

Pour arrêter et mettre hors tension TSA, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Administration** > **Arrêt**. La page **Arrêter** s'affiche.
2. Cliquez sur **Arrêter**.

Remarque : Après avoir arrêté l'appliance, vous devez mettre TSA sous tension à l'aide de l'interface web VMware ESXi ou de Hyper-V Manager.

Outils

TSA propose des outils pour vous aider à configurer l'environnement TSA.

Pour accéder à ces outils, cliquez sur **Outils** dans le panneau de navigation.

Outils réseau

Utilisez la page **Outils réseau** pour obtenir des outils et des informations de diagnostic relatifs aux protocoles de réseau utilisés par TSA.

Pour accéder à ces outils de diagnostic, cliquez sur **Outils** > **Outils réseau** dans le panneau de navigation. La page **Outils réseau** s'affiche.

La page Outils réseau comporte plusieurs pages d'onglet. Cliquez sur l'un des onglets pour accéder à la page correspondante.

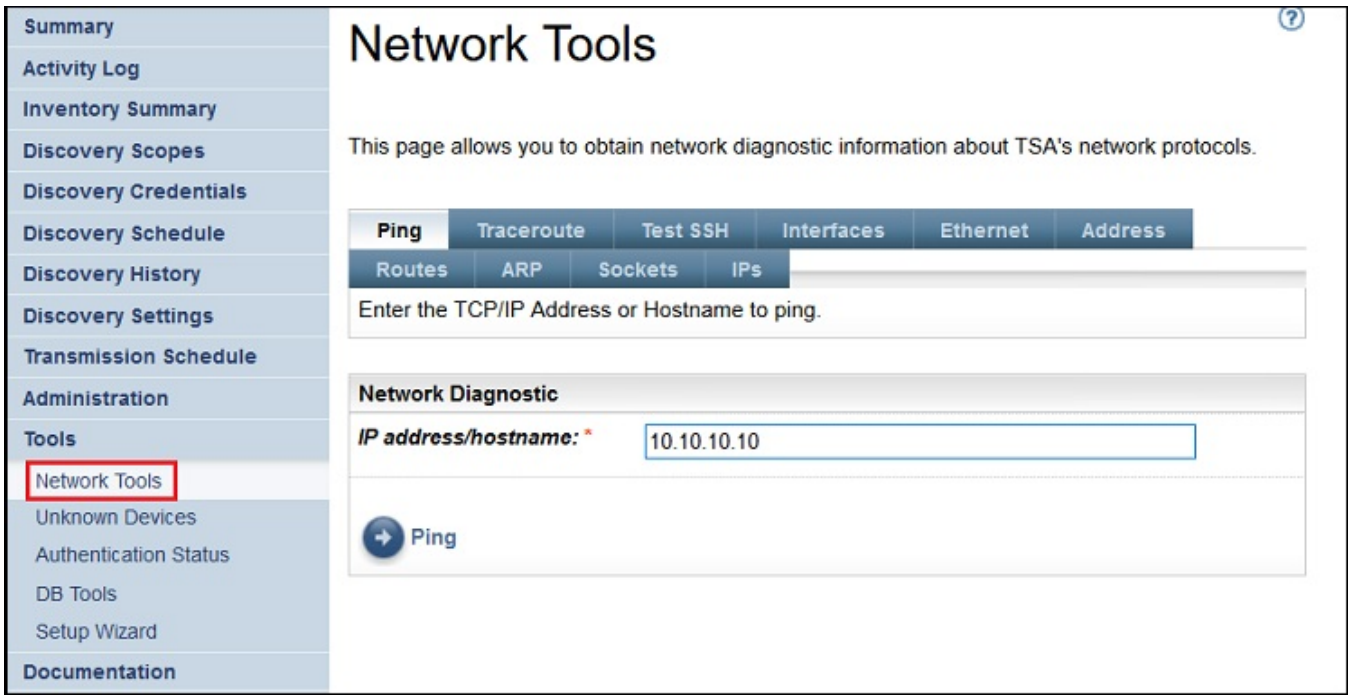

Figure 87. Outils réseau

Ping
Utilisez cette page pour envoyer une demande d'écho vers un hôte distant afin de vérifier si l'hôte est accessible et de recevoir des informations sur le nom d'hôte ou l'adresse IP.

Traceroute
Utilisez cette page pour afficher le chemin suivi par les paquets vers un hôte distant.

Tester SSH
Utilisez cette page pour tester si un hôte distant est accessible en utilisant la clé SSH et les données d'identification de la reconnaissance définies pour l'hôte.

Interfaces
Utilisez cette page pour afficher les statistiques relatives aux interfaces réseau en cours de configuration.

Ethernet
Utilisez cette page pour afficher les paramètres des cartes Ethernet en cours de configuration.

Adresse
Utilisez cette page pour afficher les adresses IP des interfaces réseau actuellement configurées.

Routes
Utilisez cette page pour afficher les tables de routage IP du noyau et les interfaces réseau correspondantes.

ARP
Utilisez cette page pour afficher le contenu des connexions de protocole de résolution d'adresse (ARP).

Sockets
Utilisez cette page pour afficher des informations sur les sockets TCP/IP.

Adresses IP
Utilisez cette page pour afficher des informations sur les règles de filtrage des paquets IP.

Remarque : Le nom d'hôte saisi ne doit pas contenir de trait de soulignement ("_").

Outils de base de données

Utilisez la page **Outils de base de données** pour exécuter les opérations de maintenance de données. Il est recommandé de n'utiliser ces fonctions qu'à la demande du support IBM.

Vous pouvez exécuter les opérations suivantes sur la base de données :

Recréer la base de données de l'inventaire

Lorsque vous recréez la base de données de l'inventaire, toutes les données d'inventaire sont perdues. De plus, les données d'identification sont également perdues si la case **Préserver les données d'identification** n'est pas cochée ou si le Gestionnaire de la reconnaissance n'est pas disponible.

Pour recréer la base de données, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Outils** > **Outils de base de données**.
2. Cochez la case **Préserver les données d'identification** dans la section **Recréer la base de données de l'inventaire** pour conserver toutes les données d'identification de la reconnaissance. Si vous ne cochez pas cette case, les donnés d'identification seront perdues et vous devrez les reconfigurer toutes. Pour plus d'informations sur les données d'identification de la reconnaissance, consultez «Données d'identification de la reconnaissance», à la page 75.

   Remarque : Les données d'identification ne peuvent être préservées que si le Gestionnaire de la reconnaissance est en cours d'exécution (état représenté en vert).
3. Cliquez sur **Recréer la base de données de l'inventaire**. Le message d'avertissement suivant s'affiche : `Cette action arrêtera temporairement le Gestionnaire de la reconnaissance. Voulez-vous vraiment recréer la base de données de l'inventaire ?`
4. Cliquez sur **OK** pour recréer la base de données de l'inventaire. Le message suivant s'affiche : `La recréation de la base de données a commencé`. L'opération peut durer environ 6 heures. Pendant ce temps, le message d'état `dbinit starting` est affiché sur la page Récapitulatif. Au bout de 6 heures, vous pouvez vérifier le **Journal d'activité** et constater que l'état est passé à `La recréation de la base de données de l'inventaire a réussi`.

   Remarque : Lors de la recréation de la base de données de l'inventaire, le Gestionnaire de la reconnaissance s'arrête temporairement et l'*Archive de nettoyage d'inventaire* est effacée.

Exécuter RUNSTATS

Pour exécuter la commande **RUNSTATS**, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Outils** > **Outils de base de données**.
2. Cliquez sur **Exécuter RUNSTATS**. Le message d'avertissement suivant s'affiche : `Voulez-vous vraiment exécuter RUNSTATS sur les tables de la base de données de l'inventaire ?`
3. Cliquez sur **OK**. Le message suivant s'affiche : `L'exécution de RUNSTATS a commencé`. Au bout de 30 minutes environ, vous pouvez vérifier le journal d'activité. Lorsque l'opération est terminée, le message suivant est ajouté au journal d'activité : `L'exécution de RUNSTATS sur la base de données de l'inventaire a réussi`.

Exécuter REORG

Pour exécuter la commande **REORG**, procédez comme suit :

1. Dans le panneau de navigation, cliquez sur **Outils** > **Outils de base de données**.
2. Cliquez sur **Exécuter REORG**. Le message de confirmation suivant s'affiche : `Voulez-vous vraiment exécuter REORG sur les tables de la base de données de l'inventaire ?`
3. Cliquez sur **OK**. Le message suivant est ajouté au journal d'activité : `L'exécution de REORG a commencé`. Au bout de 30 minutes environ, vous pouvez vérifier le journal d'activité. Lorsque

l'opération est terminée, le message suivant est ajouté au journal d'activité : `L'exécution de la commande REORG sur la base de données de l'inventaire a réussi..`

Documentation

Vous trouverez sur la page **Documentation** 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 du site web TSA à : https://ibm.biz/TSAdemo.

Procédure

Pour consulter la documentation et en apprendre plus sur Technical Support Appliance, suivez ces étapes :

1. Cliquez sur **Documentation** dans le menu de navigation de gauche.

Figure 88. Documentation

2. Pour en savoir plus sur Technical Support Appliance, cliquez sur ce lien : https://ibm.biz/TSAdemo
3. Sur la page **Installer TSA**, vous trouverez des liens vers l'image de TSA, son guide d'installation, son guide de configuration et des tutoriels.

Chapitre 7. Contacter le support IBM au sujet de Technical Support Appliance (TSA)

Le support IBM est disponible du lundi au vendredi aux heures de bureau de votre fuseau horaire.

Pourquoi et quand exécuter cette tâche

Vous pouvez contacter le support IBM de deux manières :

1. Ouvrez un dossier (cas) sur le portail du support IBM
2. Créez une demande de service via le centre d'appels IBM

Ouvrir un dossier (cas) sur le portail du support IBM

Procédure

1. Connectez-vous à https://www.ibm.com/mysupport/s/

   Remarque : Pour accéder au portail du support IBM, vous devez d'abord créer un compte.
2. Cliquez sur **Ouvrir un cas** en haut à droit du portail. La page correspondante s'affiche.
3. Sélectionnez le **Type de support**.
4. Entrez le **Titre**, le **Fabricant** et le **Produit**.

   Remarque : Pour adresser votre demande directement à l'équipe Technical Support Appliance, entrez `Technical Support Appliance` dans le champ **Produit**.
5. Sélectionnez la **Gravité**
6. Entrez la **Description** et sélectionnez votre langue préférée.
7. Si vous êtes disposé à communiquer en anglais au cas où aucun agent parlant votre langue ne serait disponible, sélectionnez **Oui**.
8. Cliquez sur **Soumettre**.

Créer une demande de service via le centre d'appels IBM

Procédure

1. Composez le numéro de téléphone exact du pays d'origine https://www.ibm.com/planetwide
2. Sélectionnez la langue.
3. Sélectionnez 1 (produits IBM).
4. Sélectionnez 2 (support logiciel).
5. Utilisez l'ID de produit *5621IZX01* ou le nom de produit *Technical Support Appliance*.
6. Vous êtes invité à fournir les informations suivantes :
   - N° société / Région
   - Client / Nom de la société
   - Adresse / Ville / Etat / Code postal
   - Bâtiment / Salle
   - Numéro de téléphone du lieu où TSA est installé.
   - Nom du contact / E-mail / N° téléphone
   - Description du problème

- Niveau de sévérité

Annexe A. Installation de TSA avec VMware vSphere Client

Avant de commencer
TSA exige de charger VMware ESXi 6.5 ou version ultérieure pour contrôler le matériel.

Pourquoi et quand exécuter cette tâche
Suivez ces étapes pour installer l'image de TSA. Pour plus d'informations sur la configuration requise, voir «Configuration requise pour TSA», à la page 5.

Remarque : La procédure (étapes 1 à 12) est un exemple / une référence indiquant comment déployer l'image de TSA. Certaines de ces étapes peuvent varier selon vos procédures locales de déploiement de machines virtuelles.

Procédure

Pour installer TSA, procédez comme suit :

1. Démarrez VMware vSphere Client.
2. Connectez-vous pour accéder au système ESXi.
3. Dans vSphere Client, cliquez sur **File** > **Deploy OVF Template**. L'assistant **Deploy OVF Template** s'affiche.

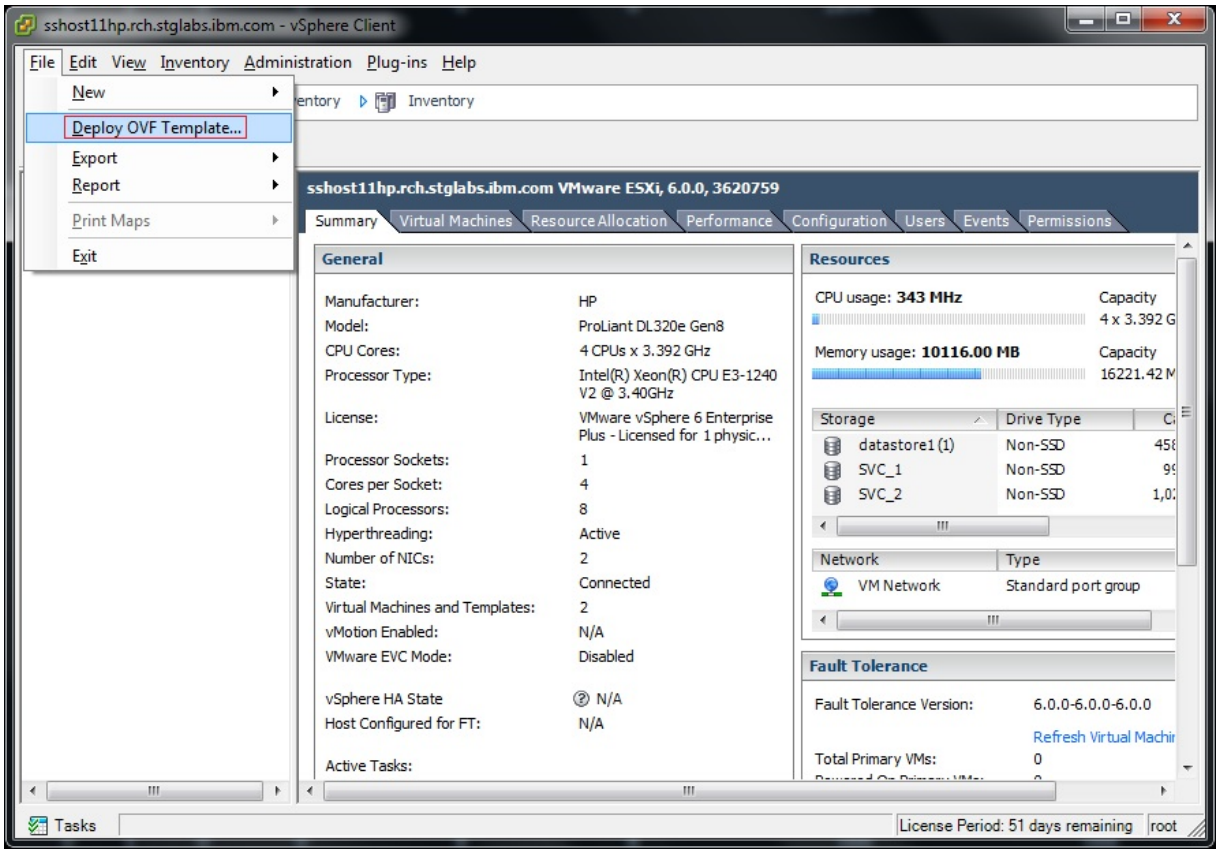

Figure 89. Déploiement d'un modèle OVF

4. Cliquez sur **Parcourir** et sélectionnez l'image qui est enregistrée sur votre système.

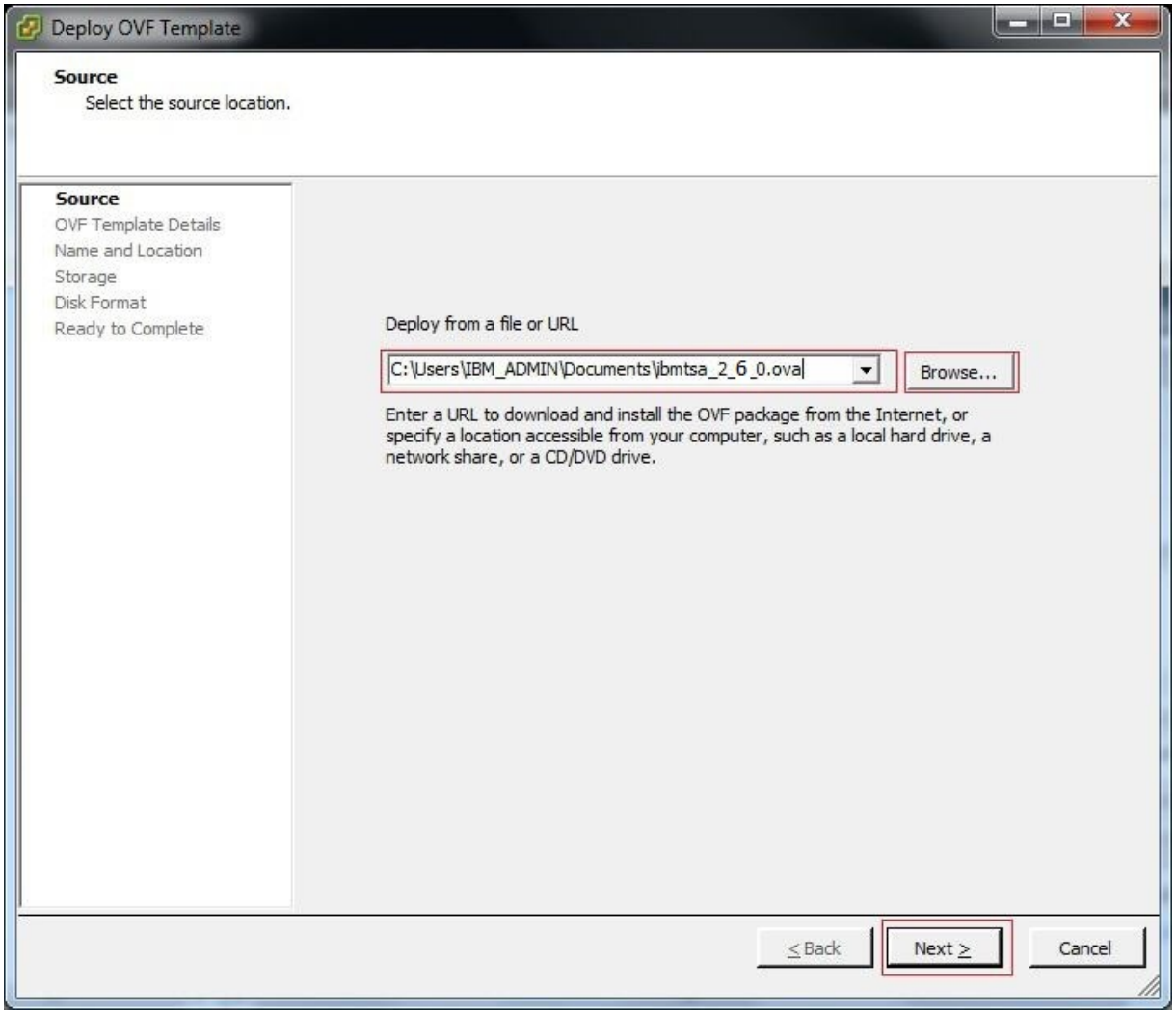

Figure 90. Source du modèle OVF

5. Cliquez sur **Suivant**. Les **Détails du modèle OVF** s'affichent.
6. Cliquez sur **Suivant**. Le panneau **Nom et emplacement** s'affiche.

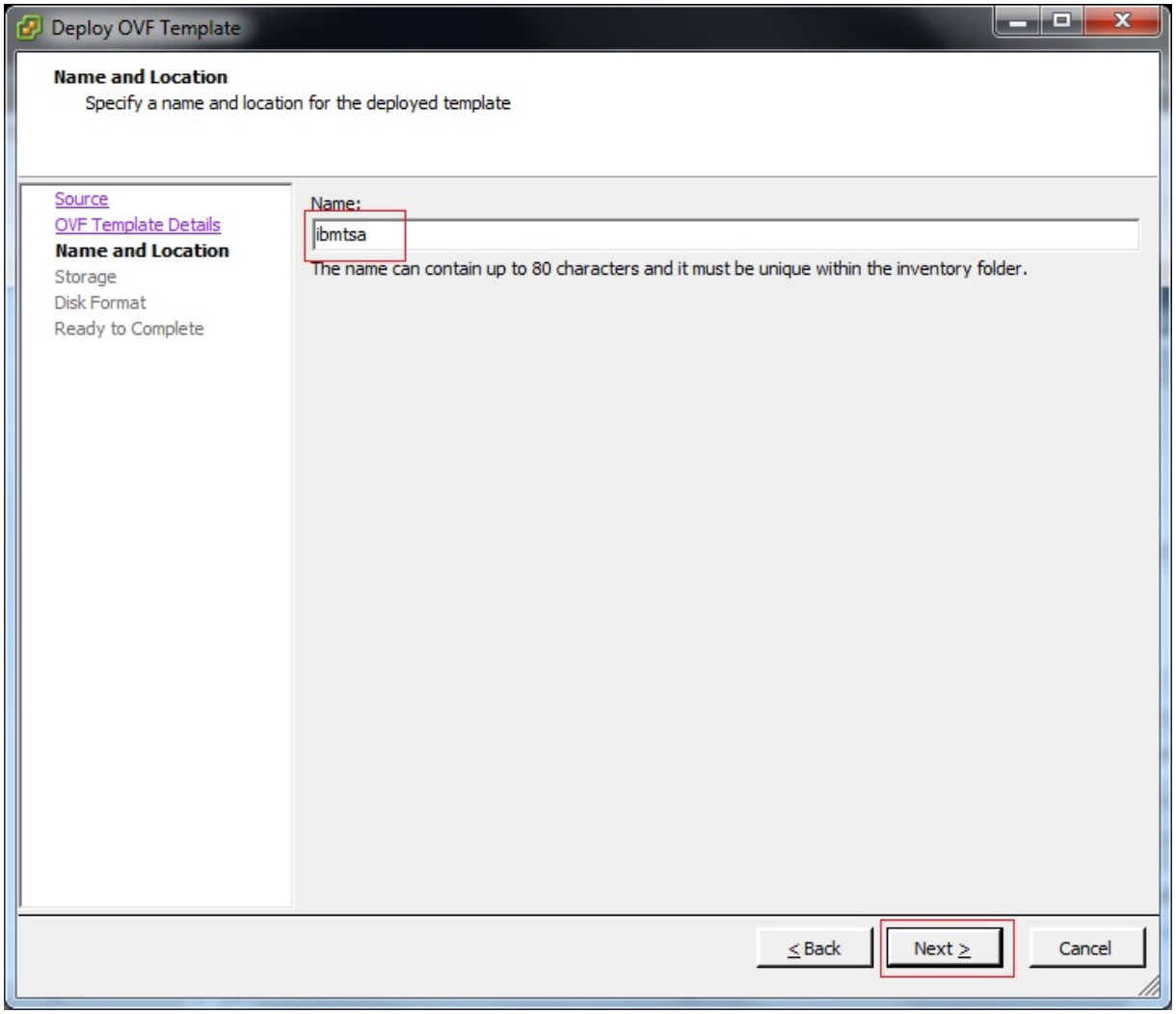

Figure 91. Nom et emplacement

7. Dans le panneau **Nom et emplacement**, entrez le **Nom** de votre machine virtuelle ou utilisez la valeur par défaut et cliquez sur **Suivant**.
8. Dans le panneau **Stockage**, sélectionnez le magasin de données (stockage des fichiers de machine virtuelle) et cliquez sur **Suivant**.

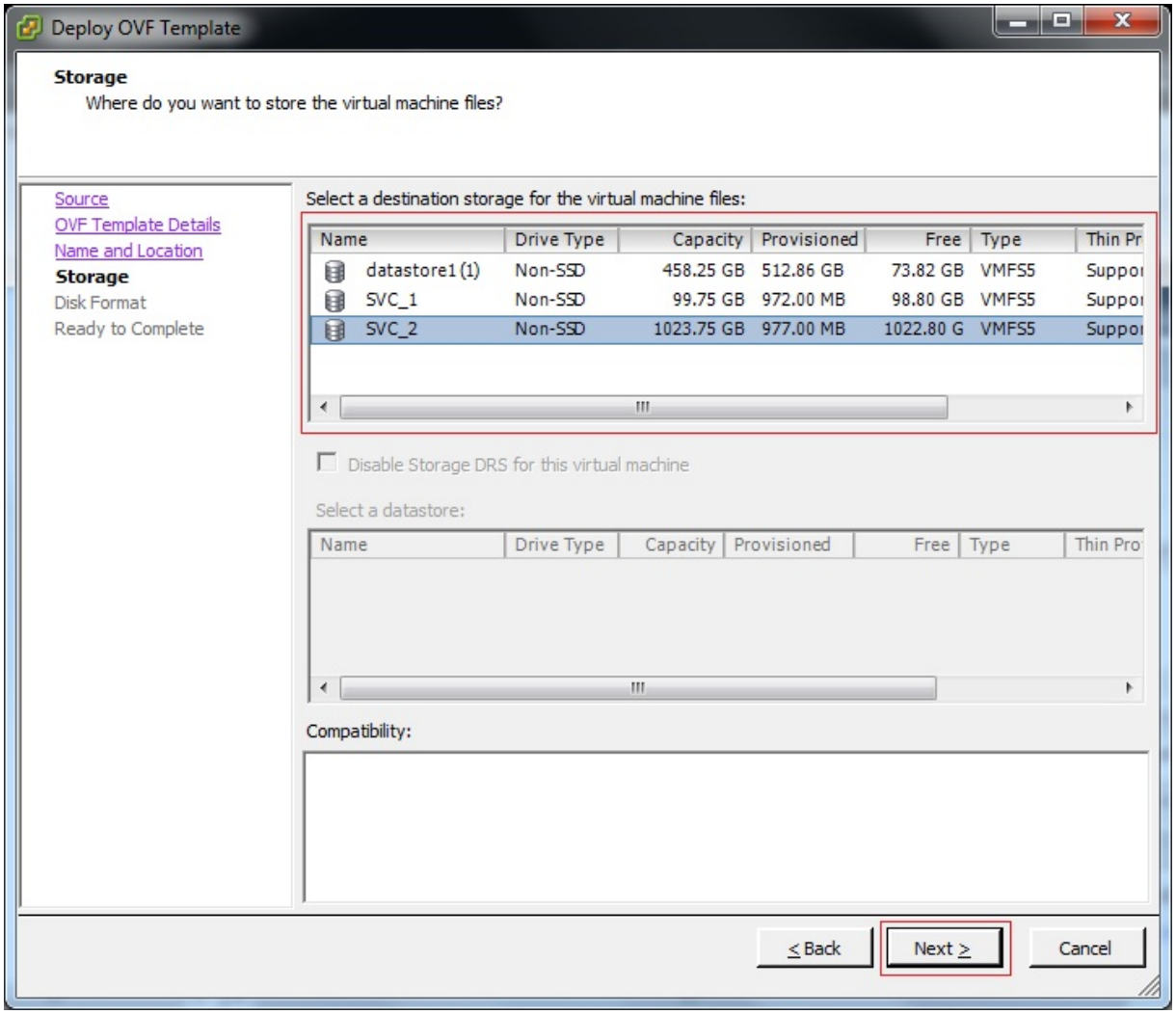

Figure 92. Stockage

9. Dans le panneau **Format de disque**, sélectionnez l'option **Thick Provision Eager Zeroed** et cliquez sur **Suivant**.

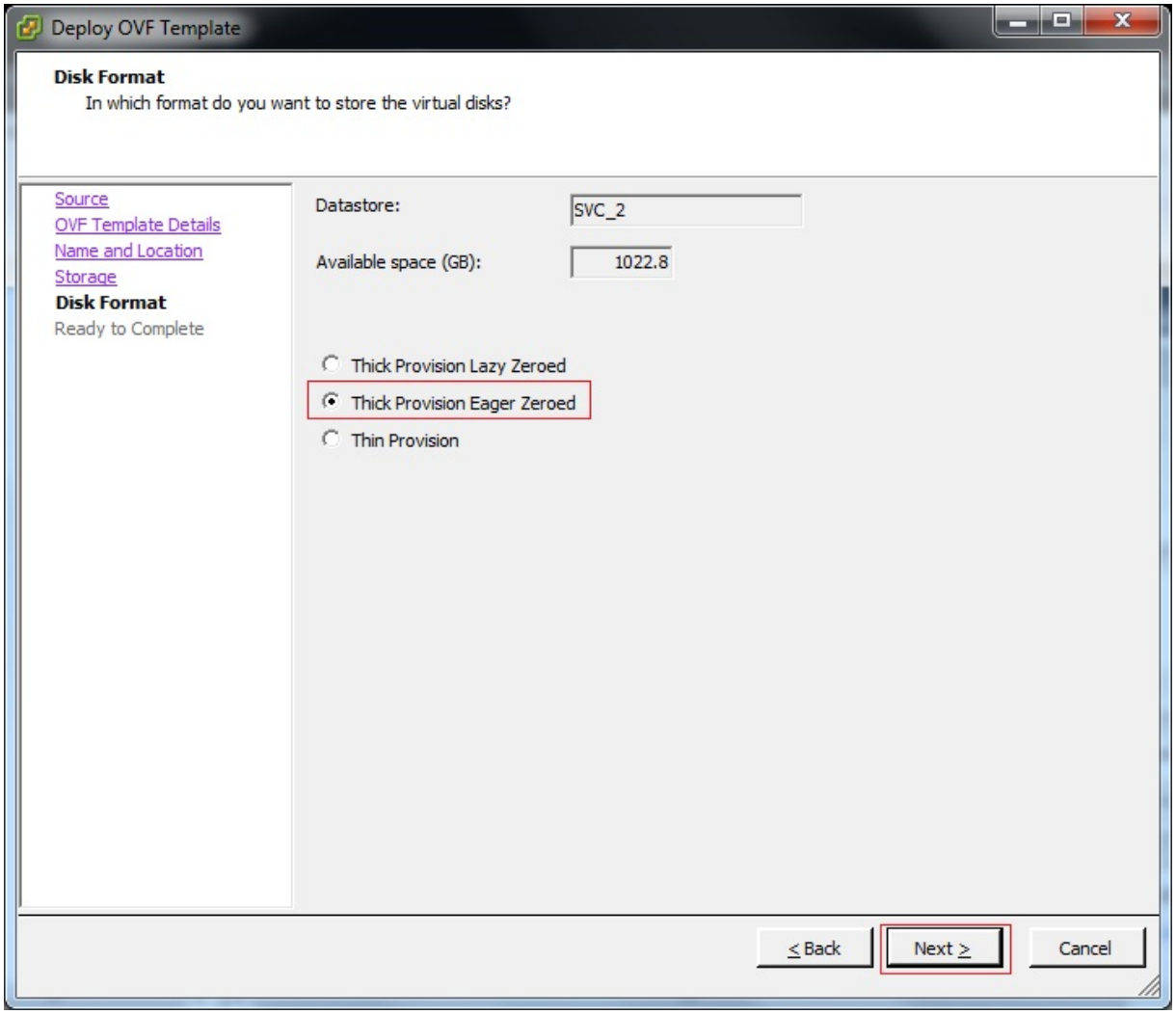

Figure 93. Format de disque

10. Si votre hyperviseur ESXi a une seule connexion réseau, passez à l'étape suivante. Sinon, sélectionnez le réseau approprié dans le panneau **Network Mapping** et cliquez sur **Suivant**.
11. Facultatif : Sélectionnez l'option **Mettre sous tension après déploiement** pour mettre automatiquement la machine virtuelle sous tension après déploiement. Vous pouvez aussi la mettre sous tension manuellement une fois le déploiement terminé.

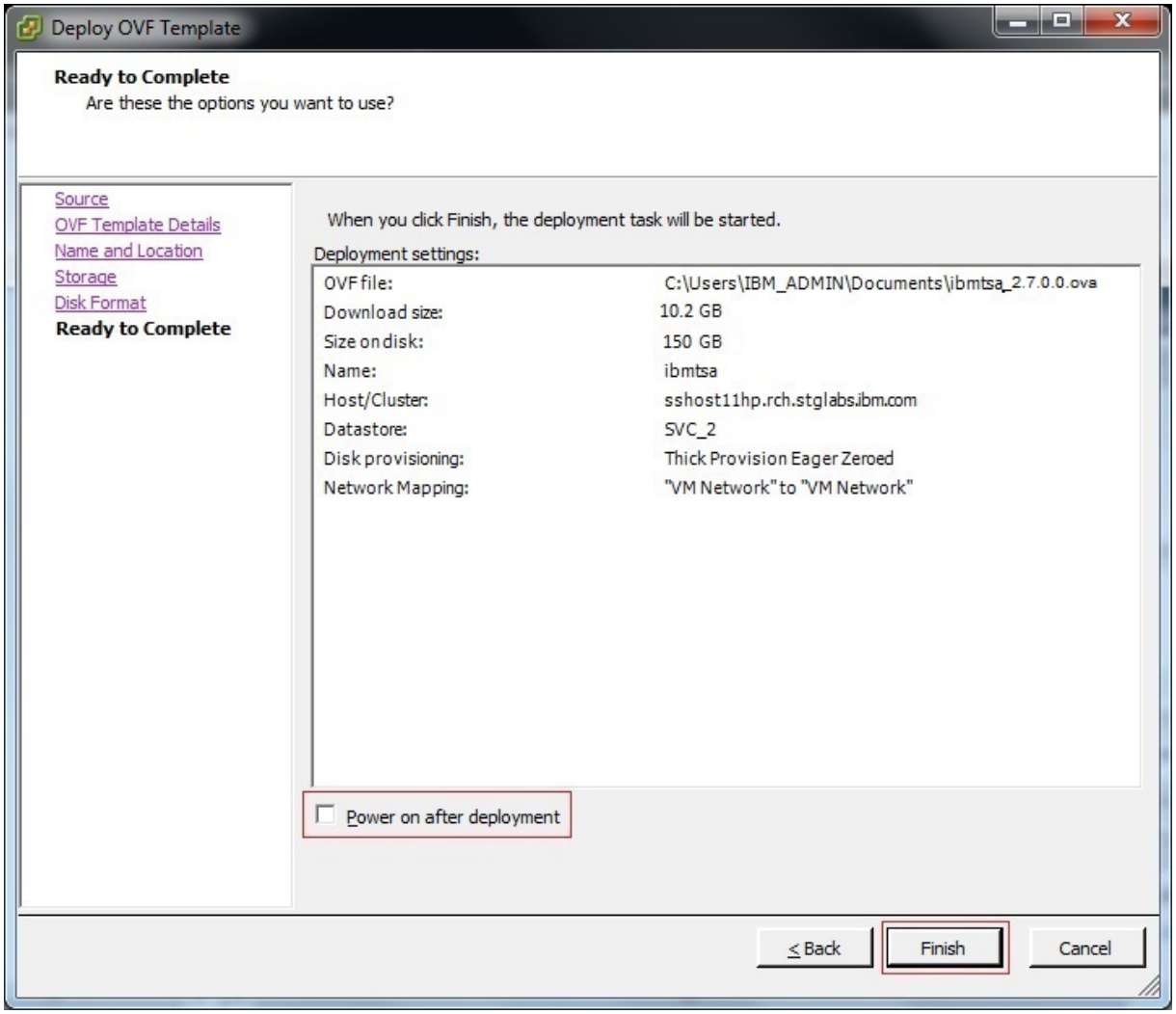

Figure 94. Prêt pour finalisation

12. Cliquez sur **Finish**. Le déploiement de TSA peut prendre environ 30 minutes mais cette durée varie selon la vitesse de la connexion réseau entre votre système et le système VMware ESXi.
13. Une fois le déploiement de TSA réussi, sélectionnez la machine virtuelle nouvellement déployée et cliquez sur l'onglet **Console** de vSphere Client.
14. Connectez-vous à la console TSA pour mettre en place la configuration réseau. Entrez **`tsausr`** comme **identifiant de connexion IBM TSA** et **`configTsa`** comme **mot de passe**.
15. Obligatoire : pour changer le mot de passe de connexion, suivez les étapes décrites à la section «Changer le mot de passe tsausr (obligatoire)», à la page 19.
16. Pour terminer l'installation, suivez les étapes décrites à la section «Configurer les données du réseau», à la page 19.

Annexe B. Configurer Technical Support Appliance

Si vous omettez de configurer des réglages dans l'**Assistant de configuration**, vous pouvez toujours revenir dessus dans le menu de navigation de gauche de TSA.

Enregistrer Technical Support Appliance

L'enregistrement permet de collecter les informations requises pour identifier TSA lorsque l'appliance renvoie des informations à IBM pour analyse.

Pourquoi et quand exécuter cette tâche
Pour enregistrer TSA, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Enregistrement**.
   La page **Enregistrement** s'affiche.

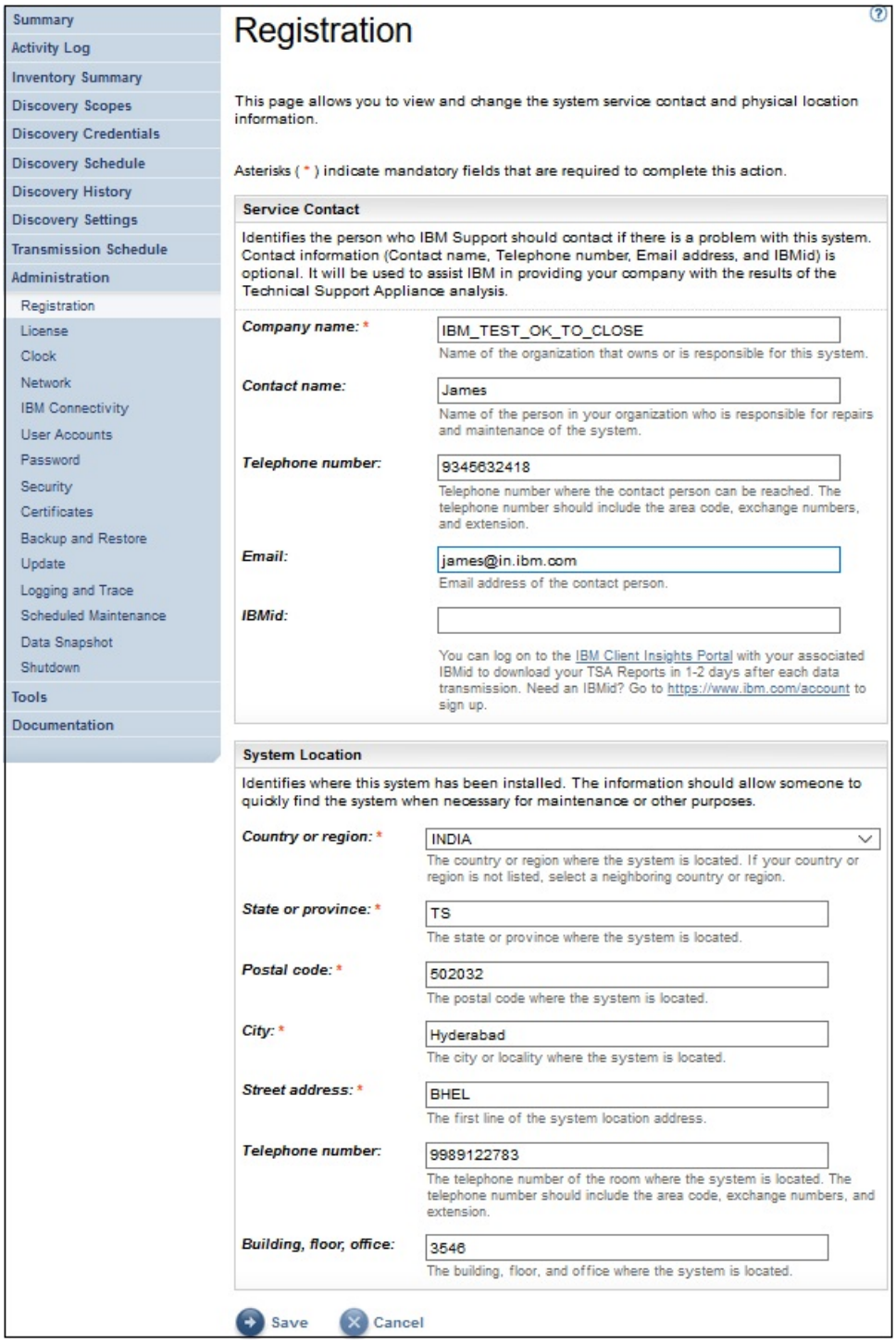

Figure 95. Enregistrement

2. Indiquez les coordonnées du contact pour la maintenance dans les champs suivants :

Nom de l'entreprise
Nom de l'entreprise qui utilise TSA.

Nom du contact
(Facultatif) Nom de la personne responsable de TSA dans l'entreprise.

Numéro de téléphone
(Facultatif) Numéro de téléphone auquel la personne responsable du système peut être contactée. Il doit comprendre l'indicatif pays, le préfixe national, le numéro national et le numéro de poste. N'utilisez pas de parenthèses dans le numéro de téléphone.

Adresse e-mail
(Facultatif) Adresse e-mail de la personne à contacter.

IBMid
(Facultatif) IBMid de la personne que vous autorisez à consulter les rapports sur IBM Client Insights Portal.

Remarque : Vous pouvez vous connecter à https://clientinsightsportal.ibm.com/ avec votre IBMid correspondant pour télécharger vos rapports TSA un ou deux jours après chaque transmission de données. Pour demander un IBMid, rendez-vous sur la page https://www.ibm.com/account.

Remarque : Le contact pour la maintenance permet d'identifier la personne que le support IBM doit contacter en cas de problème sur le système. Ces coordonnées vont permettre à IBM de fournir à votre entreprise les résultats de l'analyse de Technical Support Appliance.

3. Indiquez les informations sur l'emplacement de TSA dans les champs suivants :

Pays ou région
Pays ou région où TSA est installé.

État ou province
État ou province où TSA est installé. Si vous n'en êtes pas sûr, tapez *Inconnu*.

Code postal
Code postal du lieu où TSA est installé.

Ville
Ville ou localité où TSA est installé.

Adresse
Adresse de TSA.

Numéro de téléphone
(Facultatif) Numéro de téléphone de la pièce où TSA est installé. Il doit comprendre l'indicatif pays, le préfixe national, le numéro national et le numéro de poste. N'utilisez pas de parenthèses dans le numéro de téléphone.

Bâtiment, étage, bureau
(Facultatif) Bâtiment, étage et bureau où TSA est installé.

4. Cliquez sur **Enregistrer** pour enregistrer les informations d'enregistrement.

Paramétrer la connectivité IBM

Indiquez les informations de connexion à Internet à utiliser lors de la connexion à IBM.

Avant de commencer
Vérifiez que votre pare-feu autorise les connexions aux adresses IP et aux noms d'hôte du serveur IBM comme expliqué dans Tableau 1, à la page 6. Si votre réseau n'autorise pas l'accès aux serveurs IBM, les transactions TSA transmises au support IBM échoueront.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Connectivité IBM**.

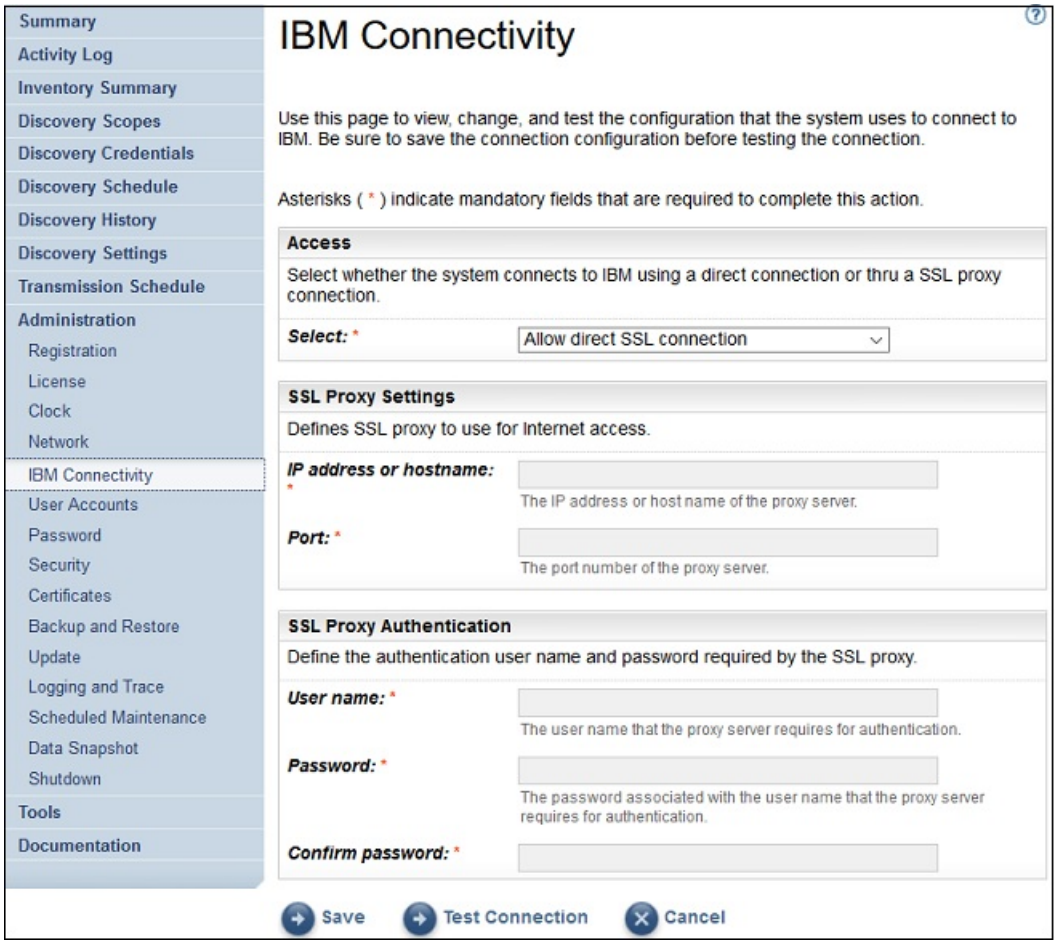

Figure 96. Connectivité IBM

2. Dans le panneau **Accès**, sélectionnez l'un des types d'accès Internet suivants :

   Autoriser une connexion SSL directe
   TSA se connecte à IBM via une connexion directe.

   Utiliser une connexion proxy SSL
   TSA se connecte à IBM via une connexion proxy SSL.

   Utiliser une connexion proxy SSL d'authentification
   TSA se connecte à IBM via une connexion proxy SSL qui nécessite une authentification.

3. Si vous avez sélectionné **Utiliser une connexion proxy SSL** ou **Utiliser une connexion proxy SSL d'authentification**, spécifiez les informations suivantes pour le serveur proxy.

   Adresse IP ou nom d'hôte
   Adresse IP ou nom d'hôte du serveur proxy.

   Remarque : Le nom d'hôte saisi ne doit pas contenir de trait de soulignement ("_").

   Port
   Numéro de port du serveur proxy.

4. Si vous avez sélectionné **Utiliser une connexion proxy SSL d'authentification**, spécifiez les informations suivantes pour le serveur proxy :

   Nom d'utilisateur
   Nom d'utilisateur requis par le serveur proxy pour l'authentification.

   Mot de passe
   Mot de passe associé au nom d'utilisateur requis par le serveur proxy pour l'authentification.

Confirmer le mot de passe
Entrez à nouveau le mot de passe. Les deux mots de passe saisis sont comparés afin de vérifier qu'ils correspondent avant que le mot de passe soit enregistré.

5. Cliquez sur **Enregistrer** pour enregistrer les informations de connexion à IBM.
6. Cliquez sur **Tester la connexion** pour tester la connexion indiquée.

Important :

- Enregistrez les paramètres de connexion avant de tester la connexion.
- Vous devez avoir une connexion à IBM opérationnelle, sinon les fonctions de TSA ne fonctionneront pas.

Concepts associés

Configuration requise pour les connexions au support IBM

TSA peut se connecter au support IBM via une connexion directe ou via un proxy fourni par l'utilisateur qui doit être configuré pour permettre la communication avec IBM. Si vous utilisez un proxy, l'inspection TLS/SSL n'est pas prise en charge. Toutes les demandes effectuées via un proxy doivent être autorisées à parvenir directement à IBM sans terminaison TLS/SSL.

Régler l'horloge

Vous devez définir l'heure système, la date et le fuseau horaire local de TSA lors de la configuration.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Horloge**.
   La page **Horloge** s'affiche.

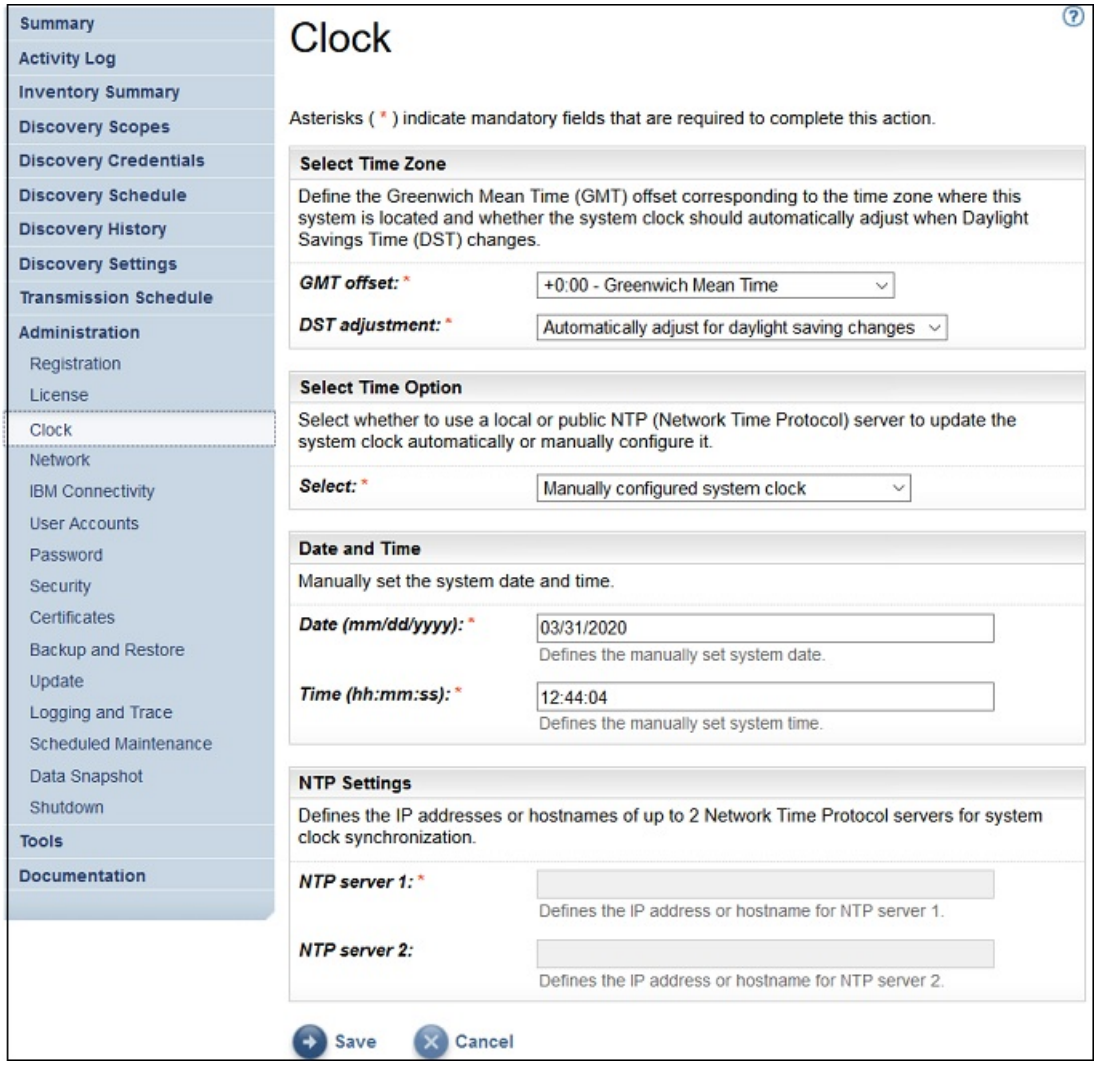

Figure 97. Horloge

2. Sélectionnez votre fuseau horaire local dans la liste déroulante **Décalage par rapport à l'heure GMT**.
3. Sélectionnez l'option d'ajustement lors des changements d'heure dans la liste déroulante **Ajustement lors des changements d'heure**.

   Remarque : Tous les fuseaux horaires n'ont pas de changement d'heure. Si cette option est sélectionnée pour un fuseau horaire où il n'y a pas de changement d'heure, une erreur se produit.
4. Sélectionnez une méthode pour mettre à jour l'horloge système dans la liste déroulante **Sélectionner l'option d'heure**.

   Les options disponibles sont la synchronisation de l'horloge système avec un serveur NTP pour une mise à jour automatique de l'horloge système, ou la configuration manuelle de l'horloge système.

   a) Si vous avez choisi de configurer l'horloge système manuellement, vous devez définir l'heure et la date système. Entrez la date et l'heure dans les champs **Date** et **Heure** correspondants.

   b) Si vous avez choisi de synchroniser l'horloge système avec un serveur NTP afin de mettre à jour automatiquement l'horloge système, vous devez indiquer l'adresse IP et le nom d'hôte de chaque serveur NTP. Tapez l'adresse IP ou le nom d'hôte pour un maximum de deux serveurs dans les champs **Serveur NTP** correspondants.

   Remarque : Assurez-vous que le serveur NTP est accessible via le réseau à TSA.
5. Cliquez sur **Enregistrer** pour enregistrer les données d'horloge.

Résultats

Remarque : Pour prendre effet, certaines modifications peuvent nécessiter un redémarrage du système. C'est le cas notamment si vous réglez la date et l'heure ou si vous passez d'une configuration manuelle à une configuration de serveur NTP.

Mise en place du planning de transmission

TSA fournit un planning par défaut pour que le processus de transmission s'exécute à un moment précis. Vous pouvez modifier ce planning selon vos besoins.

Procédure

1. Dans le panneau de navigation, cliquez sur **Planning de transmission**.

   La page **Planning de transmission** s'affiche.

   Le panneau **Planifier** affiche la prochaine exécution planifiée et les heures d'exécution planifiées. Le panneau **Historique** affiche l'état et d'autres informations sur les travaux de transmission précédents et ceux en cours d'exécution.
2. Cliquez sur **Modifier le planning**.

   La page **Planning de transmission** s'affiche.

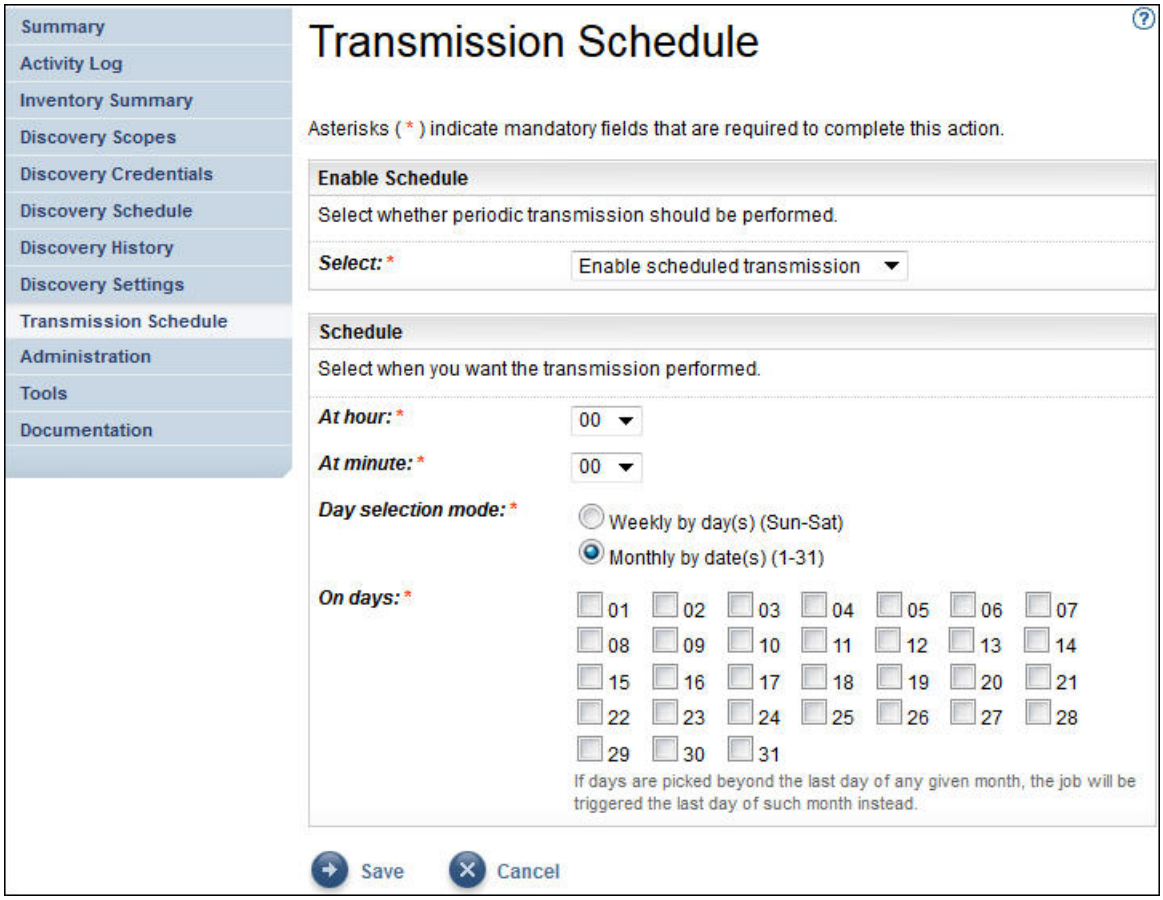

Figure 98. Modifier le planning de transmission

   a) Sélectionnez une nouvelle heure à l'aide des listes déroulantes **Heure** et **Minute**.

   b) Sélectionnez le **Mode de sélection du jour**.

      Hebdomadaire par jour(s) (dimanche au samedi)
      Pour planifier la transmission un ou plusieurs jours précis de la semaine, sélectionnez l'option **Hebdomadaire par jour(s) (dimanche au samedi)**.

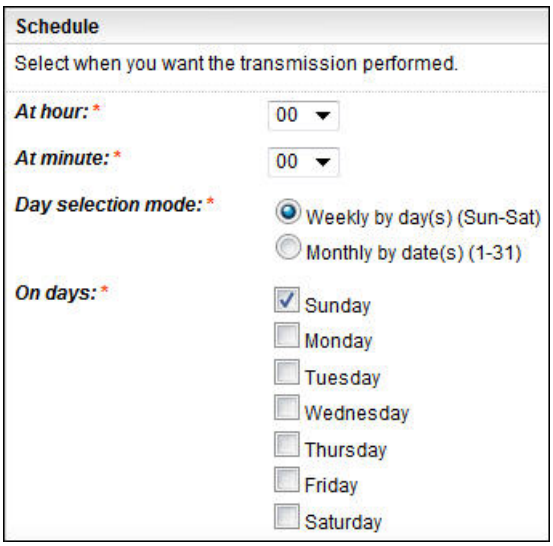

Figure 99. Hebdomadaire par jour(s) (dimanche au samedi)

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours de la semaine.

Mensuel par date(s) (1-31)

Pour planifier la transmission un ou plusieurs jours précis du mois, sélectionnez l'option **Mensuel par date(s) (1-31)**.

Pour le champ **Jours**, cochez la (les) case(s) appropriée(s) pour sélectionner un ou plusieurs jours du mois.

Remarque : Si vous sélectionnez des jours au-delà de la fin d'un mois spécifique, le travail sera déclenché le dernier jour de ce mois.

3. Cliquez sur **Enregistrer**.
   La page **Planning de transmission** s'affiche à nouveau avec le nouveau planning.

Mettre à jour

Vous pouvez rechercher et télécharger les mises à jour de TSA.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Mise à jour**.
   La page **Mettre à jour** s'affiche.

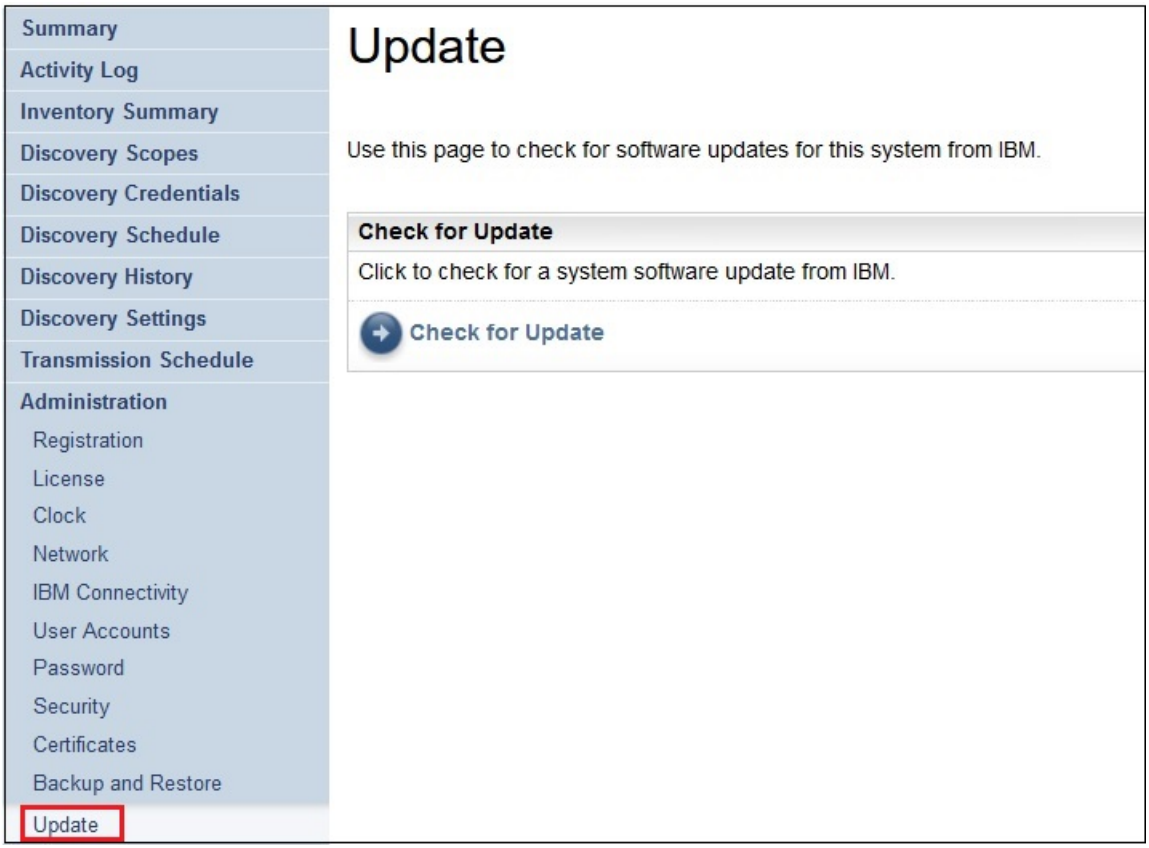

Figure 100. Mise à jour

2. Cliquez sur **Rechercher la mise à jour**.
   La page **Mises à jour disponibles** répertorie toutes les mises à jour disponibles.

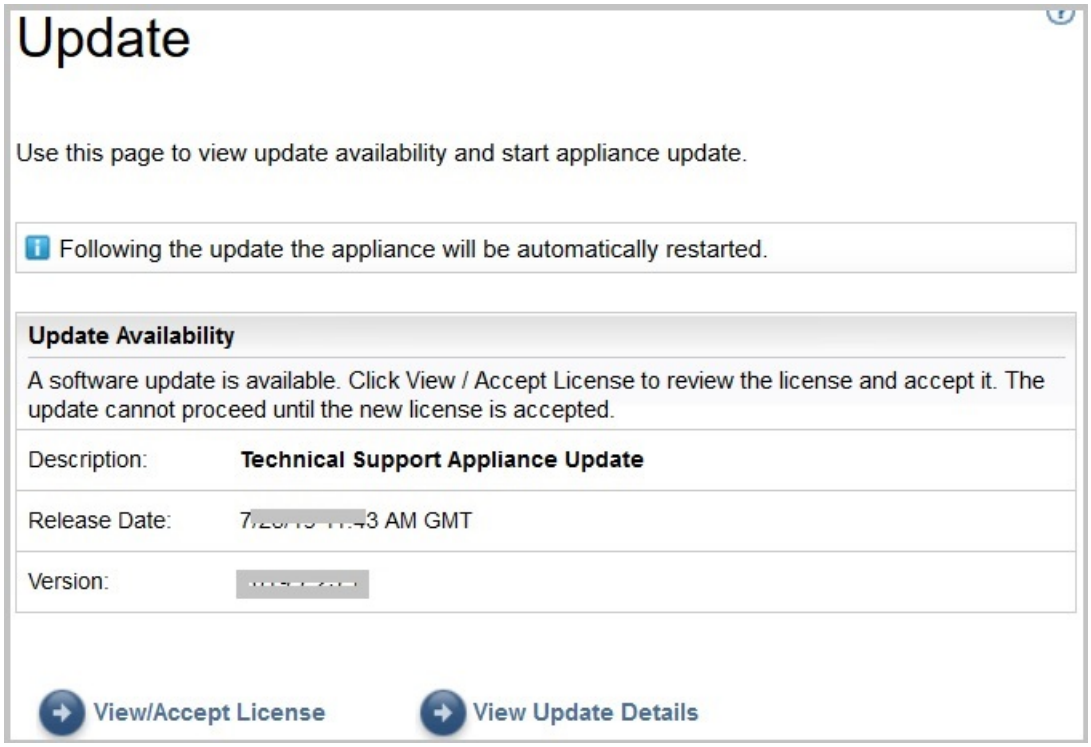

Figure 101. Mises à jour disponibles

a) Pour certaines nouvelles versions de TSA, vous devez accepter un nouveau contrat de licence avant d'effectuer la mise à jour. S'il y a une nouvelle licence, cliquez sur **Voir/accepter la licence** ; la page **Contrat de licence** s'affiche.

b) Cliquez sur le bouton **Accepter** de la page **Contrat de licence** pour accepter le nouveau contrat de licence. La page **Mise à jour** réapparaît et affiche le bouton **Exécuter la mise à jour**. S'il n'y a pas d'obligation d'accepter un nouveau contrat de licence, le bouton **Voir/accepter la licence** ne s'affiche pas et vous pouvez immédiatement cliquer sur **Exécuter la mise à jour**.

Remarque :

- Une fois que vous avez accepté la licence, le bouton **Voir/accepter la licence** n'est plus visible.
- Dans le panneau de navigation, cliquez sur **Administration** > **Licence** pour afficher le dernier contrat de licence que vous avez accepté.

c) Pour installer les mises à jour, cliquez sur **Exécuter la mise à jour**.

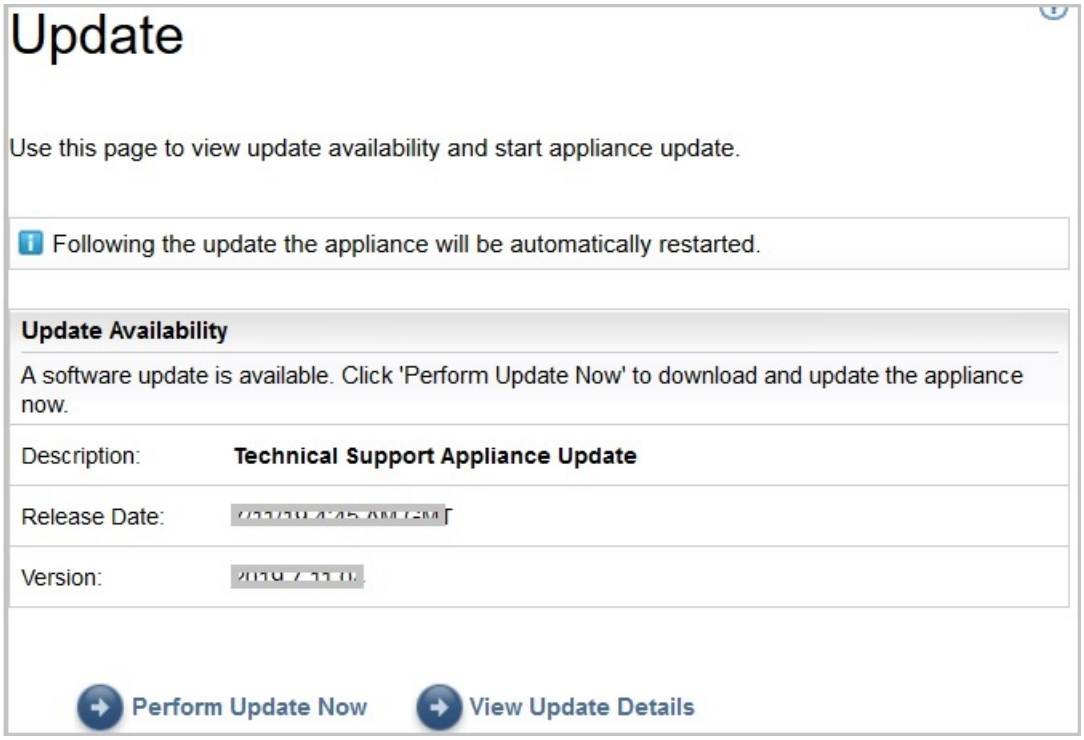

Figure 102. Exécuter la mise à jour

Lorsque la mise à jour est terminée, TSA redémarre automatiquement.

d) Pour afficher des informations sur le contenu de la mise à jour, cliquez sur **Voir les détails de la mise à jour**.

Annexe C. Configurer les données du réseau DHCP

Pour configurer les données du réseau DHCP, procédez comme suit :

Procédure

1. Sélectionnez l'option **1) Paramétrer la configuration réseau** dans le **Menu de configuration de TSA**.

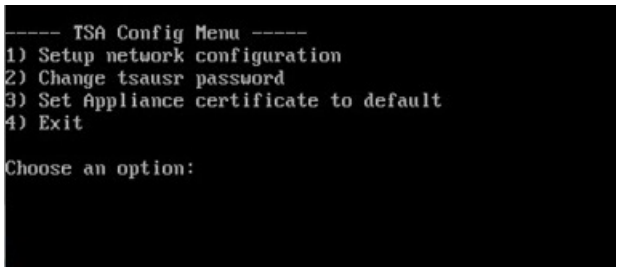

Figure 103. Mettre en place la configuration du réseau

2. Entrez les données de configuration réseau suivantes.

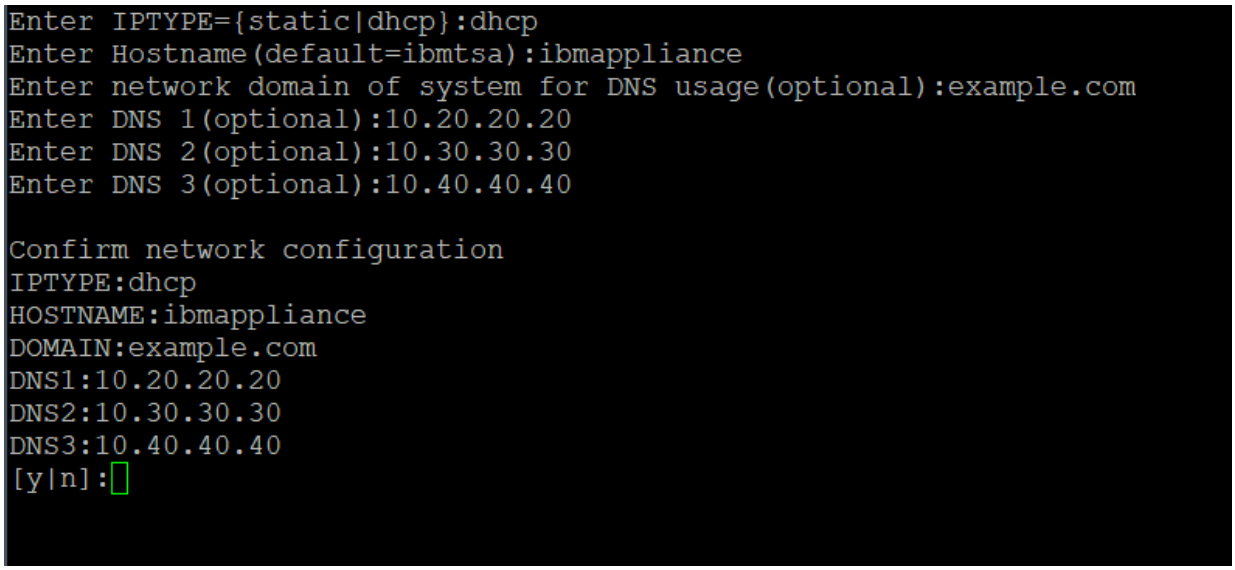

Figure 104. Configuration réseau

a) **Entrez TYPEIP = {statique|dhcp}**. Entrez dhcp.

TYPEIP : dhcp

Entrer nom d'hôte(valeur par défaut=ibmtsa). Vous pouvez changer le nom d'hôte par rapport à sa valeur par défaut. Assurez-vous que le nom d'hôte utilisé est unique.

Entrer le domaine de réseau du système pour utilisation DNS (facultatif).

Entrer DNS 1(facultatif), **Entrer DNS 2(facultatif)** et **Entrer DNS 3 (facultatif)**.

Les données de configuration réseau indiquées s'affichent pour confirmation.

b) Entrer **[o|n]** pour confirmer ou annuler la configuration réseau. Si vous entrez **o**, la configuration réseau est enregistrée et le système redémarre automatiquement.

Remarque : Si une configuration est incorrecte, vous pouvez en modifier les données. Entrez **n** pour ignorer les paramètres actuels et recommencez la configuration à partir de l'étape «2.a», à la page 135

c) Le système redémarre 15 secondes après afin que la nouvelle configuration réseau soit prise en compte.

d) Après le redémarrage du système, connectez-vous au Virtualization Manager et prenez note de l'**Adresse IP** sous l'onglet **Summary**.

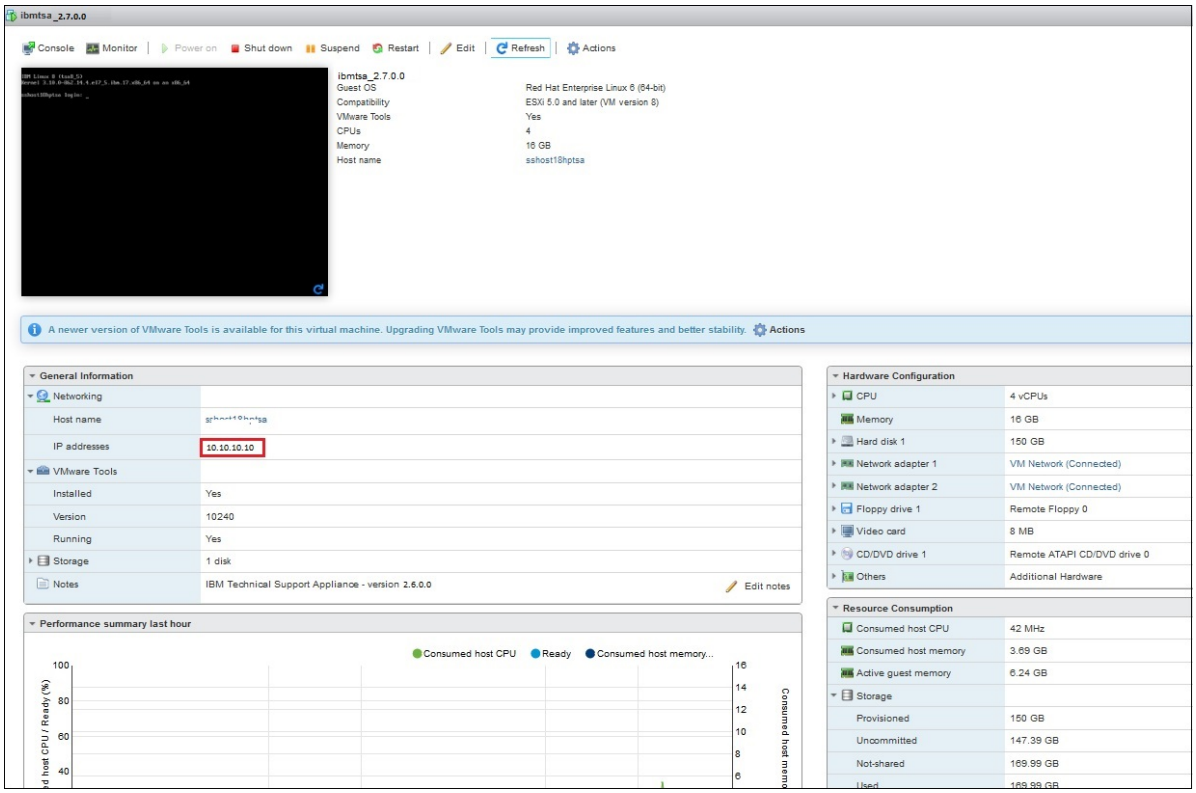

Figure 105. Adresse IP DHCP

e) Accédez à TSA depuis votre navigateur en utilisant l'adresse URL obtenue à l'étape précédente. Exemple : `https://newhost1.new.abclabs.example.com`

Remarque : Lors de la première connexion, il se peut que votre navigateur affiche une exception de sécurité. Vous devez accepter le certificat de sécurité et poursuivre la procédure de connexion à TSA.

Annexe D. Comptes d'utilisateur et groupes d'utilisateurs

Vous pouvez utiliser des comptes d'utilisateur et des groupes d'utilisateurs pour accorder l'accès aux fonctions TSA.

Avant de commencer

TSA est installé avec un compte d'utilisateur nommé **admin**. Ce compte a l'autorisation d'exécuter toutes les fonctions TSA. Peut-être souhaiterez-vous ajouter d'autres comptes d'utilisateur pour :

- Permettre à un autre utilisateur d'agir comme remplaçant de l'utilisateur **admin**.
- Autoriser certains utilisateurs à accéder à un nombre limité de fonctions sur TSA.

Pourquoi et quand exécuter cette tâche

L'exécution d'une fonction de TSA exige un certain niveau d'autorisation. Si un utilisateur authentifié tente d'exécuter une fonction sans avoir le niveau d'autorisation adéquat, un message d'erreur s'affiche et la fonction ne s'exécute pas.

Dans TSA, les niveaux d'autorisation sont associés à des groupes d'utilisateurs. Ces utilisateurs font partie d'un ou plusieurs groupes d'utilisateurs et du fait de cette appartenance, ils ont le niveau d'autorisation requis pour exécuter certaines fonctions.

TSA est livré avec un groupe d'utilisateurs **Administrateur** et un compte d'utilisateur **admin**. Le groupe d'utilisateurs **Administrateur** dispose d'un accès non restreint à toutes les fonctions système. Le compte d'utilisateur **admin** est affecté au groupe d'utilisateurs **Administrateur**.

Afficher des comptes d'utilisateur et des groupes d'utilisateurs

Vous pouvez afficher des comptes d'utilisateur et des groupes d'utilisateurs existants.

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.
   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Pour afficher les comptes d'utilisateur existants, cliquez sur l'onglet **Comptes**.
   Le tableau Comptes d'utilisateur affiche les comptes d'utilisateur existants.

   Conseil : Pour voir le détail d'un compte d'utilisateur spécifique, cliquez sur le nom du compte d'utilisateur. Le panneau **Généralités** à droite affiche le nom d'utilisateur, le nom complet et la description associée au compte d'utilisateur sélectionné. Cliquez sur le panneau **Membre de** à droite pour voir les groupes d'utilisateurs auxquels appartient ce compte d'utilisateur.
3. Pour afficher les groupes d'utilisateurs existants, cliquez sur l'onglet **Groupes**.
   Le tableau Groupes d'utilisateurs affiche les groupes d'utilisateurs existants.

   Conseil : Pour voir le détail d'un groupe d'utilisateurs spécifique, cliquez sur le nom du groupe d'utilisateurs. Le panneau **Généralités** à droite affiche le nom et le niveau d'autorisation associé au groupe d'utilisateurs. Cliquez sur le panneau **Restrictions de périmètre** à droite pour voir les ensembles de périmètres que peut découvrir le groupe d'utilisateurs sélectionné. Cliquez sur le panneau **Membres** pour voir les comptes d'utilisateur associés à ce groupe d'utilisateurs.

Ajouter des comptes d'utilisateur et des groupes d'utilisateurs

Vous pouvez ajouter des comptes d'utilisateur et des groupes d'utilisateurs pour contrôler l'accès aux fonctions TSA.

Concepts associés

Périmètres de reconnaissance et ensembles de périmètres

Les périmètres de reconnaissance identifient les ressources qui doivent être reconnues par TSA. Les périmètres de reconnaissance sont groupés par ensembles de périmètres de reconnaissance.

Ajouter un groupe d'utilisateurs

Vous pouvez ajouter des groupes d'utilisateurs pour contrôler l'accès aux fonctions TSA.

Pourquoi et quand exécuter cette tâche

Pour ajouter un groupe d'utilisateurs, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.
   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Cliquez sur l'onglet **Groupes**.

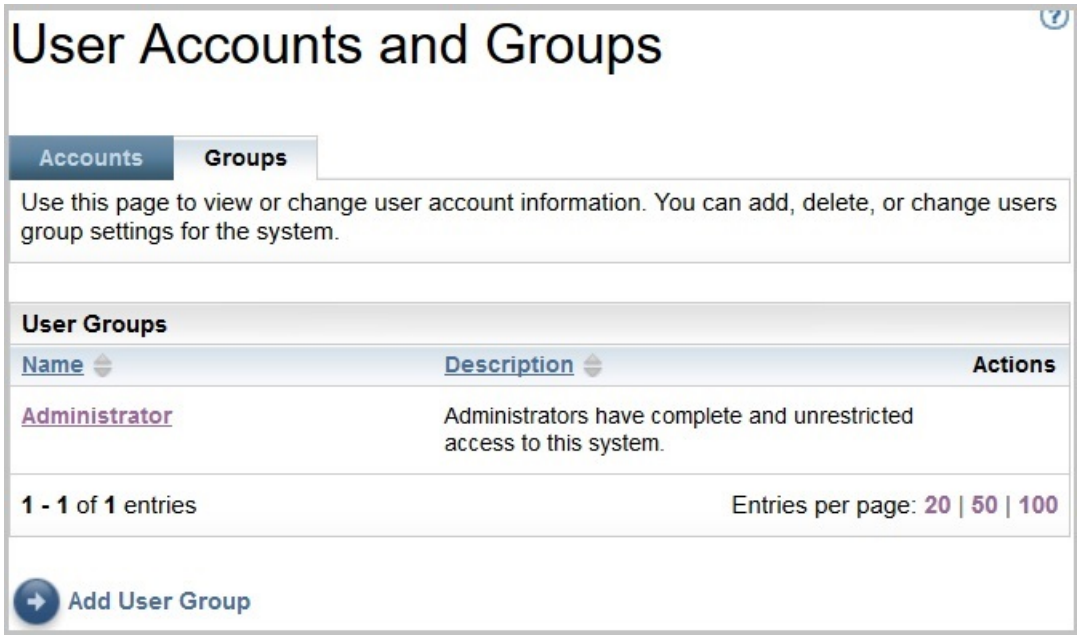

Figure 106. Groupes

3. Cliquez sur **Ajouter un groupe d'utilisateurs**.
   La page **Groupe d'utilisateurs** s'affiche.

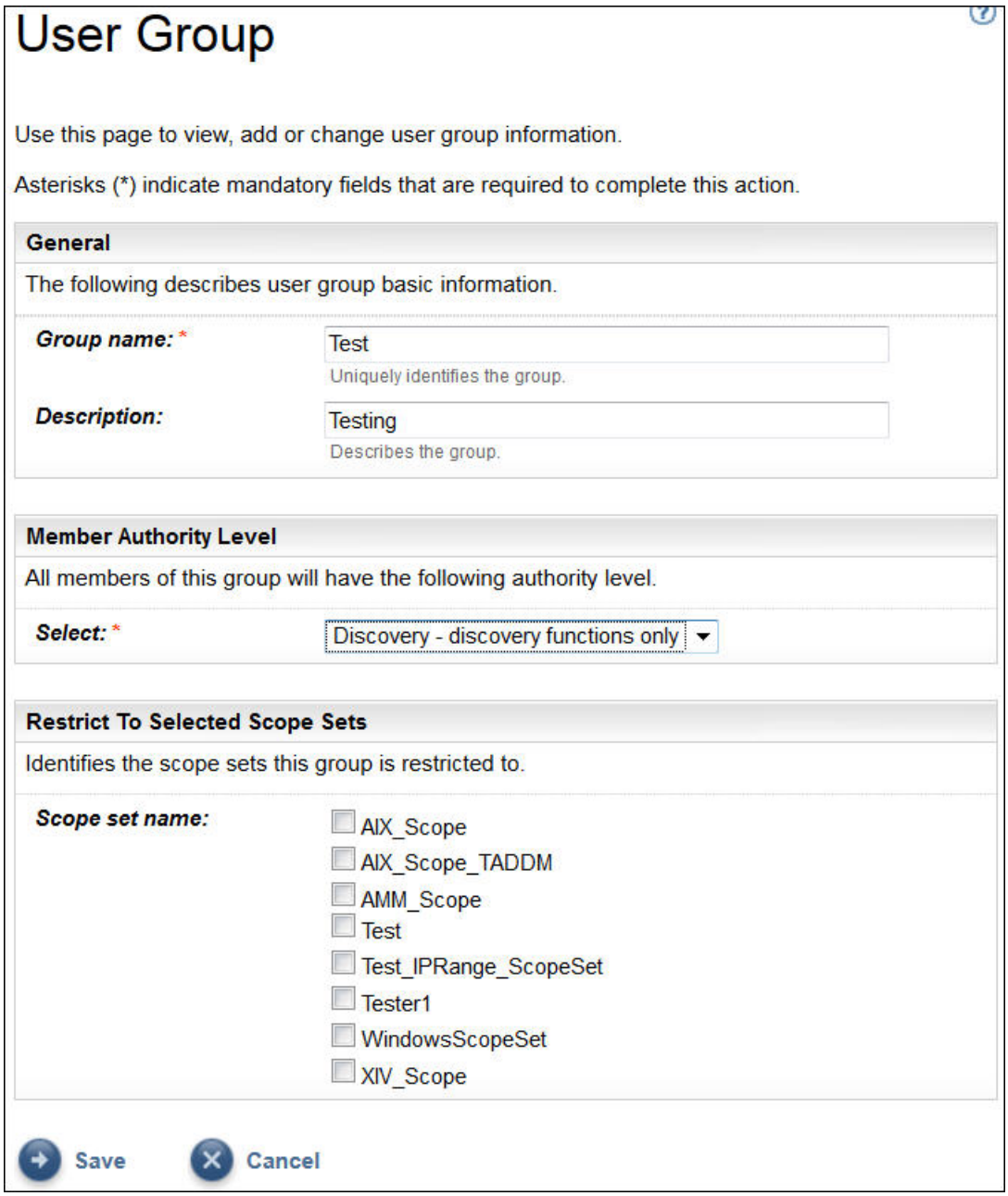

Figure 107. Ajouter un groupe d'utilisateurs

4. Dans le champ **Nom de groupe**, entrez un nom unique pour ce groupe d'utilisateurs.
5. Facultatif : Dans le champ **Description**, entrez une description pour ce groupe d'utilisateurs.
6. Sélectionnez le niveau d'autorisation souhaité pour les membres de ce groupe d'utilisateurs.

   TSA définit les niveaux d'autorisation de groupe suivants :

   - **Administrateur** – aucune restriction
   - **Reconnaissance** – fonctions de reconnaissance seulement
   - **Visiteur** – accès en lecture seule
7. Si vous indiquez le niveau d'autorisation *Reconnaissance* pour ce groupe d'utilisateurs, vous devez sélectionner au moins un ensemble de périmètres qui soit restreint à ce groupe d'utilisateurs.

   Pour plus d'informations sur les ensembles de périmètres, voir «Périmètres de reconnaissance et ensembles de périmètres», à la page 2.
8. Cliquez sur **Enregistrer** pour enregistrer le groupe d'utilisateurs.

La page **Comptes et groupes d'utilisateurs** s'affiche avec le nouveau groupe d'utilisateurs dans la liste.

Ajouter un compte d'utilisateur

Vous pouvez ajouter des comptes d'utilisateur pour contrôler l'accès aux fonctions TSA.

Pourquoi et quand exécuter cette tâche

Pour ajouter un compte d'utilisateur, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.
   La page **Comptes et groupes d'utilisateurs** s'affiche.

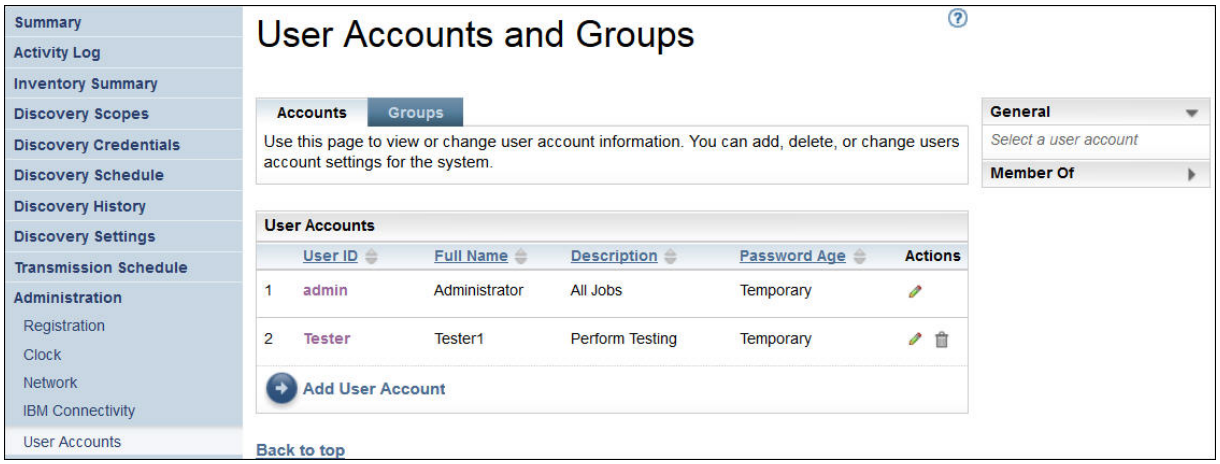

Figure 108. Comptes et groupes d'utilisateurs

2. Pour définir un nouveau compte d'utilisateur, cliquez sur **Ajouter un compte d'utilisateur**.
   La page **Compte d'utilisateur** s'affiche.

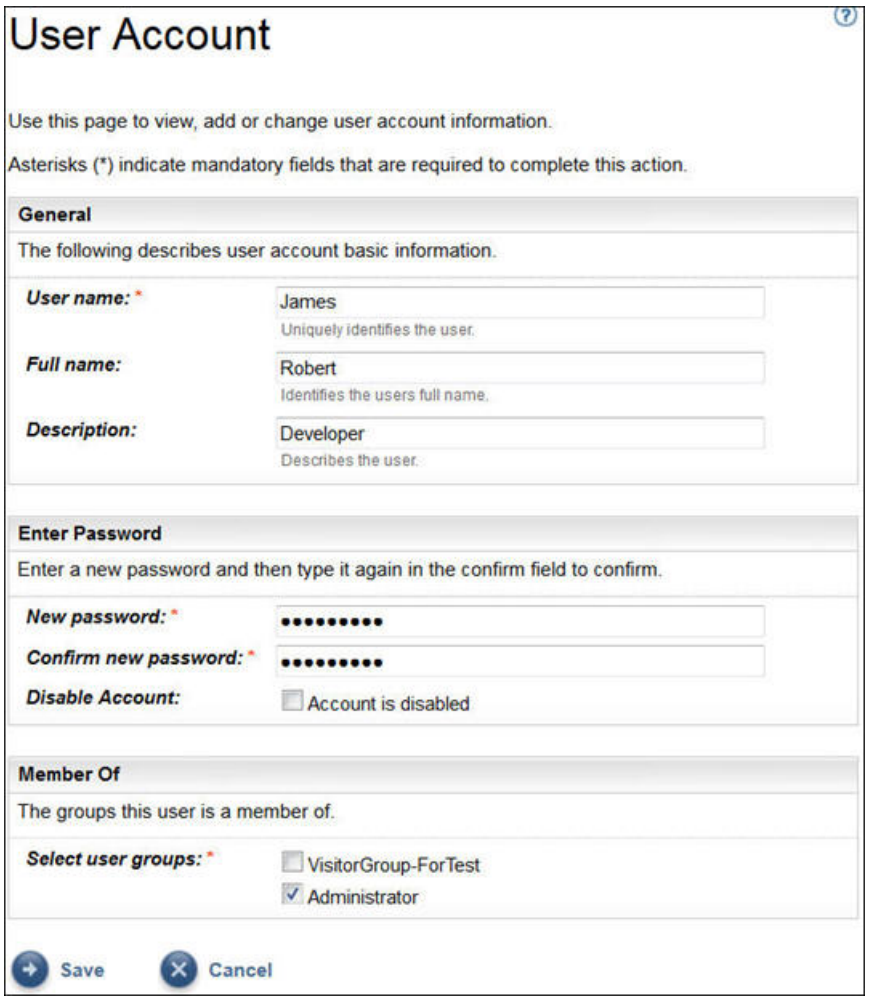

Figure 109. Ajouter un compte d'utilisateur

3. Dans le champ **Nom d'utilisateur**, entrez un nom pour ce compte d'utilisateur.
4. Facultatif : Dans le champ **Nom complet**, entrez un nom complet pour l'utilisateur de ce compte.
5. Facultatif : Dans le champ **Description**, entrez une description pour ce compte d'utilisateur.
6. Dans le champ **Nouveau mot de passe**, entrez un mot de passe pour ce compte d'utilisateur.

   Le mot de passe doit respecter les règles suivantes :

   - 8 caractères minimum
   - Au moins un caractère alphabétique et un caractère non alphabétique
   - Ne doit pas contenir le nom de l'utilisateur
   - Doit être différent des huit mots de passe précédents
   - Doit être changé au moins une fois tous les 30 jours (par défaut) ou comme indiqué dans la section «Modifier l'âge du mot de passe», à la page 104, mais pas plus d'une fois par jour.
7. Dans le champ **Confirmer le mot de passe**, entrez à nouveau le mot de passe de ce compte d'utilisateur.

   Les deux mots de passe saisis sont comparés afin de vérifier qu'ils correspondent avant que le mot de passe soit enregistré.

   Remarque : Le mot de passe doit être changé lors de la première connexion à ce compte d'utilisateur.
8. Si vous voulez désactiver ce compte d'utilisateur, cochez la case **Le compte est désactivé**.

   Désactiver le compte vous permet d'empêcher l'utilisation de ce compte sans avoir à le supprimer.

   Remarque : Vous ne pouvez ni désactiver le compte **admin**, ni le changer de groupe.

9. Sélectionnez les groupes d'utilisateurs associés à ce compte d'utilisateur. Au moins un groupe d'utilisateurs doit être sélectionné. L'utilisateur disposera du niveau d'autorisation défini pour les groupes sélectionnés.
10. Cliquez sur **Enregistrer** pour enregistrer le compte d'utilisateur.

    La page **Comptes et groupes d'utilisateurs** s'affiche avec le nouveau compte d'utilisateur dans la liste.

Modifier des comptes d'utilisateur et des groupes d'utilisateurs

Vous pouvez modifier des comptes d'utilisateur et des groupes d'utilisateurs existants.

Modifier des comptes d'utilisateur

Vous pouvez modifier des comptes d'utilisateur existants.

Pourquoi et quand exécuter cette tâche

Pour modifier un compte d'utilisateur, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.

   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Cliquez sur l'onglet **Comptes** puis cliquez sur l'icône **Modifier** en regard du compte d'utilisateur concerné.

   La page **Compte d'utilisateur** s'affiche.
3. Dans le panneau **Généralités**, vous pouvez modifier les informations de base de ce compte d'utilisateur.
4. Dans le panneau **Entrer le mot de passe**, vous pouvez modifier le mot de passe et les informations d'administration du mot de passe. Vous pouvez aussi désactiver ce compte d'utilisateur.

   Le mot de passe doit respecter les règles suivantes :

   - 8 caractères minimum
   - Au moins un caractère alphabétique et un caractère non alphabétique
   - Ne doit pas contenir le nom de l'utilisateur
   - Doit être différent des huit mots de passe précédents
   - Doit être modifié au moins une fois tous les 90 jours, mais pas plus d'une fois par jour.

   Remarque : Le mot de passe doit être changé lors de la première connexion à ce compte d'utilisateur.
5. Si vous voulez désactiver ce compte d'utilisateur, cochez la case **Le compte est désactivé**.

   Désactiver le compte vous permet d'empêcher l'utilisation de ce compte sans avoir à le supprimer. Pour plus d'informations sur la suppression d'un compte d'utilisateur, voir la section «Supprimer des comptes d'utilisateur et des groupes d'utilisateurs», à la page 144.

   Remarque : Vous ne pouvez ni désactiver le compte **admin**, ni le changer de groupe.

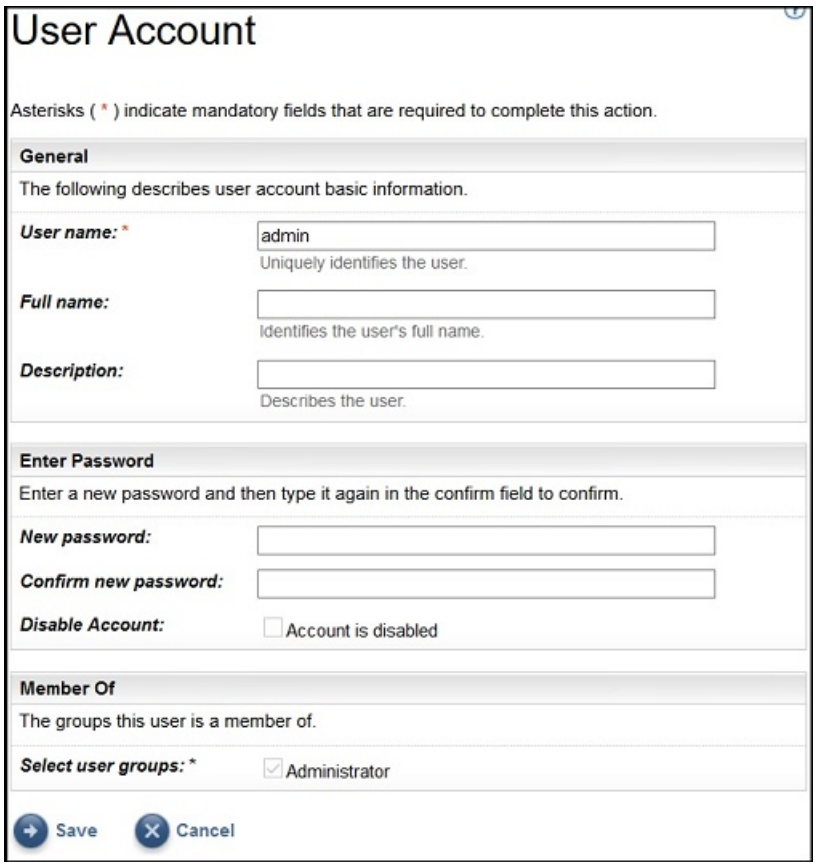

Figure 110. Modifier un compte d'utilisateur admin

6. Dans le panneau **Membre de**, vous pouvez modifier les groupes d'utilisateurs auxquels appartient ce compte d'utilisateur. Le compte d'utilisateur doit être membre d'au moins un groupe d'utilisateurs.
7. Cliquez sur **Enregistrer** pour enregistrer vos modifications.
   Les informations modifiées s'affichent sur la page **Comptes et groupes d'utilisateurs**.

Modifier des groupes d'utilisateurs

Vous pouvez modifier les groupes d'utilisateurs existants.

Avant de commencer

Remarque : Vous ne pouvez pas changer le groupe **Administrateur**.

Pourquoi et quand exécuter cette tâche

Pour modifier un groupe d'utilisateurs, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.
   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Cliquez sur l'onglet **Groupes** puis cliquez sur l'icône **Modifier** en regard du groupe d'utilisateurs concerné.
   La page **Groupe d'utilisateurs** s'affiche.
3. Dans le panneau **Généralités**, vous pouvez modifier les informations de base de ce groupe d'utilisateurs.
4. Dans le panneau **Niveau d'autorisation des membres**, vous pouvez préciser si ce groupe d'utilisateurs a un niveau d'autorisation *Administrateur*, *Reconnaissance* ou *Lecture seule*.

5. Si vous avez spécifié le niveau d'autorisation *Reconnaissance* dans le panneau **Niveau d'autorisation des membres**, vous pouvez changer les ensembles de périmètres que ce groupe d'utilisateur sera autorisé à découvrir dans le panneau **Limiter aux ensembles de périmètres sélectionnés**.
6. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

   Les informations modifiées s'affichent sur la page **Comptes et groupes d'utilisateurs**.

Supprimer des comptes d'utilisateur et des groupes d'utilisateurs

Vous pouvez supprimer des comptes d'utilisateur et des groupes d'utilisateurs existants.

Supprimer des comptes d'utilisateur

Vous pouvez supprimer des comptes d'utilisateur existants.

Pourquoi et quand exécuter cette tâche

Remarque : Le compte d'utilisateur **admin** ne peut pas être supprimé.

Pour supprimer un compte d'utilisateur, procédez comme suit :

Procédure

1. Dans le panneau de navigation, cliquez sur **Administration** > **Comptes d'utilisateur**.

   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Cliquez sur l'onglet **Comptes** puis sur l'icône Supprimer à côté du compte d'utilisateur à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression du compte d'utilisateur.

Supprimer des groupes d'utilisateurs

Vous pouvez supprimer des groupes d'utilisateurs existants.

Pourquoi et quand exécuter cette tâche

Remarque : Le groupe d'utilisateurs **Administrateur** ne peut pas être supprimé.

Pour supprimer un groupe d'utilisateurs, procédez comme suit :

Procédure

1. Cliquez sur **Administration** > **Comptes d'utilisateur**.

   La page **Comptes et groupes d'utilisateurs** s'affiche.
2. Cliquez sur l'onglet **Groupes** puis cliquez sur l'icône Supprimer en regard du groupe d'utilisateurs à supprimer.
3. Cliquez sur **OK** pour confirmer la suppression du groupe d'utilisateurs.

   Remarque : Un groupe d'utilisateurs ne peut être supprimé que si plus aucun utilisateur n'y est affecté.

Accessibilité

Technical Support Appliance n'interfère pas avec les fonctions d'accessibilité des navigateurs pris en charge. Pour obtenir la liste complète des fonctions d'accessibilité, visitez la page Accessibilité du navigateur pris en charge que vous utilisez. Pour connaître la liste des navigateurs pris en charge, voir la section «Navigateurs web requis», à la page 5.

Les publications relatives à ce produit sont éditées au format PDF Adobe et doivent être conformes aux normes d'accessibilité. Si vous rencontrez des difficultés lors de l'utilisation des fichiers PDF et que vous voulez demander un format Web pour une publication, envoyez votre demande par e-mail à l'adresse suivante :

icfeedbk@us.ibm.com

ou par voie postale à l'adresse suivante :

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

Dans votre demande, veillez à bien indiquer le titre de la publication - "Guide de l'installation de TSA (Technical Support Appliance) " en objet.

Lorsque vous envoyez des informations à IBM, vous accordez à IBM un droit non exclusif d'utiliser ou de diffuser ces informations de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part.

Mentions légales

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service NONE. puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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 Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBMpeut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Marques

IBM, le logo IBM et ibm.com sont des marques ou des marques déposées d'International Business Machines Corp., enregistrées auprès de nombreuses juridictions dans le monde. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques déposées IBM est disponible sur Internet dans la section "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Hyper-V et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

VMware, le logo VMware, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server et VMware vSphere sont des marques de VMware, Inc. ou de ses filiales aux États-Unis et/ou dans d'autres juridictions.

Référence :

(1P) P/N: