Administration de Platform Services Controller

ESXi 6.5
vCenter Server 6.5

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-002010-00

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos de l'administration de Platform Services Controller

La documentation *Administration de Platform Services Controller* explique comment VMware® Platform Services Controller™ s'adapte à votre environnement vSphere et vous aide à effectuer les tâches courantes telles que la gestion des certificats et la configuration de vCenter Single Sign-On.

Documentation connexe

Un document complémentaire, *Sécurité vSphere*, explique comment vous pouvez définir des autorisations, décrit les fonctions de sécurité disponibles et les mesures que vous pouvez prendre pour protéger votre environnement contre les attaques, et fait référence aux privilèges.

Outre ces documents, VMware publie un *Guide de sécurisation renforcée* pour chaque version de vSphere. Ces guides sont disponibles à la page http://www.vmware.com/security/hardening-guides.html. Le *Guide de sécurisation renforcée* est une feuille de calcul comprenant des entrées pour différents problèmes potentiels de sécurité. Il offre des éléments pour trois profils de risque.

Public cible

Ces informations sont destinées aux administrateurs qui souhaitent configurer Platform Services Controller et les services associés. Elles sont destinées aux administrateurs Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

vSphere Web Client et vSphere Client (client HTML 5)

Les instructions relatives aux tâches présentées dans ce guide se basent sur vSphere Web Client. Vous pouvez également exécuter la plupart des tâches de ce guide en utilisant la nouvelle version de vSphere Client. La terminologie, la topologie et le workflow de la nouvelle interface utilisateur de vSphere Client correspondent fidèlement aux aspects et éléments de l'interface utilisateur de vSphere Web Client. Vous pouvez appliquer les instructions de vSphere Web Client à la nouvelle version de vSphere Client sauf mention du contraire.

Remarque Les fonctionnalités de vSphere Web Client n'ont pas toutes été mises en œuvre pour vSphere Client dans la version vSphere 6.5. Pour obtenir une liste actualisée des fonctionnalités non prises en charge, consultez le *Guide des mises à jour des fonctionnalités de vSphere Client* sur http://www.vmware.com/info?id=1413.

Démarrage avec Platform Services Controller 1

Platform Services Controller fournit des services d'infrastructure communs à l'environnement vSphere. Ces services incluent la gestion des licences, la gestion des certificats et l'authentification avec vCenter Single Sign-On.

Ce chapitre aborde les rubriques suivantes :

Types de déploiement de vCenter Server et de Platform Services Controller

Vous pouvez déployer le dispositif vCenter Server Appliance ou installer vCenter Server pour Windows avec une instance intégrée ou externe de Platform Services Controller. Vous pouvez également déployer une instance de Platform Services Controller comme un dispositif ou l'installer sous Windows. Si nécessaire, vous pouvez utiliser un environnement à systèmes d'exploitation mixtes.

Avant de déployer vCenter Server Appliance ou d'installer vCenter Server pour Windows, vous devez déterminer le modèle de déploiement convenant à votre environnement. Pour chaque déploiement ou installation, vous devez sélectionner l'un des trois types de déploiement.

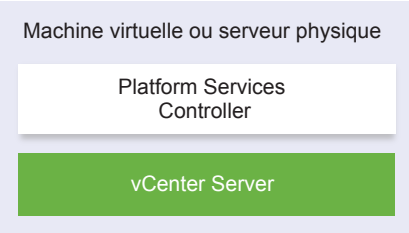
Tableau 1-1. Types de déploiement de vCenter Server et de Platform Services Controller

Type de déploiement	Description
vCenter Server avec une instance intégrée de Platform Services Controller	Tous les services qui sont fournis avec l'instance de Platform Services Controller sont déployés ensemble avec les services vCenter Server sur la même machine virtuelle ou le même serveur physique.
Platform Services Controller	Seuls les services qui sont fournis avec l'instance de Platform Services Controller sont déployés sur la machine virtuelle ou le serveur physique.
vCenter Server avec une instance externe de Platform Services Controller (Nécessite une instance externe de Platform Services Controller)	Seuls les services vCenter Server sont déployés sur la machine virtuelle ou le serveur physique. Vous devez enregistrer une telle instance de vCenter Server dans une instance de Platform Services Controller que vous avez précédemment déployée ou installée.

vCenter Server avec une instance intégrée de Platform Services Controller

C'est un type de déploiement autonome qui dispose de son propre domaine vCenter Single Sign-On avec un site unique. vCenter Server avec une instance intégrée de Platform Services Controller convient à de petits environnements. Vous ne pouvez pas joindre d'autres instances de vCenter Server ou de Platform Services Controller à ce domaine vCenter Single Sign-On.

Figure 1-1. vCenter Server avec une instance intégrée de Platform Services Controller



L'installation de vCenter Server avec un Platform Services Controller intégré offre les avantages suivants :

- La connexion entre vCenter Server et l'instance de Platform Services Controller n'est pas établie sur le réseau, et vCenter Server n'est pas sujet aux interruptions de service liées aux problèmes de connectivité et de résolution de noms entre vCenter Server et l'instance de Platform Services Controller.
- Si vous installez vCenter Server sur des machines virtuelles ou des serveurs physiques Windows, vous avez besoin d'un moins grand nombre de licences Windows.
- Vous gérer moins de machines virtuelles ou de serveurs physiques.

L'installation d'une instance de vCenter Server avec une instance intégrée de Platform Services Controller présente les inconvénients suivants :

- Il y a une instance de Platform Services Controller pour chaque produit, ce qui peut aller au-delà des besoins et accroître la consommation de ressources.
- Le modèle convient aux petits environnements.

Vous pouvez configurer le dispositif vCenter Server Appliance avec une instance intégrée de Platform Services Controller dans une configuration vCenter High Availability. Pour plus d'informations, consultez *Disponibilité vSphere*.

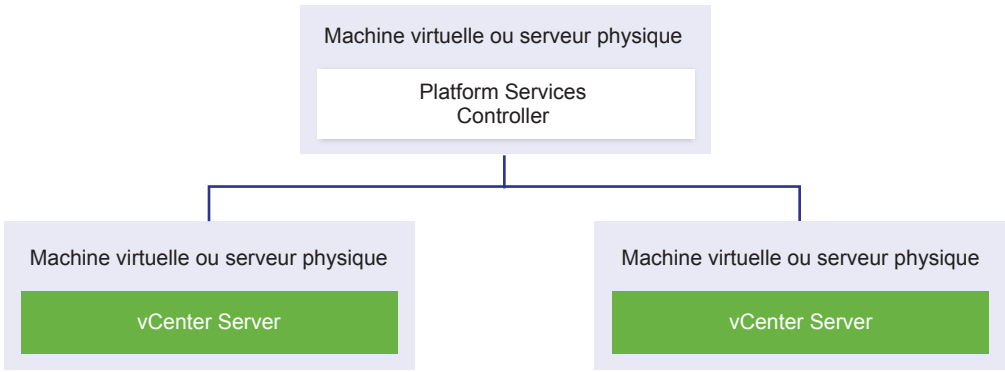
Remarque Après le déploiement ou l'installation de vCenter Server avec une instance intégrée de Platform Services Controller, vous pouvez reconfigurer le type de déploiement et passer à vCenter Server avec une instance externe de Platform Services Controller.

Platform Services Controller et vCenter Server avec une instance externe de Platform Services Controller

Lorsque vous déployez ou installez une instance de Platform Services Controller, vous pouvez créer un domaine vCenter Single Sign-On ou joindre un domaine vCenter Single Sign-On existant. Les instances jointes de Platform Services Controller répliquent leurs données d'infrastructure (par exemple, les informations d'authentification et de licences) et peuvent s'étendre sur plusieurs sites vCenter Single Sign-On. Pour plus d'informations, consultez « Description des domaines vSphere, des noms de domaine et des sites », page 14.

Vous pouvez enregistrer plusieurs instances de vCenter Server dans une instance externe commune de Platform Services Controller. Les instances de vCenter Server utilisent par défaut le site vCenter Single Sign-On de l'instance de Platform Services Controller dans laquelle elles sont enregistrées. Toutes les instances de vCenter Server qui sont enregistrées dans une instance commune ou différentes instances jointes de Platform Services Controller sont connectées en mode Enhanced Linked Mode.

Figure 1-2. Exemple de deux instances de vCenter Server avec une instance externe commune de Platform Services Controller



L'installation de vCenter Server avec un Platform Services Controller externe présente les avantages suivants :

- Moins de ressources consommées par les services partagés dans les instances de Platform Services Controller.
- Le modèle convient aux grands environnements.

L'installation de vCenter Server avec un Platform Services Controller externe présente les inconvénients suivants :

- La connexion entre vCenter Server et Platform Services Controller peut présenter des problèmes de connectivité et de résolution de nom.
- Si vous installez vCenter Server sur des machines virtuelles ou des serveurs physiques Windows, vous avez besoin d'un plus grand nombre de licences Microsoft Windows.
- Vous devez gérer un plus grand nombre de machines virtuelles ou de serveurs physiques.

Pour obtenir des informations sur les valeurs maximales de Platform Services Controller et de vCenter Server, reportez-vous à la documentation *Configurations maximales*.

Pour obtenir des informations sur la configuration du dispositif vCenter Server Appliance avec une instance externe de Platform Services Controller dans une configuration vCenter High Availability, reportez-vous à *Disponibilité vSphere*.

Environnement de systèmes d'exploitation mixtes

Une instance de vCenter Server installée sur Windows peut être enregistrée dans unPlatform Services Controller installé sur Windows ou un dispositif Platform Services Controller. vCenter Server Appliance peut être enregistré dans une instance de Platform Services Controller installée sous Windows ou dans un dispositif Platform Services Controller. vCenter Server et le dispositif vCenter Server Appliance peuvent tous deux être enregistrés dans la même instance de Platform Services Controller.

Figure 1-3. Exemple d'environnement de systèmes d'exploitation mixtes avec une instance externe de Platform Services Controller sous Windows

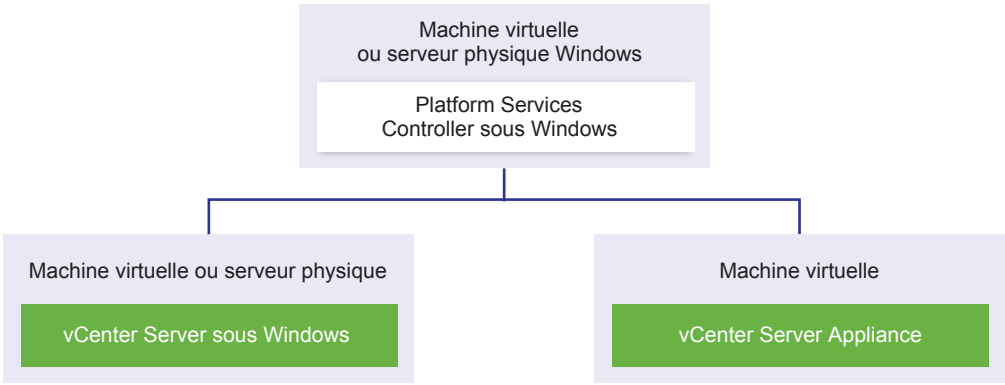
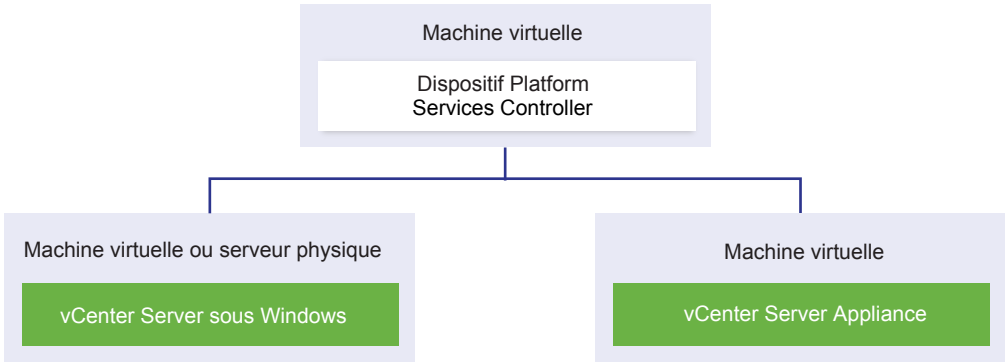


Figure 1-4. Exemple d'environnement de systèmes d'exploitation mixtes avec un dispositif Platform Services Controller externe



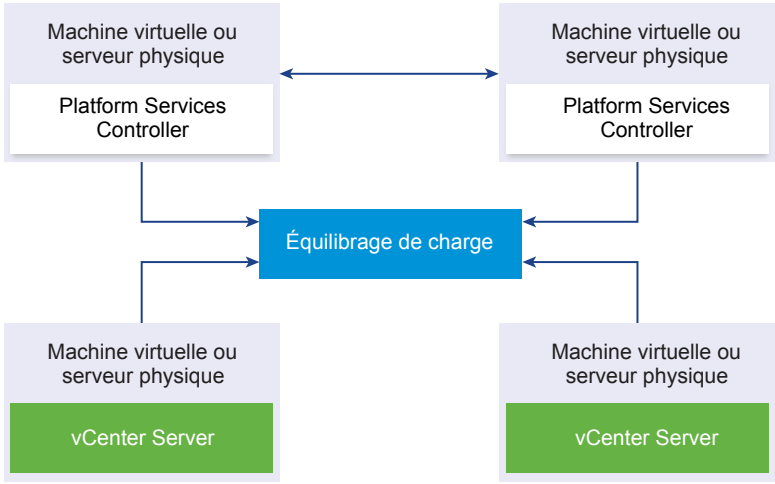
Remarque Pour simplifier l'administration et la maintenance, utilisez uniquement des dispositifs ou uniquement des installations Windows de vCenter Server et de Platform Services Controller.

Topologies de déploiement avec des instances externes de Platform Services Controller et haute disponibilité

Pour garantir la haute disponibilité de Platform Services Controller dans des déploiements externes, vous devez installer ou déployer au moins deux instances jointes de Platform Services Controller dans votre domaine vCenter Single Sign-On. Lorsque vous utilisez un équilibrage de charge de tiers, vous pouvez garantir un basculement automatique sans interruption de service.

Platform Services Controller avec un équilibrage de charge

Figure 1-5. Exemple d'une paire d'instances de Platform Services Controller à charge équilibrée



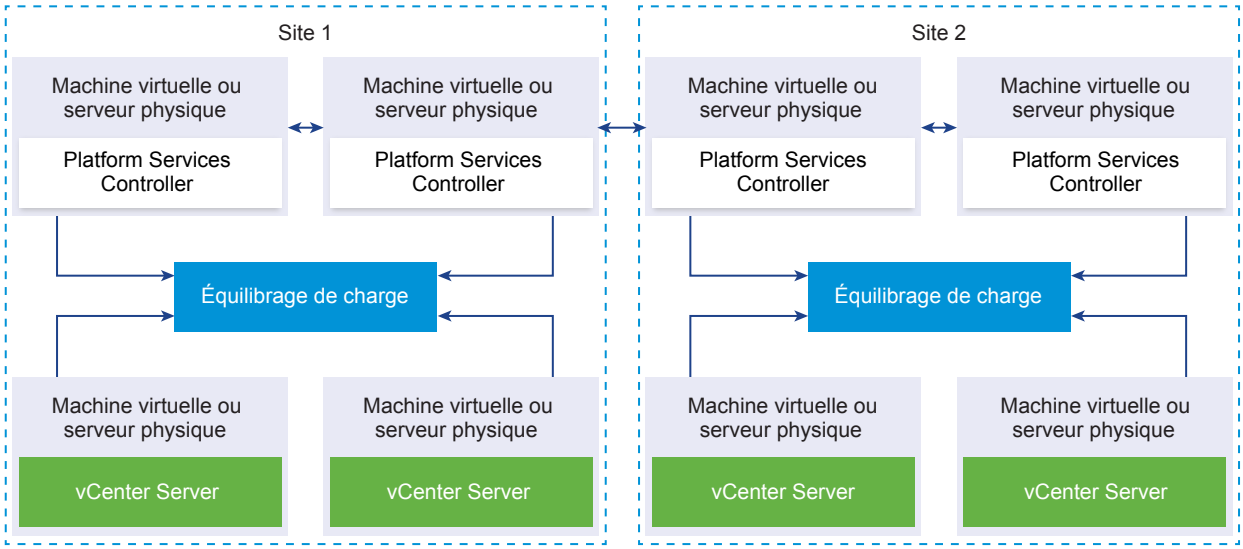
Vous pouvez utiliser un équilibrage de charge de tiers par site pour configurer la haute disponibilité de Platform Services Controller avec basculement automatique pour ce site. Pour plus d'informations sur le nombre maximal d'instances de Platform Services Controller derrière un équilibrage de charge, reportez-vous à la documentation *Configurations maximales*.

Important Pour configurer la haute disponibilité de Platform Services Controller derrière un équilibrage de charge, les instances de Platform Services Controller doivent correspondre au même type de système d'exploitation. Les instances de Platform Services Controller à systèmes d'exploitation mixtes derrière un équilibrage de charge ne sont pas prises en charge.

Les instances de vCenter Server sont connectées à l'équilibrage de charge. Lorsqu'une instance de Platform Services Controller cesse de répondre, l'équilibrage de charge distribue automatiquement la charge entre les autres instances opérationnelles de Platform Services Controller sans interruption de service.

Platform Services Controller avec équilibrages de charge entre sites vCenter Single Sign-On

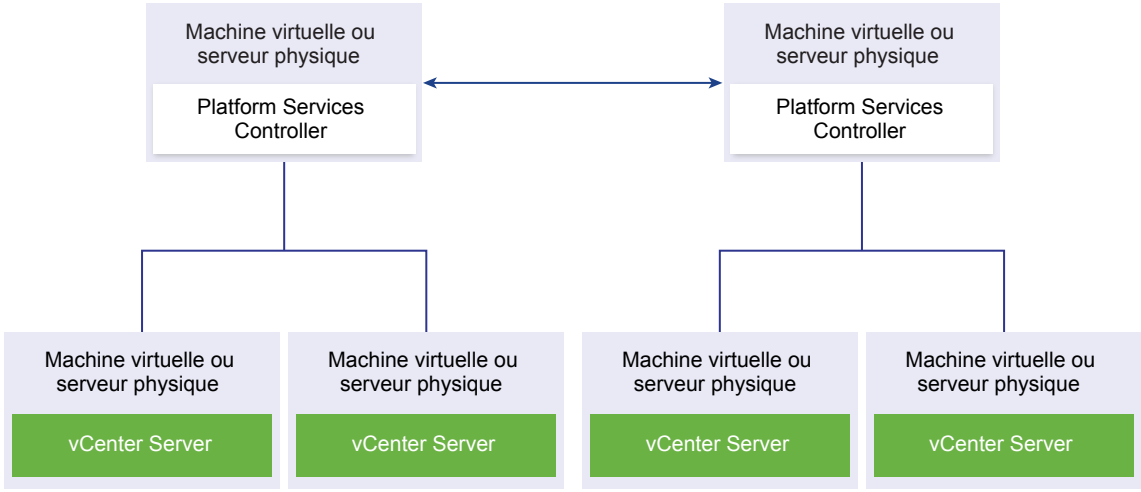
Figure 1-6. Exemple de deux paires d'instances de Platform Services Controller à charge équilibrée entre deux sites



Votre domaine vCenter Single Sign-on peut s'étendre sur plusieurs sites. Pour garantir la haute disponibilité de Platform Services Controller avec basculement automatique à l'échelle du domaine, vous devez configurer un équilibrage de charge distinct dans chaque site.

Platform Services Controller sans équilibrage de charge

Figure 1-7. Exemple de deux instances jointes de Platform Services Controller sans équilibrage de charge



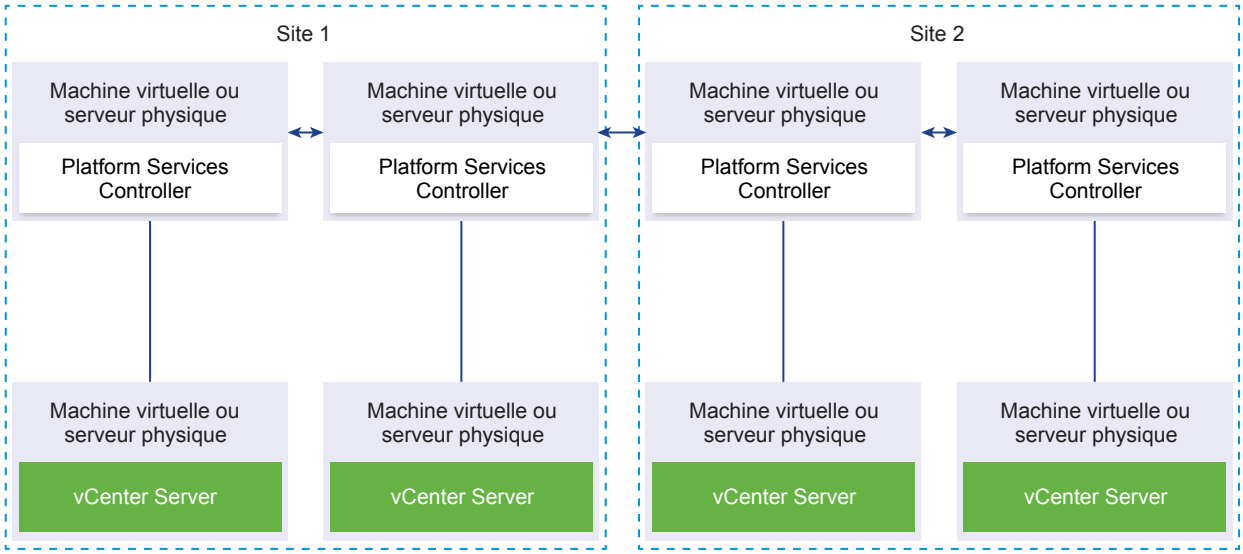
Lorsque vous joignez deux instances de Platform Services Controller ou plus dans le même site sans équilibrage de charge, vous configurez la haute disponibilité de Platform Services Controller avec un basculement manuel pour ce site.

Lorsqu'une instance de Platform Services Controller cesse de répondre, vous devez basculer manuellement sur les instances de vCenter Server qui sont enregistrées à cet effet en les repointant vers d'autres instances opérationnelles de Platform Services Controller dans le même site. Pour plus d'informations sur le repointage d'instances de vCenter Server vers d'autres instances externes de Platform Services Controller, reportez-vous à *Installation et configuration de vSphere*.

Remarque Si votre domaine vCenter Single Sign-On inclut trois instances de Platform Services Controller ou plus, pour mesurer la fiabilité de Platform Services Controller lorsqu'une des instances échoue, vous pouvez créer une topologie en anneau manuellement. Pour créer une topologie en anneau, utilisez la commande `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` sur la première et la dernière instance de Platform Services Controller que vous avez déployées.

Platform Services Controller sans équilibrage de charge entre des sites vCenter Single Sign-On

Figure 1-8. Exemple de deux paires jointes d'instances de Platform Services Controller entre deux sites sans équilibrage de charge



Votre domaine vCenter Single Sign-on peut s'étendre sur plusieurs sites. Lorsqu'aucun équilibrage de charge n'est disponible, vous pouvez manuellement repointer vCenter Server d'une instance en panne de Platform Services Controller vers une instance opérationnelle dans le même site. Pour plus d'informations sur le repointage d'instances de vCenter Server vers d'autres instances externes de Platform Services Controller, reportez-vous à *Installation et configuration de vSphere*.

Important Le repointage de vCenter Server entre des sites et des domaines n'est pas pris en charge. Si aucune instance opérationnelle de Platform Services Controller n'est disponible dans le site, vous devez déployer ou installer une nouvelle instance de Platform Services Controller dans ce site en tant que partenaire de réplication d'une instance opérationnelle de Platform Services Controller d'un autre site.

Description des domaines vSphere, des noms de domaine et des sites

Chaque Platform Services Controller est associé à un domaine vCenter Single Sign-On. Le nom de domaine par défaut est vsphere.local. Vous pouvez le modifier lors de l'installation du premier Platform Services Controller. Le domaine détermine l'espace d'authentification local. Vous pouvez diviser un domaine en plusieurs sites et attribuer chaque Platform Services Controller et chaque vCenter Server à un site. Les sites sont des constructions logiques, mais correspondent généralement à un lieu géographique.

Domaine Platform Services Controller

Lorsque vous installez un Platform Services Controller, vous êtes invité à créer un domaine vCenter Single Sign-On ou à rejoindre un domaine existant.

Le nom de domaine est utilisé par le VMware Directory Service (vmdir) pour toute la structure interne du protocole LDAP (Lightweight Directory Access Protocol).

Avec vSphere 6.0 et ultérieur, vous pouvez donner à votre domaine vSphere un nom unique. Pour empêcher les conflits d'authentification, choisissez un nom qui n'est pas utilisé par OpenLDAP, Microsoft Active Directory et d'autres services de répertoire.

Remarque Il n'est pas possible de modifier le domaine auquel appartient une instance Platform Services Controller ou vCenter Server.

Si vous réalisez une mise à niveau depuis vSphere 5.5, votre nom de domaine vSphere reste celui par défaut (vsphere.local). Vous ne pouvez changer le nom d'un domaine, dans aucune version de vSphere.

Après avoir spécifié le nom de votre domaine, vous pouvez ajouter des utilisateurs et des groupes. Généralement, il est plus logique d'ajouter une source d'identité Active Directory ou LDAP et de permettre aux utilisateurs et aux groupes de cette source de s'authentifier. Vous avez également la possibilité d'ajouter des instances vCenter Server ou Platform Services Controller, ou d'autres produits VMware, tels que vRealize Operations, au domaine.

Sites Platform Services Controller

Vous pouvez organiser les domaines Platform Services Controller en sites logiques. Un site du VMware Directory Service est un conteneur logique pour grouper des instances Platform Services Controller au sein d'un domaine vCenter Single Sign-On.

Vous êtes invité à indiquer le nom du site lors de l'installation ou de la mise à niveau d'un Platform Services Controller. Consultez la documentation de *Installation et configuration de vSphere*.

Capacités du Platform Services Controller

Platform Services Controller prend en charge des services tels que la gestion des identités, la gestion des certificats et la gestion des licences dans vSphere.

Capacités clés

Platform Services Controller inclut plusieurs services, présentés dans « Services Platform Services Controller », page 15, et possède les capacités clés suivantes :

- Authentification via vCenter Single Sign-On
- Provisionnement des composants vCenter Server et des hôtes ESXi avec les certificats VMware Certificate Manager (VMCA) par défaut
- Utilisation de certificats personnalisés stockés dans VMware Endpoint Certificate Store (VECS)

Modèles de déploiement

Vous pouvez installer Platform Services Controller sur un système Windows ou déployer le dispositif de Platform Services Controller.

Le modèle de déploiement dépend de la version de Platform Services Controller que vous utilisez. Reportez-vous à « Types de déploiement de vCenter Server et de Platform Services Controller », page 7.

Gestion des services Platform Services Controller

Gérez les services Platform Services Controller dans l'interface Web de Platform Services Controller, de vSphere Web Clientou en utilisant un script et une interface de ligne de commande disponibles.

Différents services Platform Services Controller prennent en charge différentes interfaces.

Tableau 1-2. Interfaces pour la gestion des services Platform Services Controller

Interface	Description
Interface Web de Platform Services Controller	Interface Web pour la gestion de tous les services, y compris vCenter Single Sign-On et Common Access Card. Connectez-vous à https://*psc_hostname_or_IP*/psc.
vSphere Web Client	Interface Web pour la gestion de certains services. Certains services, tels que l'authentification par carte à puce, sont configurables uniquement dans l'interface Web de Platform Services Controller.
Utilitaire de gestion de certificats	Outil de ligne de commande prenant en charge la génération d'une demande de signature de certificat et le remplacement des certificats. Reportez-vous à « Gestion de certificats avec l'utilitaire vSphere Certificate Manager », page 92.
Interfaces de ligne de commande pour la gestion des services Platform Services Controller	Ensemble de commandes pour la gestion des certificats, le magasin de certificats VMware Endpoint (VECS) et VMware Directory Service (vmdir). Reportez-vous à Chapitre 4, « Gestion des services et des certificats avec des interfaces de lignes de commande », page 133.

Services Platform Services Controller

Avec Platform Services Controller, tous les produits VMware d'un même environnement peuvent partager le domaine d'authentification ainsi que d'autres services. Ces services incluent la gestion des certificats, l'authentification et l'octroi de licences.

Platform Services Controller inclut les principaux services d'infrastructure suivants.

Tableau 1-3. Services Platform Services Controller

Service	Description
`applmgmt` (VMware Appliance Management Service)	Gère la configuration du dispositif et fournit des points de terminaison API publics pour la gestion du cycle de vie du dispositif. Inclus sur le dispositif de Platform Services Controller.
`vmware-cis-license` (VMware License Service)	Chaque instance de Platform Services Controllerinclut VMware License Service, qui offre une gestion des licences centralisée et une fonctionnalité de production de rapports pour les produits VMware de votre environnement. L'inventaire du service de licence procède à une réplication sur toutes les instances de Platform Services Controller du domaine, à des intervalles de 30 secondes.

Tableau 1-3. Services Platform Services Controller (suite)

Service	Description
`vmware-cm` (VMware Component Manager)	Component manager offre des fonctionnalités d'enregistrement et de recherche de services.
`vmware-psc-client` (VMware Platform Services Controller Client)	Serveur principal de l'interface Web Platform Services Controller.

`vmware-sts-idmd`
(VMware Identity Management Service)
`vmware-stsd`
(VMware Security Token Service)
	Services sous-jacents à la fonctionnalité vCenter Single Sign-On, qui fournit des services d'authentification sécurisés aux composants logiciels et aux utilisateurs VMware.
	En utilisant vCenter Single Sign-On, les composants VMware communiquent à l'aide d'un mécanisme d'échange de jeton SAML sécurisé. vCenter Single Sign-On construit un domaine de sécurité interne (par défaut, vsphere.local) dans lequel les composants logiciels VMware sont enregistrés lors de l'installation ou de la mise à niveau.

`vmware-rhttpproxy` (VMware HTTP Reverse Proxy)	Le proxy inverse est exécuté sur chaque nœud Platform Services Controller et chaque système vCenter Server. Il constitue un point d'entrée unique dans le nœud et permet aux services exécutés sur ce nœud de communiquer en toute sécurité.
`vmware-sca` (VMware Service Control Agent)	Gère les configurations de service. Vous pouvez utiliser l'interface de ligne de commande `service-control` pour gérer chaque configuration de service.
`vmware-statsmonitor` (VMware Appliance Monitoring Service)	Surveille la consommation de ressources du système d'exploitation invité vCenter Server Appliance.
`vmware-vapi-endpoint` (VMware vAPI Endpoint)	Le point de terminaison de l'API de l'automatisation de vSphere fournit un point d'accès unique aux services vAAPI. Vous pouvez modifier les propriétés du service vAAPI Endpoint à partir de l'instance de vSphere Web Client. Pour plus de détails sur les points de terminaison vAAPI, reportez-vous au *Guide de programmation VMware vCloud Suite SDK*.
`vmafdd` VMware Authentication Framework	Service qui offre un cadre côté client pour l'authentification vmdir et qui sert le VMware Endpoint Certificate Store (VECS).
`vmcad` VMware Certificate Service	Approvisionne chaque composant logiciel VMware qui possède les bibliothèques client vmafd et chaque hôte ESXi d'un certificat signé disposant de l'autorité de certification racine VMCA. Vous pouvez changer les certificats par défaut à l'aide de l'utilitaire Certificate Manager ou de l'interface WebPlatform Services Controller. VMware Certificate Service utilise VMware Endpoint Certificate Store (VECS) comme référentiel local sur chaque instance de Platform Services Controller. Bien que vous puissiez décider de ne pas utiliser VMCA mais plutôt des certificats personnalisés, vous devez ajouter les certificats à VECS.
`vmdird` VMware Directory Service	Fournit un service de répertoire LDAP à locataires et à maîtres multiples qui stocke les informations relatives à l'authentification, au certificat, à la recherche et à la licence. Ne mettez pas à jour les données de `vmdird` à l'aide d'un navigateur LDAP. Si votre domaine contient plusieurs instances de Platform Services Controller, une mise à jour du contenu vmdir d'une seule instance de vmdir est propagée vers toutes les autres instances de vmdir.

Tableau 1-3. Services Platform Services Controller (suite)

Service	Description
`vmdnsd` VMware Domain Name Service	Non utilisé dans vSphere version 6.

`vmonapi`
VMware Lifecycle Manager API
`vmware-vmon`
VMware Service Lifecycle Manager
	Démarre et arrête les services vCenter Server et surveille l'état de santé du service API. Le service `vmware-vmon` est un service centralisé indépendant des plates-formes. Il gère le cycle de vie de Platform Services Controller et de vCenter Server. Affiche les API et les interfaces de ligne de commande pour les applications tierces.

`lwsmd` Likewise Service Manager	Facilite la liaison de l'hôte à un domaine Active Directory ainsi que l'authentification utilisateur subséquente.

Accéder à l'interface Web de Platform Services Controller

Vous pouvez utiliser l'interface Web de Platform Services Controller pour configurer vCenter Single Sign-On, gérer les certificats et configurer l'authentification à deux facteurs.

Remarque Cette interface inclut des options de configuration, notamment Configuration de la bannière de connexion et Configuration de l'authentification par carte à puce qui ne sont pas disponibles dans vSphere Web Client.

Procédure

1 Dans votre navigateur Web, connectez-vous à l'adresse https://*psc_ip_or_hostname*/psc.

Dans les environnements qui utilisent Platform Services Controller, utilisez https://*vc_ip_or_hostname*/psc

2 Connectez-vous en tant qu'utilisateur administrateur dans le domaine vCenter Single Sign-On (vsphere.local par défaut).

Gérer les services Platform Services Controller à partir de vSphere Web Client

Vous pouvez gérer vCenter Single Sign-On et le service d'attribution de licence à partir de vSphere Web Client.

Utilisez l'interface Web ou les interfaces de ligne de commande de Platform Services Controller plutôt que vSphere Web Client pour gérer les services suivants.

- Certificats
- VECS (VMware Endpoint Certificate Store)
- Authentification à deux facteurs, notamment par carte d'accès commun (CAC)
- Page de connexion

Procédure

1 Connectez-vous à une instance de vCenter Server associée à l'instance de Platform Services Controller en tant qu'utilisateur disposant de privilèges d'administrateur dans le domaine vCenter Single Sign-On local (vsphere.local par défaut).

2 Sélectionnez **Administration**, puis cliquez sur l'élément à gérer.

Option	Description
Single Sign-On	Configurer vCenter Single Sign-On. ■ Définir des stratégies. ■ Gérer les sources d'identité. ■ Gérer le certificat à signature STS. ■ Gérer les fournisseurs de services SAML. ■ Gérer les utilisateurs et les groupes.
Attribution de licences	Configurer l'attribution de licence.

Utiliser des scripts pour gérer les services Platform Services Controller

Platform Services Controller inclut des scripts pour la génération de demandes de signature de certificat, la gestion des certificats et la gestion des services.

Par exemple, vous pouvez utiliser l'utilitaire `certool` pour générer des demandes de signature de certificat et remplacer des certificats, pour les scénarios avec instance intégrée de Platform Services Controller et les scénarios avec instance externe de Platform Services Controller. Reportez-vous à « Gestion de certificats avec l'utilitaire vSphere Certificate Manager », page 92.

Utilisez les interfaces de ligne de commande pour les tâches de gestion non prises en charge par les interfaces Web ou pour créer des scripts personnalisés pour votre environnement.

Tableau 1-4. Interfaces de ligne de commande pour la gestion de certificats et services associés

CLI	Description	Liens
`certool`	Génère et gère les certificats et les clés. Fait partie de VMCA.	« Référence des commandes d'initialisation de certool », page 136
`vecs-cli`	Gère les contenus des instances de VMware Certificate Store. Fait partie de VMAFD.	« Référence des commandes vecs-cli », page 141
`dir-cli`	Crée et met à jour les certificats dans le Vmware Directory Service. Fait partie de VMAFD.	« Référence des commandes dir-cli », page 147
`sso-config`	Utilitaire pour la configuration de l'authentification par carte à puce	« Authentification à deux facteurs de vCenter Server », page 38
`service-control`	Commande de démarrage, d'arrêt et d'énumération de services	Exécutez cette commande pour arrêter les services avant d'exécuter d'autres commandes d'interface de ligne de commande.

Procédure

1 Connectez-vous à l'interpréteur de commande Platform Services Controller.

Dans la plupart des cas, vous devez être l'utilisateur racine ou administrateur. Reportez-vous à « Privilèges requis pour l'exécution d'interfaces de lignes de commande », page 134 pour plus de détails.

2 Accédez à une interface de ligne de commande à l'un des emplacements par défaut suivants.

Les privilèges requis dépendent de la tâche à effectuer. Dans certains cas, vous êtes invité à entrer le mot de passe deux fois à des fins de protection des informations sensibles.

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
```

	`C:\Program Files\VMware\vCenter Server\vmcad\certool.exe`
	`C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config`
	`VCENTER_INSTALL_PATH``\bin\service-control`

Linux	`/usr/lib/vmware-vmafd/bin/vecs-cli`
	`/usr/lib/vmware-vmafd/bin/dir-cli`
	`/usr/lib/vmware-vmca/bin/certool`
	`/opt/vmware/bin`
	Sous Linux, la commande `service-control` ne requiert pas de spécifier le chemin.

Gestion du dispositif Platform Services Controller

Vous pouvez gérer le dispositif Platform Services Controller dans l'interface de gestion du dispositif virtuel ou de l'interpréteur de commande du dispositif.

Si vous utilisez un environnement avec une instance de Platform Services Controller intégrée, vous gérez le dispositif qui inclut Platform Services Controller et vCenter Server. Voir *Configuration de vCenter Server Appliance*.

Tableau 1-5. Interfaces pour la gestion du dispositif Platform Services Controller

Interface	Description
Interface VAMI de Platform Services Controller	Utilisez cette interface pour reconfigurer les paramètres système d'un déploiement Platform Services Controller.
Interpréteur de commande du dispositif Platform Services Controller	Utilisez cette interface de ligne de commande pour effectuer des opérations de gestion de service sur VMCA, VECS et VMDIR. Reportez-vous aux sections « Gestion de certificats avec l'utilitaire vSphere Certificate Manager », page 92 et Chapitre 4, « Gestion des services et des certificats avec des interfaces de lignes de commande », page 133.

Gérer le dispositif avec l'interface VAMI (Virtual Appliance Management Interface) de Platform Services Controller

Dans un environnement comportant une instance externe de Platform Services Controller, vous pouvez utiliser l'interface VAMI de Platform Services Controller pour configurer les paramètres système du dispositif. Ces paramètres incluent la synchronisation de l'heure, les paramètres réseau et les paramètres de connexion SSH. Vous pouvez également modifier le mot de passe racine, joindre le dispositif à un domaine Active Directory et quitter un domaine Active Directory.

Dans un environnement comportant une instance intégrée de Platform Services Controller, vous gérez les dispositifs qui incluent Platform Services Controller et vCenter Server.

Procédure

1 Dans un navigateur Web, accédez à l'interface Web de Platform Services Controller à l'adresse https://*platform_services_controller_ip*:5480.

2 Si un message d'avertissement sur un certificat SSL non approuvé s'affiche, résolvez le problème en fonction de la stratégie de sécurité de l'entreprise et du navigateur Web utilisé.

3 Connectez-vous en tant qu'utilisateur racine.

Le mot de passe racine par défaut est le mot de passe racine du dispositif virtuel que vous avez défini lors du déploiement de ce dernier.

Vous pouvez consulter la page Informations sur le système de l'interface VAMI de Platform Services Controller.

Gérer le dispositif dans l'interpréteur de commandes du dispositif

Vous pouvez utiliser les utilitaires de gestion des services et les interfaces de ligne de commande dans l'interpréteur de commandes du dispositif. Vous pouvez utiliser TTY1 pour vous connecter à la console ou employer SSH pour vous connecter à l'interpréteur de commandes.

Procédure

1 Activez la connexion SSH si nécessaire.

a Connectez-vous à l'interface VAMI.

b Dans le navigateur, sélectionnez **Accès**, puis cliquez sur **Modifier**.

c Cliquez sur la case à cocher **Activer la connexion SSH**, puis cliquez sur **OK**.

Vous pouvez suivre les mêmes instructions pour activer l'interpréteur de commandes de dépistage du dispositif.

2 Accédez à l'interpréteur de commande du dispositif.

- Si vous avez un accès direct à la console du dispositif, sélectionnez **Se connecter** et appuyez sur Entrée.
- Pour vous connecter à distance, utilisez SSH ou une autre connexion de console à distance pour ouvrir une session sur le dispositif.

3 Connectez-vous en tant qu'utilisateur racine avec le mot de passe que vous avez défini lors du déploiement initial du dispositif.

Si vous avez modifié le mot de passe racine, utilisez le nouveau mot de passe.

Ajouter un dispositif Platform Services Controller à un domaine Active Directory

Si vous souhaitez ajouter une source d'identité Active Directory à Platform Services Controller, vous devez joindre le dispositif Platform Services Controller à un domaine Active Directory.

Si vous utilisez une instance de Platform Services Controller qui est installée sur Windows, vous pouvez utiliser le domaine auquel la machine appartient.

Procédure

1 Connectez-vous à l'interface Web de Platform Services Controller à l'adresse http://*psc_ip_or_dns*/psc en tant qu'utilisateur administrateur.

2 Cliquez sur **Paramètres des dispositifs**, puis cliquez sur **Gérer**.

3 Cliquez sur **Joindre**, spécifiez le domaine, une unité d'organisation, ainsi qu'un nom d'utilisateur et un mot de passe, puis cliquez sur **OK**.

Authentification vSphere à l'aide de vCenter Single Sign-On 2

vCenter Single Sign-On est un broker d'authentification et une infrastructure d'échange de jetons de sécurité. Lorsqu'un utilisateur ou un utilisateur de solution peut s'authentifier dans vCenter Single Sign-On, il reçoit un jeton SAML. Par la suite, l'utilisateur peut utiliser le jeton SAML pour s'authentifier auprès des services vCenter. L'utilisateur peut ensuite réaliser les actions pour lesquels il dispose des privilèges.

Comme le trafic est chiffré pour toutes les communications et que seuls les utilisateurs authentifiés peuvent réaliser les actions pour lesquels ils disposent des privilèges, votre environnement est sécurisé.

À partir de vSphere 6.0, vCenter Single Sign-On est intégré à Platform Services Controller. Platform Services Controller contient les services partagés prenant en charge vCenter Server et les composants vCenter Server. Ces services comprennent vCenter Single Sign-On, VMware Certificate Authority et License Service. Pour plus d'informations sur Platform Services Controller, reportez-vous à la section *Installation et configuration de vSphere*.

Pour l'établissement de liaison initial, les utilisateurs s'authentifient avec un nom d'utilisateur et un mot de passe, tandis que les utilisateurs de solution s'authentifient par le biais d'un certificat. Pour plus d'informations sur le remplacement des certificats des utilisateurs de solution, reportez-vous à la section Chapitre 3, « Certificats de sécurité vSphere », page 71.

La prochaine étape consiste à autoriser les utilisateurs pouvant s'authentifier à exécuter certaines tâches. Dans la plupart des cas, vous attribuez des privilèges vCenter Server, généralement en attribuant l'utilisateur à un groupe possédant un rôle. vSphere comprend d'autres modèles d'autorisations, telles que les autorisations globales. Consultez la documentation de *Sécurité vSphere*.

Ce chapitre aborde les rubriques suivantes :

Comprendre vCenter Single Sign-On

Pour gérer efficacement vCenter Single Sign-On, vous devez comprendre l'architecture sous-jacente et son impact sur l'installation et les mises à niveau.

Domaines et sites vCenter Single Sign-On 6.0 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_sso_6_domains_sites)

Protection de votre environnement par vCenter Single Sign-On

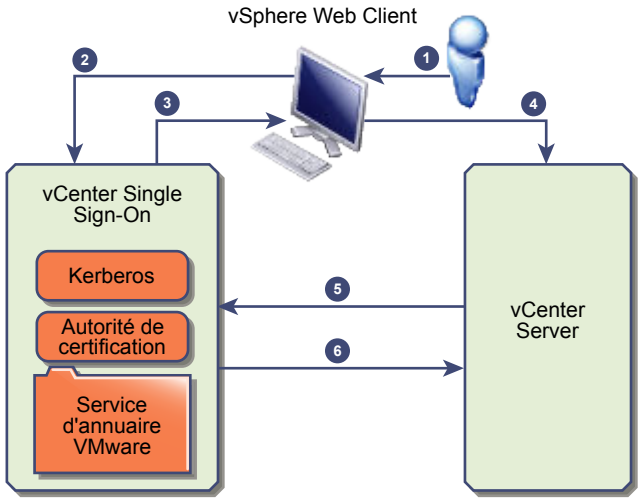
vCenter Single Sign-On permet aux composants vSphere de communiquer entre eux au moyen d'un mécanisme d'échange de jetons sécurisé au lieu d'obliger les utilisateurs à s'authentifier séparément pour chaque composant.

vCenter Single Sign-On utilise une combinaison de STS (Security Token Service), de SSL pour la sécurisation du trafic et de l'authentification des utilisateurs humains par Active Directory ou OpenLDAP et des utilisateurs de solution par le biais de certificats.

Établissement de liaison vCenter Single Sign-On pour les utilisateurs humains

L'illustration suivante présente l'établissement de liaison pour les utilisateurs humains.

Figure 2-1. Établissement de liaison vCenter Single Sign-On pour les utilisateurs humains



1 Un utilisateur se connecte à vSphere Web Client avec un nom d'utilisateur et un mot de passe pour accéder au système vCenter Server ou à un autre service vCenter.

   L'utilisateur peut également se connecter sans mot de passe et cocher la case **Utiliser l'authentification de session Windows**.

2 vSphere Web Client transmet les informations de connexion au service vCenter Single Sign-On. Celui-ci vérifie alors le jeton SAML de vSphere Web Client. Si vSphere Web Client dispose d'un jeton valide, vCenter Single Sign-On vérifie ensuite que l'utilisateur figure bien dans la source d'identité configurée (par exemple, Active Directory).

   - Si seul le nom d'utilisateur est employé, vCenter Single Sign-On effectue la vérification dans le domaine par défaut.
   - Si un nom de domaine est inclus avec le nom d'utilisateur (*DOMAIN*\user1 ou user1@*DOMAIN*), vCenter Single Sign-On vérifie ce domaine.

3 Si l'utilisateur peut s'authentifier auprès de la source d'identité, vCenter Single Sign-On renvoie un jeton qui représente l'utilisateur pour vSphere Web Client.

4 vSphere Web Client transmet le jeton au système vCenter Server.

5 vCenter Server vérifie auprès du serveur vCenter Single Sign-On que le jeton est valide et n'a pas expiré.

6 Le serveur vCenter Single Sign-On renvoie le jeton au système vCenter Server en exploitant la structure d'autorisation de vCenter Server pour autoriser l'accès de l'utilisateur.

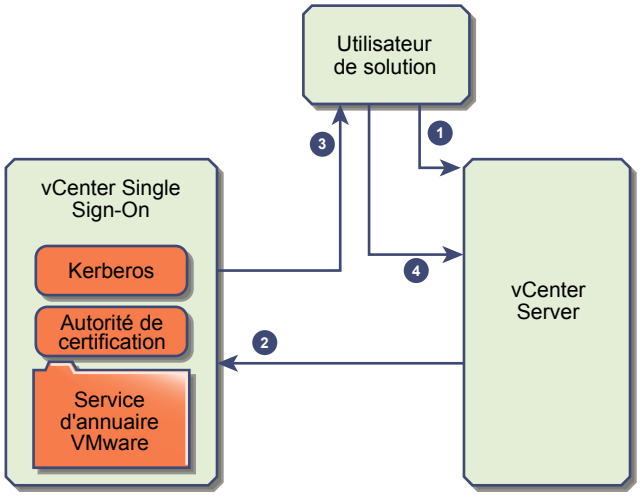
L'utilisateur peut désormais s'authentifier, puis afficher et modifier les objets pour lesquels il possède les privilèges pertinents.

Remarque Le rôle Aucun accès est attribué initialement à chaque utilisateur. Pour qu'un utilisateur puisse se connecter, un administrateur vCenter Server doit au moins lui attribuer le rôle Lecture seule. Consultez la documentation de *Sécurité vSphere*.

Établissement de liaison vCenter Single Sign-On pour les utilisateurs de solution

Les utilisateurs de solution sont des ensembles de services utilisés dans l'infrastructure vCenter Server (les extensions vCenter Server ou vCenter Server, par exemple). Les extensions VMware et éventuellement les extensions tierces peuvent également s'authentifier auprès de vCenter Single Sign-On.

Figure 2-2. Établissement de liaison vCenter Single Sign-On pour les utilisateurs de solution



Pour les utilisateurs de solution, l'interaction se déroule comme suit :

1 L'utilisateur de solution tente de se connecter à un service vCenter.

2 L'utilisateur de solution est redirigé vers vCenter Single Sign-On. Si l'utilisateur de solution est nouveau dans vCenter Single Sign-On, il doit présenter un certificat valide.

3 Si le certificat est valide, vCenter Single Sign-On attribue un jeton SAML (jeton de support) à l'utilisateur de solution. Le jeton est signé par vCenter Single Sign-On.

4 L'utilisateur de solution est ensuite redirigé vers vCenter Single Sign-On et peut effectuer des tâches, selon les autorisations qui lui sont attribuées.

5 La prochaine fois que l'utilisateur de solution devra s'authentifier, il pourra utiliser le jeton SAML pour se connecter à vCenter Server.

Cet établissement de liaison est automatique par défaut, car VMCA provisionne les utilisateurs de solution à l'aide de certificats pendant le démarrage. Si la stratégie de l'entreprise requiert des certificats signés par une autorité de certification tierce, vous pouvez remplacer les certificats d'utilisateur de solution par ces certificats signés par une autorité de certification tierce. Si ces certificats ne sont pas valides, vCenter Single Sign-On attribue un jeton SAML à l'utilisateur de solution. Reportez-vous à « Utiliser des certificats personnalisés avec vSphere », page 127.

Composants vCenter Single Sign-On

vCenter Single Sign-On inclut Security Token Service (STS), un serveur d'administration, vCenter Lookup Service et le service d'annuaire VMware (vmdir). Le service d'annuaire VMware est également utilisé pour la gestion des certificats.

Au moment de l'installation, les composants sont déployés sous la forme d'un déploiement intégré ou en tant qu'éléments de Platform Services Controller.

STS (Security Token Service)

Le services STS envoie des jetons SAML (Security Assertion Markup Language). Ces jetons de sécurité représentent l'identité d'un utilisateur dans l'un des types de sources d'identité pris en charge par vCenter Single Sign-On. Les jetons SAML permettent aux utilisateurs humains et aux utilisateurs de solutions qui s'authentifient correctement auprès de vCenter Single Sign-On d'utiliser tous les services vCenter pris en charge par vCenter Single Sign-On sans devoir se réauthentifier auprès de chaque service.

Le service vCenter Single Sign-On attribue un certificat de signature à tous les jetons pour les signer et stocke ces certificats sur le disque. Le certificat du service est également stocké sur le disque.

Serveur d'administration

Le serveur d'administration autorise les utilisateurs disposant des privilèges d'administrateur sur vCenter Single Sign-On à configurer le serveur vCenter Single Sign-On et à gérer les utilisateurs et les groupes dans vSphere Web Client. Au départ, seul l'utilisateur administrator@*your_domain_name* dispose de ces privilèges. Dans vSphere 5.5, il s'agissait obligatoirement de l'utilisateur administrator@vsphere.local. Dans vSphere 6.0, vous pouvez modifier le domaine vSphere lors de l'installation de vCenter Server ou du déploiement de vCenter Server Appliance avec une nouvelle instance de Platform Services Controller. Attribuez au domaine un nom différent que celui du domaine Microsoft Active Directory ou OpenLDAP.

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) est associé au domaine que vous indiquez lors de l'installation. Il est inclus dans chaque déploiement intégré et chaque instance de Platform Services Controller. Ce service est un service d'annuaire mutualisé et masterisé qui met à disposition un annuaire LDAP sur le port 389. Le service utilise toujours le port 11711 pour la compatibilité descendante avec vSphere 5.5 et les systèmes antérieurs.

Si votre environnement inclut plusieurs instances de Platform Services Controller, une mise à jour du contenu vmdir d'une seule instance de vmdir est propagée vers toutes les autres instances de vmdir.

À partir de vSphere 6.0, VMware Directory Service stocke les informations de certificat, en plus des informations vCenter Single Sign-On.

Identity Management Service

Gère les demandes concernant les sources d'identité et l'authentification STS.

Incidence de vCenter Single Sign-On sur l'installation

À partir de la version 5.1, vSphere inclut un service vCenter Single Sign-On dans le cadre de l'infrastructure de gestion de vCenter Server. Cette modification a une incidence sur l'installation de vCenter Server.

L'authentification avec vCenter Single Sign-On améliore la sécurité de vSphere, car les composants logiciels de vSphere communiquent entre eux en utilisant un mécanisme d'échange de jetons sécurisés, et tous les autres utilisateurs s'authentifient également avec vCenter Single Sign-On.

À partir de vSphere 6.0, vCenter Single Sign-On est inclus dans un déploiement intégré ou comme partie intégrante du Platform Services Controller. Le Platform Services Controller contient tous les services requis pour la communication entre les composants vSphere, notamment vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service et le service de licence.

L'ordre d'installation est important.

Première installation Si votre installation est distribuée, vous devez installer Platform Services Controller avant d'installer vCenter Server ou de déployer vCenter Server Appliance. Pour un déploiement intégré, l'installation s'effectue automatiquement dans l'ordre approprié.

Installations suivantes Pour environ quatre instances de vCenter Server, une instance de Platform Services Controller peut servir l'intégralité de votre environnement vSphere. Vous pouvez connecter les nouvelles instances de vCenter Server au même Platform Services Controller. Au-delà d'environ quatre instances de vCenter Server, vous pouvez installer un Platform Services Controller supplémentaire pour améliorer les performances. Le service vCenter Single Sign-On sur chaque Platform Services Controller synchronise les données d'authentification avec toutes les autres instances. Le nombre précis dépend du niveau d'utilisation des instances de vCenter Server et d'autres facteurs.

Pour obtenir des informations détaillées sur les modèles de déploiement, les avantages et les inconvénients de chaque type de déploiement, reportez-vous à *Installation et configuration de vSphere*.

Utilisation de vCenter Single Sign-On avec vSphere

Lorsqu'un utilisateur se connecte à un composant vSphere ou lorsqu'un utilisateur de solution vCenter Server accède à un autre service vCenter Server, vCenter Single Sign-On procède à l'authentification. Les utilisateurs doivent être authentifiés auprès de vCenter Single Sign-On et disposer de privilèges suffisants pour interagir avec les objets vSphere.

vCenter Single Sign-On authentifie à la fois les utilisateurs de solutions et les autres utilisateurs.

- Les utilisateurs de solutions représentent un ensemble de services au sein de votre environnement vSphere. Durant l'installation, VMCA attribue par défaut un certificat à chaque utilisateur de solution. L'utilisateur de solution emploie ce certificat pour s'authentifier auprès de vCenter Single Sign-On. vCenter Single Sign-On émet un jeton SAML pour l'utilisateur de solution. Celui-ci peut alors interagir avec d'autres services au sein de l'environnement.
- Lorsque d'autres utilisateurs se connectent à l'environnement, par exemple à partir de vSphere Web Client, vCenter Single Sign-On demande un nom d'utilisateur et un mot de passe. Si vCenter Single Sign-On trouve un utilisateur possédant ces informations d'identification dans la source d'identité correspondante, il attribue un jeton SAML à cet utilisateur. L'utilisateur peut maintenant accéder à d'autres services de l'environnement sans devoir s'authentifier à nouveau.

  Les objets visibles par l'utilisateur et les actions que celui-ci peut effectuer sont généralement déterminés par les paramètres d'autorisation vCenter Server. Les administrateurs vCenter Server attribuent ces autorisations depuis l'interface **Permissions** de vSphere Web Client, pas au moyen de vCenter Single Sign-On. Consultez la documentation de *Sécurité vSphere*.

Utilisateurs de vCenter Single Sign-On et de vCenter Server

À l'aide de vSphere Web Client, les utilisateurs s'authentifient auprès de vCenter Single Sign-On en entrant leurs informations d'identification sur la page de connexion de vSphere Web Client. Une fois connectés à vCenter Server, les utilisateurs authentifiés peuvent afficher toutes leurs instances de vCenter Server ou d'autres objets vSphere pour lesquels leur rôle leur accorde des privilèges. Aucune autre authentification n'est requise.

Après l'installation, l'administrateur du domaine vCenter Single Sign-On, par défaut administrator@vsphere.local, possède un accès administrateur au vCenter Single Sign-On et au vCenter Server. Cet utilisateur peut alors ajouter des sources d'identité, définir la source d'identité par défaut, et gérer les utilisateurs et les groupes dans le domaine vCenter Single Sign-On (vsphere.local par défaut).

Tous les utilisateurs pouvant s'authentifier auprès de vCenter Single Sign-On ont la possibilité de réinitialiser leur mot de passe, même si celui-ci a expiré, à condition qu'ils le connaissent. Reportez-vous à « Changer le mot de passe de vCenter Single Sign-On », page 69. Seuls les administrateurs vCenter Single Sign-On peuvent réinitialiser le mot de passe des utilisateurs qui n'en ont plus.

Utilisateurs administrateurs de vCenter Single Sign-On

L'interface administrative vCenter Single Sign-On est accessible depuis vSphere Web Client et depuis l'interface web de Platform Services Controller.

Pour configurer vCenter Single Sign-On et gérer les utilisateurs et les groupes vCenter Single Sign-On, l'utilisateur administrator@vsphere.local ou un utilisateur du groupe d'administrateurs vCenter Single Sign-On doit se connecter à vSphere Web Client. Après authentification, cet utilisateur peut accéder à l'interface d'administration de vCenter Single Sign-On à partir de vSphere Web Client et gérer les sources d'identité et les domaines par défaut, spécifier les stratégies de mot de passe et effectuer d'autres tâches d'administration. Reportez-vous à « Configuration des sources d'identité vCenter Single Sign-On », page 29.

Remarque Vous ne pouvez pas renommer l'utilisateur administrateur vCenter Single Sign-On (administrator@vsphere.local par défaut ou administrator@*mondomaine* si un autre domaine a été spécifié lors de l'installation). Pour une sécurité accrue, envisagez de créer des utilisateurs nommés supplémentaires dans le domaine vCenter Single Sign-On et de leur attribuer des privilèges d'administration. Vous pouvez ensuite arrêtez d'utiliser le compte d'administrateur.

Utilisateurs ESXi

Les hôtes ESXi autonomes ne sont pas intégrés avec vCenter Single Sign-On ou avec Platform Services Controller. Voir *Sécurité vSphere* pour des informations sur l'ajout d'un hôte ESXi à Active Directory.

Si vous créez des utilisateurs ESXi locaux pour un hôte ESXi géré avec l'instance de VMware Host Client, vCLI ou PowerCLI. vCenter Server n'a pas connaissance de ces utilisateurs. La création d'utilisateurs locaux peut donc créer une confusion, particulièrement si vous utilisez les mêmes noms d'utilisateurs. Les utilisateurs qui peuvent s'authentifier auprès du vCenter Single Sign-On peuvent voir et gérer les hôtes ESXi s'ils possèdent les autorisations correspondantes sur l'objet hôte ESXi.

Remarque Si possible, gérez les autorisations pour les hôtes ESXi via vCenter Server.

Comment se connecter aux composants de vCenter Server

Vous pouvez vous connecter au moyen de vSphere Web Client ou de l'interface web de Platform Services Controller.

Lorsqu'un utilisateur se connecte à un système vCenter Server à partir de vSphere Web Client, le comportement de la connexion n'est pas le même selon que l'utilisateur se trouve ou non dans le domaine par défaut (c'est-à-dire le domaine défini comme source d'identité par défaut).

- Les utilisateurs qui se trouvent dans le domaine par défaut peuvent se connecter avec leurs nom d'utilisateur et mot de passe.
- Les utilisateurs qui se trouvent dans un domaine qui a été ajouté à vCenter Single Sign-On en tant que source d'identité, mais qui n'est pas le domaine par défaut, peuvent se connecter à vCenter Server, mais ils doivent spécifier le domaine de l'une des manières suivantes.
  - En incluant un préfixe de nom de domaine : par exemple, MONDOMAINE\utilisateur1
  - En incluant le domaine : par exemple, utilisateur1@mondomaine.com
- Les utilisateurs qui se trouvent dans un domaine qui n'est pas une source d'identité vCenter Single Sign-On ne peuvent pas se connecter à vCenter Server. Si le domaine que vous ajoutez à vCenter Single Sign-On fait partie d'une hiérarchie de domaines, Active Directory détermine si les utilisateurs des autres domaines de la hiérarchie sont ou non authentifiés.

Si votre environnement comprend une hiérarchie Active Directory, reportez-vous à l'article 2064250 de la base de connaissances VMware pour plus d'informations sur les configurations prises en charge et non prises en charge.

Remarque À partir de vSphere 6.0 Update 2, l'authentification à deux facteurs est prise en charge. Reportez-vous à « Authentification à deux facteurs de vCenter Server », page 38.

Groupes du domaine vCenter Single Sign-On

Le domaine vCenter Single Sign-On (par défaut, vsphere.local) inclut plusieurs groupes prédéfinis. Ajoutez des utilisateurs à l'un de ces groupes pour leur permettre d'effectuer les actions correspondantes.

Reportez-vous à « Gestion des utilisateurs et des groupes vCenter Single Sign-On », page 61.

Pour tous les objets de la hiérarchie de vCenter Server, les autorisations sont attribuées en couplant un utilisateur et un rôle avec l'objet. Par exemple, vous pouvez sélectionner un pool de ressources et attribuer les privilèges de lecture de cet objet de pool de ressources à un groupe d'utilisateurs en leur attribuant le rôle correspondant.

Pour certains services qui ne sont pas gérés directement par vCenter Server, les privilèges sont déterminés par l'appartenance à l'un des groupes vCenter Single Sign-On. Par exemple, tout utilisateur qui est membre du groupe Administrateur peut gérer vCenter Single Sign-On. Tout utilisateur membre du groupe CAAdmins peut gérer VMware Certificate Authority et tout utilisateur appartenant au groupe LicenseService.Administrators peut gérer les licences.

Les groupes suivants sont prédéfinis dans vsphere.local.

Remarque Un grand nombre de ces groupes sont internes à vsphere.local ou donnent aux utilisateurs des privilèges d'administration de haut niveau. Avant d'ajouter des utilisateurs à l'un de ces groupes, réfléchissez bien aux risques encourus.

Ne supprimez pas les groupes prédéfinis du domaine vsphere.local. Si vous le faites, des erreurs d'authentification ou de provisionnement de certificats peuvent se produire.

Tableau 2-1. Groupes du domaine vsphere.local

Privilège	Description
Utilisateurs	Les utilisateurs du domaine vCenter Single Sign-On (par défaut, vsphere.local).
SolutionUsers	Utilisateurs de solution. Ce groupe contient les services vCenter. Chaque utilisateur de solution s'authentifie individuellement auprès de vCenter Single Sign-On avec un certificat. Par défaut, VMCA provisionne les utilisateurs de solution à l'aide de certificats. N'ajoutez aucun membre à ce groupe explicitement.
CAAdmins	Les membres du groupe CAAdmins possèdent des privilèges d'administration pour VMCA. En général, il est déconseillé d'ajouter des membres à ces groupes.
DCAdmins	Les membres du groupe DCAdmins peuvent exercer des actions d'administrateur de contrôleur de domaine sur VMware Directory Service. **Remarque** Ne gérez pas le contrôleur de domaine directement. Utilisez plutôt la CLI `vmdir` ou vSphere Web Client pour effectuer les tâches correspondantes.
SystemConfiguration.BashShellAdministrators	Ce groupe est disponible uniquement pour les déploiements de vCenter Server Appliance. Tout utilisateur appartenant à ce groupe peut activer et désactiver l'accès à l'interpréteur de commandes de dépistage. Par défaut, tout utilisateur qui se connecte à vCenter Server Appliance à l'aide de SSH peut uniquement accéder aux commandes disponibles dans le shell restreint. Les utilisateurs de ce groupe peuvent accéder à l'interpréteur de commandes de dépistage.
ActAsUsers	Les membres de ce groupe sont autorisés à recevoir des jetons actas de vCenter Single Sign-On.
ExternalIPDUsers	vSphere n'utilise pas ce groupe interne. Il est nécessaire en conjonction avec VMware vCloud Air.
SystemConfiguration.Administrators	Les membres du groupe SystemConfiguration.Administrators peuvent afficher et gérer la configuration du système dans vSphere Web Client. Ces utilisateurs peuvent afficher, démarrer, redémarrer et dépanner les services et consulter et gérer les nœuds disponibles.
DCClients	Ce groupe est utilisé en interne pour permettre aux nœuds de gestion d'accéder aux données qui se trouvent dans VMware Directory Service. **Remarque** Ne modifiez pas ce groupe. Toute modification pourrait compromettre votre infrastructure de certificats.
ComponentManager.Administrators	Les membres du groupe ComponentManager.Administrators peuvent appeler des API du gestionnaire de composants qui enregistrent des services ou annulent leur enregistrement, c'est-à-dire qui modifient les services. L'appartenance à ce groupe n'est pas requise pour pouvoir accéder en lecture à ces services.
LicenseService.Administrators	Les membres du groupe LicenseService.Administrators peuvent accéder en écriture à toutes les données liées à la gestion des licences et peuvent ajouter, supprimer, attribuer des touches série et en annuler l'attribution pour toutes les ressources de produits enregistrées dans le service de licence.
Administrateurs	Administrateurs de VMware Directory Service (vmdir). Les membres de ce groupe peuvent effectuer des tâches d'administration vCenter Single Sign-On. En général, il est déconseillé d'ajouter des membres à ce groupe.

Configuration des sources d'identité vCenter Single Sign-On

Lorsqu'un utilisateur se connecte avec seulement un nom d'utilisateur, vCenter Single Sign-On vérifie dans la source d'identité par défaut si cet utilisateur peut s'authentifier. Lorsqu'un utilisateur se connecte et inclut le nom de domaine dans l'écran de connexion, vCenter Single Sign-On vérifie si le domaine spécifié a été ajouté comme source d'identité. Vous pouvez ajouter des sources d'identité, en supprimer et modifier celles par défaut.

Vous pouvez configurer vCenter Single Sign-On depuis vSphere Web Client ou l'interface Web de Platform Services Controller. Pour configurer vCenter Single Sign-On, vous devez disposer des privilèges d'administrateur de vCenter Single Sign-On. Les privilèges d'administrateur vCenter Single Sign-On sont différents du rôle d'administrateur sur vCenter Server ou ESXi. Dans une nouvelle installation, seul l'administrateur de vCenter Single Sign-On (administrator@vsphere.local par défaut) peut s'authentifier dans vCenter Single Sign-On.

Sources d'identité pour vCenter Server avec vCenter Single Sign-On

Grâce aux sources d'identité, vous pouvez associer un ou plusieurs domaines à vCenter Single Sign-On. Un domaine est un référentiel d'utilisateurs et de groupes que le serveur vCenter Single Sign-On peut utiliser pour l'authentification des utilisateurs.

Une source d'identité est un ensemble de données d'utilisateurs et de groupes. Les données d'utilisateurs et de groupes sont stockées dans Active Directory, OpenLDAP ou localement dans le système d'exploitation de la machine sur laquelle vCenter Single Sign-On est installé.

Après l'installation, chaque instance de vCenter Single Sign-On dispose de la source d'identité *your_domain_name*, par exemple vsphere.local. Cette source d'identité est interne à vCenter Single Sign-On. Un administrateur vCenter Single Sign-On peut ajouter des sources d'identité, définir la source d'identité par défaut et créer des utilisateurs et des groupes dans la source d'identité vsphere.local.

Types de sources d'identité

Les versions de vCenter Server antérieures à la version 5.1 prenaient en charge les utilisateurs Active Directory et les utilisateurs du système d'exploitation local en tant que référentiels d'utilisateurs. Par conséquent, les utilisateurs du système d'exploitation local peuvent toujours s'authentifier dans le système vCenter Server. vCenter Server version 5.1 et version 5.5 utilisent vCenter Single Sign-On pour l'authentification. Pour obtenir la liste des sources d'identité prises en charge par vCenter Single Sign-On 5.1, reportez-vous à la documentation de vSphere 5.1. vCenter Single Sign-On 5.5 prend en charge les types de référentiels d'utilisateurs suivants en tant que sources d'identité, mais ne prend en charge qu'une source d'identité par défaut.

- Active Directory 2003 et les versions ultérieures. S'affiche comme **Active Directory (authentification Windows intégrée)** dans vSphere Web Client. vCenter Single Sign-On vous permet de spécifier un domaine Active Directory unique comme source d'identité. Le domaine peut avoir des domaines enfants ou être un domaine racine de la forêt. L'article 2064250 de la base de connaissances VMware traite des relations de confiance Microsoft Active Directory prises en charge par vCenter Single Sign-On.
- Active Directory sur LDAP. vCenter Single Sign-On prend en charge plusieurs sources d'identité Active Directory sur LDAP. Ce type de source d'identité est inclus à des fins de compatibilité avec le service vCenter Single Sign-On inclus avec vSphere 5.1. Nommé **Active Directory comme serveur LDAP** dans vSphere Web Client.
- OpenLDAP 2.4 et versions ultérieures. vCenter Single Sign-On prend en charge plusieurs sources d'identité OpenLDAP. Cette source d'identité est nommée **OpenLDAP** dans vSphere Web Client.
- Utilisateurs du système d'exploitation local. Les utilisateurs du système d'exploitation local sont les utilisateurs du système d'exploitation sur lequel le serveur vCenter Single Sign-On est en cours d'exécution. La source d'identité du système d'exploitation local existe uniquement dans les déploiements de base du serveur vCenter Single Sign-On. Elle n'est pas disponible dans les déploiements de plusieurs instances de vCenter Single Sign-On. Une seule source d'identité de système d'exploitation local est autorisée. Cette source d'identité est nommée **localos** dans vSphere Web Client.

  Remarque N'utilisez pas les utilisateurs du système d'exploitation local si le Platform Services Controller ne se trouve pas sur la même machine que le système vCenter Server. L'emploi d'utilisateurs du système d'exploitation local peut sembler pertinent dans un déploiement intégré mais n'est pas recommandée.

- Utilisateurs du système vCenter Single Sign-On Lorsque vous installez vCenter Single Sign-On, une seule source d'identité système est créée. Par défaut, cette source d'identité est nommée vsphere.local, mais vous pouvez choisir un nom différent lors de l'installation.

Remarque À tout moment, il n'existe qu'un seul domaine par défaut. Si un utilisateur d'un domaine autre que le domaine par défaut se connecte, il doit ajouter le nom de domaine (*DOMAIN\user*) pour s'authentifier.

Les sources d'identité de vCenter Single Sign-On sont gérées par les administrateurs de vCenter Single Sign-On.

Vous pouvez ajouter des sources d'identité à une instance du serveur vCenter Single Sign-On. Les sources d'identité distantes sont limitées aux mises en œuvre des serveurs Active Directory et OpenLDAP.

Définir le domaine par défaut de vCenter Single Sign-On

Chaque source d'identité de vCenter Single Sign-On est associée à un domaine. vCenter Single Sign-On utilise le domaine par défaut pour authentifier un utilisateur qui se connecte sans nom de domaine. Les utilisateurs qui appartiennent à un domaine qui n'est pas le domaine par défaut doivent inclure le nom de domaine lorsqu'ils se connectent.

Lorsqu'un utilisateur se connecte à un système vCenter Server à partir de vSphere Web Client, le comportement de la connexion n'est pas le même selon que l'utilisateur se trouve ou non dans le domaine par défaut (c'est-à-dire le domaine défini comme source d'identité par défaut).

- Les utilisateurs qui se trouvent dans le domaine par défaut peuvent se connecter avec leurs nom d'utilisateur et mot de passe.
- Les utilisateurs qui se trouvent dans un domaine qui a été ajouté à vCenter Single Sign-On en tant que source d'identité, mais qui n'est pas le domaine par défaut, peuvent se connecter à vCenter Server, mais ils doivent spécifier le domaine de l'une des manières suivantes.
  - En incluant un préfixe de nom de domaine : par exemple, MONDOMAINE\utilisateur1
  - En incluant le domaine : par exemple, utilisateur1@mondomaine.com
- Les utilisateurs qui se trouvent dans un domaine qui n'est pas une source d'identité vCenter Single Sign-On ne peuvent pas se connecter à vCenter Server. Si le domaine que vous ajoutez à vCenter Single Sign-On fait partie d'une hiérarchie de domaines, Active Directory détermine si les utilisateurs des autres domaines de la hiérarchie sont ou non authentifiés.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Dans l'onglet **Sources d'identité**, sélectionnez une source d'identité, puis cliquez sur l'icône **Défini comme domaine par défaut**.

Dans l'affichage des domaines, le domaine par défaut est marqué de la mention (par défaut) dans la colonne Domaine.

Ajouter une source d'identité de vCenter Single Sign-On

Les utilisateurs peuvent se connecter à vCenter Server uniquement s'ils sont dans un domaine qui a été ajouté comme source d'identité vCenter Single Sign-On. Les utilisateurs administrateurs de vCenter Single Sign-On peuvent ajouter des sources d'identité dans l'interface de vSphere Web Client ou de Platform Services Controller.

Une source d'identité peut être un domaine Active Directory natif (authentification Windows intégrée) ou un service d'annuaire OpenLDAP. Pour des raisons de compatibilité descendante, Active Directory comme serveur LDAP est également disponible. Reportez-vous à « Sources d'identité pour vCenter Server avec vCenter Single Sign-On », page 29

Immédiatement après l'installation, les sources d'identité et utilisateurs par défaut suivants sont disponibles :

localos — Tous les utilisateurs du système d'exploitation local. Si vous effectuez une mise à niveau, les utilisateurs localos qui peuvent déjà s'authentifier peuvent continuer à le faire. L'utilisation de la source d'identité localos n'est pas justifiée dans les environnements qui utilisent une instance intégrée de Platform Services Controller.

vsphere.local — Contient les utilisateurs internes de vCenter Single Sign-On.

Prérequis

Si vous ajoutez une source d'identité Active Directory, vCenter Server Appliance ou la machine Windows sur laquelle vCenter Server est en cours d'exécution doit être dans le domaine Active Directory. Reportez-vous à « Ajouter un dispositif Platform Services Controller à un domaine Active Directory », page 20.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Dans l'onglet **Sources d'identité**, cliquez sur l'icône **Ajouter source d'identité**.

5 Sélectionnez le type de source d'identité et entrez les paramètres de source d'identité.

Option	Description
Active Directory (authentification Windows intégrée)	Utilisez cette option pour les mises en œuvre Active Directory natives. Si vous souhaitez utiliser cette option, la machine sur laquelle le service vCenter Single Sign-On s'exécute doit se trouver dans un domaine Active Directory. Reportez-vous à « Paramètres de source d'identité Active Directory », page 33.
Active Directory comme serveur LDAP	Cette option est disponible à des fins de compatibilité descendante. Elle nécessite la spécification du contrôleur de domaine et d'autres informations. Reportez-vous à « Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP », page 35.
OpenLDAP	Utilisez cette option pour une source d'identité OpenLDAP. Reportez-vous à « Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP », page 35.
LocalOS	Utilisez cette option pour ajouter le système d'exploitation local comme source d'identité. Le système vous demande uniquement le nom du système d'exploitation. Si vous sélectionnez cette option, tous les utilisateurs sur la machine spécifiée sont visibles par vCenter Single Sign-On, même si ces utilisateurs ne font pas partie d'un autre domaine.

Remarque Si le compte d'utilisateur est verrouillé ou désactivé, les authentifications et les recherches d'utilisateurs et de groupes dans le domaine Active Directory échouent. Le compte d'utilisateur doit disposer d'un accès en lecture seule sur l'UO utilisateur et du groupe, et il doit être en mesure de lire les attributs de l'utilisateur et du groupe. Active Directory fournit cet accès par défaut. Utilisez un utilisateur spécial de service pour plus de sécurité.

6 Si vous avez configuré une source d'identité Active Directory comme serveur LDAP ou OpenLDAP, cliquez sur **Tester la connexion** pour vous assurer que vous pouvez vous connecter à la source d'identité.

7 Cliquez sur **OK**.

Suivant

Lorsqu'une source d'identité est ajoutée, tous les utilisateurs peuvent être authentifiés mais disposent du rôle **Aucun accès**. Un utilisateur disposant de privilèges vCenter Server **Modify.permissions** peut attribuer des privilèges à des utilisateurs ou des groupes d'utilisateurs pour leur permettre de se connecter à vCenter Server ainsi que d'afficher et de gérer des objets. Consultez la documentation de *Sécurité vSphere*.

Paramètres de source d'identité Active Directory

Si vous sélectionnez le type de source d'identité **Active Directory (authentification Windows intégrée)**, vous pouvez utiliser le compte de l'ordinateur local en tant que nom de principal du service (SPN, Service Principal Name) ou spécifier un SPN de manière explicite. Vous pouvez utiliser cette option uniquement si le serveur vCenter Single Sign-On est joint à un domaine Active Directory.

Conditions préalables à l'utilisation d'une source d'identité Active Directory

Vous pouvez configurer vCenter Single Sign-On pour utiliser une source d'identité Active Directory uniquement si cette source d'identité est disponible.

- Pour une installation Windows, joignez la machine Windows au domaine Active Directory.

- Pour vCenter Server Appliance, suivez les instructions de la documentation *Configuration de vCenter Server Appliance*.

Remarque Active Directory (authentification Windows intégrée) utilise toujours la racine de la forêt du domaine Active Directory. Pour configurer votre source d'identité d'authentification Windows intégrée avec un domaine enfant dans votre forêt Active Directory, reportez-vous à l'article 2070433 de la base de connaissances VMware.

Sélectionnez **Utiliser un compte d'ordinateur** pour accélérer la configuration. Si vous prévoyez de renommer l'ordinateur local sur lequel s'exécute vCenter Single Sign-On, il est préférable de spécifier un SPN de manière explicite.

Remarque Dans vSphere 5.5, vCenter Single Sign-On utilise le compte de l'ordinateur même si vous spécifiez le SPN. Reportez-vous à l'article 2087978 de la base de connaissances VMware.

Tableau 2-2. Ajouter des paramètres de source d'identité

Zone de texte	Description
Nom de domaine	Nom de domaine complet du nom de domaine, par exemple mondomain.com. Ne fournissez pas une adresse IP. Ce nom de domaine doit pouvoir être résolu par DNS par le système vCenter Server Si vous utilisez vCenter Server Appliance, utilisez les informations sur la configuration des paramètres réseau pour mettre à jour les paramètres de serveur DNS.
Utiliser un compte d'ordinateur	Sélectionnez cette option pour utiliser le compte de l'ordinateur local en tant que SPN. Lorsque vous sélectionnez cette option, vous spécifiez uniquement le nom de domaine. Si vous prévoyez de renommer l'ordinateur, ne sélectionnez pas cette option.
Utiliser le nom de principal du service (SPN)	Sélectionnez cette option si vous prévoyez de renommer l'ordinateur local. Vous devez spécifier un SPN, un utilisateur pouvant s'authentifier auprès de la source d'identité et un mot de passe pour cet utilisateur.
Nom de principal du service (SPN)	SPN permettant à Kerberos d'identifier le service Active Directory. Incluez le domaine dans le nom (`STS/example.com`, par exemple). Le SPN doit être unique dans le domaine. L'exécution de la commande `setspn –S` permet de vérifier qu'aucun doublon n'est créé. Pour obtenir des informations sur l'outil de ligne de commande `setspn`, reportez-vous à la documentation de Microsoft.
Nom d'utilisateur principal (UPN) **Mot de passe**	Nom et mot de passe d'un utilisateur pouvant s'authentifier auprès de cette source d'identité. Utilisez le format d'adresse e-mail (`jchin@mydomain.com`, par exemple). Vous pouvez vérifier le nom d'utilisateur principal (UPN, User Principal Name) dans l'Éditeur ASDI (Active Directory Service Interfaces Editor).

Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP

Active Directory est disponible en tant que source d'identité du serveur LDAP pour assurer la compatibilité descendante. Utilisez l'option Active Directory (authentification Windows intégrée) pour une installation nécessitant moins d'entrées. La source d'identité du serveur OpenLDAP est disponible pour les environnements qui utilisent OpenLDAP.

Si vous configurez une source d'identité OpenLDAP, consultez l'article 2064977 de la base de connaissances VMware pour connnaître les conditions préalables supplémentaires.

Tableau 2-3. Active Directory en tant que serveur LDAP et paramètres OpenLDAP

Champ	Description
Nom	Nom de la source d'identité.
Nom de domaine (DN) de base des utilisateurs	Nom unique de base pour les utilisateurs.
Nom de domaine	Nom de domaine complet du domaine, par exemple, exemple.com. N'entrez pas une adresse IP dans ce champ.
Alias du domaine	Pour les sources d'identité Active Directory, le nom NetBIOS du domaine. Ajoutez le nom NetBIOS du domaine Active Directory en tant qu'alias de la source d'identité si vous utilisez les authentifications SSPI. Pour les sources d'identité OpenLDAP, le nom du domaine en lettres majuscules est ajouté si vous ne spécifiez pas d'alias.
DN de base des groupes	Nom unique de base pour les groupes.
URL du serveur principal	Serveur LDAP du contrôleur de domaine principale du domaine. Utilisez le format suivant : ldap://hostname:port ou ldaps://hostname:port. Le port est généralement 389 pour ldap: connections et 636 pour ldaps: connections. Pour les déploiements de contrôleurs multi-domaines Active Directory, le port est généralement 3268 pour ldap: connections et 3269 pour ldaps: connections. Un certificat qui établit la confiance du point terminal LDAP du serveur Active Directory est requis lorsque vous utilisez ldaps:// dans l'URL LDAP principale ou secondaire.
URL secondaire du serveur	Adresse du serveur LDAP d'un contrôleur de domaine secondaire utilisé pour le basculement.
Choisir un certificat	Si vous souhaitez utiliser LDAPS avec la source d'identité de votre serveur LDAP Active Directory et OpenLDAP, le bouton Choisir un certificat devient disponible une fois que vous avez tapé **`ldaps://`** dans le champ d'URL. Aucune URL secondaire n'est requise.
Nom d'utilisateur	ID d'un utilisateur du domaine qui dispose au minimum d'un accès en lecture seule au nom de domaine (DN) de base pour les utilisateurs et les groupes.
Mot de passe	Mot de passe de l'utilisateur spécifié par Nom d'utilisateur.

Modifier une source d'identité de vCenter Single Sign-On

Les utilisateurs vSphere sont définis dans une source d'identité. Vous pouvez modifier les détails d'une source d'identité associée à vCenter Single Sign-On.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur l'onglet **Sources d'identité**.

5 Cliquez avec le bouton droit sur la source d'identité dans le tableau et sélectionnez **Modifier la source d'identité**.

6 Modifiez les paramètres de source d'identité. Les options disponibles dépendent du type de source d'identité sélectionné.

Option	Description
Active Directory (authentification Windows intégrée)	Utilisez cette option pour les mises en œuvre Active Directory natives. Si vous souhaitez utiliser cette option, la machine sur laquelle le service vCenter Single Sign-On s'exécute doit se trouver dans un domaine Active Directory. Reportez-vous à « Paramètres de source d'identité Active Directory », page 33.
Active Directory comme serveur LDAP	Cette option est disponible à des fins de compatibilité descendante. Elle nécessite la spécification du contrôleur de domaine et d'autres informations. Reportez-vous à « Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP », page 35.
OpenLDAP	Utilisez cette option pour une source d'identité OpenLDAP. Reportez-vous à « Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP », page 35.
LocalOS	Utilisez cette option pour ajouter le système d'exploitation local comme source d'identité. Le système vous demande uniquement le nom du système d'exploitation. Si vous sélectionnez cette option, tous les utilisateurs sur la machine spécifiée sont visibles par vCenter Single Sign-On, même si ces utilisateurs ne font pas partie d'un autre domaine.

7 Cliquez sur **Tester la connexion** pour vous assurer que vous pouvez vous connecter à la source d'identité.

8 Cliquez sur **OK**.

Supprimer une source d'identité vCenter Single Sign-On

Vous pouvez supprimer une source d'identité de la liste des sources d'identité enregistrées. Lorsque vous le faites, les utilisateurs de cette source d'identité ne peuvent plus s'authentifier auprès de vCenter Single Sign-On.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Dans l'onglet **Sources d'identité**, sélectionnez une source d'identité et cliquez sur l'icône **Supprimer une source d'identité**.

5 Cliquez sur **Oui** lorsque vous êtes invité à confirmer.

Utiliser vCenter Single Sign-On avec l'authentification de session Windows

Vous pouvez utiliser vCenter Single Sign-On avec l'authentification de session Windows (SSPI). Vous devez lier Platform Services Controller à un domaine Active Directory avant de pouvoir utiliser SSPI.

L'utilisation de SSPI accélère la procédure d'ouverture de session pour l'utilisateur qui est actuellement connecté à une machine.

Prérequis

- Lier le dispositif Platform Services Controller ou la machine Windows sur laquelle Platform Services Controller est exécuté à un domaine Active Directory. Reportez-vous à « Ajouter un dispositif Platform Services Controller à un domaine Active Directory », page 20.
- Vérifiez que le domaine est correctement configuré. Reportez-vous à l'article 2064250 de la base de connaissances VMware.

Procédure

1 Naviguer à la page de connexion de vSphere Web Client.

2 Cochez la case **Utiliser l'authentification de session Windows**.

3 Connectez-vous à l'aide du nom d'utilisateur et du mot de passe Active Directory.

- Si le domaine Active Directory est la source d'identité par défaut, ouvrez une session avec votre nom d'utilisateur, par exemple jlee.
- Sinon, incluez le nom de domaine, par exemple jlee@example.com.

Authentification à deux facteurs de vCenter Server

vCenter Single Sign-On vous permet de vous authentifier comme utilisateur d'une source d'identité connue de vCenter Single Sign-On, ou à l'aide de l'authentification de session Windows. À partir de vSphere 6.0 Update 2, vous pouvez également vous authentifier en utilisant une carte à puce (Carte d'accès commun ou CAC basée sur UPN), ou en utilisant un jeton RSA SecurID.

Méthodes d'authentification à deux facteurs

Les méthodes d'authentification à deux facteurs sont souvent requises par les agences gouvernementales ou les grandes entreprises.

Authentification par carte à puce

L'authentification par carte à puce permet un accès uniquement aux utilisateurs qui attachent une carte physique au lecteur USB de l'ordinateur auquel ils se connectent. L'authentification par carte d'accès commun (CAC, Common Access Card) en est un exemple.

L'administrateur peut déployer la PKI afin que les certificats de la carte à puce soient les seuls certificats clients émis par l'autorité de certification. Pour de tels déploiements, seuls les certificats de la carte à puce sont présentés à l'utilisateur. L'utilisateur sélectionne un certificat et est invité à entrer un code PIN. Seuls les utilisateurs disposant de la carte physique et du code PIN correspondant au certificat peuvent se connecter.

Authentification RSA SecurID

Pour l'authentification RSA SecurID, votre environnement doit inclure une instance de RSA Authentication Manager correctement configurée. Si Platform Services Controller est configuré pour pointer vers le serveur RSA et que l'authentification RSA SecurID est activée, les utilisateurs peuvent se connecter avec leur nom d'utilisateur et leur jeton.

Pour plus de détails, reportez-vous aux deux articles du blog vSphere Blog relatifs à la configuration de RSA SecurID.

Remarque vCenter Single Sign-On prend uniquement en charge l'authentification SecurID native. Il ne prend pas en charge l'authentification RADIUS.

Spécification d'une méthode d'authentification autre que la méthode par défaut

Les administrateurs peuvent configurer une méthode d'authentification autre que la méthode par défaut à partir de l'interface Web Platform Services Controller ou en utilisant le script `sso-config`.

- Pour l'authentification par carte à puce, vous pouvez réaliser la configuration vCenter Single Sign-On à partir de l'interface Web Platform Services Controller ou à l'aide de `sso-config`. La configuration inclut l'activation de l'authentification par carte à puce et la configuration des stratégies de révocation du certificat.
- Pour RSA SecurID, utilisez le script `sso-config` pour configurer RSA Authentication Manager pour le domaine et pour activer l'authentification par jeton RSA. Vous ne pouvez pas configurer l'authentification RSA SecurID à partir de l'interface Web. Cependant, si vous activez l'authentification RSA SecurID, cette méthode d'authentification apparaît dans l'interface Web.

Combinaison des méthodes d'authentification

Vous pouvez activer ou désactiver chaque méthode d'authentification séparément à l'aide de `sso-config`. Conservez l'activation de l'authentification par nom d'utilisateur et par mot de passe pendant que vous testez une méthode d'authentification à deux facteurs puis, à l'issue du test, définissez une seule méthode d'authentification à activer.

Stratégie d'authentification par carte à puce

Une carte à puce est une petite carte en plastique dotée d'une puce de circuit intégré. De nombreuses agences gouvernementales et grandes entreprises utilisent des cartes à puce comme carte d'accès commun (CAC, Common Access Card) pour renforcer la sécurité de leurs systèmes et respecter les réglementations de sécurité. Une carte à puce est utilisée lorsque chaque machine inclut un lecteur de carte à puce. Les pilotes matériels qui gèrent la carte à puce sont généralement préinstallés.

Lorsque vous configurez l'authentification par carte à puce pour vCenter Single Sign-On, les utilisateurs qui se connectent à un système vCenter Server ou Platform Services Controller sont invités à s'authentifier avec une combinaison de carte à puce et de code PIN, de la façon suivante :

1. Lorsque l'utilisateur insère la carte à puce dans le lecteur de carte à puce, vCenter Single Sign-On lit les certificats présents sur la carte.
2. vCenter Single Sign-On invite l'utilisateur à sélectionner un certificat, puis à entrer le code PIN de ce certificat.
3. vCenter Single Sign-On vérifie si le certificat sur la carte à puce est connu et si le code PIN est correct. Si la vérification de révocation est activée, vCenter Single Sign-On vérifie également si le certificat est révoqué.
4. Si le certificat est connu et s'il n'est pas révoqué, l'utilisateur est authentifié et peut effectuer des tâches pour lesquelles il détient les autorisations.

Remarque Il convient généralement de maintenir activée l'authentification par nom et par mot de passe pendant les tests. Une fois les tests terminés, désactivez l'authentification par nom d'utilisateur et par mot de passe, puis activez l'authentification par carte à puce. Par la suite, vSphere Web Client autorise uniquement la connexion par carte à puce. Seuls les utilisateurs disposant de privilèges racines ou d'administrateur sur la machine peuvent réactiver l'authentification par nom d'utilisateur et par mot de passe en se connectant directement à Platform Services Controller.

Configuration et utilisation de l'authentification par carte à puce

Vous pouvez configurer votre environnement de manière à exiger une authentification par carte à puce lorsqu'un utilisateur se connecte à vCenter Server ou à l'instance associée de Platform Services Controller à partir de vSphere Web Client.

La configuration que vous choisissez pour l'authentification par carte à puce dépend de la version de vSphere que vous utilisez.

Version de vSphere	Procédure	Liens
6.0 Mise à jour 2 Versions ultérieures de vSphere 6.0	1 Configurez le serveur Tomcat. 2 Activez et configurez l'authentification par carte à puce.	Centre de documentation vSphere 6.0.
6.5 et versions ultérieures	1 Configurez le proxy inversé. 2 Activez et configurez l'authentification par carte à puce.	« Configurer le proxy inverse pour demander des certificats clients », page 40 « Utiliser la ligne de commande pour gérer l'authentification par carte à puce », page 41 « Utiliser l'interface Web de Platform Services Controller pour gérer l'authentification par carte à puce », page 44

Configurer le proxy inverse pour demander des certificats clients

Avant d'activer l'authentification par carte à puce, vous devez configurer le proxy inverse sur le système Platform Services Controller. Si votre environnement utilise une instance de Platform Services Controller intégrée, exécutez cette tâche sur le système dans lequel vCenter Server et Platform Services Controller sont exécutés.

La configuration du proxy inverse est une condition requise dans vSphere 6.5 et version ultérieure.

Prérequis

Copiez les certificats de l'autorité de certification dans le système Platform Services Controller.

Procédure

1 Connectez-vous à Platform Services Controller.

SE	Description
Dispositif	Connectez-vous à l'interpréteur de commande du dispositif en tant qu'utilisateur racine.
Windows	Connectez-vous à une invite de commandes Windows en tant qu'utilisateur administrateur.

2 Créez un magasin d'autorités de certification de client approuvé.

Ce magasin contient les certificats approuvés de l'autorité de certification émettrice pour le certificat client. Dans le cas présent, le client est le navigateur à partir duquel le processus d'authentification par carte à puce invite l'utilisateur final à entrer des informations.

L'exemple suivant illustre la création d'un magasin de certificats sur le dispositif Platform Services Controller.

Pour un seul certificat :

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

Pour plusieurs certificats :

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

3 Sauvegardez le fichier `config.xml` qui inclut la définition du proxy inverse et ouvrez le fichier `config.xml` dans un éditeur.

SE	Description
Dispositif	`/etc/vmware-rhttpproxy/config.xml`
Windows	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml`

4 Apportez les modifications suivantes et enregistrez le fichier.

```
<http>
<maxConnections> 2048 </maxConnections>
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

Le fichier `config.xml` inclut ces éléments, mais ils sont mis en commentaire. Annulez la mise en commentaire des lignes concernées dans le nœud `<http>` et mettez à jour `<clientCAListFile>`.

5 Redémarrez le service.

SE	Description
Dispositif	`service vmware-rhttpproxy restart`
Windows	Redémarrez le système d'exploitation ou redémarrez l'instance de VMware HTTP Reverse Proxy à partir de Service Manager.

Utiliser la ligne de commande pour gérer l'authentification par carte à puce

Vous pouvez employer l'utilitaire `sso-config` pour gérer l'authentification par carte à puce depuis la ligne de commande. L'utilitaire prend en charge toutes les tâches de configuration des cartes à puce.

La configuration des types d'authentification et des paramètres de révocation pris en charge est stockée dans VMware Directory Service et est répliquée dans toutes les instances de Platform Services Controller d'un domaine vCenter Single Sign-On.

Si l'authentification par nom d'utilisateur et mot de passe est désactivée et si un problème survient avec l'authentification par carte à puce, les utilisateurs ne peuvent pas se connecter. Dans ce cas, un utilisateur racine ou administrateur peut activer l'authentification par nom d'utilisateur et mot de passe dans la ligne de commande de Platform Services Controller. La commande suivante active l'authentification par nom d'utilisateur et mot de passe :

SE	Commande
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` Si vous utilisez le locataire par défaut, utilisez vsphere.local comme nom de locataire.
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` Si vous utilisez le locataire par défaut, utilisez vsphere.local comme nom de locataire.

Si vous utilisez OCSP pour une vérification de la révocation, vous pouvez vous servir de l'OCSP spécifié dans l'extension AIA du certificat de carte à puce. Vous pouvez également remplacer la valeur par défaut et configurer un ou plusieurs répondeurs OCSP de remplacement. Par exemple, vous pouvez configurer des répondeurs OCSP qui sont locaux par rapport au site vCenter Single Sign-On pour traiter la demande de vérification de révocation.

Remarque Si OCSP n'est pas défini dans votre certificat, activez plutôt la liste de révocation de certificats (CRL).

Prérequis

- Vérifiez que votre environnement utilise Platform Services Controller version 6.5 et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Platform Services Controller version 6.0 Update 2 prend en charge l'authentification par carte à puce, mais la procédure de configuration est différente.
- Vérifiez qu'une infrastructure à clé publique (PKI, Public Key Infrastructure) d'entreprise est configurée dans votre environnement et que les certificats répondent aux exigences suivantes :
  - Un nom d'utilisateur principal (UPN, User Principal Name) doit correspondre à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).
  - Le certificat doit spécifier l'authentification client dans la stratégie d'application ou le champ Utilisation avancée de la clé, sinon le navigateur n'affiche pas le certificat.
- Vérifiez que le certificat de l'interface Web Platform Services Controller est approuvé par la station de travail de l'utilisateur final. Sinon, le navigateur ne procédera pas à l'authentification.
- Ajoutez une source d'identité Active Directory à vCenter Single Sign-On.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent ensuite effectuer des tâches de gestion, car ils sont en mesure de s'authentifier et disposent de privilèges d'administrateur vCenter Server.

  Remarque L'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, ne peut pas effectuer une authentification par carte à puce.

- Configurez le proxy inverse et redémarrez la machine physique ou virtuelle. Reportez-vous à « Configurer le proxy inverse pour demander des certificats clients », page 40.

Procédure

1 Obtenez les certificats et copiez-les dans un dossier que l'utilitaire `sso-config` peut voir.

Option	Description
Windows	Connectez-vous à l'installation Windows de Platform Services Controller et utilisez WinSCP ou un utilitaire similaire pour copier les fichiers.

Dispositif	a Connectez-vous à la console du dispositif, soit directement soit à l'aide de SSH.
	b Activez l'interpréteur de commande du dispositif de la façon suivante.
	`shell`
	`chsh -s "/bin/bash" root`
	c Utilisez WinSCP ou un utilitaire similaire pour copier les certificats dans le dossier `/usr/lib/vmware-sso/vmware-sts/conf` dans Platform Services Controller.
	d Vous pouvez éventuellement désactiver l'interpréteur de commande du dispositif de la façon suivante.
	`chsh -s "bin/appliancesh" root`

2 Pour activer l'authentification par carte à puce pour VMware Directory Service (vmdir), exécutez la commande suivante.

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts first_trusted_cert.cer,
second_trusted_cert.cer  -t tenant
```

Par exemple :

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts MySmartCA1.cer,
MySmartCA2.cer  -t vsphere.local
```

3 Pour désactiver toutes les autres méthodes d'authentification, exécutez les commandes suivantes.

```
sso-config.[bat|sh] -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 (Facultatif) Pour définir une liste blanche des stratégies de certificat, exécutez la commande suivante.

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

Pour spécifier plusieurs stratégies, séparez-les par une commande, par exemple :

```
sso-config.bat -set_authn_policy -certPolicies
2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

Cette liste blanche spécifie les ID objet des stratégies autorisées dans l'extension de stratégie de certificat du certificat. Un certificat X509 peut posséder une extension de stratégie de certificat.

5 (Facultatif) Activez et configurez la vérification de révocation à l'aide d'OCSP.

a Activez la vérification de révocation à l'aide d'OCSP.

```
sso-config.[bat|sh]  -set_authn_policy -t tenantName  -useOcsp true
```

b Si le lien du répondeur OCSP n'est pas fourni via l'extension AIA des certificats, fournissez l'URL du répondeur OCSP de remplacement et le certificat de l'autorité OCSP.

L'OCSP de remplacement est configuré par site PSC. Vous pouvez spécifier plusieurs répondeurs OCSP de remplacement pour votre site vCenter Single Sign-On pour permettre le basculement.

```
sso-config.[bat|sh] -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl
http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

Remarque La configuration est appliquée au site vCenter Single Sign-On actuel par défaut. Spécifiez le paramètre `siteID` uniquement si vous configurez un OCSP de remplacement pour d'autres sites vCenter Single Sign-On.

Inspirez-vous de l'exemple suivant.

```
 .sso-config.[bat|sh] -t vsphere.local -add_alt_ocsp -ocspUrl
http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -
ocspSigningCert ./DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP reponder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c Pour afficher les paramètres du répondeur OCSP de remplacement, exécutez cette commande.

```
sso-config.[bat|sh] -t tenantName -get_alt_ocsp]
```

d Pour supprimer les paramètres du répondeur OCSP de remplacement, exécutez cette commande.

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 (Facultatif) Pour répertorier les informations de configuration, exécutez la commande suivante.

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

Utiliser l'interface Web de Platform Services Controller pour gérer l'authentification par carte à puce

Vous pouvez activer et désactiver l'authentification par carte à puce, personnaliser la page de connexion, puis configurer la stratégie de révocation à partir de l'interface Web de Platform Services Controller.

Si l'authentification par carte à puce est activée et que les autres méthodes d'authentification sont désactivées, les utilisateurs doivent se connecter en utilisant l'authentification par carte à puce.

Si l'authentification par nom d'utilisateur et mot de passe est désactivée et si un problème survient avec l'authentification par carte à puce, les utilisateurs ne peuvent pas se connecter. Dans ce cas, un utilisateur racine ou administrateur peut activer l'authentification par nom d'utilisateur et mot de passe dans la ligne de commande de Platform Services Controller. La commande suivante active l'authentification par nom d'utilisateur et mot de passe :

SE	Commande
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` Si vous utilisez le locataire par défaut, utilisez vsphere.local comme nom de locataire.
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` Si vous utilisez le locataire par défaut, utilisez vsphere.local comme nom de locataire.

Prérequis

- Vérifiez que votre environnement utilise Platform Services Controller version 6.5 et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Platform Services Controller version 6.0 Update 2 prend en charge l'authentification par carte à puce, mais la procédure de configuration est différente.
- Vérifiez qu'une infrastructure à clé publique (PKI, Public Key Infrastructure) d'entreprise est configurée dans votre environnement et que les certificats répondent aux exigences suivantes :
  - Un nom d'utilisateur principal (UPN, User Principal Name) doit correspondre à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).
  - Le certificat doit spécifier l'authentification client dans la stratégie d'application ou le champ Utilisation avancée de la clé, sinon le navigateur n'affiche pas le certificat.
- Vérifiez que le certificat de l'interface Web Platform Services Controller est approuvé par la station de travail de l'utilisateur final. Sinon, le navigateur ne procédera pas à l'authentification.
- Ajoutez une source d'identité Active Directory à vCenter Single Sign-On.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent ensuite effectuer des tâches de gestion, car ils sont en mesure de s'authentifier et disposent de privilèges d'administrateur vCenter Server.

  Remarque L'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, ne peut pas effectuer une authentification par carte à puce.

- Configurez le proxy inverse et redémarrez la machine physique ou virtuelle. Reportez-vous à « Configurer le proxy inverse pour demander des certificats clients », page 40.

Procédure

1 Obtenez les certificats et copiez-les dans un dossier que l'utilitaire `sso-config` peut voir.

Option	Description
Windows	Connectez-vous à l'installation Windows de Platform Services Controller et utilisez WinSCP ou un utilitaire similaire pour copier les fichiers.

Dispositif	a Connectez-vous à la console du dispositif, soit directement soit à l'aide de SSH.
	b Activez l'interpréteur de commande du dispositif de la façon suivante.
	`shell`
	`chsh -s "/bin/bash" root`
	`csh -s "bin/appliance/sh" root`
	c Utilisez WinSCP ou un utilitaire similaire pour copier les certificats dans le dossier `/usr/lib/vmware-sso/vmware-sts/conf` dans Platform Services Controller.
	d Vous pouvez éventuellement désactiver l'interpréteur de commande du dispositif de la façon suivante.
	`chsh -s "bin/appliancesh" root`

2 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	**`https://`*`vc_hostname_or_IP`*`/vsphere-client`**
Platform Services Controller	**`https://`*`psc_hostname_or_IP`*`/psc`** Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

3 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

4 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

5 Cliquez sur **Configuration de la carte à puce**, puis sélectionnez l'onglet **Certificats d'autorité de certification approuvés**.

6 Pour ajouter un ou plusieurs certificats approuvés, cliquez sur **Ajouter un certificat**, cliquez sur **Parcourir**, sélectionnez tous les certificats des autorités de certification approuvées, puis cliquez sur **OK**.

7 Pour spécifier la configuration de l'authentification, cliquez sur **Modifier** en regard de **Configuration de l'authentification**, puis sélectionnez des méthodes d'authentification ou annulez cette sélection.

Vous ne pouvez ni activer ni désactiver l'authentification RSA SecurID à partir de cette interface Web. Cependant, si RSA SecurID a été activé depuis la ligne de commande, l'état s'affiche dans l'interface Web.

Suivant

Votre environnement peut nécessiter une configuration OCSP améliorée.

- Si votre réponse OCSP est émise par une autorité de certification différente de l'autorité de certification de signature de la carte à puce, fournissez le certificat de l'autorité de certification de signature OCSP.
- Vous pouvez configurer un ou plusieurs répondeurs OCSP locaux pour chaque site Platform Services Controller dans un déploiement à sites multiples. Vous pouvez configurer ces répondeurs OCSP de remplacement à l'aide de l'interface de ligne de commande. Reportez-vous à « Utiliser la ligne de commande pour gérer l'authentification par carte à puce », page 41.

Définir les stratégies de révocation pour l'authentification par carte à puce

Vous pouvez personnaliser la vérification de la révocation du certificat, et vous pouvez spécifier le ou les emplacements dans lesquels vCenter Single Sign-On doit rechercher des informations sur les certificats révoqués.

Vous pouvez personnaliser le comportement à l'aide de l'interface Web de Platform Services Controller ou en utilisant le script `sso-config`. Les paramètres que vous sélectionnez dépendent en partie de l'étendue de la prise en charge de l'autorité de certification.

- Si la vérification de la révocation est désactivée, vCenter Single Sign-On ignore tous les paramètres CRL ou OCSP. vCenter Single Sign-On ne réalise aucun contrôle sur les certificats.
- Si la vérification de la révocation est activée, la configuration recommandée dépend de la configuration de la PKI.

  OCSP uniquement — Si l'autorité de certification émettrice prend en charge un répondeur OCSP, activez **OCSP** et désactivez **CRL comme basculement pour OCSP**.

  CRL uniquement — Si l'autorité de certification émettrice ne prend pas en charge OSCP, activez la **vérification CRL** et désactivez la **vérification OSCP**.

  OSCP et CRL — Si l'autorité de certification émettrice prend en charge un répondeur OCSP et une CRL, vCenter Single Sign-On vérifie d'abord le répondeur OCSP. Si le répondeur renvoie un état inconnu ou n'est pas disponible, vCenter Single Sign-On vérifie la CRL. Dans ce cas, activez la **vérification OCSP** et la **vérification CRL**, et activez **CRL comme basculement pour OCSP**.

- Si la vérification de la révocation est activée, les utilisateurs avancés peuvent spécifier les paramètres supplémentaires suivants.

  URL OSCP — Par défaut, vCenter Single Sign-On vérifie l'emplacement du répondeur OCSP qui est défini dans le certificat en cours de validation. Vous pouvez spécifier explicitement l'emplacement si l'extension de l'accès aux informations de l'autorité est absente du certificat ou si vous souhaitez la remplacer.

  Utiliser la liste de révocation des certificats — Par défaut, vCenter Single Sign-On vérifie l'emplacement de la liste de révocation des certificats qui est défini dans le certificat en cours de validation. Désactivez cette option si l'extension du point de distribution CRL est absente du certificat ou si vous souhaitez remplacer la valeur par défaut.

  Emplacement de la liste de révocation des certificats — Utilisez cette propriété si vous désactivez **Utiliser la liste de révocation des certificats** et que vous souhaitez spécifier un emplacement (fichier ou URL HTTP) où se trouve la liste de révocation de certificats.

Vous pouvez limiter davantage les certificats que vCenter Single Sign-On accepte en ajoutant une stratégie de certificat.

Prérequis

- Vérifiez que votre environnement utilise Platform Services Controller version 6.5 et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Platform Services Controller version 6.0 Update 2 prend en charge l'authentification par carte à puce, mais la procédure de configuration est différente.
- Vérifiez qu'une infrastructure à clé publique (PKI, Public Key Infrastructure) d'entreprise est configurée dans votre environnement et que les certificats répondent aux exigences suivantes :
  - Un nom d'utilisateur principal (UPN, User Principal Name) doit correspondre à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).
  - Le certificat doit spécifier l'authentification client dans la stratégie d'application ou le champ Utilisation avancée de la clé, sinon le navigateur n'affiche pas le certificat.
- Vérifiez que le certificat de l'interface Web Platform Services Controller est approuvé par la station de travail de l'utilisateur final. Sinon, le navigateur ne procédera pas à l'authentification.
- Ajoutez une source d'identité Active Directory à vCenter Single Sign-On.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent ensuite effectuer des tâches de gestion, car ils sont en mesure de s'authentifier et disposent de privilèges d'administrateur vCenter Server.

Remarque L'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, ne peut pas effectuer une authentification par carte à puce.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur **Paramètres de révocation de certificats**, et activez ou désactivez la vérification de la révocation.

5 Si des stratégies de certificat sont en vigueur dans votre environnement, vous pouvez ajouter une stratégie dans le volet **Stratégies de certificat acceptées**.

Configurer l'authentification RSA SecurID

Vous pouvez configurer votre environnement pour exiger que les utilisateurs se connectent avec un jeton RSA SecurID plutôt qu'avec un mot de passe. La configuration de SecurID est uniquement prise en charge à partir de la ligne de commande.

Pour plus de détails, reportez-vous aux deux articles du blog vSphere Blog relatifs à la configuration de RSA SecurID.

Remarque RSA Authentication Manager exige que l'ID d'utilisateur soit un identifiant unique qui utilise de 1 à 255 caractères ASCII. Les caractères esperluette (&), pour cent (%), supérieur à (>), inférieur à (<) et guillemet simple (`) ne sont pas autorisés.

Prérequis

- Vérifiez que votre environnement utilise Platform Services Controller version 6.5 et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Platform Services Controller version 6.0 Update 2 prend en charge l'authentification par carte à puce, mais la procédure de configuration est différente.
- Vérifiez que votre environnement dispose d'une instance de RSA Authentication Manager correctement configurée et que les utilisateurs disposent de jetons RSA. RSA Authentication Manager version 8.0 ou version ultérieure est requis.
- Vérifiez que la source d'identité qui est utilisée par RSA Manager a été ajoutée à vCenter Single Sign-On. Reportez-vous à « Ajouter une source d'identité de vCenter Single Sign-On », page 32.
- Vérifiez que le système RSA Authentication Manager peut résoudre le nom d'hôte de Platform Services Controller et que le système Platform Services Controller peut résoudre le nom d'hôte de RSA Authentication Manager.
- Exportez le fichier `sdconf.rec` depuis RSA Manager en sélectionnant **Accès > Agents d'authentification > Générer le fichier de configuration**. Décompressez le fichier `AM_Config.zip` résultant pour trouver le fichier `sdconf.rec`.
- Copiez le fichier `sdconf.rec` sur le nœud de Platform Services Controller.

Procédure

1 Changez le répertoire dans lequel le script `sso-config` réside.

Option	Description
Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services`
Dispositif	`/opt/vmware/bin`

2 Pour activer l'authentification RSA SecurID, exécutez la commande suivante.

```
sso-config.[sh|bat]  -t tenantName  -set_authn_policy -securIDAuthn true
```

tenantName est le nom du domaine vCenter Single Sign-On, vsphere.local par défaut.

3 (Facultatif) Pour désactiver les autres méthodes d'authentification, exécutez la commande suivante.

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t vsphere.local
```

4 Pour configurer l'environnement afin que le locataire du site actuel utilise le site RSA, exécutez la commande suivante.

```
sso-config.[sh|bat] -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-sdConfFile Path]
```

Par exemple :

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

Vous pouvez spécifier les options suivantes :

Option	Description
siteID	ID de site Platform Services Controller facultatif. Platform Services Controller prend en charge une instance de RSA Authentication Manager ou un cluster par site. Si vous ne spécifiez pas explicitement cette option, la configuration RSA vaut pour le site actuel Platform Services Controller. Utilisez cette option uniquement lorsque vous ajoutez un site différent.
agentName	Défini dans RSA Authentication Manager.
sdConfFile	Copie du fichier `sdconf.rec` qui est téléchargée à partir de RSA Manager et inclut des informations de configuration pour RSA Manager, telles que l'adresse IP.

5 (Facultatif) Pour changer les valeurs par défaut de la configuration du locataire, exécutez la commande suivante.

```
sso-config.[sh|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size] [-maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList Alg1,Alg2,...]
```

La valeur par défaut est généralement appropriée, par exemple :

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 (Facultatif) Si votre source d'identité n'utilise pas le nom d'utilisateur principal comme ID d'utilisateur, configurez l'attribut userID de la source d'identité.

L'attribut userID détermine l'attribut LDAP qui doit être utilisé comme l'userID RSA.

```
sso-config.[sh|bat] -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Location]
```

Par exemple :

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
```

7 Pour afficher les paramètres actuels, exécutez la commande suivante.

```
sso-config.sh -t tenantName -get_rsa_config
```

Si l'authentification par nom d'utilisateur et par mot de passe est désactivée et que l'authentification par jeton SecurID est activée, les utilisateurs doivent se connecter avec leur nom d'utilisateur et le jeton SecurID. La connexion avec le nom d'utilisateur et le mot de passe n'est plus possible.

Gérer la page de connexion

À partir de vSphere 6.0 Update 2, vous pouvez inclure une page de connexion dans votre environnement. Vous pouvez activer et désactiver la page de connexion, et vous pouvez exiger que les utilisateurs cliquent sur une case à cocher de consentement explicite.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Cliquez sur **Single Sign-On**, sur **Configuration**, puis sur l'onglet **Page de connexion**.

4 Cliquez sur **Modifier** et configurez la page de connexion.

Option	Description
État	Cochez la case **Activé** pour activer la page de connexion. Vous ne pouvez pas modifier la page de connexion si vous ne cochez pas cette case.
Consentement explicite	Cochez la case **Consentement explicite** pour exiger que l'utilisateur coche une case avant de se connecter. Vous pouvez également afficher un message sans case à cocher.
Titre	Titre de la page. Par défaut, le texte de la page de connexion est `I agree to the`. Vous pouvez ajouter des informations à ce message, par exemple `Terms and Conditions`.
Message	Message affiché pour l'utilisateur lorsqu'il clique sur la page, par exemple, le texte des conditions générales. Le message est requis si vous utilisez le consentement explicite.

Utilisation de vCenter Single Sign-On comme fournisseur d'identité pour un autre fournisseur de services

vSphere Web Client est automatiquement enregistré en tant que fournisseur de services SAML 2.0 approuvé auprès de vCenter Single Sign-On. Vous pouvez ajouter d'autres fournisseurs de services approuvés à une fédération d'identités dans laquelle vCenter Single Sign-On agit en tant que fournisseur d'identité SAML. Les fournisseurs de services doivent être conformes au protocole SAML 2.0. Une fois la fédération configurée, le fournisseur de services octroie l'accès à un utilisateur si ce dernier peut s'authentifier auprès de vCenter Single Sign-On.

Remarque vCenter Single Sign-On peut être le fournisseur d'identité pour d'autres fournisseurs de services.vCenter Single Sign-On ne peut pas être un fournisseur de services utilisant un autre fournisseur d'identité.

Un fournisseur de services SAML enregistré peut octroyer l'accès à un utilisateur qui dispose déjà d'une session en direct, c'est-à-dire qui est connecté au fournisseur d'identité. Par exemple, vRealize Automation 7.0 et versions ultérieures prend en charge vCenter Single Sign-On comme fournisseur d'identité. Vous pouvez configurer une fédération à partir de vCenter Single Sign-On et de vRealize Automation. Ensuite, vCenter Single Sign-On peut réaliser l'authentification lorsque vous vous connectez à vRealize Automation.

Pour joindre un fournisseur de services SAML à la fédération d'identités, vous devez configurer une relation de confiance entre le fournisseur de services et le fournisseur d'identité grâce à l'échange de métadonnées SAML.

Vous devez effectuer des tâches d'intégration pour vCenter Single Sign-On et le service qui utilise vCenter Single Sign-On.

1 Exportez des métadonnées de fournisseur d'identité vers un fichier, puis importez-les dans le fournisseur de services.

2 Exportez des métadonnées de fournisseur de services et importez-les dans le fournisseur d'identité.

Vous pouvez utiliser l'interface de vSphere Web Client dans vCenter Single Sign-On pour exporter les métadonnées de fournisseur d'identité et pour les importer à partir du fournisseur de services. Si vous faites appel à vRealize Automation en tant que fournisseur de services, consultez la documentation vRealize Automation pour obtenir plus de détails sur l'exportation des métadonnées du fournisseur de services et l'importation des métadonnées du fournisseur d'identité.

Remarque Le service doit entièrement prendre en charge la norme SAML 2.0, sinon l'intégration ne fonctionne pas.

Joindre un fournisseur de services SAML à la fédération des identités

Vous ajoutez un fournisseur de services SAML à vCenter Single Sign-On, puis ajoutez vCenter Single Sign-On comme fournisseur d'identité à ce service. Ensuite, lorsque les utilisateurs se connectent au fournisseur de services, ce dernier authentifie ces utilisateurs avec vCenter Single Sign-On.

Prérequis

Le service cible doit intégralement prendre en charge la norme SAML 2.0 et les métadonnées du fournisseur de services doivent comporter l'élément `SPSSODescriptor`.

Si les métadonnées ne suivent pas strictement le schéma de métadonnées SAML 2.0, vous devrez éventuellement les modifier avant de les importer. Par exemple, si vous utilisez un fournisseur de services SAML de fédération Active Directory (ADFS, Active Directory Federation Services), vous devez modifier les métadonnées avant de pouvoir les importer. Supprimez les éléments non standard suivants :

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

Procédure

1 Exportez les métadonnées du fournisseur de services dans un fichier.

2 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

3 Importez les métadonnées du fournisseur de services dans vCenter Single Sign-On.

   a Sélectionnez l'onglet **Fournisseurs de service SAML**.

   b Dans la boîte de dialogue **Métadonnées de votre fournisseur de services SAML**, importez les métadonnées en copiant la chaîne XML ou en important un fichier.

4 Exportez les métadonnées du fournisseur d'identités de vCenter Single Sign-On.

   a Dans la zone de texte **Métadonnées pour votre fournisseur de services SAML**, cliquez sur **Télécharger**.

   b Spécifiez un emplacement du fichier.

5 Connectez-vous au fournisseur de services SAML (par exemple, VMware vRealize Automation 7.0) et suivez ses instructions pour ajouter les métadonnées vCenter Single Sign-On à ce fournisseur de service.

   Pour obtenir plus de détails sur l'importation des métadonnées dans ce produit, reportez-vous à la documentation de vRealize Automation.

STS (Security Token Service)

Le service d'émission de jeton de sécurité (STS) de vCenter Single Sign-On est un service Web qui émet, valide et renouvelle les jetons de sécurité.

Les utilisateurs présentent leurs informations d'identification principales à l'interface STS pour acquérir des jetons SAML. Les informations d'identification principales dépendent du type d'utilisateur.

Utilisateur Nom d'utilisateur et mot de passe disponibles dans une source d'identité vCenter Single Sign-On.

Utilisateur d'application Certificat valide.

STS authentifie l'utilisateur en fonction des informations d'identification principales et crée un jeton SAML contenant les attributs de l'utilisateur. STS signe le jeton SAML avec son certificat de signature STS et attribue le jeton à l'utilisateur. Par défaut, le certificat de signature STS est généré par VMCA. Vous pouvez remplacer le certificat de signature STS par défaut à partir de vSphere Web Client. Ne remplacez pas le certificat de signature STS à moins que la stratégie de sécurité de votre entreprise nécessite le remplacement de tous les certificats.

Une fois qu'un utilisateur dispose d'un jeton SAML, ce dernier est envoyé dans le cadre des demandes HTTP de l'utilisateur, éventuellement via divers proxies. Seul le destinataire prévu (le fournisseur de services) peut utiliser les informations du jeton SAML.

Actualiser le certificat STS

Le serveur vCenter Single Sign-On comprend un service de jetons de sécurité (STS). Le service de jetons de sécurité est un service Web qui émet, valide, et renouvelle les jetons de sécurité. Lorsque le certificat STS existant expire ou change, vous pouvez l'actualiser manuellement via vSphere Web Client.

Pour acquérir un jeton SAML, l'utilisateur présente les informations d'identification principales au serveur de jetons sécurisés (STS). Les informations d'identification principales dépendent du type d'utilisateur :

Utilisateur de solution Certificat valide

Autres utilisateurs Nom d'utilisateur et mot de passe disponibles dans une source d'identité vCenter Single Sign-On.

Le STS authentifie l'utilisateur à l'aide des informations d'identification principales et crée un jeton SAML contenant les attributs de l'utilisateur. Le service STS signe le jeton SAML avec son certificat de signature STS, puis attribue le jeton à un utilisateur. Par défaut, le certificat de signature STS est généré par VMCA.

Une fois qu'un utilisateur dispose d'un jeton SAML, ce dernier est envoyé dans le cadre des demandes HTTP de l'utilisateur, éventuellement via divers proxies. Seul le destinataire prévu (le fournisseur de services) peut utiliser les informations du jeton SAML.

Vous pouvez remplacer le certificat de signature STS existant dans vSphere Web Client, si votre stratégie d'entreprise l'exige ou si vous souhaitez mettre à jour un certificat qui a expiré.

Avertissement Ne remplacez pas le fichier qui réside dans le système de fichiers. Cette opération entraîne la survenue d'erreurs inattendues et difficiles à résoudre.

Remarque Après avoir remplacé le certificat, vous devez redémarrer le nœud afin de redémarrer le service vSphere Web Client et le service STS.

Prérequis

Copiez le certificat que vous venez d'ajouter au keystore Java à partir de Platform Services Controller vers votre poste de travail local.

Dispositif Platform Services Controller	*certificate_location*/keys/root-trust.jks Par exemple : /keys/root-trust.jks Par exemple : /root/newsts/keys/root-trust.jks
Installation Windows	*certificate_location*\root-trust.jks Par exemple : C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks

Procédure

1. Connectez-vous à vSphere Web Client en tant qu'administrator@vsphere.local ou un autre utilisateur disposant de privilèges d'administrateur de vCenter Single Sign-On.

   Les utilisateurs disposant de privilèges d'administrateur vCenter Single Sign-On appartiennent au groupe Administrateurs du domaine vCenter Single Sign-On local, vsphere.local par défaut.

2. Sélectionnez l'onglet **Certificats**, puis le sous-onglet **Signature STS** et cliquez sur l'icône **Ajouter un certificat de signature STS**.

3. Ajoutez le certificat.

   a. Cliquez sur **Parcourir** pour accéder au fichier JKS du magasin de clés qui contient le nouveau certificat, puis cliquez sur **Ouvrir**.

   b. Tapez le mot de passe lorsque vous y êtes invité.

   c. Cliquez sur le haut de la chaîne d'alias STS, puis cliquez sur **OK**.

   d. Retapez le mot de passe lorsque vous y êtes invité.

4. Cliquez sur **OK**.

5. Redémarrez le nœud Platform Services Controller pour démarrer le service STS et l'instance de vSphere Web Client.

   Le redémarrage est indispensable au fonctionnement correct de l'authentification.

Générer un nouveau certificat de signature STS sur le dispositif

Si vous souhaitez remplacer le certificat de signature de service de jeton de sécurité (STS) de vCenter Single Sign-On, vous devez générer un nouveau certificat et l'ajouter au magasin de clés Java. Cette procédure concerne le déploiement d'un dispositif intégré ou d'un dispositif Platform Services Controller externe.

Remarque Ce certificat est valable dix ans et n'est pas un certificat externe. Ne remplacez pas ce certificat à moins que la stratégie de sécurité de votre entreprise ne l'exige.

Reportez-vous à la section « Générer un nouveau certificat de signature STS dans une installation vCenter Windows », page 56 si vous exécutez une installation Windows de Platform Services Controller.

Procédure

1 Créez un répertoire de niveau supérieur pour contenir le nouveau certificat et vérifiez l'emplacement du répertoire.

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newst
```

2 Copiez le fichier `certool.cfg` dans un nouveau répertoire.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

3 Ouvrez votre copie du fichier `certool.cfg` et modifiez-la afin d'utiliser l'adresse IP locale et le nom d'hôte de Platform Services Controller.

Le pays doit être indiqué, à l'aide de deux caractères, comme le montre l'exemple suivant.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Générez la clé.

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/sts.key
--pubkey=/root/newsts/sts.pub
```

5 Générez le certificat.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --
privkey=/root/newsts/sts.key --config=/root/newsts/certool.cfg
```

6 Convertissez le certificat au format PK12.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key -
certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout pass:changeme
-out newsts.p12
```

7 Ajoutez le certificat au magasin de clés Java (JKS).

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype
pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore root-trust.jks -
deststoretype JKS -deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype JKS -
storepass testpassword -keypass testpassword -file /etc/vmware-sso/keys/ssoserverRoot.crt -
alias root-ca
```

8 Lorsque vous y êtes invité, entrez **Yes** pour accepter le placement du certificat dans le keystore.

Suivant

Vous pouvez à présent importer le nouveau certificat. Reportez-vous à « Actualiser le certificat STS », page 53.

Générer un nouveau certificat de signature STS dans une installation vCenter Windows

Pour remplacer le certificat de signature STS par défaut, vous devez d'abord générer un nouveau certificat et l'ajouter au keystore Java. Cette procédure explique les étapes dans une installation Windows.

Remarque Ce certificat est valable dix ans et n'est pas un certificat externe. Ne remplacez pas ce certificat à moins que la stratégie de sécurité de votre entreprise ne l'exige.

Si vous utilisez un dispositif virtuel, consultez « Générer un nouveau certificat de signature STS sur le dispositif », page 55.

Procédure

1 Créez un répertoire pour contenir le nouveau certificat.

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 Copiez le fichier `certool.cfg` et placez-le dans ce nouveau répertoire.

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```

3 Ouvrez votre copie du fichier `certool.cfg` et modifiez-la afin d'utiliser l'adresse IP locale et le nom d'hôte de Platform Services Controller.

La saisie d'un pays est obligatoire. Le nom de ce pays doit comporter deux caractères. Inspirez-vous de l'exemple suivant.

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 Générez la clé.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

5 Générez le certificat.

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

6 Convertissez le certificat au format PK12.

```
"C:\Program Files\VMware\vCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer -
inkey sts.key -certfile ..\ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -
out newsts.p12
```

7 Ajoutez le certificat au magasin de clés Java (JKS).

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore -srckeystore
newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore
root-trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importcert -keystore root-
trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -
file ..\ssoserverRoot.crt -alias root-ca
```

Suivant

Vous pouvez à présent importer le nouveau certificat. Reportez-vous à « Actualiser le certificat STS », page 53.

Déterminer la date d'expiration d'un certificat LDAPS SSL

Si vous sélectionnez une source d'identité LDAP et que vous décidez d'utiliser LDAPS, vous pouvez télécharger un certificat SSL pour le trafic LDAP. Les certificats SSL expirent après une durée de vie prédéfinie. Connaître la date d'expiration d'un certificat vous permet de remplacer ou de renouveler ce dernier avant cette date.

Les informations d'expiration des certificats s'affichent uniquement si vous utilisez un serveur Active Directory LDAP ou OpenLDAP, et que vous spécifiez une URL `ldaps://` pour le serveur. L'onglet Magasin d'approbations de sources d'identité reste vide pour les autres types de sources d'identité ou pour le trafic `ldap://`.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	**`https://vc_hostname_or_IP/vsphere-client`**
Platform Services Controller	**`https://psc_hostname_or_IP/psc`** Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur l'onglet **Certificats**, puis sur **Magasin d'approbations de sources d'identité**.

5 Recherchez le certificat et vérifiez la date d'expiration dans la zone de texte **Date de fin de validité**.

Vous verrez peut-être un avertissement en haut de l'onglet indiquant qu'un certificat est sur le point d'expirer.

Gestion des stratégies vCenter Single Sign-On

Les stratégies vCenter Single Sign-On permettent d'appliquer les règles de sécurité au sein de votre environnement. Vous pouvez consulter et modifier la stratégie de mot de passe, la stratégie de verrouillage et la stratégie des jetons par défaut de vCenter Single Sign-On.

Modifier la stratégie de mot de passe de vCenter Single Sign-On

La stratégie de mot de passe vCenter Single Sign-On régit le format et l'expiration des mots de passe utilisateur vCenter Single Sign-On. La stratégie de mot de passe s'applique uniquement aux utilisateurs inclus dans le domaine vCenter Single Sign-On (vsphere.local).

Par défaut, les mots de passe de vCenter Single Sign-On expirent après 90 jours. vSphere Web Client vous envoie un rappel lorsque votre mot de passe est sur le point d'expirer.

Remarque La stratégie de mot de passe s'applique uniquement aux comptes d'utilisateurs et non aux comptes système tels qu'administrator@vsphere.local.

Reportez-vous à « Changer le mot de passe de vCenter Single Sign-On », page 69.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur l'onglet **Politiques** et sélectionnez **Stratégies des mots de passe**.

5 Cliquez sur **Modifier**.

6 Modifiez les paramètres de la stratégie de mot de passe.

Option	Description
Description	Description de la stratégie de mot de passe.
Durée de vie maximale	Nombre maximal de jours de validité d'un mot de passe au terme duquel l'utilisateur doit le changer.
Restreindre la réutilisation	Nombre de mots de passe précédents qui ne peuvent pas être réutilisés. Par exemple, si vous tapez 6, l'utilisateur ne peut pas réutiliser l'un des six derniers mots de passe.
Longueur maximale	Nombre maximal de caractères autorisés dans le mot de passe.
Longueur minimale	Le nombre minimum de caractères requis dans le mot de passe. La longueur minimale ne doit pas être inférieure au minimum combiné des exigences de caractères alphabétiques, numériques et spéciaux.
Exigences de caractères	Nombre minimal de types de caractères différents requis dans le mot de passe. Vous pouvez spécifier le nombre de chaque type de caractère, comme suit : ■ Spéciaux : & # % ■ Alphabétiques : A b c D ■ Majuscules : A B C ■ Minuscules : a b c ■ Numériques : 1 2 3 Le nombre minimal de caractères alphabétiques ne doit pas être inférieur aux caractères combinés de lettres majuscules et minuscules. Dans vSphere 6.0 et versions ultérieures, les caractères non-ASCII sont pris en charge dans les mots de passe. Dans les versions précédentes de vCenter Single Sign-On, les caractères pris en charge sont plus limités.
Caractères identiques adjacents	Nombre maximal de caractères adjacents identiques autorisés dans le mot de passe. Par exemple, si vous entrez 1, le mot de passe suivant n'est pas autorisé : p@$$word. Le nombre doit être supérieur à 0.

7 Cliquez sur **OK**.

Modifier la stratégie de verrouillage de vCenter Single Sign-On

Une stratégie de verrouillage de vCenter Single Sign-On spécifie à quel moment le compte vCenter Single Sign-On d'un utilisateur est verrouillé si ce dernier tente de se connecter avec des informations d'identification incorrectes. Les administrateurs peuvent modifier la stratégie de verrouillage.

Si un utilisateur se connecte à vsphere.local à plusieurs reprises à l'aide d'un mot de passe incorrect, il est verrouillé. La stratégie de verrouillage permet aux administrateurs de spécifier le nombre maximal de tentatives de connexion infructueuses et de définir l'intervalle de temps entre deux échecs. La règle indique également le délai qui doit s'écouler avant que le compte soit automatiquement déverrouillé.

Remarque La stratégie de verrouillage s'applique aux comptes d'utilisateurs et non aux comptes système tels qu'administrator@vsphere.local.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur l'onglet **Règles** et sélectionnez **Règle de verrouillage**.

5 Cliquez sur **Modifier**.

6 Modifiez les paramètres.

Option	Description
Description	Description facultative de la stratégie de verrouillage.
Nombre maximal de tentatives de connexion échouées	Nombre maximal de tentatives de connexion infructueuses autorisées avant que le compte soit verrouillé.
Intervalle de temps entre deux échecs	Délai pendant lequel les échecs doivent se produire pour déclencher un verrouillage.
Délai de déverrouillage	Durée pendant laquelle le compte reste verrouillé. Si vous entrez 0, l'administrateur doit déverrouiller le compte de manière explicite.

7 Cliquez sur **OK**.

Modifier la stratégie des jetons de vCenter Single Sign-On

La stratégie des jetons de vCenter Single Sign-On spécifie les propriétés liées aux jetons telles que la tolérance d'horloge et le nombre de renouvellements. Vous pouvez modifier la stratégie des jetons pour garantir que la spécification du jeton répond aux normes de sécurité de votre entreprise.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

   Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Configuration**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Configuration**.

4 Cliquez sur l'onglet **Règles** et sélectionnez **Règle des jetons**.

   vSphere Web Client affiche les paramètres de configuration actuels. vCenter Single Sign-On utilise les paramètres par défaut, si vous ne les avez pas modifiés.

5 Modifiez les paramètres de configuration de la stratégie des jetons.

Option	Description
Tolérance de l'horloge	Différence de temps, en millisecondes, que vCenter Single Sign-On tolère entre l'horloge d'un client et l'horloge du contrôleur de domaine. Si la différence de temps est supérieure à la valeur spécifiée, vCenter Single Sign-On déclare que le jeton n'est pas valide.
Nombre maximum de renouvellements de jetons	Nombre maximal de fois qu'un jeton peut être renouvelé. Une fois le nombre maximal de tentatives de renouvellement atteint, un nouveau jeton de sécurité est nécessaire
Nombre maximum de délégations de jetons	Des jetons détenteurs de clé peuvent être délégués à des services de l'environnement vSphere. Un service qui utilise un jeton délégué s'exécute de la part du principal qui a fourni le jeton. Une demande de jeton spécifie une identité DelegateTo. La valeur de DelegateTo peut être un jeton de solution ou une référence à un jeton de solution. Cette valeur indique le nombre de fois qu'un jeton détenteur de clé peut être délégué.
Durée de vie maximale d'un jeton de support	Avec les jetons au porteur l'authentification repose sur la simple possession du jeton. Les jetons au porteur sont destinés à être utilisés pour une opération unique, à court terme. Un jeton au porteur ne vérifie ni l'identité de l'utilisateur ni l'entité qui envoie la demande. Cette valeur spécifie la durée de vie d'un jeton au porteur avant que celui-ci doive être réédité.
Durée de vie maximale d'un jeton de détenteur de clé	Avec les jetons détenteurs de clé, l'authentification repose sur les artéfacts de sécurité intégrés au jeton. Les jetons détenteurs de clé peuvent être utilisés pour la délégation. Un client peut obtenir un jeton détenteur de clé et le déléguer à une autre entité. Le jeton contient les demandes pour identifier l'expéditeur et le délégué. Dans l'environnement vSphere, un système vCenter Server obtient des jetons délégués de la part d'un utilisateur et les utilise pour effectuer des opérations. Cette valeur détermine la durée de vie d'un jeton détenteur de clé avant que celui-ci soit marqué comme non valide.

6 Cliquez sur **OK**.

Gestion des utilisateurs et des groupes vCenter Single Sign-On

Un utilisateur administrateur de vCenter Single Sign-On peut gérer des utilisateurs et des groupes du domaine vsphere.local dans vSphere Web Client.

L'utilisateur administrateur de vCenter Single Sign-On peut effectuer les tâches suivantes.

- Ajouter des utilisateurs vCenter Single Sign-On page 63

  Les utilisateurs répertoriés dans l'onglet **Utilisateurs** de vSphere Web Client sont internes à vCenter Single Sign-On et appartiennent au domaine vsphere.local. Ajoutez des utilisateurs à ce domaine dans l'une des interfaces de gestion de vCenter Single Sign-On.

- Désactiver et activer des utilisateurs de vCenter Single Sign-On page 64

  Lorsqu'un compte d'utilisateur vCenter Single Sign-On est désactivé, l'utilisateur ne peut pas se connecter au serveur vCenter Single Sign-On tant qu'un administrateur n'active pas le compte. Vous pouvez activer et désactiver des comptes dans l'une des interfaces de gestion de vCenter Single Sign-On.

- Supprimer un utilisateur vCenter Single Sign-On page 64

  Vous pouvez supprimer des utilisateurs qui sont dans le domaine vsphere.local dans l'interface de gestion de vCenter Single Sign-On. Vous ne pouvez pas supprimer des utilisateurs du système d'exploitation local ou d'un autre domaine dans l'interface de gestion de vCenter Single Sign-On.

- Modifier un utilisateur de vCenter Single Sign-On page 65

  Vous pouvez modifier le mot de passe ou d'autres informations d'un utilisateur vCenter Single Sign-On dans une interface de gestion de vCenter Single Sign-On. Vous ne pouvez pas renommer d'utilisateurs dans le domaine vsphere.local. Vous ne pouvez donc pas renommer administrator@vsphere.local.

- Ajouter un groupe vCenter Single Sign-On page 66

  L'onglet vCenter Single Sign-On **Groupes** affiche les groupes du domaine local, vsphere.local par défaut. Ajoutez des groupes si vous avez besoin d'un conteneur pour les membres de groupe (principaux).

- Ajouter des membres à un groupe vCenter Single Sign-On page 67

  Les membres d'un groupe vCenter Single Sign-On peuvent être des utilisateurs ou d'autres groupes issus d'une ou de plusieurs sources d'identité. Vous pouvez ajouter de nouveaux membres à partir de vSphere Web Client.

- Supprimer des membres d'un groupe vCenter Single Sign-On page 68

  Vous pouvez supprimer des membres d'un groupe vCenter Single Sign-On en utilisant vSphere Web Client ou l'interface web de Platform Services Controller. Lorsque vous supprimez un membre (utilisateur ou groupe) d'un groupe, vous ne devez pas supprimer le membre du système.

- Supprimer des utilisateurs de la solution vCenter Single Sign-On page 68

  vCenter Single Sign-On affiche les utilisateurs de solution. Un utilisateur de solution est une collection de services. Plusieurs utilisateurs de solution vCenter Server sont prédéfinis et s'authentifient auprès de vCenter Single Sign-On dans le cadre de l'installation. Dans les situations de dépannage, par exemple si une désinstallation ne s'effectue pas proprement, vous pouvez supprimer des utilisateurs de solution individuels de vSphere Web Client.

- Changer le mot de passe de vCenter Single Sign-On page 69

  Les utilisateurs du domaine local, vsphere.local par défaut, peuvent modifier leurs mots de passe vCenter Single Sign-On à partir d'une interface Web. Les utilisateurs se trouvant dans d'autres domaines changent leur mot de passe en suivant les règles du domaine concerné.

Ajouter des utilisateurs vCenter Single Sign-On

Les utilisateurs répertoriés dans l'onglet **Utilisateurs** de vSphere Web Client sont internes à vCenter Single Sign-On et appartiennent au domaine vsphere.local. Ajoutez des utilisateurs à ce domaine dans l'une des interfaces de gestion de vCenter Single Sign-On.

Vous pouvez sélectionner d'autres domaines et afficher des informations sur les utilisateurs de ces domaines, mais vous ne pouvez pas ajouter des utilisateurs aux autres domaines dans une interface de gestion de vCenter Single Sign-On.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Si vsphere.local n'est pas le domaine sélectionné actuellement, sélectionnez-le dans le menu déroulant.

Vous ne pouvez pas ajouter des utilisateurs aux autres domaines.

5 Dans l'onglet **Utilisateurs**, cliquez sur l'icône**Nouvel utilisateur**.

6 Tapez un nom d'utilisateur et un mot de passe pour le nouvel utilisateur.

Vous ne pouvez pas modifier le nom d'utilisateur après sa création.

Le mot de passe doit répondre aux exigences des règles de mot de passe du système.

7 (Facultatif) Tapez le prénom et le nom de famille du nouvel utilisateur.

8 (Facultatif) Entrez une adresse e-mail et une description pour l'utilisateur.

9 Cliquez sur **OK**.

Lorsque vous ajoutez un utilisateur, celui-ci ne dispose initialement d'aucun privilège lui donnant la possibilité d'effectuer des opérations de gestion.

Suivant

Ajoutez l'utilisateur à un groupe du domaine vsphere.local (par exemple, au groupe d'utilisateurs pouvant administrer VMCA (CAAdmins) ou au groupe d'utilisateurs pouvant administrer vCenter Single Sign-On (Administrators)). Reportez-vous à « Ajouter des membres à un groupe vCenter Single Sign-On », page 67.

Désactiver et activer des utilisateurs de vCenter Single Sign-On

Lorsqu'un compte d'utilisateur vCenter Single Sign-On est désactivé, l'utilisateur ne peut pas se connecter au serveur vCenter Single Sign-On tant qu'un administrateur n'active pas le compte. Vous pouvez activer et désactiver des comptes dans l'une des interfaces de gestion de vCenter Single Sign-On.

Les comptes d'utilisateur désactivés demeurent disponibles dans le système vCenter Single Sign-On, mais l'utilisateur ne peut plus ouvrir de session ni effectuer d'opérations sur le serveur. Les utilisateurs disposant des privilèges d'administrateur peuvent désactiver et activer des comptes dans la page Utilisateurs et groupes vCenter.

Prérequis

Vous devez être membre du groupe d'administrateurs vCenter Single Sign-On pour désactiver et activer des utilisateurs vCenter Single Sign-On.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Sélectionnez un compte d'utilisateur, cliquez sur l'icône **Désactiver**, puis cliquez sur **Oui** lorsque vous y êtes invité.

5 Pour réactiver l'utilisateur, cliquez avec le bouton droit sur le nom d'utilisateur, sélectionnez **Activer**, puis cliquez sur **Oui** lorsque vous y êtes invité.

Supprimer un utilisateur vCenter Single Sign-On

Vous pouvez supprimer des utilisateurs qui sont dans le domaine vsphere.local dans l'interface de gestion de vCenter Single Sign-On. Vous ne pouvez pas supprimer des utilisateurs du système d'exploitation local ou d'un autre domaine dans l'interface de gestion de vCenter Single Sign-On.

Avertissement Si vous supprimez l'utilisateur administrateur du domaine vsphere.local, vous ne pourrez plus vous connecter à vCenter Single Sign-On. Réinstallez vCenter Server et ses composants.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Sélectionnez l'onglet **Utilisateurs**, puis le domaine vsphere.local.

5 Dans la liste des utilisateurs, sélectionnez celui que vous souhaitez supprimer et cliquez sur l'icône **Supprimer**.

Soyez prudent lorsque vous effectuez cette opération, car elle est irréversible.

Modifier un utilisateur de vCenter Single Sign-On

Vous pouvez modifier le mot de passe ou d'autres informations d'un utilisateur vCenter Single Sign-On dans une interface de gestion de vCenter Single Sign-On. Vous ne pouvez pas renommer d'utilisateurs dans le domaine vsphere.local. Vous ne pouvez donc pas renommer administrator@vsphere.local.

Vous pouvez créer des utilisateurs supplémentaires ayant les mêmes privilèges que administrator@vsphere.local.

Les utilisateurs de vCenter Single Sign-On sont enregistrés dans le domaine vsphere.local de vCenter Single Sign-On.

Vous pouvez vérifier les stratégies de mot de passe vCenter Single Sign-On à partir de vSphere Web Client. Connectez-vous en tant qu'administrator@vsphere.local et sélectionnez **Configuration > Stratégies > Stratégies de mots de passe**.

Voir aussi « Modifier la stratégie de mot de passe de vCenter Single Sign-On », page 58.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Cliquez sur l'onglet **Users**.

5 Cliquez avec le bouton droit sur l'utilisateur et sélectionnez **Modifier l'utilisateur**.

6 Modifiez les attributs utilisateur.

Vous ne pouvez pas modifier le nom d'utilisateur de l'utilisateur.

Le mot de passe doit répondre aux exigences des règles de mot de passe du système.

7 Cliquez sur **OK**.

Ajouter un groupe vCenter Single Sign-On

L'onglet vCenter Single Sign-On **Groupes** affiche les groupes du domaine local, vsphere.local par défaut. Ajoutez des groupes si vous avez besoin d'un conteneur pour les membres de groupe (principaux).

Vous ne pouvez pas ajouter des groupes à d'autres domaines, par exemple le domaine Active Directory, dans l'onglet **Groupes** de vCenter Single Sign-On.

Si vous n'ajoutez pas de source d'identité à vCenter Single Sign-On, la création de groupes et l'ajout d'utilisateurs peuvent vous aider à organiser le domaine local.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Sélectionnez l'onglet **Groupes** et cliquez sur l'icône **Nouveau groupe**.

5 Entrez le nom et la description du groupe.

Vous ne pouvez pas modifier le nom du groupe après l'avoir créé.

6 Cliquez sur **OK**.

Suivant

- Ajoutez des membres au groupe.

Ajouter des membres à un groupe vCenter Single Sign-On

Les membres d'un groupe vCenter Single Sign-On peuvent être des utilisateurs ou d'autres groupes issus d'une ou de plusieurs sources d'identité. Vous pouvez ajouter de nouveaux membres à partir de vSphere Web Client.

Pour plus d'informations relatives au contexte, reportez-vous à l'article 2095342 de la base de connaissances VMware.

Les groupes répertoriés dans l'onglet **Groupes** de l'interface Web appartiennent au domaine vsphere.local. Reportez-vous à « Groupes du domaine vCenter Single Sign-On », page 27.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Cliquez sur l'onglet **Groupes** et cliquez sur le groupe (par exemple, Administrateurs).

5 Dans la zone Membres du groupe, cliquez sur l'icône **Ajouter des membres**.

6 Sélectionnez la source d'identité contenant le membre à ajouter au groupe.

7 (Facultatif) Entrez un terme de recherche et cliquez sur **Rechercher**.

8 Sélectionnez le membre et cliquez sur **Ajouter**.

Vous pouvez ajouter plusieurs membres.

9 Cliquez sur **OK**.

Supprimer des membres d'un groupe vCenter Single Sign-On

Vous pouvez supprimer des membres d'un groupe vCenter Single Sign-On en utilisant vSphere Web Client ou l'interface web de Platform Services Controller. Lorsque vous supprimez un membre (utilisateur ou groupe) d'un groupe, vous ne devez pas supprimer le membre du système.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Sélectionnez l'onglet **Groupes** et cliquez sur le groupe.

5 Dans la liste des membres du groupe, sélectionnez l'utilisateur ou le groupe à supprimer et cliquez sur l'icône **Supprimer un membre**.

6 Cliquez sur **OK**.

L'utilisateur est supprimé du groupe, mais il est toujours disponible dans le système.

Supprimer des utilisateurs de la solution vCenter Single Sign-On

vCenter Single Sign-On affiche les utilisateurs de solution. Un utilisateur de solution est une collection de services. Plusieurs utilisateurs de solution vCenter Server sont prédéfinis et s'authentifient auprès de vCenter Single Sign-On dans le cadre de l'installation. Dans les situations de dépannage, par exemple si une désinstallation ne s'effectue pas proprement, vous pouvez supprimer des utilisateurs de solution individuels de vSphere Web Client.

Lorsque vous supprimez l'ensemble de services associés à un utilisateur de solution vCenter Server ou à un utilisateur de solution tierce de votre environnement, l'utilisateur de solution est supprimé de l'affichage vSphere Web Client. Si vous supprimez de force une application ou si le système devient irrécupérable alors que l'utilisateur de solution est toujours dans le système, vous pouvez supprimer explicitement l'utilisateur de solution de vSphere Web Client.

Important Si vous supprimez un utilisateur de solution, les services correspondants ne peuvent plus s'authentifier auprès de vCenter Single Sign-On.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Accédez à l'interface utilisateur de configuration de l'utilisateur vCenter Single Sign-On.

Option	Description
vSphere Web Client	a Dans le menu **Accueil**, sélectionnez **Administration**. b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
Platform Services Controller	Cliquez sur **Single Sign-On**, puis sur **Utilisateurs et groupes**.

4 Cliquez sur l'onglet **Utilisateurs de la solution**, puis sur le nom d'utilisateur de solution.

5 Cliquez sur l'icône **Supprimer un utilisateur de la solution**.

6 Cliquez sur **Yes**.

Les services associés à l'utilisateur de solution n'ont plus accès à vCenter Server et ne peuvent plus fonctionner comme services vCenter Server.

Changer le mot de passe de vCenter Single Sign-On

Les utilisateurs du domaine local, vsphere.local par défaut, peuvent modifier leurs mots de passe vCenter Single Sign-On à partir d'une interface Web. Les utilisateurs se trouvant dans d'autres domaines changent leur mot de passe en suivant les règles du domaine concerné.

La stratégie de verrouillage vCenter Single Sign-On détermine la date d'expiration de votre mot de passe. Par défaut, les mots de passe de vCenter Single Sign-On expirent après 90 jours, mais les mots de passe d'administrateur tels que le mot de passe d'administrator@vsphere.local n'expirent pas. Les interfaces de gestion de vCenter Single Sign-On affichent un avertissement lorsque votre mot de passe est sur le point d'expirer.

Cette procédure explique comment vous pouvez modifier un mot de passe valide.

Si le mot de passe est expiré, l'administrateur du domaine local, administrator@vsphere.local par défaut, peut réinitialiser le mot de passe en utilisant la commande `dir-cli password reset`. Seuls les membres du groupe d'administrateurs du domaine vCenter Single Sign-On peuvent réinitialiser les mots de passe.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Dans le volet de navigation supérieur, à gauche du menu Aide, cliquez sur votre nom d'utilisateur pour dérouler le menu.

Vous pouvez également sélectionner **Single Sign-On > Utilisateurs et groupes** et **Modifier un utilisateur** dans le menu contextuel.

4 Sélectionnez **Modifier le mot de passe** et tapez votre mot de passe actuel.

5 Tapez un nouveau mot de passe et confirmez-le.

Le mot de passe doit être conforme à la stratégie de mot de passe.

6 Cliquez sur **OK**.

Recommandations en matière de sécurité pour vCenter Single Sign-On

Suivez les recommandations en matière de sécurité de vCenter Single Sign-On afin de protéger votre environnement vSphere.

L'authentification vSphere 6.0 et l'infrastructure de certificats améliorent la sécurité de votre environnement vSphere. Pour vous assurer que l'infrastructure n'est pas compromise, suivez les recommandations pour vCenter Single Sign-On.

Vérifier l'expiration du mot de passe

La stratégie de mot de passe de vCenter Single Sign-On par défaut a une durée de validité de 90 jours. Au terme des 90 jours, le mot de passe expire et la capacité de connexion est compromise. Vérifiez l'expiration et actualisez les mots de passe régulièrement dans les délais impartis.

Configurer NTP

Assurez-vous que tous les systèmes utilisent la même source d'heure relative (en intégrant le décalage de localisation applicable) et que la source d'heure relative peut être mise en corrélation avec une norme horaire acceptée (par exemple, l'heure UTC (Coordinated Universal Time). La synchronisation des systèmes est essentielle pour garantir la validité des certificats vCenter Single Sign-On et celle d'autres certificats vSphere.

NTP simplifie également le suivi d'un éventuel intrus dans les fichiers journaux. Des réglages d'heure incorrects compliquent l'analyse et la corrélation de fichiers journaux pour détecter d'éventuelles attaques et compromettent la précision des audits.

Certificats de sécurité vSphere 3

Les services vCenter utilisent SSL pour communiquer en toute sécurité entre eux, ainsi qu'avec ESXi. Les communications SSL garantissent la confidentialité et l'intégrité des données. Les données sont protégées et ne peuvent pas être modifiées en cours de transit sans détection.

Les services vCenter Server tels qu'une instance de vSphere Web Client utilisent également les certificats pour l'authentification initiale auprès de vCenter Single Sign-On. vCenter Single Sign-On fournit à chaque ensemble de services (utilisateur de solution) un jeton SAML grâce auquel l'utilisateur de solution peut s'authentifier.

Dans vSphere 6.0 et les versions ultérieures, VMCA (VMware Certificate Authority) fournit à chaque hôte ESXi et à chaque service vCenter Server un certificat signé par défaut par VMCA.

Vous pouvez remplacer les certificats par de nouveaux certificats signés par VMCA, désigner VMCA comme autorité de certification subordonnée ou remplacer tous les certificats par des certificats personnalisés. Plusieurs options s'offrent à vous :

Tableau 3-1. Différentes approches du remplacement de certificat

Option	Reportez-vous à
Utilisez l'interface Web Platform Services Controller (vSphere 6.0 Update 1 et version ultérieure).	« Gestion de certificats avec l'interface Web Platform Services Controller », page 83
Utilisez l'utilitaire de gestion de certificat vSphere dans l'invite de commande.	« Gestion de certificats avec l'utilitaire vSphere Certificate Manager », page 92
Utilisez les commandes CLI pour remplacer des certificats manuellement.	Chapitre 4, « Gestion des services et des certificats avec des interfaces de lignes de commande », page 133

Gestion des certificats vSphere (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere6_cert_infrastructure)

Ce chapitre aborde les rubriques suivantes :

Présentation de la gestion de certificats

Le travail nécessaire pour configurer ou mettre à jour votre infrastructure de certificats dépend des exigences de votre environnement, de la nature de l'activité (selon que vous effectuez une nouvelle installation ou une mise à niveau) et de votre intention d'utiliser ESXi ou vCenter Server.

Administrateurs qui ne remplacent pas les certificats VMware

VMCA peut prendre en charge la gestion de tous les certificats. VMCA fournit aux composants de vCenter Server et aux hôtes ESXi des certificats qui utilisent VMCA comme autorité de certification racine. Si vous effectuez une mise à niveau vers vSphere 6 à partir d'une version précédente de vSphere, tous les certificats auto-signés sont remplacés par des certificats signés par VMCA.

Si, actuellement, vous ne remplacez pas de certificats VMware, votre environnement commence à utiliser des certificats signés par VMCA au lieu de certificats auto-signés.

Administrateurs qui remplacent les certificats VMware par des certificats personnalisés

Si la stratégie d'entreprise exige que les certificats soient signés par une autorité de certification tierce ou d'entreprise, ou si elle exige des informations de certificat personnalisé, vous disposez de plusieurs choix pour une nouvelle installation.

- Faites signer le certificat racine VMCA par une autorité de certification tierce ou d'entreprise. Remplacez le certificat racine VMCA par ce certificat signé. Dans ce scénario, le certificat VMCA est un certificat intermédiaire. VMCA fournit aux composants de vCenter Server et aux hôtes ESXi des certificats qui incluent la chaîne complète de certificats.
- Si la stratégie d'entreprise n'autorise pas les certificats intermédiaires dans la chaîne, vous pouvez remplacer les certificats de façon explicite. Vous pouvez utiliser l'interface Web de Platform Services Controller, l'utilitaire vSphere Certificate Manager, ou effectuer le remplacement manuel des certificats en utilisant les interfaces de ligne de commande de gestion de certificats.

Lors de la mise à niveau d'un environnement qui utilise des certificats personnalisés, vous pouvez conserver certains certificats.

- Les hôtes ESXi conservent leurs certificats personnalisés pendant la mise à niveau. Assurez-vous que le processus de mise à niveau de vCenter Server ajoute tous les certificats racines pertinents au magasin TRUSTED_ROOTS dans VECS sur vCenter Server.

  Une fois la mise à niveau vers vSphere 6.0 ou version ultérieure effectuée, vous pouvez définir le mode des certificats sur **Personnalisé**. Si le mode de certificat est VMCA (valeur par défaut) et si l'utilisateur effectue une actualisation des certificats à partir de vSphere Web Client, les certificats signés par l'autorité de certification VMware (VMCA) remplacent les certificats personnalisés.
- Pour les composants vCenter Server, ce qui se produit dépend de l'environnement existant.
  - Lors de la mise à niveau d'une installation simple vers un déploiement intégré, vCenter Server conserve les certificats personnalisés. Après la mise à niveau, votre environnement fonctionne comme auparavant.
  - Pour une mise à niveau d'un déploiement multisite, vCenter Single Sign-On peut se trouver sur une machine différente de celle des autres composants vCenter Server. Dans ce cas, le processus de mise à niveau crée un déploiement à plusieurs nœuds qui inclut un nœud Platform Services Controller et un ou plusieurs nœuds de gestion.

    Dans ce scénario, les certificats vCenter Server et vCenter Single Sign-On sont conservés. Les certificats sont utilisés en tant que certificats SSL de machine.

En outre, VMCA attribue un certificat signé par VMCA à chaque utilisateur de solution (collection de services vCenter). L'utilisateur de solution utilise ce certificat uniquement pour s'authentifier auprès de vCenter Single Sign-On. Souvent, la stratégie d'entreprise n'exige pas que les certificats d'utilisateur de solution soient remplacés.

Vous ne pouvez plus utiliser l'outil de remplacement des certificats vSphere 5.5, qui était disponible pour les installations vSphere 5.5. La nouvelle architecture se traduit par la distribution et le placement d'un service différent. Un nouvel utilitaire de ligne de commande, vSphere Certificate Manager, est disponible pour la plupart des tâches de gestion de certificats.

Interfaces de certificats vSphere

Pour vCenter Server, vous pouvez afficher et remplacer les certificats avec les outils et les interfaces ci-après.

Tableau 3-2. Interfaces pour la gestion des certificats vCenter Server

Interface	Utilisez
l'interface Web de Platform Services Controller	Effectuez les tâches de certificat courantes à l'aide d'une interface utilisateur graphique.
Utilitaire vSphere Certificate Manager	Effectuez les tâches courantes de remplacement de certificat à partir de la ligne de commande de l'installation de vCenter Server.
Interfaces de ligne de commande de gestion de certificats	Effectuez toutes les tâches de gestion de certificats avec `dir-cli`, `certool` et `vecs-cli`.
vSphere Web Client	Affichez les certificats, y compris les informations d'expiration.

Pour ESXi, effectuez la gestion des certificats à partir de vSphere Web Client. VMCA provisionne les certificats et les stocke localement sur l'hôte ESXi. VMCA ne stocke pas les certificats de l'hôte ESXi dans VMDIR ou dans VECS. Consultez la documentation de *Sécurité vSphere*.

Certificats vCenter pris en charge

Pour vCenter Server, Platform Services Controller et pour les machines et services associés, les certificats suivants sont pris en charge :

- Certificats qui sont générés et signés par VMware Certificate Authority (VMCA).
- Certificats personnalisés.
  - Certificats d'entreprise qui sont générés à partir de votre propre infrastructure de clés publiques (PKI) interne.
  - Certificats signés par une autorité de certification tierce qui sont générés à partir d'une infrastructure de clés publiques (PKI) externe telle que Verisign, GoDaddy, etc.

Les certificats auto-signés créés au moyen d'OpenSSL dans lesquels il n'existe aucune autorité de certification racine ne sont pas pris en charge.

Présentation du remplacement des certificats

Vous pouvez effectuer différents types de remplacement de certificats selon la stratégie et les besoins de l'entreprise pour le système que vous configurez. Vous pouvez effectuer un remplacement de certificat à l'aide de Platform Services Controller en utilisant l'utilitaire vSphere Certificate Manager, ou le remplacer manuellement à l'aide des interfaces de ligne de commande incluses dans votre installation.

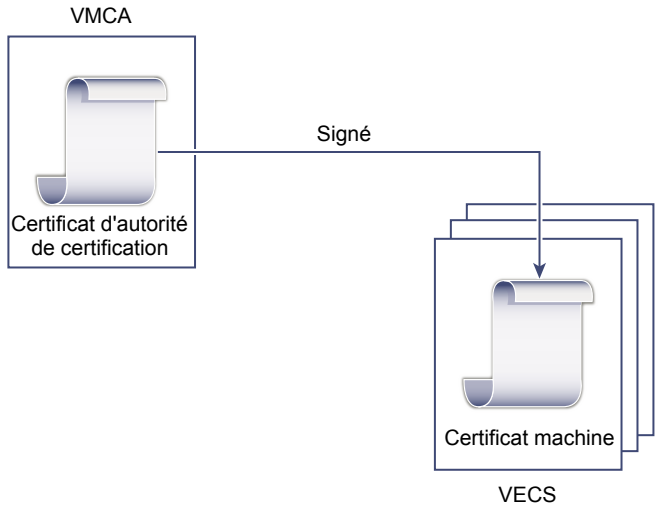
VMCA est inclus dans chaque Platform Services Controller et dans chaque déploiement intégré. VMCA provisionne chaque nœud, chaque utilisateur de solutions vCenter Server et chaque hôte ESXi avec un certificat qui est signé par VMCA comme autorité de certification. Les utilisateurs de solution vCenter Server sont des groupes de services vCenter Server.

Vous pouvez remplacer les certificats par défaut. Pour les composants de vCenter Server, vous pouvez utiliser un ensemble d'outils de ligne de commande inclus dans votre installation. Vous avez plusieurs options.

Remplacer par des certificats signés par VMCA

Si votre certificat VMCA expire ou si vous souhaitez le remplacer pour d'autres raisons, vous pouvez utiliser les interfaces de ligne de commande de gestion de certificats pour effectuer ce processus. Par défaut, le certificat racine VMCA expire au bout de dix ans, tous les certificats signés par VMCA expirent au moment de l'expiration du certificat racine, c'est-à-dire au terme d'une période maximale de dix ans.

Figure 3-1. Les certificats signés par VMCA sont stockés dans VECS



Vous pouvez utiliser les options vSphere Certificate Manager suivantes :

- Remplacer le certificat SSL machine par un certificat VMCA
- Remplacer le certificat d'utilisateur de solution par un certificat VMCA

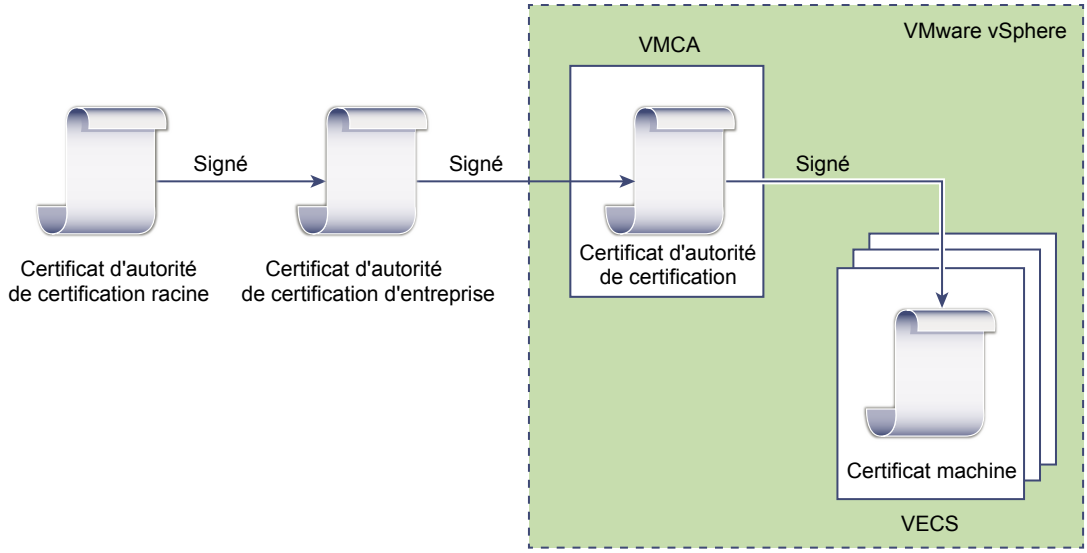
Pour le remplacement manuel de certificat, reportez-vous à « Remplacer les certificats existants signés par l'autorité de certification VMware (VMCA) par de nouveaux certificats », page 106.

Faire de VMCA une autorité de certificat intermédiaire

Vous pouvez remplacer le certificat racine VMCA par un certificat qui est signé par une autorité de certification d'entreprise ou une autorité de certification tierce. VMCA signe le certificat racine personnalisé chaque fois qu'il provisionne des certificats, ce qui en fait une autorité de certification intermédiaire.

Remarque Si vous effectuez une nouvelle installation qui inclut un Platform Services Controller externe, installez d'abord le Platform Services Controller et remplacez le certificat racine VMCA. Installez ensuite d'autres services ou ajoutez des hôtes ESXi à votre environnement. Si vous effectuez une nouvelle installation avec un Platform Services Controller intégré, remplacez le certificat racine VMCA avant d'ajouter des hôtes ESXi. Dans ce cas, VMCA signe l'intégralité de la chaîne et vous n'avez pas à générer de nouveaux certificats.

Figure 3-2. Les certificats signés par une autorité de certification tierce ou d'entreprise utilisent VMCA comme autorité de certification intermédiaire



Vous pouvez utiliser les options vSphere Certificate Manager suivantes :

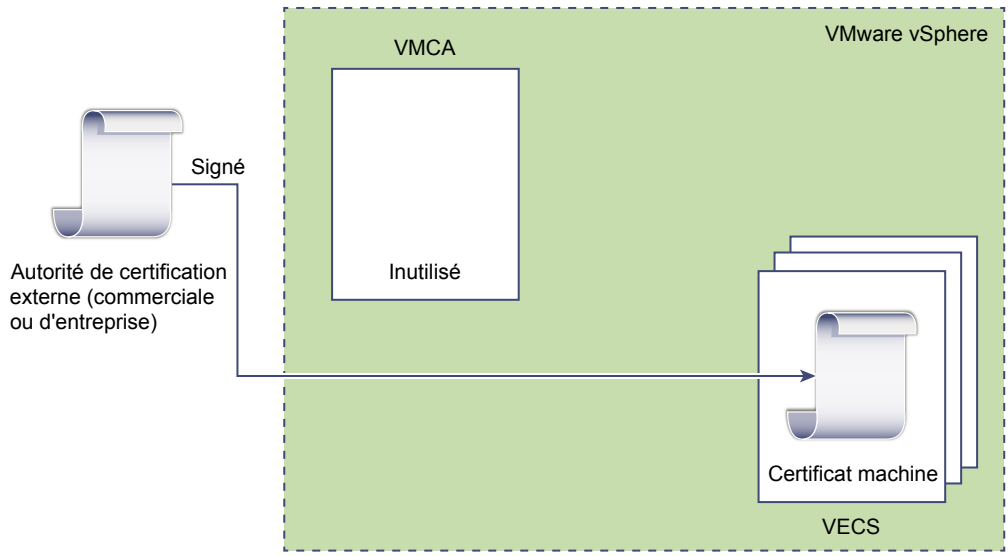
- Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats
- Remplacer le certificat SSL machine par un certificat VMCA (déploiement multi-nœud)
- Remplacer le certificat d'utilisateur de solution par un certificat VMCA (déploiement multi-nœud)

Pour le remplacement manuel de certificat, reportez-vous à « Utiliser VMCA en tant qu'autorité de certificat intermédiaire », page 116.

Ne pas utiliser VMCA, provisionner avec des certificats personnalisés

Vous pouvez remplacer les certificats signés par VMCA existants par des certificats personnalisés. Si vous utilisez cette approche, vous êtes responsable de l'intégralité du provisionnement et de la surveillance des certificats.

Figure 3-3. Les certificats externes sont stockés directement dans VECS



Vous pouvez utiliser les options vSphere Certificate Manager suivantes :

- Remplacer le certificat SSL de machine par un certificat personnalisé
- Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Pour le remplacement manuel de certificat, reportez-vous à « Utiliser des certificats personnalisés avec vSphere », page 127.

Déploiement hybride

Vous pouvez demander à VMCA de fournir une partie des certificats, mais utiliser des certificats personnalisés pour d'autres parties de votre infrastructure. Par exemple, comme les certificats d'utilisateur de solution sont utilisés uniquement pour s'authentifier auprès de vCenter Single Sign-On, envisagez de demander à VMCA de provisionner ces certificats. Remplacez les certificats SSL machine par des certificats personnalisés pour sécuriser l'ensemble du SSL.

Souvent, les stratégies d'entreprise n'autorisent pas les autorités de certificat intermédiaires. Dans ce type de situation, un déploiement hybride constitue une bonne solution. En effet, il réduit au maximum le nombre de certificats à remplacer et sécurise l'ensemble du trafic. Un déploiement hybride autorise uniquement le trafic interne (c'est-à-dire le trafic des utilisateurs de solutions) à utiliser les certificats par défaut signés par VMCA.

Remplacement des certificats ESXi

Pour les hôtes ESXi, vous pouvez modifier le comportement de provisionnement de certificats à partir de vSphere Web Client. Pour plus d'informations, reportez-vous à la documentation *Sécurité vSphere*.

Tableau 3-3. Options de remplacement de certificat ESXi

Option	Description
Mode VMware Certificate Authority (par défaut)	Lorsque vous renouvelez des certificats à partir de vSphere Web Client, VMCA émet les certificats pour les hôtes. Si vous modifiez le certificat racine VMCA de manière à inclure une chaîne de certificats, les certificats hôtes incluent la chaîne complète.
Mode d'autorité de certification personnalisée	Vous permet de manuellement mettre à jour et d'utiliser des certificats qui ne sont pas signés ou émis par VMCA.
Mode d'empreinte	Peut être utilisé pour conserver les certificats 5.5 pendant l'actualisation. Utilisez ce mode uniquement de façon temporaire dans des situations de débogage.

Situations dans lesquelles vSphere utilise des certificats

Dans vSphere 6.0 et version ultérieure, VMware Certificate Authority (VMCA) provisionne votre environnement avec des certificats. Les certificats incluent des certificats SSL de machine pour des connexions sécurisées, des certificats d'utilisateur de solution pour l'authentification des services auprès de vCenter Single Sign-On et des certificats pour les hôtes ESXi.

Les certificats suivants sont utilisés.

Tableau 3-4. Certificats dans vSphere 6.0

Certificat	Alloué	Commentaires
Certificats ESXi	VMCA (par défaut)	Stockés localement sur l'hôte ESXi
Certificats SSL de la machine	VMCA (par défaut)	Stockés dans VECS
Certificats d'utilisateurs de solutions	VMCA (par défaut)	Stockés dans VECS

Tableau 3-4. Certificats dans vSphere 6.0 (suite)

Certificat	Alloué	Commentaires
Certificat de signature SSL vCenter Single Sign-On	Provisionné au cours de l'installation.	Gérez ce certificat dans vSphere Web Client. Ne modifiez pas ce certificat dans le système de fichiers pour éviter de provoquer des résultats imprévisibles.
Certificat SSL de VMware Directory Service (VMDIR)	Provisionné au cours de l'installation.	À partir de vSphere 6.5, le certificat SSL de machine est utilisé comme certificat vmdir.

ESXi

Les certificats ESXi sont stockés localement sur chaque hôte dans le répertoire `/etc/vmware/ssl`. Les certificats ESXi sont provisionnés par VMCA par défaut, mais vous pouvez utiliser plutôt des certificats personnalisés. Les certificats ESXi sont provisionnés lorsque l'hôte est d'abord ajouté à vCenter Server et lorsque l'hôte se reconnecte.

Certificats SSL de la machine

Le certificat SSL de la machine pour chaque nœud est utilisé pour créer un socket SSL sur le côté serveur. Les clients SSL se connectent au socket SSL. Le certificat est utilisé pour la vérification du serveur et pour la communication sécurisée telle que HTTPS ou LDAPS.

Chaque nœud dispose de son propre certificat SSL de machine. Les nœuds incluent l'instance de vCenter Server l'instance de Platform Services Controller ou l'instance du déploiement intégré. Tous les services exécutés sur ce nœud utilisent ce certificat SSL de machine pour exposer leurs points de terminaison SSL.

Les services suivants utilisent le certificat SSL de machine.

- Le service de proxy inverse sur chaque nœud Platform Services Controller. Les connexions SSL vers des services vCenter individuels accèdent toujours au proxy inverse. Le trafic n'accède pas aux services eux-mêmes.
- Le service vCenter (vpxd) sur les nœuds de gestion et les nœuds intégrés.
- Le service VMware Directory Service (vmdir) sur les nœuds d'infrastructure et les nœuds intégrés.

Les produits VMware utilisent des certificats X.509 version 3 (X.509v3) standard pour chiffrer les informations de session. Les informations de session circulent entre les composants via SSL.

Certificats d'utilisateurs de solutions

Un utilisateur de solution encapsule un ou plusieurs services vCenter Server. Chaque utilisateur de solution doit être authentifié auprès de vCenter Single Sign-On. Les utilisateurs de solutions utilisent des certificats pour s'authentifier auprès de vCenter Single Sign-On par le biais d'un échange de jeton SAML.

Un utilisateur de solution présente le certificat à vCenter Single Sign-On lorsqu'il doit s'authentifier après un redémarrage ou après l'expiration d'un délai. Le délai (délai du détenteur de clé) peut être défini à partir de l'interface Web de vSphere Web Client ou de Platform Services Controller et correspond par défaut à 2 592 000 secondes (30 jours).

Par exemple, l'utilisateur de solution vpxd présente son certificat à vCenter Single Sign-On lorsqu'il se connecte à vCenter Single Sign-On. L'utilisateur de solution vpxd reçoit un jeton SAML à partir de vCenter Single Sign-On et peut utiliser ce jeton pour s'authentifier auprès d'autres utilisateurs de solutions et services.

Les magasins de certificats d'utilisateurs de solutions suivants sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré :

- `machine` : utilisé par le gestionnaire de composants, le serveur de licences et le service de journalisation.

  Remarque Le certificat d'utilisateurs de solution de machine n'a rien à voir avec le certificat SSL de machine. Le certificat d'utilisateur de solution de machine est utilisé pour l'échange de jetons SAML ; le certificat SSL de machine est utilisé pour les connexions SSL sécurisées d'une machine.

- `vpxd` : magasin de démon du service vCenter (vpxd) sur les nœuds de gestion et les déploiements intégrés. vpxd utilise le certificat d'utilisateur de solution qui est stocké dans ce magasin pour s'authentifier auprès de vCenter Single Sign-On.
- `vpxd-extensions` : magasin d'extensions vCenter. Inclut le service Auto Deploy, Inventory Service et d'autres services ne faisant pas partie d'autres utilisateurs de solution.
- `vsphere-webclient` : magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance.

Chaque nœud Platform Services Controller comprend un certificat `machine`.

Certificats internes

Les certificats vCenter Single Sign-On ne sont pas stockés dans VECS et ne sont pas gérés avec des outils de gestion de certificats. En règle générale, les modifications ne sont pas nécessaires, mais dans des situations spéciales, vous pouvez remplacer ces certificats.

Certificat de signature vCenter Single Sign-On

Le service vCenter Single Sign-On inclut un fournisseur d'identité qui émet des jetons SAML utilisés dans vSphere à des fins d'authentification. Un jeton SAML représente l'identité de l'utilisateur et contient également des informations d'appartenance au groupe. Lorsque vCenter Single Sign-On émet des jetons SAML, il signe chacun d'eux avec le certificat de signature pour permettre aux clients de vCenter Single Sign-On de vérifier que le jeton SAML provient d'une source de confiance.

vCenter Single Sign-On émet des jetons détenteurs de clé SAML pour les utilisateurs de solution et des jetons au porteur pour les autres utilisateurs, qui se connectent avec un nom d'utilisateur et un mot de passe.

Vous pouvez remplacer ce certificat dans vSphere Web Client. Reportez-vous à « Actualiser le certificat STS », page 53.

Certificat SSL de VMware Directory Service

À partir de vSphere 6.5, le certificat SSL de machine est utilisé comme certificat d'annuaire VMware. Pour les versions antérieures de vSphere, reportez-vous à la documentation correspondante.

Certificats de chiffrement des machines virtuelles vSphere

La solution de chiffrement de machine virtuelle vSphere se connecte à un serveur de gestion de clés (KMS) externe. Selon la méthode utilisée par la solution pour s'authentifier auprès du KMS, des certificats peuvent être générés et stockés dans VECS. Consultez la documentation de *Sécurité vSphere*.

Personnaliser des exigences en matière de certificats

Lorsque vous souhaitez utiliser des certificats d'une tierce partie au sein de votre environnement, vous devez vérifier leur conformité à certaines exigences. Les certificats fournis par VMCA sont déjà conformes à ces exigences.

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8

- x509 version 3
- Pour les certificats racines, l'extension d'autorité de certification doit être définie sur vrai et la signature de certification doit figurer dans la liste de conditions requises.
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Format CRT
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
- Heure de début antérieure d'un jour à l'heure actuelle
- CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.

Remarque Les algorithmes md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4 et sha1WithRSAEncryption 1.2.840.113549.1.1.5 ne sont pas recommandés. L'algorithme RSASSA-PSS avec OID 1.2.840.113549.1.1.10 n'est pas pris en charge.

VMCA et VMware Core Identity Services

Les services d'identité de base font partie de chaque déploiement intégré et de chaque nœud de services de plate-forme. VMCA fait partie de chaque groupe de services d'identité de base VMware. Utilisez l'interface de ligne de commande de gestion et vSphere Web Client pour interagir avec ces services.

Les services d'identité de base VMware regroupent plusieurs composants.

Tableau 3-5. Services d'identité de base

Service	Description	Inclus dans
Service d'annuaire VMware (vmdir)	Prend en charge la gestion des certificats SAML pour l'authentification conjointement avec vCenter Single Sign-On.	Platform Services Controller Déploiement intégré
Autorité de certification VMware (VMCA)	Émet des certificats pour les utilisateurs de solutions VMware, des certificats pour les machines sur lesquelles les services sont exécutés et des certificats hôtes ESXi. VMCA peut être utilisé tel quel ou comme autorité de certification intermédiaire. VMCA émet des certificats uniquement pour les clients capables de s'authentifier auprès de vCenter Single Sign-On dans le même domaine.	Platform Services Controller Déploiement intégré
Démon VMware Authentication Framework (VMAFD)	Inclut le magasin de certificats de point de terminaison (VECS) et plusieurs autres services d'authentification. Les administrateurs VMware interagissent avec VECS ; les autres services sont utilisés en interne.	Platform Services Controller vCenter Server Déploiement intégré

Présentation du magasin de certificats VMware Endpoint

VMware Endpoint Certificate Store (VECS) sert de référentiel local (côté client) pour les certificats, les clés privées et les autres informations liées aux certificats qui peuvent être stockés dans un magasin de clés. Vous pouvez décider de ne pas utiliser VMCA en tant qu'autorité de certification et de signature de certificat, mais vous devez utiliser VECS pour stocker tous les certificats, clés et autres éléments de vCenter. Les certificats ESXi sont stockés localement sur chaque hôte et non dans VECS.

VECS s'exécute dans le cadre du démon VMware Authentication Framework (VMAFD). VECS fonctionne sur chaque déploiement intégré, nœud de Platform Services Controller et nœud de gestion ; il contient les magasins de clés qui renferment les certificats et les clés.

VECS interroge périodiquement VMware Directory Service (vmdir) en vue d'éventuelles mises à jour du magasin TRUSTED_ROOTS. Vous pouvez également gérer explicitement les certificats et les clés dans VECS à l'aide des commandes `vecs-cli`. Reportez-vous à « Référence des commandes vecs-cli », page 141.

VECS inclut les magasins suivants.

Tableau 3-6. Magasins dans VECS

Magasin	Description
Magasin de certificats SSL de la machine (MACHINE_SSL_CERT)	■ Utilisé par le service de proxy inverse sur chaque nœud vSphere. ■ Utilisé par VMware Directory Service (vmdir) sur les déploiements intégrés et sur chaque nœud Platform Services Controller. Tous les services de vSphere 6.0 communiquent par l'intermédiaire d'un proxy inversé qui utilise le certificat SSL de machine. Pour la compatibilité descendante, les services 5.x utilisent toujours des ports spécifiques. En conséquence, certains services tels que vpxd ont toujours leur port ouvert.
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.
Magasins d'utilisateurs de solution ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient	VECS inclut un magasin pour chaque utilisateur de solution. L'objet de chaque certificat d'utilisateur de solution doit être unique (par exemple, le certificat de la machine ne peut pas avoir le même objet que le certificat vpxd). Les certificats d'utilisateurs de solutions sont utilisés pour l'authentification avec vCenter Single Sign-On. vCenter Single Sign-On vérifie que le certificat est valide, mais ne vérifie pas d'autres attributs de certificat. Dans un déploiement intégré, tous les certificats d'utilisateur de la solution se trouvent sur le même système. Les magasins de certificats d'utilisateurs de solutions suivants sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré : ■ `machine` : utilisé par le gestionnaire de composants, le serveur de licences et le service de journalisation. **Remarque** Le certificat d'utilisateurs de solution de machine n'a rien à voir avec le certificat SSL de machine. Le certificat d'utilisateur de solution de machine est utilisé pour l'échange de jetons SAML ; le certificat SSL de machine est utilisé pour les connexions SSL sécurisées d'une machine. ■ `vpxd` : magasin de démon du service vCenter (vpxd) sur les nœuds de gestion et les déploiements intégrés. vpxd utilise le certificat d'utilisateur de solution qui est stocké dans ce magasin pour s'authentifier auprès de vCenter Single Sign-On. ■ `vpxd-extensions` : magasin d'extensions vCenter. Inclut le service Auto Deploy, Inventory Service et d'autres services ne faisant pas partie d'autres utilisateurs de solution. ■ `vsphere-webclient` : magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance. Chaque nœud Platform Services Controller comprend un certificat `machine`.

Tableau 3-6. Magasins dans VECS (suite)

Magasin	Description
Magasin de sauvegardes de vSphere Certificate Manager Utility (BACKUP_STORE)	Utilisé par VMCA (VMware Certificate Manager) pour prendre en charge la restauration de certificat. Seul l'état le plus récent est stocké en tant que sauvegarde ; vous ne pouvez pas revenir en arrière de plus d'une étape.
Autres magasins	D'autres magasins peuvent être ajoutés par des solutions. Par exemple, la solution Virtual Volumes ajoute un magasin SMS. Ne modifiez pas les certificats dans ces magasins, sauf si la documentation VMware ou un article de la base de connaissances VMware vous y invite. **Remarque** La suppression du magasin TRUSTED_ROOTS_CRLS peut endommager votre infrastructure de certificats. Ne supprimez pas et ne modifiez pas le magasin TRUSTED_ROOTS_CRLS.

Le service vCenter Single Sign-On conserve le certificat de signature de jeton et son certificat SSL sur le disque. Vous pouvez modifier le certificat de signature de jeton à partir de vSphere Web Client.

Certains certificats sont stockés dans le système de fichiers, temporairement pendant le démarrage, ou de façon permanente. Ne modifiez pas les certificats figurant dans le système de fichiers. Utilisez la commande `vecs-cli` pour agir sur les certificats stockés dans VECS.

Remarque Ne modifiez aucun fichier de certificat sur le disque sauf sur instruction de la documentation VMware ou des articles de la base de connaissances. Toute modification pourrait donner lieu à un comportement imprévisible.

Gestion de la révocation de certificat

Si vous pensez que l'un de vos certificats a été compromis, remplacez tous les certificats existants, y compris le certificat racine VMCA.

vSphere 6.0 prend en charge le remplacement des certificats, mais n'applique pas la révocation des certificats pour les hôtes ESXi ou pour les systèmes vCenter Server.

Supprimez les certificats révoqués de tous les nœuds. Si vous ne supprimez pas les certificats révoqués, une attaque de l'intercepteur peut engendrer la compromission par l'emprunt d'identité avec les informations d'identification du compte.

Remplacement des certificats dans les déploiements à grande échelle

Le remplacement des certificats dans les déploiements qui incluent plusieurs nœuds de gestion et un ou plusieurs nœuds Platform Services Controller est semblable au remplacement dans les déploiements intégrés. Dans les deux cas, vous pouvez utiliser l'utilitaire de gestion des certificats vSphere ou remplacer les certificats manuellement. Certaines pratiques recommandées guident le processus de remplacement.

Remplacement des certificats dans les environnements en mode haute disponibilité qui incluent un équilibreur de charge

Dans les environnements comportant moins de huit systèmes vCenter Server, VMware recommande généralement une instance unique de Platform Services Controller et le service vCenter Single Sign-On associé. Dans les environnements plus importants, envisagez d'utiliser plusieurs instances du Platform Services Controller, protégées par un équilibrage de charge réseau. Le livre blanc *Guide de déploiement de vCenter Server 6.0* sur le site Web de VMware présente cette configuration.

Remplacement des certificats SSL de la machine dans les environnements qui incluent plusieurs nœuds de gestion

Si votre environnement inclut plusieurs nœuds de gestion et un seul Platform Services Controller, vous pouvez remplacer les certificats avec l'utilitaire vSphere Certificate Manager ou manuellement avec des commandes de l'interface de ligne de commande de vSphere.

vSphere Certificate Manager

Exécutez vSphere Certificate Manager sur chaque machine. Sur les nœuds de gestion, vous êtes invité à fournir l'adresse IP de Platform Services Controller. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat.

Remplacement manuel de certificats

Pour le remplacement manuel des certificats, exécutez les commandes de remplacement des certificats sur chaque machine. Sur les nœuds de gestion, vous devez spécifier le Platform Services Controller avec le paramètre `--server`. Consultez les rubriques suivantes pour plus d'informations :

- « Remplacer les certificats SSL de la machine par des certificats signés par VMCA », page 108
- « Remplacer les certificats SSL de la machine (autorité de certification intermédiaire) », page 119
- « Remplacer les certificats SSL de machine par des certificats personnalisés », page 129

Remplacement des certificats d'utilisateurs de solutions dans les environnements qui incluent plusieurs nœuds de gestion

Si votre environnement comporte plusieurs nœuds de gestion et un seul Platform Services Controller, suivez la procédure ci-dessous pour remplacer des certificats.

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

vSphere Certificate Manager

Exécutez vSphere Certificate Manager sur chaque machine. Sur les nœuds de gestion, vous êtes invité à fournir l'adresse IP de Platform Services Controller. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat.

Remplacement manuel de certificats

1. Générez ou demandez un certificat. Vous devez disposer des certificats suivants :
   - Un certificat d'utilisateur de solution de machine sur Platform Services Controller.
   - Un certificat d'utilisateur de solution de machine sur chaque nœud de gestion.
   - Un certificat pour chacun des utilisateurs de solutions suivants sur chaque nœud de gestion :
     - utilisateur de solution vpxd
     - utilisateur de solution vpxd-extension
     - utilisateur de solution vsphere-webclient

2 Remplacez les certificats sur chaque nœud. La précision de la procédure dépend du type de remplacement de certificat que vous effectuez. Reportez-vous à « Gestion de certificats avec l'utilitaire vSphere Certificate Manager », page 92

Consultez les rubriques suivantes pour plus d'informations :

- « Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA », page 111
- « Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire) », page 122
- « Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés », page 130

Remplacement des certificats dans les environnements qui incluent des solutions internes

Certaines solutions telles que VMware vCenter Site Recovery Manager ou VMware vSphere Replication sont toujours installées sur une autre machine que celle du système vCenter Server ou Platform Services Controller. Si vous remplacez le certificat SSL machine par défaut sur le système vCenter Server ou Platform Services Controller, une erreur de connexion se produit si la solution tente de se connecter au système vCenter Server.

Vous pouvez exécuter le script `ls_update_certs` pour résoudre le problème. Reportez-vous à l'article 2109074 de la base de connaissances VMware pour obtenir plus de détails.

Gestion de certificats avec l'interface Web Platform Services Controller

Vous pouvez afficher et gérer des certificats en vous connectant à l'interface Web Platform Services Controller. Vous pouvez réaliser de nombreuses tâches de gestion de certificats via l'utilitaire vSphere Certificate Manager ou à l'aide de cette interface Web.

L'interface Web Platform Services Controller vous permet de réaliser ces tâches de gestion.

- Affichez les magasins de certificats actuels, et ajoutez et supprimez des entrées de magasin de certificats.
- Explorez l'instance de VMware Certificate Authority (VMCA) associée à cette instance de Platform Services Controller.
- Affichez les certificats générés par VMware Certificate Authority.
- Renouvelez les certificats existants ou remplacez des certificats.

Les workflows de remplacement de certificat sont en grande partie entièrement pris en charge à partir de l'interface Web de Platform Services Controller. Pour générer des demandes de signature de certificat, vous pouvez employer l'utilitaire vSphere Certificate Manager.

Workflows pris en charge

Après l'installation d'une instance de Platform Services Controller, VMware Certificate Authority sur ce nœud provisionne tous les autres nœuds de l'environnement avec des certificats par défaut. Vous pouvez utiliser l'un des workflows suivants pour renouveler ou remplacer des certificats.

Renouveler les certificats	Vous pouvez demander à VMCA de générer un nouveau certificat racine et de renouveler tous les certificats de votre environnement depuis l'interface Web de Platform Services Controller.
Faire de VMCA une autorité de certificat intermédiaire	Vous pouvez générer une demande de signature de certificat à l'aide de l'utilitaire vSphere Certificate Manager, modifier le certificat que vous avez reçu de CSR pour ajouter VMCA à la chaîne, puis ajouter la chaîne de certificats et la clé privée à votre environnement. Lorsque vous renouvelez tous les certificats, VMCA provisionne toutes les machines et tous les utilisateurs de solutions avec des certificats qui sont signés par la chaîne complète.
Remplacer des certificats par des certificats personnalisés	Si vous ne souhaitez pas utiliser VMCA, vous pouvez générer des demandes de signature de certificat pour les certificats que vous souhaitez remplacer. L'autorité de certification renvoie un certificat racine et un certificat signé pour chaque demande de signature de certificat. Vous pouvez télécharger le certificat racine et les certificats personnalisés à partir de Platform Services Controller.

Dans un environnement mixte, vous pouvez utiliser des commandes d'interface de ligne de commande pour remplacer le certificat vCenter Single Sign-On après le remplacement des autres certificats. Reportez-vous à « Remplacer le certificat VMware Directory Service dans des environnement en mode mixte », page 116.

Explorer les magasins de certificats à partir de l'interface Web Platform Services Controller

Une instance du magasin de certificats VECS (VMware Endpoint Certificate Store) est incluse sur chaque nœud Platform Services Controller et chaque nœud vCenter Server. Vous pouvez explorer les différents magasins compris dans VMware Endpoint Certificate Store à partir de l'interface Web Platform Services Controller.

Consultez la section « Présentation du magasin de certificats VMware Endpoint », page 79 pour plus d'informations sur les différents magasins dans VECS.

Prérequis

Pour la plupart des tâches de gestion, vous devez disposer d'un mot de passe pour l'administrateur du compte de domaine local, administrator@vsphere.local, ou d'un domaine distinct si vous avez modifié le domaine lors de l'installation.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

   Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Sous Certificats, cliquez sur **Magasin de certificats** et explorez le magasin.

4 Sélectionnez le magasin dans le magasin VECS (VMware Endpoint Certificate Store) que vous souhaitez explorer à partir du menu déroulant.

   La section « Présentation du magasin de certificats VMware Endpoint », page 79 décrit le contenu des magasins individuels.

5 Pour afficher les détails d'un certificat, sélectionnez celui-ci et cliquez sur l'icône **Afficher les détails**.

6 Pour supprimer une entrée du magasin sélectionné, cliquez sur l'icône **Supprimer une entrée**.

   Par exemple, si vous remplacez le certificat existant, vous pouvez ensuite supprimer l'ancien certificat racine. Supprimez des certificats uniquement si vous êtes sûr qu'ils ne sont plus utilisés.

Remplacer les certificats par de nouveaux certificats signés par VMCA depuis l'interface Web de Platform Services Controller

Vous pouvez remplacer tous les certificats signés par VMCA par de nouveaux certificats signés par VMCA ; ce processus se nomme renouvellement de certificat. Vous pouvez renouveler les certificats sélectionnés ou tous les certificats de votre environnement depuis l'interface web Platform Services Controller.

Prérequis

Pour la gestion des certificats, vous devez fournir le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut). Si vous renouvelez des certificats pour un système vCenter Server, il vous faut également fournir les informations d'identification vCenter Single Sign-On pour un utilisateur possédant des privilèges d'administration sur le système vCenter Server.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

   Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.

4 Renouvelez le certificat SSL de la machine pour le système local.

   a Cliquez sur l'onglet **Certificats de machine**.

   b Sélectionnez le certificat, cliquez sur **Renouveler**, puis répondez **Oui** à l'invite.

5 (facultatif) Renouvelez les certificats d'utilisateur de solution pour le système local.

   a Cliquez sur l'onglet **Certificats d'utilisateur de solution**.

   b Sélectionnez un certificat, puis cliquez sur **Renouveler** pour renouveler les certificats individuels sélectionnés ou cliquez sur **Renouveler tout** pour renouveler tous les certificats d'utilisateur de solution.

   c Répondez **Oui** à l'invite.

6 Si votre environnement inclut un Platform Services Controller externe, vous pouvez renouveler les certificats pour chaque système vCenter Server.

   a Cliquez sur le bouton **Se déconnecter** dans le panneau Gestion des certificats.

   b Lorsque vous y êtes invité, spécifiez l'adresse IP ou le nom de domaine du système vCenter Server ainsi que le nom d'utilisateur et le mot de passe d'un administrateur vCenter Server pouvant s'authentifier auprès de vCenter Single Sign-On.

   c Renouvelez le certificat SSL de la machine dans vCenter Server et, si vous le souhaitez, chaque certificat d'utilisateur de solution.

   d Si votre environnement comprend plusieurs systèmes vCenter Server, répétez la procédure pour chaque système.

Suivant

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement *VCENTER_INSTALL_PATH*\bin.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

Faire de VMCA une autorité de certification intermédiaire depuis l'interface web de Platform Services Controller

Vous pouvez faire signer le certificat VMCA par une autre autorité de certification afin que VMCA devienne par la suite une autorité de certification intermédiaire. Tous les certificats générés par VMCA incluent la chaîne complète.

Vous pouvez réaliser cette configuration en utilisant l'utilitaire vSphere Certificate Manager, les CLI ou l'interface web Platform Services Controller.

Prérequis

1 Générer la demande de signature de certificat.

2 Modifiez le certificat que vous recevez et placez le certificat racine VMCA actuel en bas.

« Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire) », page 97 explique les deux étapes.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Pour remplacer le certificat existant par le certificat chaîné, procédez comme suit :

a Dans Certificats, cliquez sur **Autorité de certification** et sélectionnez l'onglet **Certificat racine**.

b Cliquez sur **Remplacer le certificat**. Ajoutez le fichier de clé privée et le fichier de certificat (chaîne complète), puis cliquez sur **OK**.

c Dans la boîte de dialogue **Remplacer le certificat racine**, cliquez sur **Parcourir** et sélectionnez la clé privée, cliquez de nouveau sur **Parcourir** et sélectionnez le certificat, puis cliquez sur **OK**.

Par la suite, VMCA signe tous les certificats qu'il émet avec le nouveau certificat racine chaîné.

4 Renouvelez le certificat SSL de la machine pour le système local.

a Sous Certificats, cliquez sur **Gestion des certificats**, puis cliquez dans l'onglet **Certificats de la machine**.

b Sélectionnez le certificat, cliquez sur **Renouveler**, puis répondez **Oui** à l'invite.

VMCA remplace le certificat de la machine SSL par le certificat signé par la nouvelle autorité de certification.

5 (Facultatif) Renouvelez les certificats d'utilisateur de solution pour le système local.

a Cliquez sur l'onglet **Certificats d'utilisateur de solution**.

b Sélectionnez un certificat, puis cliquez sur **Renouveler** pour renouveler des certificats individuels sélectionnés ou cliquez sur **Renouveler tout** pour remplacer tous les certificats et répondez **Oui** à l'invite.

VMCA remplace le certificat d'utilisateur de solution ou tous les certificats d'utilisateur de solution par des certificats signés par la nouvelle autorité de certification.

6 Si votre environnement inclut un Platform Services Controller externe, vous pouvez renouveler les certificats pour chaque système vCenter Server.

a Cliquez sur le bouton **Se déconnecter** dans le panneau Gestion des certificats.

b Lorsque vous y êtes invité, spécifiez l'adresse IP ou le nom de domaine du système vCenter Server ainsi que le nom d'utilisateur et le mot de passe d'un administrateur vCenter Server pouvant s'authentifier auprès de vCenter Single Sign-On.

c Renouvelez le certificat SSL de la machine dans vCenter Server et, si vous le souhaitez, chaque certificat d'utilisateur de solution.

d Si votre environnement comprend plusieurs systèmes vCenter Server, répétez la procédure pour chaque système.

Suivant

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement *VCENTER_INSTALL_PATH*\bin.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

Configurer votre système pour utiliser des certificats personnalisés depuis Platform Services Controller

Vous pouvez utiliser Platform Services Controller pour configurer votre environnement de manière à utiliser des certificats personnalisés.

Vous pouvez générer des demandes de signature de certificat (CSR, Certificate Signing Requests) pour chaque machine et pour chaque utilisateur de solution employant l'utilitaire Certificate Manager. Lorsque vous soumettez les demandes de signature de certificat à votre autorité de certification interne ou tierce, l'autorité de certification renvoie les certificats signés et le certificat racine. Vous pouvez télécharger le certificat racine et les certificats signés à partir de l'interface utilisateur de Platform Services Controller.

Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés)

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR, Certificate Signing Request) que vous pouvez ensuite utiliser avec votre autorité de certification d'entreprise ou envoyer à une autorité de certification externe. Vous pouvez utiliser les certificats avec les différents processus de remplacement de certificat pris en charge.

Vous pouvez exécuter l'outil Certificate Manager sur la ligne de commande comme suit :

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Prérequis

vSphere Certificate Manager vous invite à fournir des informations. Les invites dépendent de votre environnement et du type de certificat que vous souhaitez remplacer.

- Pour la génération d'une demande de signature de certificat, vous êtes invité à entrer le mot de passe de l'utilisateur administrator@vsphere.local ou de l'administrateur du domaine vCenter Single Sign-On auquel vous vous connectez.
- Si vous générez une demande de signature de certificat dans un environnement avec une instance de Platform Services Controller externe, vous êtes invité à entrer le nom d'hôte ou l'adresse IP de Platform Services Controller.

- Pour générer une demande de signature du certificat SSL d'une machine, vous êtes invité à entrer les propriétés du certificat, qui sont stockées dans le fichier `certool.cfg`. Pour la plupart des champs, vous pouvez accepter les valeurs par défaut ou entrer des valeurs spécifiques au site. Le FQDN de la machine est requis.

Procédure

1. Sur chaque machine de votre environnement, démarrez vSphere Certificate Manager et sélectionnez l'option 1.
2. Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
3. Sélectionnez l'option 1 pour générer la demande de signature de certificat, répondez aux invites et quittez Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat et les fichiers clés dans le répertoire.
4. Si vous souhaitez remplacer tous les certificats d'utilisateurs de solutions, redémarrez Certificate Manager.
5. Sélectionnez l'option 5.
6. Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
7. Sélectionnez l'option 1 pour générer les demandes de signature de certificat, répondez aux invites et quittez Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat et les fichiers clés dans le répertoire.

   Sur chaque nœud de Platform Services Controller, Certificate Manager génère un certificat et une paire de clés. Sur chaque nœud vCenter Server, Certificate Manager génère quatre certificats et paires de clés.

Suivant

Effectuez le remplacement de certificats.

Ajouter un certificat racine approuvé au magasin de certificats

Si vous souhaitez utiliser des certificats tiers dans votre environnement, vous devez ajouter un certificat racine approuvé au magasin de certificats.

Prérequis

Obtenez le certificat racine personnalisé de votre autorité de certification tierce ou interne.

Procédure

1. Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

   Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.

4 Sélectionnez **Certificats racines approuvés**, puis cliquez sur **Ajouter un certificat**.

5 Cliquez sur **Parcourir** et sélectionnez l'emplacement de la chaîne de certificats.

   Vous pouvez utiliser un fichier de type CER, PEM ou CRT.

Suivant

Remplacez les certificats SSL de la machine et, facultativement, les certificats d'utilisateur de solution par des certificats signés par cette autorité de certification.

Ajouter des certificats personnalisés à partir de Platform Services Controller

Vous pouvez ajouter des certificats SSL de la machine et des certificats d'utilisateur de solution personnalisés au magasin de certificats à partir de Platform Services Controller.

Dans la plupart des cas, il suffit de remplacer le certificat SSL de la machine pour chaque composant. Le certificat de l'utilisateur de solution reste derrière un proxy.

Prérequis

Générez des demandes de signature de certificat (CSR, Certificate Signing Request) pour chaque certificat que vous souhaitez remplacer. Vous pouvez générer les CSR avec l'utilitaire Certificate Manager. Placez le certificat et la clé privée dans un emplacement accessible par Platform Services Controller.

Procédure

1 Dans un navigateur Web, connectez-vous à vSphere Web Client ou à Platform Services Controller.

Option	Description
vSphere Web Client	`https://vc_hostname_or_IP/vsphere-client`
Platform Services Controller	`https://psc_hostname_or_IP/psc` Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

2 Spécifiez le nom d'utilisateur et le mot de passe pour administrator@vsphere.local ou un autre membre du groupe d'administrateurs de vCenter Single Sign-On.

   Si vous avez spécifié un autre domaine lors de l'installation, connectez-vous en tant qu'administrator@*mydomain*.

3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.

4 Pour remplacer un certificat de la machine, procédez comme suit :

   a Sélectionnez l'onglet **Certificats de la machine** et cliquez sur le certificat que vous souhaitez remplacer.

   b Cliquez sur **Remplacer**, puis sur **Parcourir** pour remplacer la chaîne de certificats, puis sur **Parcourir** pour remplacer la clé privée.

5 Pour remplacer les certificats d'utilisateur de la solution, procédez comme suit :

a Sélectionnez l'onglet **Certificats d'utilisateurs de solutions**, puis cliquez sur le premier des quatre certificats d'un composant, par exemple, **machine**.

b Cliquez sur **Remplacer**, puis sur **Parcourir** pour remplacer la chaîne de certificats, puis sur **Parcourir** pour remplacer la clé privée.

c Recommencez le processus pour les trois autres certificats du même composant.

Suivant

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement *VCENTER_INSTALL_PATH*\bin.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

Gestion des certificats depuis vSphere Web Client

Vous pouvez explorer les certificats à partir de vSphere Web Client et définir le seuil pour les avertissements d'expiration. Réalisez toutes les autres tâches de gestion depuis l'interface web de Platform Services Controller.

Reportez-vous à « Gestion de certificats avec l'interface Web Platform Services Controller », page 83.

Afficher les certificats vCenter dans vSphere Web Client

Vous pouvez afficher les certificats connus de l'autorité de certification vCenter (VMCA) pour savoir si les certificats actifs sont sur le point d'expirer, vérifier les certificats expirés et consulter l'état du certificat racine. Vous devez effectuer toutes les tâches de gestion des certificats au moyen des interfaces de ligne de commande de gestion des certificats.

Vous pouvez afficher les certificats associés à l'instance de VMCA incluse dans votre déploiement intégré ou fournie avec Platform Services Controller. Les informations relatives aux certificats sont répliquées dans les instances du service d'annuaire VMware (vmdir).

Lorsque vous tentez d'afficher les certificats dans vSphere Web Client, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Spécifiez le nom et le mot de passe d'un utilisateur disposant de privilèges pour l'autorité de certification VMware, c'est-à-dire un utilisateur du groupe CAAdmins vCenter Single Sign-On.

Procédure

1 Connectez-vous à vCenter Server en tant que administrator@vsphere.local ou un autre utilisateur du groupe CAAdmins vCenter Single Sign-On.

2 Dans le menu Accueil, sélectionnez **Administration**.

3 Cliquez sur **Nœuds**, puis sélectionner le nœud pour lequel vous souhaitez afficher ou gérer des certificats.

4 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Autorité de certification**.

5 Cliquez sur le type de certificat pour lequel vous voulez afficher des informations relatives au certificat.

Option	Description
Certificats actifs	Affiche les certificats actifs, y compris les informations de validation les concernant. L'icône verte de date de fin de validité change lorsque la date d'expiration du certificat approche.
Certificats révoqués	Affiche la liste des certificats révoqués. Non pris en charge dans cette version.
Certificats expirés	Répertorie les certificats arrivés à expiration.
Certificats racine	Affiche les certificats racines disponibles pour cette instance de l'autorité de certification vCenter.

6 Sélectionnez un certificat et cliquez sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat.

Les détails comprennent le nom du sujet, l'émetteur, la validité et l'algorithme.

Définir le seuil pour les avertissements d'expiration du certificat vCenter

Depuis vSphere 6.0, vCenter Server gère tous les certificats du magasin VECS (VMware Endpoint Certificate Store) et émet une alarme lorsque le délai d'expiration d'un certificat est inférieur ou égal à 30 jours. Vous pouvez modifiez le délai d'avertissement à l'aide de l'option avancée `vpxd.cert.threshold`.

Procédure

1 Connectez-vous à vSphere Web Client.

2 Sélectionnez l'objet vCenter Server et cliquez sur **Configurer**.

3 Cliquez sur **Paramètres avancés** et filtrez pour le **`seuil`**.

4 Modifiez le paramètre de `vpxd.cert.threshold` en saisissant la valeur souhaitée et cliquez sur **OK**.

Gestion de certificats avec l'utilitaire vSphere Certificate Manager

L'utilitaire vSphere Certificate Manager vous permet de réaliser la plupart des tâches de gestion des certificats de manière interactive, à partir de la ligne de commande. vSphere Certificate Manager vous demande la tâche à réaliser, l'emplacement des certificats, ainsi que d'autres informations si nécessaire, puis active et arrête les services et remplace les certificats.

Si vous utilisez vSphere Certificate Manager, vous n'avez pas à placer les certificats dans VECS (VMware Endpoint Certificate Store), ni à démarrer et à arrêter les services.

Avant d'exécuter vSphere Certificate Manager, veillez à bien comprendre le processus de remplacement et procurez-vous les certificats que vous souhaitez utiliser.

Avertissement vSphere Certificate Manager gère un niveau d'annulation. Si vous exécutez vSphere Certificate Manager deux fois et remarquez que vous avez endommagé votre environnement par inadvertance, l'outil ne peut pas annuler la première des deux exécutions.

Emplacement de l'utilitaire Certificate Manager

Vous pouvez exécuter l'outil sur la ligne de commande comme suit :

Windows `C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat`

Linux `/usr/lib/vmware-vmca/bin/certificate-manager`

1 Options de Certificate Manager et les workflows dans ce document page 93

Vous exécutez les options de Certificate Manager de manière séquentielle pour effectuer un workflow. Par exemple, plusieurs options générant des demandes de signature de certificat sont utilisées dans différents workflows.

2 Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats page 95

Vous pouvez régénérer le certificat racine VMCA et remplacer le certificat SSL de la machine locale, ainsi que les certificats d'utilisateur de la solution locale par des certificats signés par VMCA. Dans les déploiements à nœuds multiples, exécutez vSphere Certificate Manager avec cette option sur Platform Services Controller, réexécutez ensuite l'utilitaire sur tous les autres nœuds et sélectionnez `Replace Machine SSL certificate with VMCA Certificate` et `Replace Solution user certificates with VMCA certificates`.

3 Faire de VMCA une autorité de certification intermédiaire (Certificate Manager) page 96

Vous pouvez faire de VMCA une autorité de certification intermédiaire en suivant les invites de l'utilitaire Certificate Manager. À la fin du processus, VMCA signe tous les nouveaux certificats avec la chaîne complète. Si vous le souhaitez, vous pouvez utiliser Certificate Manager pour remplacer tous les certificats existants par de nouveaux certificats signés par VMCA.

4 Remplacer tous les certificats par des certificats personnalisés (Certificate Manager) page 101

Vous pouvez employer l'utilitaire vSphere Certificate Manager pour remplacer tous les certificats par des certificats personnalisés. Avant de démarrer le processus, vous devez envoyer des demandes de signature de certificat (CSR) à votre autorité de certification. Vous pouvez utiliser Certificate Manager pour générer les demandes de signature de certificat.

5 Restaurer la dernière opération effectuée via la republication des anciens certificats page 105

Lorsque vous effectuez une opération de gestion de certificats en utilisant vSphere Certificate Manager, l'état actuel du certificat est stocké dans le magasin BACKUP_STORE de VECS avant le remplacement des certificats. Vous pouvez restaurer la dernière opération effectuée et revenir à l'état antérieur.

6 Réinitialiser tous les certificats page 105

Utilisez l'option `Réinitialiser tous les certificats` si vous voulez remplacer tous les certificats vCenter existants par des certificats signés par VMCA.

Options de Certificate Manager et les workflows dans ce document

Vous exécutez les options de Certificate Manager de manière séquentielle pour effectuer un workflow. Par exemple, plusieurs options générant des demandes de signature de certificat sont utilisées dans différents workflows.

Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats.

Il s'agit d'un workflow à option unique (option 2) pouvant être utilisé de façon autonome dans le workflow de certificat intermédiaire. Reportez-vous à « Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats », page 95.

Faire de VMCA une autorité de certification intermédiaire

Pour faire de VMCA une autorité de certification intermédiaire, vous devez exécuter Certificate Manager plusieurs fois. Le workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions. Il explique la marche à suivre dans les environnements comportant des instances intégrées de Platform Services Controller ou des instances externes de Platform Services Controller.

1 Pour générer une demande de signature de certificat, sélectionnez l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats. Vous devrez ensuite éventuellement fournir des informations sur le certificat. Lorsqu'un message vous invite à choisir de nouveau une option, sélectionnez Option 1.

   Soumettez la demande de signature de certificat à votre autorité de certification externe ou d'entreprise. Vous recevez un certificat signé et un certificat racine de l'autorité de certification.

2 Combinez le certificat racine VMCA au certificat racine de l'autorité de certification et enregistrez le fichier.

3 Sélectionnez l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats. Ce processus remplace tous les certificats sur la machine locale.

4 Dans un déploiement à nœuds multiples, vous devez remplacer les certificats sur chaque nœud.

   a Vous remplacez d'abord le certificat SSL de la machine par le (nouveau) certificat VMCA (option 3).

   b Vous remplacez ensuite les certificats de l'utilisateur de solutions par le (nouveau) certificat VMCA (option 6).

Reportez-vous à « Faire de VMCA une autorité de certification intermédiaire (Certificate Manager) », page 96

Remplacement de tous les certificats par des certificats personnalisés

Pour remplacer tous les certificats par des certificats personnalisés, vous devez exécuter Certificate Manager plusieurs fois. Le workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions. Il explique la marche à suivre dans les environnements comportant des instances intégrées de Platform Services Controller ou des instances externes de Platform Services Controller.

1 Vous générez des demandes de signature de certificat pour le certificat SSL de la machine et les certificats d'utilisateurs de solutions séparément sur chaque machine.

   a Pour générer des demandes de signature de certificat pour le certificat SSL de la machine, vous sélectionnez l'option 1.

   b Si la stratégie de l'entreprise impose le remplacement de tous les certificats, vous sélectionnez également l'option 5.

2 Après la réception des certificats signés et du certificat racine de votre autorité de certification, vous remplacez le certificat SSL de machine sur chaque machine à l'aide de l'option 1.

3 Si vous souhaitez également remplacer les certificats d'utilisateurs de solutions, vous sélectionnez l'option 5.

4 Enfin, dans un déploiement à nœuds multiples, vous devez répéter le processus sur chaque nœud.

Reportez-vous à « Remplacer tous les certificats par des certificats personnalisés (Certificate Manager) », page 101.

Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats

Vous pouvez régénérer le certificat racine VMCA et remplacer le certificat SSL de la machine locale, ainsi que les certificats d'utilisateur de la solution locale par des certificats signés par VMCA. Dans les déploiements à nœuds multiples, exécutez vSphere Certificate Manager avec cette option sur Platform Services Controller, réexécutez ensuite l'utilitaire sur tous les autres nœuds et sélectionnez `Replace Machine SSL certificate with VMCA Certificate` et `Replace Solution user certificates with VMCA certificates`.

Lorsque vous remplacez le certificat SSL machine existant par un nouveau certificat signé par VMCA, vSphere Certificate Manager vous invite à fournir des informations et à entrer toutes les valeurs, à l'exception du mot passe et de l'adresse IP de Platform Services Controller, dans le fichier `certool.cfg`.

- Mot de passe pour administrator@vsphere.local.
- Code pays à deux lettres
- Nom de la société
- Nom de l'organisation
- Unité d'organisation
- État
- Ville
- adresse IP (facultatif)
- E-mail
- Nom de l'hôte, à savoir le nom de domaine complet de la machine dont vous souhaitez remplacer le certificat. Si le nom de l'hôte ne correspond pas au nom de domaine complet, le remplacement du certificat ne se fait pas correctement et votre environnement risque de devenir instable.
- Adresse IP du Platform Services Controller si vous exécutez la commande sur un nœud de gestion

Prérequis

Vous devez disposer des informations suivantes lorsque vous exécutez vSphere Certificate Manager avec cette option.

- Mot de passe pour administrator@vsphere.local.
- Nom de domaine complet de la machine pour laquelle vous souhaitez générer un nouveau certificat signé par VMCA. Toutes les autres propriétés sont configurées par défaut sur les valeurs prédéfinies mais peuvent être modifiées.

Procédure

1. Démarrez vSphere Certificate Manager sur un déploiement intégré ou sur une instance de Platform Services Controller.
2. Sélectionnez l'option 4.
3. Répondez aux invites.

   Certificate Manager génère un nouveau certificat racine VMCA basé sur votre entrée et remplace tous les certificats sur le système où vous exécutez Certificate Manager. Si vous utilisez un déploiement intégré, le processus de remplacement est terminé après que Certificate Manager a redémarré les services.

4 Si votre environnement inclut une instance externe de Platform Services Controller, vous devez remplacer les certificats sur chaque système vCenter Server.

   a Connectez-vous au système vCenter Server.

   b Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

   Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

   Windows

   ```
   service-control --stop --all
   service-control --start VMWareAfdService
   service-control --start VMWareDirectoryService
   service-control --start VMWareCertificateService
   ```

   vCenter Server Appliance

   ```
   service-control --stop --all
   service-control --start vmafdd
   service-control --start vmdird
   service-control --start vmcad
   ```

   c Redémarrez tous les services.

   ```
   service-control --start --all
   ```

   d Pour remplacer le certificat SSL de la machine, exécutez vSphere Certificate Manager avec l'option 3, `Replace Machine SSL certificate with VMCA Certificate`.

   e Pour remplacer les certificats d'utilisateurs de solutions, exécutez Certificate Manager avec l'option 6, `Replace Solution user certificates with VMCA certificates`.

Faire de VMCA une autorité de certification intermédiaire (Certificate Manager)

Vous pouvez faire de VMCA une autorité de certification intermédiaire en suivant les invites de l'utilitaire Certificate Manager. À la fin du processus, VMCA signe tous les nouveaux certificats avec la chaîne complète. Si vous le souhaitez, vous pouvez utiliser Certificate Manager pour remplacer tous les certificats existants par de nouveaux certificats signés par VMCA.

Pour faire de VMCA une autorité de certification intermédiaire, vous devez exécuter Certificate Manager plusieurs fois. Le workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions. Il explique la marche à suivre dans les environnements comportant des instances intégrées de Platform Services Controller ou des instances externes de Platform Services Controller.

1 Pour générer une demande de signature de certificat, sélectionnez l'option 1, Remplacer le certificat SSL de machine par un certificat personnalisé, puis l'option 1.

   Vous recevez un certificat signé et un certificat racine de l'autorité de certification.

2 Combinez le certificat racine VMCA au certificat racine de l'autorité de certification et enregistrez le fichier.

3 Sélectionnez l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats. Ce processus remplace tous les certificats sur la machine locale.

4 Dans un déploiement à nœuds multiples, vous devez remplacer les certificats sur chaque nœud.

   a Vous remplacez d'abord le certificat SSL de la machine par le (nouveau) certificat VMCA (option 3).

   b Vous remplacez ensuite les certificats de l'utilisateur de solutions par le (nouveau) certificat VMCA (option 6).

Procédure

1 Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire) page 97

   Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat. Soumettez ces demandes de signature de certificat à l'autorité de certification de votre entreprise ou à une autorité de certification externe pour une signature. Vous pouvez utiliser les certificats signés avec les différents processus de remplacement de certificat pris en charge.

2 Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats page 99

   Vous pouvez envoyer le certificat racine VMCA comme une demande de signature de certificat à une autorité de certification d'enterprise ou de tiers, et combiner le certificat VMCA signé au certificat racine VMCA. Après le remplacement du certificat racine VMCA par la chaîne de certificats, tous les certificats que VMCA génère incluent la chaîne complète.

3 Remplacer le certificat SSL machine par un certificat VMCA (autorité de certification intermédiaire) page 100

   Dans un déploiement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous devez remplacer explicitement le certificat SSL machine. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats SSL machine qui sont altérés ou sur le point d'expirer.

4 Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA (autorité de certification intermédiaire) page 101

   Dans un environnement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous pouvez remplacer explicitement les certificats d'utilisateurs de solutions. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats d'utilisateurs de solutions qui sont altérés ou sur le point d'expirer.

Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire)

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat. Soumettez ces demandes de signature de certificat à l'autorité de certification de votre entreprise ou à une autorité de certification externe pour une signature. Vous pouvez utiliser les certificats signés avec les différents processus de remplacement de certificat pris en charge.

- Vous pouvez utiliser vSphere Certificate Manager pour générer la demande de signature de certificat.
- Si vous préférez créer la demande de signature de certificat manuellement, le certificat envoyé pour signature doit satisfaire les conditions suivantes :
  - Taille de clé : 2 048 bits ou plus
  - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
  - x509 version 3
  - Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises.
  - La signature CRL doit être activée.

- `Enhanced Key Usage` ne doit contenir ni `Client Authentication` ni `Server Authentication`.
- L'heure doit être synchronisée sur tous les nœuds de votre environnement.
- Aucune limite explicite à la longueur de la chaîne de certificats. VMCA utilise la valeur par défaut OpenSSL, qui est de dix certificats.
- VMCA ne prend pas en charge les certificats comportant des caractères génériques ou plusieurs noms DNS.
- Vous ne pouvez pas créer d'autorités de certification filiales de VMCA.

  Reportez-vous à l'article 2112009 de la base de connaissances de VMware, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

Prérequis

vSphere Certificate Manager vous invite à fournir des informations. Les invites dépendent de votre environnement et du type de certificat que vous souhaitez remplacer.

Pour la génération d'une demande de signature de certificat, vous êtes invité à entrer le mot de passe de l'utilisateur administrator@vsphere.local ou de l'administrateur du domaine vCenter Single Sign-On auquel vous vous connectez.

Procédure

1 Démarrez vSphere Certificate Manager et sélectionnez l'option 2.

  Initialement, vous utilisez cette option pour générer la demande de signature de certificat, pas pour remplacer des certificats.

2 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.

3 Sélectionnez l'option 1 pour générer la demande de signature de certificat et répondez aux invites.

  Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat à signer (fichier `*.csr`) et le fichier de clés correspondant (fichier `*.key`) dans le répertoire.

4 Envoyez le certificat pour signature à l'autorité de certification d'entreprise ou à l'autorité de certification externe, puis nommez le fichier `root_signing_cert.cer`.

5 Dans un éditeur de texte, combinez les certificats de la façon suivante.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

6 Enregistrez le fichier en tant que `root_signing_chain.cer`.

Suivant

Remplacez le certificat racine existant par le certificat racine chaîné. Reportez-vous à « Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats », page 99.

Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats

Vous pouvez envoyer le certificat racine VMCA comme une demande de signature de certificat à une autorité de certification d'enterprise ou de tiers, et combiner le certificat VMCA signé au certificat racine VMCA. Après le remplacement du certificat racine VMCA par la chaîne de certificats, tous les certificats que VMCA génère incluent la chaîne complète.

Exécutez vSphere Certificate Manager sur une installation intégrée ou sur un Platform Services Controller externe pour remplacer le certificat racine VMCA par un certificat de signature personnalisé.

Prérequis

- Générez la chaîne de certificats.
  - Vous pouvez utiliser vSphere Certificate Manager pour créer la demande de signature de certificat ou pour créer manuellement la demande de signature de certificat.
  - Après la réception du certificat signé de l'autorité de certification de tiers ou d'entreprise, combinez-le au certificat racine VMCA initial pour créer la chaîne complète.

    Reportez-vous à « Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire) », page 97 pour les conditions requise des certificats et le processus de combinaison des certificats.
- Rassemblez les informations qui vous seront nécessaires.
  - Mot de passe pour administrator@vsphere.local.
  - Certificat personnalisé valable pour Root (fichier .crt).
  - Clé personnalisée valide pour l'utilisateur racine (fichier .key).

Procédure

1. Démarrez vSphere Certificat Manager sur une installation intégrée ou un Platform Services Controller externe et sélectionnez l'option 2.
2. Sélectionnez de nouveau l'option 2 pour démarrer le remplacement des certificats et répondez aux invites.
   a. Spécifiez le chemin complet du certificat racine lorsque vous y êtes invité.
   b. Si vous remplacez des certificats pour la première fois, vous êtes invité à saisir des informations utilisées pour le certificat SSL de machine.

      Ces informations, qui incluent le domaine requis de la machine, sont conservées dans le fichier `certool.cfg`.
3. Si vous remplacez le certificat racine sur l'instance de Platform Services Controller dans un déploiement à nœuds multiples, procédez comme suit pour chaque nœud vCenter Server.
   a. Redémarrez les services sur le nœud vCenter Server
   b. Régénérez tous les certificats de l'instance vCenter Server en utilisant les options 3 (Remplacer les certificats SSL de la machine par des certificats signés par VMCA) et 6 (Remplacer les certificats d'utilisateurs de solution par des certificats signés par VMCA).

   Lorsque vous remplacez les certificats, VMCA signe avec la chaîne complète.

Suivant

Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à « Remplacer le certificat VMware Directory Service dans des environnement en mode mixte », page 116.

Remplacer le certificat SSL machine par un certificat VMCA (autorité de certification intermédiaire)

Dans un déploiement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous devez remplacer explicitement le certificat SSL machine. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats SSL machine qui sont altérés ou sur le point d'expirer.

Lorsque vous remplacez le certificat SSL machine existant par un nouveau certificat signé par VMCA, vSphere Certificate Manager vous invite à fournir des informations et à entrer toutes les valeurs, à l'exception du mot passe et de l'adresse IP de Platform Services Controller, dans le fichier `certool.cfg`.

- Mot de passe pour administrator@vsphere.local.
- Code pays à deux lettres
- Nom de la société
- Nom de l'organisation
- Unité d'organisation
- État
- Ville
- adresse IP (facultatif)
- E-mail
- Nom de l'hôte, à savoir le nom de domaine complet de la machine dont vous souhaitez remplacer le certificat. Si le nom de l'hôte ne correspond pas au nom de domaine complet, le remplacement du certificat ne se fait pas correctement et votre environnement risque de devenir instable.
- Adresse IP du Platform Services Controller si vous exécutez la commande sur un nœud de gestion

Prérequis

- Redémarrez explicitement tous les nœuds vCenter Server si vous avez remplacé le certificat racine VMCA dans un déploiement à plusieurs nœuds.
- Vous devez disposer des informations suivantes pour exécuter Certificate Manager avec cette option.
  - Mot de passe pour administrator@vsphere.local.
  - Nom de domaine complet de la machine pour laquelle vous souhaitez générer un nouveau certificat signé par VMCA. Toutes les autres propriétés sont configurées par défaut sur les valeurs prédéfinies mais peuvent être modifiées.
  - Le nom d'hôte ou l'adresse IP de Platform Services Controller si vous utilisez un système vCenter Server disposant d'un Platform Services Controller externe.

Procédure

1 Démarrez vSphere Certificate Manager et sélectionnez l'option 3.

2 Répondez aux invites.

  Certificate Manager enregistre les informations dans le fichier `certool.cfg`.

vSphere Certificate Manager remplace le certificat machine SSL.

Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA (autorité de certification intermédiaire)

Dans un environnement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous pouvez remplacer explicitement les certificats d'utilisateurs de solutions. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats d'utilisateurs de solutions qui sont altérés ou sur le point d'expirer.

Prérequis

- Redémarrez explicitement tous les nœuds vCenter Server si vous avez remplacé le certificat racine VMCA dans un déploiement à plusieurs nœuds.
- Vous devez disposer des informations suivantes pour exécuter Certificate Manager avec cette option.
  - Mot de passe pour administrator@vsphere.local.
  - Le nom d'hôte ou l'adresse IP de Platform Services Controller si vous utilisez un système vCenter Server disposant d'un Platform Services Controller externe.

Procédure

1 Démarrez vSphere Certificate Manager et sélectionnez l'option 6.

2 Répondez aux invites.

vSphere Certificate Manager remplace tous les certificats d'utilisateurs de solutions.

Remplacer tous les certificats par des certificats personnalisés (Certificate Manager)

Vous pouvez employer l'utilitaire vSphere Certificate Manager pour remplacer tous les certificats par des certificats personnalisés. Avant de démarrer le processus, vous devez envoyer des demandes de signature de certificat (CSR) à votre autorité de certification. Vous pouvez utiliser Certificate Manager pour générer les demandes de signature de certificat.

Une option consiste à uniquement remplacer le certificat SSL de la machine, puis d'utiliser les certificats d'utilisateurs de solutions fournis par VMCA. Les certificats d'utilisateurs de solutions sont utilisés uniquement pour la communication entre les composants de vSphere.

Lorsque vous utilisez des certificats personnalisés, vous remplacez les certificats signés par VMCA par des certificats personnalisés. Vous pouvez utiliser l'interface Web de Platform Services Controller, l'utilitaire vSphere Certificate Manager ou l'interface de ligne de commande pour procéder à un remplacement manuel des certificats. Les certificats sont stockés dans VECS.

Pour remplacer tous les certificats par des certificats personnalisés, vous devez exécuter Certificate Manager plusieurs fois. Le workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions. Il explique la marche à suivre dans les environnements comportant des instances intégrées de Platform Services Controller ou des instances externes de Platform Services Controller.

1 Vous générez des demandes de signature de certificat pour le certificat SSL de la machine et les certificats d'utilisateurs de solutions séparément sur chaque machine.
   a Pour générer des demandes de signature de certificat pour le certificat SSL de la machine, vous sélectionnez l'option 1.
   b Si la stratégie de l'entreprise n'autorise pas un déploiement hybride, vous sélectionnez l'option 5.

2 Après la réception des certificats signés et du certificat racine de votre autorité de certification, vous remplacez le certificat SSL de machine sur chaque machine à l'aide de l'option 1.

3 Si vous souhaitez également remplacer les certificats d'utilisateurs de solutions, vous sélectionnez l'option 5.

4 Enfin, dans un déploiement à nœuds multiples, vous devez répéter le processus sur chaque nœud.

Procédure

1 Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés) page 102

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR, Certificate Signing Request) que vous pouvez ensuite utiliser avec votre autorité de certification d'entreprise ou envoyer à une autorité de certification externe. Vous pouvez utiliser les certificats avec les différents processus de remplacement de certificat pris en charge.

2 Remplacer le certificat SSL de machine par un certificat personnalisé page 103

Le certificat SSL de machine est utilisé par le service de proxy inverse sur chaque nœud de gestion, Platform Services Controller et chaque déploiement intégré. Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Vous pouvez remplacer le certificat sur chaque nœud par un certificat personnalisé.

3 Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés page 104

Bon nombre d'entreprises demandent uniquement à ce que vous remplaciez les certificats de services accessibles de façon externe. Toutefois, Certificate Manager prend uniquement en charge le remplacement des certificats de l'utilisateur de solution. Les utilisateurs de solutions sont des collections de services, par exemple, tous les services associés à vSphere Web Client dans les déploiements multi-nœuds remplacent le certificat de l'utilisateur de solution de la machine sur Platform Services Controller et l'ensemble complet d'utilisateurs de solutions sur chaque nœud de gestion.

Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés)

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR, Certificate Signing Request) que vous pouvez ensuite utiliser avec votre autorité de certification d'entreprise ou envoyer à une autorité de certification externe. Vous pouvez utiliser les certificats avec les différents processus de remplacement de certificat pris en charge.

Vous pouvez exécuter l'outil Certificate Manager sur la ligne de commande comme suit :

Windows `C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat`

Linux `/usr/lib/vmware-vmca/bin/certificate-manager`

Prérequis

vSphere Certificate Manager vous invite à fournir des informations. Les invites dépendent de votre environnement et du type de certificat que vous souhaitez remplacer.

- Pour la génération d'une demande de signature de certificat, vous êtes invité à entrer le mot de passe de l'utilisateur administrator@vsphere.local ou de l'administrateur du domaine vCenter Single Sign-On auquel vous vous connectez.
- Si vous générez une demande de signature de certificat dans un environnement avec une instance de Platform Services Controller externe, vous êtes invité à entrer le nom d'hôte ou l'adresse IP de Platform Services Controller.
- Pour générer une demande de signature du certificat SSL d'une machine, vous êtes invité à entrer les propriétés du certificat, qui sont stockées dans le fichier `certool.cfg`. Pour la plupart des champs, vous pouvez accepter les valeurs par défaut ou entrer des valeurs spécifiques au site. Le FQDN de la machine est requis.

Procédure

1. Sur chaque machine de votre environnement, démarrez vSphere Certificate Manager et sélectionnez l'option 1.
2. Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
3. Sélectionnez l'option 1 pour générer la demande de signature de certificat, répondez aux invites et quittez Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat et les fichiers clés dans le répertoire.
4. Si vous souhaitez remplacer tous les certificats d'utilisateurs de solutions, redémarrez Certificate Manager.
5. Sélectionnez l'option 5.
6. Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
7. Sélectionnez l'option 1 pour générer les demandes de signature de certificat, répondez aux invites et quittez Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat et les fichiers clés dans le répertoire.

   Sur chaque nœud de Platform Services Controller, Certificate Manager génère un certificat et une paire de clés. Sur chaque nœud vCenter Server, Certificate Manager génère quatre certificats et paires de clés.

Suivant

Effectuez le remplacement de certificats.

Remplacer le certificat SSL de machine par un certificat personnalisé

Le certificat SSL de machine est utilisé par le service de proxy inverse sur chaque nœud de gestion, Platform Services Controller et chaque déploiement intégré. Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Vous pouvez remplacer le certificat sur chaque nœud par un certificat personnalisé.

Prérequis

Avant de commencer, vous avez besoin d'une demande de signature de certificat pour chaque machine de votre environnement. Vous pouvez générer la demande de signature de certificat à l'aide de vSphere Certificate Manager ou explicitement.

1. Pour générer la demande de signature de certificat à l'aide de vSphere Certificate Manager, reportez-vous à « Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés) », page 88.
2. Pour générer la demande de signature de certificat explicitement, demander un certificat pour chaque machine de votre autorité de certification tierce ou d'entreprise. Le certificat doit répondre à la configuration requise suivante :
   - Taille de clé : 2 048 bits ou plus (codée au format PEM)
   - Format CRT
   - x509 version 3
   - SubjectAltName doit contenir DNS Name=<machine_FQDN>

- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Reportez-vous également à l'article 2112014 de la base de connaissances, Obtention de certificats vSphere depuis une autorité de certification Microsoft.

Procédure

1 Démarrez vSphere Certificate Manager et sélectionnez l'option 1.

2 Sélectionnez l'option 2 pour démarrer le remplacement des certificats et répondre aux invites.

vSphere Certificate Manager vous invite à fournir les informations suivantes :

- Mot de passe pour administrator@vsphere.local.
- Certificat personnalisé SSL valide de la machine (fichier .crt).
- Clé personnalisée SSL valide de la machine (fichier .key).
- Certificat de signature valide pour le certificat personnalisé SSL de la machine (fichier .crt).
- Si vous exécutez la commande sur un nœud de gestion dans un déploiement à plusieurs nœuds, adresse IP de Platform Services Controller.

Suivant

Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à « Remplacer le certificat VMware Directory Service dans des environnement en mode mixte », page 116.

Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Bon nombre d'entreprises demandent uniquement à ce que vous remplaciez les certificats de services accessibles de façon externe. Toutefois, Certificate Manager prend uniquement en charge le remplacement des certificats de l'utilisateur de solution. Les utilisateurs de solutions sont des collections de services, par exemple, tous les services associés à vSphere Web Client dans les déploiements multi-nœuds remplacent le certificat de l'utilisateur de solution de la machine sur Platform Services Controller et l'ensemble complet d'utilisateurs de solutions sur chaque nœud de gestion.

Prérequis

Avant de commencer, vous avez besoin d'une demande de signature de certificat pour chaque machine de votre environnement. Vous pouvez générer la demande de signature de certificat à l'aide de vSphere Certificate Manager ou explicitement.

1 Pour générer la demande de signature de certificat à l'aide de vSphere Certificate Manager, reportez-vous à « Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés) », page 88.

2 Demandez un certificat pour chaque utilisateur de solution sur chaque nœud auprès de votre autorité de certification tierce ou d'entreprise. Vous pouvez générer la demande de signature de certificat à l'aide de vSphere Certificate Manager ou la préparer vous-même. La demande de signature de certificat doit répondre aux exigences suivantes :

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format CRT
- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>

- Chaque certificat d'utilisateur de la solution doit avoir un paramètre `Subject` différent. Vous pouvez par exemple saisir le nom de l'utilisateur de la solution (tel que vpxd) ou un autre identifiant unique.
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Reportez-vous également à l'article 2112014 de la base de connaissances, Obtention de certificats vSphere depuis une autorité de certification Microsoft.

Procédure

1 Démarrez vSphere Certificate Manager et sélectionnez l'option 5.

2 Sélectionnez l'option 2 pour démarrer le remplacement des certificats et répondre aux invites.

vSphere Certificate Manager vous invite à fournir les informations suivantes :

- Mot de passe pour administrator@vsphere.local.
- Certificat et clé de l'utilisateur de solution de machine
- Si vous exécutez vSphere Certificate Manager sur un nœud Platform Services Controller, vous êtes invité à saisir le certificat et la clé (`vpxd.crt` et `vpxd.key`) pour l'utilisateur de solution de machine.
- Si vous exécutez vSphere Certificate Manager sur un nœud de gestion ou sur un déploiement intégré, vous êtes invité à indiquer l'ensemble complet de certificats et de clés (`vpxd.crt` et `vpxd.key`) pour tous les utilisateurs de solution.

Suivant

Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à « Remplacer le certificat VMware Directory Service dans des environnement en mode mixte », page 116.

Restaurer la dernière opération effectuée via la republication des anciens certificats

Lorsque vous effectuez une opération de gestion de certificats en utilisant vSphere Certificate Manager, l'état actuel du certificat est stocké dans le magasin BACKUP_STORE de VECS avant le remplacement des certificats. Vous pouvez restaurer la dernière opération effectuée et revenir à l'état antérieur.

Remarque L'opération de restauration restaure le contenu de BACKUP_STORE. Si vous exécutez vSphere Certificate Manager avec deux options différentes, puis que vous tentez d'effectuer une restauration, seule la dernière opération est restaurée.

Réinitialiser tous les certificats

Utilisez l'option `Réinitialiser tous les certificats` si vous voulez remplacer tous les certificats vCenter existants par des certificats signés par VMCA.

Si vous utilisez cette option, tous les certificats personnalisés qui se trouvent actuellement dans VECS sont remplacés.

- Sur un nœud Platform Services Controller, vSphere Certificate Manager peut régénérer le certificat racine et remplacer le certificat SSL de machine et le certificat d'utilisateur de solution de machine.
- Sur un nœud de gestion, vSphere Certificate Manager peut remplacer le certificat SSL de machine et tous les certificats d'utilisateurs de solutions de machine.
- Dans un déploiement intégré, vSphere Certificate Manager peut remplacer tous les certificats.

Les certificats remplacés dépendent des options que vous sélectionnez.

Remplacement manuel de certificats

Dans des situations particulières, par exemple si vous voulez remplacer un seul type de certificat d'utilisateur de solution, vous ne pouvez pas utiliser l'utilitaire vSphere Certificate Manager. Dans ce cas, vous pouvez utiliser les interfaces de ligne de commande incluses dans votre installation pour le remplacement de certificat.

Régles générales de démarrage et d'arrêt des services

Pour certaines parties du remplacement manuel de certificat, vous devez arrêter tous les services, puis démarrer uniquement les services qui gèrent l'infrastructure de certificats. Si vous n'arrêtez les services qu'en cas de besoin, vous pouvez réduire les interruptions.

Suivez ces règles générales.

- N'arrêtez pas les services pour générer de nouvelles paires de clé publique/privée ou de nouveaux certificats.
- Si vous êtes le seul administrateur, il n'est pas nécessaire d'arrêter les services lorsque vous ajoutez un nouveau certificat racine. L'ancien certificat racine demeure disponible et tous les services peuvent toujours s'authentifier avec ce certificat. Arrêtez, puis redémarrez immédiatement tous les services après avoir ajouté le certificat racine pour éviter les problèmes avec vos hôtes.
- Si votre environnement inclut plusieurs administrateurs, arrêtez les services avant d'ajouter un nouveau certificat racine et redémarrez-le après l'ajout d'un nouveau certificat.
- Arrêtez les services juste avant d'effectuer les tâches suivantes :
  - Supprimer un certificat d'utilisateur de solution de machine ou tout certificat d'utilisateur de solution dans VECS.
  - Remplacer un certificat d'utilisateur de solution dans vmdir (service d'annuaire VMware).

Remplacer les certificats existants signés par l'autorité de certification VMware (VMCA) par de nouveaux certificats

Si le certificat racine VMCA expire dans un avenir proche ou si vous voulez le remplacer pour d'autres raisons, vous pouvez générer un nouveau certificat racine et l'ajouter au service d'annuaire VMware. Vous pouvez alors générer de nouveaux certificats SSL de machine et certificats d'utilisateurs de solutions au moyen du nouveau certificat racine.

Faites appel à l'utilitaire vSphere Certificate Manager pour remplacer les certificats dans la plupart des cas.

Si vous avez besoin d'un contrôle précis, ce scénario fournit des instructions pas à pas permettant de remplacer l'ensemble complet de certificats au moyen de commandes d'interface de ligne de commande. Vous pouvez remplacer uniquement des certificats individuels au moyen de la procédure indiquée dans la tâche correspondante.

Prérequis

Seul l'utilisateur administrator@vsphere.local ou d'autres utilisateurs du groupe peuvent effectuer des tâches de gestion de certificats. Reportez-vous à « Ajouter des membres à un groupe vCenter Single Sign-On », page 67.

Procédure

1 Générer un nouveau certificat racine signé par VMCA page 107

Vous générez de nouveaux certificats signés par VMCA avec l'interface de ligne de commande `certool` ou l'utilitaire vSphere Certificate Manager, et publiez les certificats dans vmdir.

2 Remplacer les certificats SSL de la machine par des certificats signés par VMCA page 108

Une fois que vous avez généré un nouveau certificat racine signé par VMCA, vous pouvez remplacer tous les certificats SSL de machine de votre environnement.

3 Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA page 111

Après avoir remplacé les certificats SSL de la machine, vous pouvez remplacer tous les certificats des utilisateurs de solutions. Les certificats d'utilisateurs de solutions doivent être valides (ils ne sont pas arrivés à expiration), mais l'infrastructure de certificats n'utilise aucune des autres informations d'un certificat.

4 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte page 116

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Générer un nouveau certificat racine signé par VMCA

Vous générez de nouveaux certificats signés par VMCA avec l'interface de ligne de commande `certool` ou l'utilitaire vSphere Certificate Manager, et publiez les certificats dans vmdir.

Dans un déploiement à plusieurs nœuds, vous exécutez des commandes de génération de certificats racines sur Platform Services Controller.

Procédure

1 Générez un nouveau certificat auto-signé et une clé privée.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 Remplacez le certificat racine existant par le nouveau certificat.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

La commande génère le certificat et l'ajoute à vmdir, puis à VECS.

3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 (Facultatif) Publiez le nouveau certificat racine dans vmdir.

```
dir-cli trustedcert publish --cert newRoot.crt
```

La commande met à jour toutes les instances de vmdir immédiatement. Si vous n'exécutez pas la commande, la propagation du nouveau certificat dans tous les nœuds peut prendre un certain temps.

5 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Générer un nouveau certificat racine signé par VMCA

L'exemple suivant montre toutes les étapes nécessaires à la vérification des informations de l'autorité de certification racine actuelle et à la régénération du certificat racine.

1 (Facultatif) Affichez le certificat racine VMCA pour vous assurer qu'il se trouve dans le magasin de certificats.

- Sur un nœud Platform Services Controller ou une installation intégrée :

  ```
  C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
  ```

- Sur un nœud de gestion (installation externe) :

  ```
  C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
  ```

Le résultat est semblable à ce qui suit :

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (Facultatif) Affichez le magasin VECS TRUSTED_ROOTS et comparez le numéro de série du certificat qui s'y trouve au résultat de l'étape 1.

Cette commande fonctionne sur les nœuds Platform Services Controller et sur les nœuds de gestion, car VECS interroge vmdir.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS  --text
```

Dans le cas le plus simple avec un seul certificat racine, le résultat est semblable à ce qui suit :

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 Générez un nouveau certificat racine VMCA. La commande ajoute le certificat au magasin TRUSTED_ROOTS dans VECS et dans vmdir (Vmware Directory Service).

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Sous Windows, `--config` est facultatif, car la commande utilise le fichier `certool.cfg` par défaut.

Remplacer les certificats SSL de la machine par des certificats signés par VMCA

Une fois que vous avez généré un nouveau certificat racine signé par VMCA, vous pouvez remplacer tous les certificats SSL de machine de votre environnement.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un noeud vCenter Server avec une instance de Platform Services Controller externe.

Prérequis

Soyez prêt à arrêter tous les services et à démarrer ceux qui gèrent la propagation et le stockage des certificats.

Procédure

1 Faites une copie de `certool.cfg` pour toutes les machines ayant besoin d'un nouveau certificat.

Vous pouvez rechercher `certool.cfg` dans l'un des emplacements suivants :

Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 Modifiez le fichier de configuration personnalisée de chaque machine pour inclure le nom de domaine complet de la machine.

Exécutez `NSLookup` sur l'adresse IP de la machine pour voir le nom figurant dans la liste DNS et utilisez ce nom pour le champ Hostname du fichier.

3 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque fichier, en transmettant le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --config
machine1.cfg
```

4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Ajoutez le nouveau certificat à VECS.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL. Vous devez d'abord supprimer l'entrée existante, puis ajouter la nouvelle entrée.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
 --key machine1.priv
```

6 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Remplacement des certificats SSL de la machine par des certificats signés par VMCA

1 Créez un fichier de configuration pour le certificat SSL et enregistrez-le sous le nom `ssl-config.cfg` dans le répertoire actuel.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 Générez une paire de clés pour le certificat SSL de machine. Exécutez cette commande sur chaque nœud de gestion et nœud Platform Services Controller ; elle ne requiert pas d'option `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv --
pubkey=ssl-key.pub
```

Les fichiers `ssl-key.priv` et `ssl-key.pub` sont créés dans le répertoire actuel.

3 Générez le nouveau certificat SSL de machine. Ce certificat est signé par VMCA. Si vous remplacez le certificat racine VMCA par un certificat personnalisé, VMCA signe tous les certificats avec la chaîne complète.

- Sur un nœud Platform Services Controller ou une installation intégrée :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Sur vCenter Server (installation externe) :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

Le fichier `new-vmca-ssl.crt` est créé dans le répertoire actuel.

4 (Facultatif) Répertoriez le contenu de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Exemple de sortie sur Platform Services Controller :

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Exemple de sortie sur vCenter Server :

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Remplacez le certificat SSL de machine dans VECS par le nouveau certificat SSL de machine. Les valeurs `--store` et `--alias` doivent correspondre exactement aux noms par défaut.

- Sur Platform Services Controller, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Sur chaque nœud de gestion ou déploiement intégré, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT. Vous devez mettre à jour le certificat de chaque machine séparément. En effet, chaque machine possède un nom de domaine complet qui lui est propre.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Suivant

Vous pouvez également remplacer les certificats de vos hôtes ESXi. Consultez la publication *Sécurité vSphere*.

Après avoir remplacé le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les noeuds vCenter Server avec une instance de Platform Services Controller externe.

Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA

Après avoir remplacé les certificats SSL de la machine, vous pouvez remplacer tous les certificats des utilisateurs de solutions. Les certificats d'utilisateurs de solutions doivent être valides (ils ne sont pas arrivés à expiration), mais l'infrastructure de certificats n'utilise aucune des autres informations d'un certificat.

De nombreux clients VMware ne remplacent pas les certificats d'utilisateur de solution. Ils se contentent de remplacer les certificats SSL de la machine par des certificats personnalisés. Cette approche hybride répond aux exigences de leurs équipes de sécurité.

- Les certificats se trouvent derrière un proxy, ou ce sont des certificats personnalisés.
- Aucune autorité de certification intermédiaire n'est utilisée.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers le Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

Prérequis

Soyez prêt à arrêter tous les services et à démarrer ceux qui gèrent la propagation et le stockage des certificats.

Procédure

1 Faites une copie de `certool.cfg`, supprimez les champs Nom, Adresse IP, Nom DNS et E-mail, puis remplacez le nom du fichier par `sol_usr.cfg`, par exemple.

Vous pouvez nommer les certificats de la ligne de commande dans le cadre de la génération. Les autres informations ne sont pas nécessaires pour les utilisateurs de la solution. Si vous laissez les informations par défaut, les certificats générés peuvent être source de confusion.

2 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque utilisateur de solution, puis transmettez le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Pour chaque utilisateur de solution, remplacez le certificat existant dans vmdir, puis dans VECS.

L'exemple suivant indique comment remplacer les certificats pour le service vpxd.

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Remarque Les utilisateurs de solutions ne peuvent pas s'authentifier auprès de vCenter Single Sign-On si vous ne remplacez pas le certificat dans vmdir.

6 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Utilisation des certificats d'utilisateurs de solutions signés par VMCA

1 Générez une paire de clé publique/clé privée pour chaque utilisateur de solution. Cela inclut une paire pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.

   a Générez une paire de clés pour l'utilisateur de solution de machine d'un déploiement intégré ou pour l'utilisateur de solution de machine de Platform Services Controller.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   b (Facultatif) Pour les déploiements comportant un Platform Services Controller externe, générez une paire de clés pour l'utilisateur de solution de machine sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
   ```

   c Générez une paire de clés pour l'utilisateur de solution vpxd sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
   ```

   d Générez une paire de clés pour l'utilisateur de solution vpxd-extension sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
   ```

   e Générez une paire de clés pour l'utilisateur de solution vsphere-webclient sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
   ```

2 Générez des certificats d'utilisateurs de solutions qui sont signés par le nouveau certificat racine MCA pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.

   Remarque Le paramètre `--Name` doit être unique. Le fait d'inclure le nom du magasin de l'utilisateur de solution permet de voir facilement la correspondance entre un certificat et un utilisateur de solution. L'exemple inclut le nom, par exemple `vpxd` ou `vpxd-extension`, dans chaque cas.

   a Exécutez la commande suivante sur le nœud Platform Services Controller pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
   ```

   b Générez un certificat pour l'utilisateur de solution de machine sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
   ```

   c Générez un certificat pour l'utilisateur de solution vpxd sur chaque nœud de gestion.

   ```
   C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
   ```

d Générez un certificat pour l'utilisateur de solution vpxd-extensions sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e Générez un certificat pour l'utilisateur de solution vsphere-webclient sur chaque nœud de gestion en exécutant la commande suivante.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

3 Remplacez les certificats d'utilisateurs de solutions dans VECS par les nouveaux certificats d'utilisateurs de solutions.

Remarque Les paramètres `--store` et `--alias` doivent correspondre exactement aux noms par défaut des services.

a Sur le nœud Platform Services Controller, exécutez la commande suivante pour remplacer le certificat d'utilisateur de solution de machine :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud de gestion :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Remplacez le certificat d'utilisateur de solution vpxd sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Remplacez le certificat d'utilisateur de solution vpxd-extension sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

e Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

4 Mettez à jour VMware Directory Service (vmdir) avec les nouveaux certificats d'utilisateurs de solutions. Vous êtes invité à entrer un mot de passe d'administrateur vCenter Single Sign-On.

a Exécutez `dir-cli service list` pour obtenir le suffixe d'ID de service unique pour chaque utilisateur de solution. Vous pouvez exécuter cette commande sur un système Platform Services Controller ou vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

b Remplacez le certificat de machine dans vmdir sur Platform Services Controller. Par exemple, si machine-29a45d00-60a7-11e4-96ff-00505689639a correspond à l'utilisateur de solution de machine sur Platform Services Controller, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c Remplacez le certificat de machine dans vmdir sur chaque nœud de gestion. Par exemple, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'utilisateur de solution de machine sur vCenter Server, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d Remplacez le certificat d'utilisateur de solution vpxd dans vmdir sur chaque nœud de gestion. Par exemple, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e Remplacez le certificat d'utilisateur de solution vpxd-extension dans vmdir sur chaque nœud de gestion. Par exemple, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd-extension, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud de gestion. Par exemple, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vsphere-webclient, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Suivant

Redémarrez tous les services sur chaque nœud Platform Services Controller et chaque nœud de gestion.

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Remarque La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

1 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.

   a Effectuez une sauvegarde de tous les fichiers de `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Faites une copie du fichier `vmdircert.pem` sur le nœud 6.x, et renommez-le `<sso_node2.domain.com>.pem`, où `<sso_node2.domain.com>` est le nom de domaine complet du nœud .x.

   c Copiez le certificat renommé dans `C:\ProgramData\VMware\CIS\cfg\vmdird` pour remplacer le certificat de réplication existant.

2 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

   Vous pouvez redémarer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Utiliser VMCA en tant qu'autorité de certificat intermédiaire

Vous pouvez remplacer le certificat racine VMCA par un certificat signé par une autorité de certification tierce qui inclut VMCA dans la chaîne de certificats. Par la suite, tous les certificats générés par VMCA incluent l'ensemble de la chaîne. Vous pouvez remplacer des certificats existants par des certificats qui viennent d'être générés.

Procédure

1 Remplacer le certificat racine (autorité de certification intermédiaire) page 117

   La première étape du remplacement des certificats VMCA par des certificats personnalisés est la génération d'une demande de signature de certificat, l'envoi de la demande de signature de certificat pour signature et l'ajout du certificat signé à VMCA en tant que certificat racine.

2 Remplacer les certificats SSL de la machine (autorité de certification intermédiaire) page 119

Après avoir reçu le certificat signé de l'autorité de certification et en avoir fait le certificat racine VMCA, vous pouvez remplacer tous les certificats SSL de machine.

3 Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire) page 122

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution.

4 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte page 126

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Remplacer le certificat racine (autorité de certification intermédiaire)

La première étape du remplacement des certificats VMCA par des certificats personnalisés est la génération d'une demande de signature de certificat, l'envoi de la demande de signature de certificat pour signature et l'ajout du certificat signé à VMCA en tant que certificat racine.

Vous pouvez utiliser l'utilitaire Certificate Manager ou un autre outil pour générer la demande de signature de certificat. La demande de signature de certificat doit répondre à la configuration requise suivante :

- Taille de clé : 2 048 bits ou plus
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
- x509 version 3
- Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises.
- La signature CRL doit être activée.
- `Enhanced Key Usage` ne doit contenir ni `Client Authentication` ni `Server Authentication`.
- L'heure doit être synchronisée sur tous les nœuds de votre environnement.
- Aucune limite explicite à la longueur de la chaîne de certificats. VMCA utilise la valeur par défaut OpenSSL, qui est de dix certificats.
- VMCA ne prend pas en charge les certificats comportant des caractères génériques ou plusieurs noms DNS.
- Vous ne pouvez pas créer d'autorités de certification filiales de VMCA.

  Reportez-vous à l'article 2112009 de la base de connaissances de VMware, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

VMCA valide les attributs suivants du certificat lorsque vous remplacez le certificat racine :

- Taille de clé de 2 048 bits ou plus
- Utilisation de clé : signature de certification
- Contrainte de base : autorité de certification du type de sujet

Procédure

1 Générez une demande de signature de certificat et envoyez-la à votre autorité de certification.

Suivez les instructions de votre autorité de certification.

2 Préparez un fichier de certificat qui inclut le certificat VMCA signé ainsi que la chaîne complète de l'autorité de certification de votre autorité de certification tierce ou de votre autorité de certification d'entreprise, et enregistrez le fichier, par exemple sous le nom `rootca1.crt`.

   Vous pouvez le faire en copiant tous les certificats de l'autorité de certification au format PEM dans un fichier unique. Vous devez commencer par le certificat racine VMCA et terminer par le certificat racine CA PEM. Par exemple :

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

   Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

   Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

   vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Remplacez l'autorité de certification racine VMCA existante.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

   Lorsque vous exécutez cette commande, elle :

   - Ajoute le nouveau certificat racine personnalisé à l'emplacement des certificats dans le système de fichiers.
   - Ajoute le certificat racine personnalisé au magasin TRUSTED_ROOTS dans VECS (après un délai).
   - Ajoute le certificat racine personnalisé à vmdir (après un délai).

5 (Facultatif) Pour propager le changement à toutes les instances de vmdir (VMware Directory Service), publiez le nouveau certificat racine dans vmdir, en fournissant le chemin complet de chaque fichier.

   Par exemple :

```
dir-cli trustedcert publish --cert rootca1.crt
```

   La réplication entre les nœuds vmdir se produit toutes les 30 secondes. Il n'est pas nécessaire d'ajouter le certificat racine à VECS de façon explicite, car VECS interroge vmdir concernant les fichiers de certificat racine toutes les 5 minutes.

6 (Facultatif) Le cas échéant, vous pouvez forcer une opération d'actualisation de VECS.

```
vecs-cli force-refresh
```

7 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Remplacement du certificat racine

Remplacez le certificat racine VMCA par le certificat racine VMCA personnalisé en utilisant la commande certool avec l'option `--rootca`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-
certs\root.pem --privkey=C:\custom-certs\root.key
```

Lorsque vous exécutez cette commande, elle :

- Ajoute le nouveau certificat racine personnalisé à l'emplacement des certificats dans le système de fichiers.
- Ajoute le certificat racine personnalisé au magasin TRUSTED_ROOTS dans VECS.
- Ajoute le certificat racine personnalisé à vmdir.

Suivant

Vous pouvez supprimer le certificat racine VMCA initial du magasin de certificats si la stratégie de l'entreprise l'exige. Dans ce cas, vous devez remplacer le certificat de signature de vCenter Single Sign-On. Reportez-vous à « Actualiser le certificat STS », page 53

Remplacer les certificats SSL de la machine (autorité de certification intermédiaire)

Après avoir reçu le certificat signé de l'autorité de certification et en avoir fait le certificat racine VMCA, vous pouvez remplacer tous les certificats SSL de machine.

Cette procédure est en grande partie identique à celle mise en œuvre pour le remplacement par un certificat qui utilise VMCA comme autorité de certification. Néanmoins, dans ce cas, VMCA signe tous les certificats avec la chaîne complète.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un noeud vCenter Server avec une instance de Platform Services Controller externe.

Prérequis

Pour chaque certificat SSL de machine, le `SubjectAltName` doit contenir `DNS Name=<Machine FQDN>`.

Procédure

1 Faites une copie de `certool.cfg` pour toutes les machines ayant besoin d'un nouveau certificat.

Vous pouvez rechercher `certool.cfg` dans l'un des emplacements suivants :

Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 Modifiez le fichier de configuration personnalisée de chaque machine pour inclure le nom de domaine complet de la machine.

Exécutez `NSLookup` sur l'adresse IP de la machine pour voir le nom figurant dans la liste DNS et utilisez ce nom pour le champ Hostname du fichier.

3 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque machine, en transmettant le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Ajoutez le nouveau certificat à VECS.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL. Vous devez d'abord supprimer l'entrée existante, puis ajouter la nouvelle entrée.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Remplacement des certificats SSL de machine (VMCA est l'autorité de certification intermédiaire)

1 Créez un fichier de configuration pour le certificat SSL et enregistrez-le sous le nom `ssl-config.cfg` dans le répertoire actuel.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 Générez une paire de clés pour le certificat SSL de machine. Exécutez cette commande sur chaque nœud de gestion et nœud Platform Services Controller ; elle ne requiert pas d'option `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv --
pubkey=ssl-key.pub
```

Les fichiers `ssl-key.priv` et `ssl-key.pub` sont créés dans le répertoire actuel.

3 Générez le nouveau certificat SSL de machine. Ce certificat est signé par VMCA. Si vous remplacez le certificat racine VMCA par un certificat personnalisé, VMCA signe tous les certificats avec la chaîne complète.

- Sur un nœud Platform Services Controller ou une installation intégrée :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Sur vCenter Server (installation externe) :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

Le fichier `new-vmca-ssl.crt` est créé dans le répertoire actuel.

4 (Facultatif) Répertoriez le contenu de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Exemple de sortie sur Platform Services Controller :

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Exemple de sortie sur vCenter Server :

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 Remplacez le certificat SSL de machine dans VECS par le nouveau certificat SSL de machine. Les valeurs `--store` et `--alias` doivent correspondre exactement aux noms par défaut.

- Sur Platform Services Controller, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Sur chaque nœud de gestion ou déploiement intégré, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT. Vous devez mettre à jour le certificat de chaque machine séparément. En effet, chaque machine possède un nom de domaine complet qui lui est propre.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire)

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution.

De nombreux clients VMware ne remplacent pas les certificats d'utilisateur de solution. Ils se contentent de remplacer les certificats SSL de la machine par des certificats personnalisés. Cette approche hybride répond aux exigences de leurs équipes de sécurité.

- Les certificats se trouvent derrière un proxy, ou ce sont des certificats personnalisés.
- Aucune autorité de certification intermédiaire n'est utilisée.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers le Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

Prérequis

Chaque certificat d'utilisateur de la solution doit avoir un paramètre `Subject` différent. Vous pouvez par exemple saisir le nom de l'utilisateur de la solution (tel que vpxd) ou un autre identifiant unique.

Procédure

1 Faites une copie de `certool.cfg`, supprimez les champs Nom, Adresse IP, Nom DNS et E-mail, puis remplacez le nom du fichier par `sol_usr.cfg`, par exemple.

Vous pouvez nommer les certificats de la ligne de commande dans le cadre de la génération. Les autres informations ne sont pas nécessaires pour les utilisateurs de la solution. Si vous laissez les informations par défaut, les certificats générés peuvent être source de confusion.

2 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque utilisateur de solution, puis transmettez le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 Remplacement du certificat existant dans vmdir puis dans VECS.

Pour les utilisateurs de solution, vous devez ajouter les certificats dans cet ordre. Par exemple :

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

Remarque Les utilisateurs de solution ne peuvent pas se connecter à vCenter Single Sign-On si vous ne remplacez pas le certificat dans vmdir.

6 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire)

1 Générez une paire de clé publique/clé privée pour chaque utilisateur de solution. Cela inclut une paire pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.

a Générez une paire de clés pour l'utilisateur de solution de machine d'un déploiement intégré ou pour l'utilisateur de solution de machine de Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b (Facultatif) Pour les déploiements comportant un Platform Services Controller externe, générez une paire de clés pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

c Générez une paire de clés pour l'utilisateur de solution vpxd sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

d Générez une paire de clés pour l'utilisateur de solution vpxd-extension sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

e Générez une paire de clés pour l'utilisateur de solution vsphere-webclient sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

2 Générez des certificats d'utilisateurs de solutions qui sont signés par le nouveau certificat racine MCA pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.

Remarque Le paramètre `--Name` doit être unique. Le fait d'inclure le nom du magasin de l'utilisateur de solution permet de voir facilement la correspondance entre un certificat et un utilisateur de solution. L'exemple inclut le nom, par exemple `vpxd` ou `vpxd-extension`, dans chaque cas.

a Exécutez la commande suivante sur le nœud Platform Services Controller pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

b Générez un certificat pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c Générez un certificat pour l'utilisateur de solution vpxd sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d Générez un certificat pour l'utilisateur de solution vpxd-extensions sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e Générez un certificat pour l'utilisateur de solution vsphere-webclient sur chaque nœud de gestion en exécutant la commande suivante.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

3 Remplacez les certificats d'utilisateurs de solutions dans VECS par les nouveaux certificats d'utilisateurs de solutions.

Remarque Les paramètres `--store` et `--alias` doivent correspondre exactement aux noms par défaut des services.

a Sur le nœud Platform Services Controller, exécutez la commande suivante pour remplacer le certificat d'utilisateur de solution de machine :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud de gestion :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c Remplacez le certificat d'utilisateur de solution vpxd sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --
alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --
alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d Remplacez le certificat d'utilisateur de solution vpxd-extension sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 Mettez à jour VMware Directory Service (vmdir) avec les nouveaux certificats d'utilisateurs de solutions. Vous êtes invité à entrer un mot de passe d'administrateur vCenter Single Sign-On.

a Exécutez `dir-cli service list` pour obtenir le suffixe d'ID de service unique pour chaque utilisateur de solution. Vous pouvez exécuter cette commande sur un système Platform Services Controller ou vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

b Remplacez le certificat de machine dans vmdir sur Platform Services Controller. Par exemple, si machine-29a45d00-60a7-11e4-96ff-00505689639a correspond à l'utilisateur de solution de machine sur Platform Services Controller, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c Remplacez le certificat de machine dans vmdir sur chaque nœud de gestion. Par exemple, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'utilisateur de solution de machine sur vCenter Server, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d Remplacez le certificat d'utilisateur de solution vpxd dans vmdir sur chaque nœud de gestion. Par exemple, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e Remplacez le certificat d'utilisateur de solution vpxd-extension dans vmdir sur chaque nœud de gestion. Par exemple, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd-extension, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud de gestion. Par exemple, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vsphere-webclient, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Remarque La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

1 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.

   a Effectuez une sauvegarde de tous les fichiers de `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Faites une copie du fichier `vmdircert.pem` sur le nœud 6.x, et renommez-le `<sso_node2.domain.com>.pem`, où `<sso_node2.domain.com>` est le nom de domaine complet du nœud .x.

   c Copiez le certificat renommé dans `C:\ProgramData\VMware\CIS\cfg\vmdird` pour remplacer le certificat de réplication existant.

2 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

   Vous pouvez redémarer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Utiliser des certificats personnalisés avec vSphere

Si la stratégie de l'entreprise l'exige, vous pouvez remplacer partiellement ou totalement les certificats utilisés dans vSphere par des certificats signés par une autorité de certification d'entreprise ou tierce. Le cas échéant, VMCA n'est pas votre chaîne de certificats. Il vous incombe de stocker tous les certificats vCenter dans VECS.

Vous pouvez remplacer tous les certificats ou utiliser une solution hybride. Par exemple, envisagez de remplacer tous les certificats qui sont utilisés pour le trafic réseau mais de conserver les certificats d'utilisateurs de la solution signés par VMCA. Les certificats d'utilisateurs de solutions sont utilisés uniquement pour l'authentification auprès de vCenter Single Sign-On.

Remarque Si vous ne souhaitez pas utiliser VMCA, vous devrez remplacer vous-même tous les certificats, fournir de nouveaux composants avec des certificats et gérer l'expiration des certificats.

Procédure

1 Demander des certificats et importer un certificat racine personnalisé page 128

   Vous pouvez utiliser des certificats personnalisés d'une autorité de certification d'entreprise ou tierce. La première étape consiste à demander les certificats auprès de l'autorité de certification et à importer les certificats racines dans VECS.

2 Remplacer les certificats SSL de machine par des certificats personnalisés page 129

   Après avoir reçu les certificats personnalisés, vous pouvez remplacer chaque certificat de machine.

3 Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés page 130

   Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution signés par VMCA par des certificats tiers ou de l'entreprise.

4 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte page 132

   Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Demander des certificats et importer un certificat racine personnalisé

Vous pouvez utiliser des certificats personnalisés d'une autorité de certification d'entreprise ou tierce. La première étape consiste à demander les certificats auprès de l'autorité de certification et à importer les certificats racines dans VECS.

Prérequis

Le certificat doit répondre à la configuration requise suivante :

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
- x509 version 3
- Pour les certificats racines, l'extension d'autorité de certification doit être définie sur vrai et la signature de certification doit figurer dans la liste de conditions requises.
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Format CRT
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
- Heure de début antérieure d'un jour à l'heure actuelle
- CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.

Procédure

1. Envoyez des demandes de signature de certificat pour les certificats suivants à votre entreprise ou à un fournisseur tiers de certificats.
   - Un certificat SSL de machine pour chaque machine. Pour le certificat SSL de machine, le champ SubjectAltName doit contenir le nom de domaine complet (NOM DNS=*FQDN_machine*)
   - Éventuellement, quatre certificats d'utilisateurs de solutions pour chaque système intégré ou nœud de gestion. Les certificats d'utilisateurs de solutions ne doivent pas inclure d'adresse IP, de nom d'hôte ou d'adresse e-mail. Chaque certificat doit avoir un sujet de certificat différent.
   - Un certificat utilisateur de solution de machine pour les instances externes de Platform Services Controller est également possible. Ce certificat diffère du certificat SSL de machine pour l'instance de Platform Services Controller.

   En général, le résultat est un fichier PEM pour la chaîne d'approbation, plus les certificats SSL signés pour chaque Platform Services Controller ou nœud de gestion.
2. Répertoriez les magasins TRUSTED_ROOTS et SSL de machine.

   ```
   vecs-cli store list
   ```

   a. Assurez-vous que le certificat racine actuel et tous les certificats SSL de machine sont signés par VMCA.

   b. Prenez note des champs du numéro de série, de l'émetteur et du CN du sujet.

   c. (Facultatif) À l'aide d'un navigateur Web, ouvrez une connexion HTTPS à un nœud sur lequel le certificat sera remplacé, vérifiez les informations relatives au certificat et assurez-vous qu'elles correspondent à celles du certificat SSL de machine.

3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 Publiez le certificat racine personnalisé.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

Si vous ne spécifiez pas de nom d'utilisateur et de mot de passe sur la ligne de commande, vous êtes invité à le faire.

5 Redémarrez tous les services.

```
service-control --start --all
```

Suivant

Vous pouvez supprimer le certificat racine VMCA initial du magasin de certificats si la stratégie de l'entreprise l'exige. Dans ce cas, vous devez actualiser le certificat vCenter Single Sign-On. Reportez-vous à « Actualiser le certificat STS », page 53.

Remplacer les certificats SSL de machine par des certificats personnalisés

Après avoir reçu les certificats personnalisés, vous pouvez remplacer chaque certificat de machine.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un noeud vCenter Server avec une instance de Platform Services Controller externe.

Vous devez disposer des informations suivantes avant de pouvoir commencer à remplacer les certificats :

- Mot de passe pour administrator@vsphere.local.
- Certificat personnalisé SSL valide de la machine (fichier .crt).
- Clé personnalisée SSL valide de la machine (fichier .key).
- Certificat personnalisé valable pour Root (fichier .crt).
- Si vous exécutez la commande sur un noeud vCenter Server avec une instance de Platform Services Controller externe dans un déploiement à plusieurs noeuds, l'adresse IP de Platform Services Controller.

Prérequis

Vous devez avoir reçu de votre autorité de certification tierce ou d'entreprise un certificat pour chaque machine.

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format CRT

- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Procédure

1 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

2 Connectez-vous à chaque nœud et ajoutez à VECS les nouveaux certificats de machine que vous avez reçus de l'autorité de certification.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

3 Redémarrez tous les services.

```
service-control --start --all
```

Exemple : Remplacer les certificats SSL de machine par des certificats personnalisés

Vous pouvez remplacer le certificat SSL de machine sur chaque nœud en suivant la même procédure.

1 Tout d'abord, supprimez le certificat existant dans VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 Ensuite, ajoutez le certificat de remplacement.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-cat-
dhcp-1128.vmware.com.priv
```

Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution signés par VMCA par des certificats tiers ou de l'entreprise.

De nombreux clients VMware ne remplacent pas les certificats d'utilisateur de solution. Ils se contentent de remplacer les certificats SSL de la machine par des certificats personnalisés. Cette approche hybride répond aux exigences de leurs équipes de sécurité.

- Les certificats se trouvent derrière un proxy, ou ce sont des certificats personnalisés.

- Aucune autorité de certification intermédiaire n'est utilisée.

Les utilisateurs de solutions utilisent des certificats uniquement pour s'authentifier sur vCenter Single Sign-On. Si le certificat est valide, vCenter Single Sign-On affecte un jeton SAML à l'utilisateur de la solution et ce dernier l'utilise pour s'authentifier vis-à-vis des autres composants vCenter.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers le Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

Remarque Lorsque vous répertoriez les certificats d'utilisateurs de solutions dans des déploiements importants, le résultat de `dir-cli list` inclut tous les utilisateurs de solutions de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

Prérequis

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format CRT
- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Chaque certificat d'utilisateur de la solution doit avoir un paramètre `Subject` différent. Vous pouvez par exemple saisir le nom de l'utilisateur de la solution (tel que vpxd) ou un autre identifiant unique.
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Procédure

1 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

2 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds. Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

3 Pour chaque utilisateur de solution, remplacez le certificat existant dans VECS puis dans vmdir.

Vous devez ajouter les certificats dans cet ordre.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

Remarque Les utilisateurs de solutions ne peuvent pas s'authentifier auprès de vCenter Single Sign-On si vous ne remplacez pas le certificat dans vmdir.

4 Redémarrez tous les services.

```
service-control --start --all
```

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Remarque La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

1 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.

   a Effectuez une sauvegarde de tous les fichiers de `C:\ProgramData\VMware\CIS\cfg\vmdird`.

   b Faites une copie du fichier `vmdircert.pem` sur le nœud 6.x, et renommez-le `<sso_node2.domain.com>.pem`, où `<sso_node2.domain.com>` est le nom de domaine complet du nœud .x.

   c Copiez le certificat renommé dans `C:\ProgramData\VMware\CIS\cfg\vmdird` pour remplacer le certificat de réplication existant.

2 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

   Vous pouvez redémarer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Gestion des services et des certificats avec des interfaces de lignes de commande

4

Un groupe d'interfaces de ligne de commande vous permet de gérer VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) et le VMware Directory Service (vmdir). L'utilitaire vSphere Certificate Manager gère également de nombreuses tâches associées, mais les interfaces de ligne de commande sont indispensables pour la gestion manuelle des certificats et d'autres services.

Tableau 4-1. Outils d'interface de ligne de commande affectés à la gestion des certificats et des services associés

CLI	Description	Reportez-vous à
`certool`	Génère et gère les certificats et les clés. S'exécute dans le cadre de VMCAD, le service de gestion de certificats de VMware.	« Référence des commandes d'initialisation de certool », page 136
`vecs-cli`	Gère les contenus des instances de VMware Certificate Store. Fait partie de VMAFD.	« Référence des commandes vecs-cli », page 141
`dir-cli`	Crée et met à jour les certificats dans le Vmware Directory Service. Fait partie de VMAFD.	« Référence des commandes dir-cli », page 147
`sso-config`	Une partie de la configuration de vCenter Single Sign-On. Dans la plupart des cas, il est recommandé d'utiliser l'interface web de Platform Services Controller. Utilisez cette commande pour configurer l'authentification à deux facteurs.	Aide relative à la ligne de commande. « Authentification à deux facteurs de vCenter Server », page 38
`service-control`	Démarrez ou arrêtez des services, par exemple faisant partie d'un workflow de remplacement de certificat.	

Emplacements d'interfaces de lignes de commande

Par défaut, les emplacements des interfaces de lignes de commande, au sein de chaque nœud, sont les suivants.

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
```

	VCENTER_INSTALL_PATH\bin\service-control
Linux	/usr/lib/vmware-vmafd/bin/vecs-cli /usr/lib/vmware-vmafd/bin/dir-cli /usr/lib/vmware-vmca/bin/certool /opt/vmware/bin Sous Linux, la commande `service-control` ne requiert pas de spécifier le chemin.

Si vous exécutez des commandes dans un système vCenter Server disposant d'une instance externe de Platform Services Controller, vous pouvez spécifier l'instance de Platform Services Controller avec le paramètre `--server`.

Ce chapitre aborde les rubriques suivantes :

Privilèges requis pour l'exécution d'interfaces de lignes de commande

Les privilèges requis varient selon l'interface de ligne de commande utilisée et la commande à exécuter. Par exemple, pour la plupart des opérations de gestion de certificats, vous devez être administrateur du domaine vCenter Single Sign-On local (vsphere.local par défaut). Certaines commandes sont disponibles pour tous les utilisateurs.

dir-cli	Vous devez être membre du groupe d'administrateurs du domaine local (vsphere.local par défaut) pour exécuter les commandes `dir-cli`. Si vous ne spécifiez pas de nom d'utilisateur et de mot de passe, vous êtes invité à saisir le mot de passe de l'administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
vecs-cli	Dans un premier temps, seuls le propriétaire du magasin et les utilisateurs possédant des privilèges d'accès généraux peuvent accéder au magasin. Les utilisateurs appartenant au groupe d'administrateurs sur Windows et les utilisateurs racine sur Linux possèdent des privilèges d'accès généraux. Les magasins MACHINE_SSL_CERT et TRUSTED_ROOTS sont particuliers. Seul l'utilisateur racine ou l'utilisateur Administrateur, selon le type d'installation, dispose d'un accès total à ces magasins.
certool	La plupart des commandes `certool` nécessitent que l'utilisateur soit membre du groupe d'administrateurs. Tous les utilisateurs peuvent exécuter les commandes suivantes. ■ `genselfcacert` ■ `initscr` ■ `getdc`

- waitVMDIR
- waitVMCA
- genkey
- viewcert

Modification des options de configuration de certool

Lorsque vous exécutez `certool --gencert` ou d'autres commandes d'initialisation ou de gestion de certificats, la commande lit toutes les valeurs dans un fichier de configuration. Vous pouvez modifier le fichier existant, remplacer le fichier de configuration par défaut avec l'option `--config=<file name>` ou remplacer des valeurs sur la ligne de commande.

Le fichier de configuration, `certool.cfg`, se trouve à l'emplacement suivant par défaut.

SE	Emplacement
Linux	`/usr/lib/vmware-vmca/config`
Windows	`C:\Program Files\VMware\vCenter Server\vmcad\`

Le fichier comporte plusieurs champs possédant les valeurs par défaut suivantes :

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

Vous pouvez modifier les valeurs en spécifiant un fichier modifié sur la ligne de commande ou en remplaçant les valeurs individuelles sur la ligne de commande de la façon suivante.

- Créez une copie du fichier de configuration, puis modifiez-le. Utilisez l'option de ligne de commande `--config` pour spécifier le fichier. Spécifiez le chemin d'accès complet pour éviter les problèmes de nom de chemin d'accès.
- `certool --gencert --config C:\Temp\myconfig.cfg`
- Remplacez les valeurs individuelles sur la ligne de commande. Par exemple, pour remplacer Locality, exécutez la commande suivante :

  ```
  certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

Spécifiez `--Name` pour remplacer le champ CN du nom de sujet du certificat.

- Pour les certificats d'utilisateurs de solutions, le nom est <nom_utilisateur_solution>@<domaine> par convention, mais vous pouvez le modifier si une autre convention est utilisée dans votre environnement.
- Pour les certificats SSL de la machine, le nom de domaine complet de la machine est utilisé.

  VMCA autorise un seul nom DNS (dans le champ `Hostname`) et aucune autre option d'alias. Si l'adresse IP est spécifiée par l'utilisateur, elle est stockée également dans SubAltName.

Utilisez le paramètre `--Hostname` pour spécifier le nom DNS d'un SubAltName d'un certificat.

Référence des commandes d'initialisation de certool

Les commandes d'initialisation `certool` vous permettent de générer des demandes de signature de certificat, d'afficher et de générer des certificats et des clés qui sont signés par VMCA, d'importer des certificats racines et d'effectuer d'autres opérations de gestion des certificats.

Dans de nombreux cas, vous soumettez un fichier de configuration à une commande `certool`. Reportez-vous à « Modification des options de configuration de certool », page 135. Vous trouverez des exemples d'utilisation à la section « Remplacer les certificats existants signés par l'autorité de certification VMware (VMCA) par de nouveaux certificats », page 106. L'aide de la ligne de commande fournit des détails sur les options.

certool --initcsr

Génère une demande de signature de certificat. La commande génère un fichier PKCS10 et une clé privée.

Option	Description
`--initcsr`	Requis pour générer les demandes de signature de certificat.
`--privkey <key_file>`	Nom du fichier de clé privée.
`--pubkey <key_file>`	Nom du fichier de clé publique.
`--csrfile <csr_file>`	Nom du fichier de demandes de signature de certificat à envoyer au fournisseur d'autorité de certification.
`--config <config_file>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.

Exemple :

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Crée un certificat auto-signé et provisionne le serveur VMCA avec une autorité de certification racine auto-signée. Cette option offre une méthode très simple pour provisionner le serveur VMCA. Si vous préférez, vous pouvez provisionner le serveur VMCA à l'aide d'un certificat racine tiers. Ainsi, VMCA est une autorité de certification intermédiaire. Reportez-vous à « Utiliser VMCA en tant qu'autorité de certificat intermédiaire », page 116.

Cette commande génère un certificat prédaté de trois jours pour éviter les conflits de fuseau horaire.

Option	Description
`--selfca`	Requis pour générer un certificat auto-signé.
`--predate <number_of_minutes>`	Permet de définir le champ Non valide avant du certificat racine sur un nombre de minutes avant l'heure actuelle. Cette option peut s'avérer utile pour contrer les problèmes potentiels liés aux fuseaux horaires. La valeur maximale est de trois jours.

Option	Description
`--config <config_file>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server= 192.0.2.24
--srp-upn=administrator@vsphere.local
```

certool --rootca

Importe un certificat racine. Ajoute le certificat et la clé privée spécifiés à VMCA. VMCA utilise toujours le certificat racine le plus récent pour la signature, mais les autres certificats racine restent approuvés jusqu'à ce que vous les supprimiez manuellement. En d'autres termes, vous pouvez mettre à jour votre infrastructure étape par étape et, à la fin, supprimer les certificats que vous n'utilisez plus.

Option	Description
`--rootca`	Requis pour importer une autorité de certification racine.
`--cert <certfile>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.
`--privkey <key_file>`	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

Renvoie le nom de domaine que vmdir utilise par défaut.

Option	Description
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
`--port <port_num>`	Numéro de port facultatif. La valeur par défaut est le numéro 389.

Exemple :

```
certool --getdc
```

certool --waitVMDIR

Patientez jusqu'à ce que Vmware Directory Service démarre ou jusqu'à ce que le délai spécifié par `--wait` expire. Combinez cette option à d'autres options pour planifier certaines tâches, par exemple le renvoi du nom de domaine par défaut.

Option	Description
`--wait`	Nombre facultatif de minutes à attendre. La valeur par défaut est 3.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
`--port <port_num>`	Numéro de port facultatif. La valeur par défaut est le numéro 389.

Exemple :

```
certool —-waitVMDIR —-wait 5
```

certool --waitVMCA

Patienter jusqu'à ce que le service VMCA démarre ou jusqu'à ce que le délai spécifié expire. Combinez cette option à d'autres options pour planifier certaines tâches, par exemple la génération de certificats.

Option	Description
`--wait`	Nombre facultatif de minutes à attendre. La valeur par défaut est 3.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
`--port <port_num>`	Numéro de port facultatif. La valeur par défaut est le numéro 389.

Exemple :

```
certool —-waitVMCA —-selfca
```

certool --publish-roots

Force la mise à jour des certificats racines. Cette commande nécessite des privilèges d'administration.

Option	Description
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool —-publish—roots
```

Référence des commandes de gestion certool

Les commandes de gestion `certool` vous permettent d'afficher, de générer et de révoquer des certificats ainsi que d'afficher des informations sur les certificats.

certool --genkey

Génère une paire de clés, l'une privée et l'autre publique. Vous pouvez ensuite utiliser ces fichiers pour générer un certificat signé par VMCA.

Option	Description
`--genkey`	Requis pour générer une clé publique et une clé privée.
`--privkey <keyfile>`	Nom du fichier de clé privée.

Option	Description
`--pubkey <keyfile`	Nom du fichier de clé publique.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

Génère un certificat à partir du serveur VMCA. Cette commande utilise les informations fournies dans `certool.cfg` ou dans le fichier de configuration spécifié. Vous pouvez utiliser le certificat pour provisionner des certificats de machine ou des certificats d'utilisateurs de la solution.

Option	Description
`--gencert`	Requis pour générer un certificat.
`--cert <certfile>`	Nom du fichier de certificat. Ce fichier doit être codé au format PEM.
`--privkey <keyfile>`	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
`--config <config_file>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

Imprime le certificat d'autorité de certification racine actuel dans un format lisible par l'œil humain. Si vous exécutez cette commande à partir d'un nœud de gestion, utilisez le nom de machine du nœud Platform Services Controller pour récupérer l'autorité de certification racine. Cette sortie ne peut pas être utilisée en tant que certificat, elle est modifiée pour devenir lisible par l'œil humain.

Option	Description
`--getrootca`	Requis pour imprimer le certificat racine.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --getrootca --server=remoteserver
```

certool --viewcert

Imprime les champs du certificat dans un format lisible par l'œil humain.

Option	Description
`--viewcert`	Requis pour afficher un certificat.
`--cert <certfile>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.

Exemple :

```
certool --viewcert --cert=<filename>
```

certool --enumcert

Répertorie tous les certificats connus du serveur VMCA. L'option `filter` requise vous permet de répertorier tous les certificats ou uniquement les certificats révoqués, actifs ou expirés.

Option	Description
`--enumcert`	Requis pour répertorier tous les certificats.
`--filter [all | active]`	Filtre requis. Spécifiez all ou active. Les options revoked et expired ne sont pas prises en charge actuellement.

Exemple :

```
certool --enumcert --filter=active
```

certool --status

Envoie un certificat spécifié au serveur VMCA pour vérifier si le certificat a été révoqué. Imprime `Certificate: REVOKED` si le certificat est révoqué, sinon `Certificate: ACTIVE`.

Option	Description
`--status`	Requis pour vérifier l'état d'un certificat.
`--cert <certfile>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.
`--server <server>`	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --status --cert=<filename>
```

certool --genselfcacert

Génère un certificat auto-signé en fonction des valeurs fournies dans le fichier de configuration. Cette commande génère un certificat prédaté de trois jours pour éviter les conflits de fuseau horaire.

Option	Description
`--genselfcacert`	Requis pour générer un certificat auto-signé.
`--outcert <cert_file>`	Nom du fichier de certificat. Ce fichier doit être codé au format PEM.

Option	Description
`--outprivkey <key_file>`	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
`--config <config_file>`	Nom facultatif du fichier de configuration. Défini sur `certool.cfg` par défaut.

Exemple :

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

Référence des commandes vecs-cli

Le groupe de commandes `vecs-cli` vous permet de gérer les instances de VMware Certificate Store (VECS). Utilisez ces commandes en conjonction avec `dir-cli` et `certool` pour gérer votre infrastructure de certificats et autres services d'Platform Services Controller.

vecs-cli store create

Crée un magasin de certificats.

Option	Description
`--name <name>`	Nom du magasin de certificats.
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

Exemple :

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Supprime un magasin de certificats. Vous ne pouvez pas supprimer les magasins de système MACHINE_SSL_CERT, TRUSTED_ROOTS et TRUSTED_ROOT_CRLS. Les utilisateurs possédant les privilèges requis peuvent supprimer les magasins d'utilisateurs de solution.

Option	Description
`--name <name>`	Nom du magasin de certificats à supprimer.
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

Exemple :

```
vecs-cli store delete --name <store>
```

vecs-cli store list

Affichez la liste des magasins de certificats.

Option	Description
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

VECS inclut les magasins suivants.

Tableau 4-2. Magasins dans VECS

Magasin	Description
Magasin de certificats SSL de la machine (MACHINE_SSL_CERT)	■ Utilisé par le service de proxy inverse sur chaque nœud vSphere. ■ Utilisé par VMware Directory Service (vmdir) sur les déploiements intégrés et sur chaque nœud Platform Services Controller. Tous les services de vSphere 6.0 communiquent par l'intermédiaire d'un proxy inversé qui utilise le certificat SSL de machine. Pour la compatibilité descendante, les services 5.x utilisent toujours des ports spécifiques. En conséquence, certains services tels que vpxd ont toujours leur port ouvert.
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.

Tableau 4-2. Magasins dans VECS (suite)

Magasin	Description
Magasins d'utilisateurs de solution ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient	VECS inclut un magasin pour chaque utilisateur de solution. L'objet de chaque certificat d'utilisateur de solution doit être unique (par exemple, le certificat de la machine ne peut pas avoir le même objet que le certificat vpxd). Les certificats d'utilisateurs de solutions sont utilisés pour l'authentification avec vCenter Single Sign-On. vCenter Single Sign-On vérifie que le certificat est valide, mais ne vérifie pas d'autres attributs de certificat. Dans un déploiement intégré, tous les certificats d'utilisateur de la solution se trouvent sur le même système. Les magasins de certificats d'utilisateurs de solutions suivants sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré : ■ `machine` : utilisé par le gestionnaire de composants, le serveur de licences et le service de journalisation. **Remarque** Le certificat d'utilisateurs de solution de machine n'a rien à voir avec le certificat SSL de machine. Le certificat d'utilisateur de solution de machine est utilisé pour l'échange de jetons SAML ; le certificat SSL de machine est utilisé pour les connexions SSL sécurisées d'une machine. ■ `vpxd` : magasin de démon du service vCenter (vpxd) sur les nœuds de gestion et les déploiements intégrés. vpxd utilise le certificat d'utilisateur de solution qui est stocké dans ce magasin pour s'authentifier auprès de vCenter Single Sign-On. ■ `vpxd-extensions` : magasin d'extensions vCenter. Inclut le service Auto Deploy, Inventory Service et d'autres services ne faisant pas partie d'autres utilisateurs de solution. ■ `vsphere-webclient` : magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance. Chaque nœud Platform Services Controller comprend un certificat `machine`.
Magasin de sauvegardes de vSphere Certificate Manager Utility (BACKUP_STORE)	Utilisé par VMCA (VMware Certificate Manager) pour prendre en charge la restauration de certificat. Seul l'état le plus récent est stocké en tant que sauvegarde ; vous ne pouvez pas revenir en arrière de plus d'une étape.
Autres magasins	D'autres magasins peuvent être ajoutés par des solutions. Par exemple, la solution Virtual Volumes ajoute un magasin SMS. Ne modifiez pas les certificats dans ces magasins, sauf si la documentation VMware ou un article de la base de connaissances VMware vous y invite. **Remarque** La suppression du magasin TRUSTED_ROOTS_CRLS peut endommager votre infrastructure de certificats. Ne supprimez pas et ne modifiez pas le magasin TRUSTED_ROOTS_CRLS.

Exemple :

```
vecs-cli store list
```

vecs-cli store permissions

Accorde ou révoque des autorisations du magasin. Utilisez l'option `--grant` ou `--revoke`.

Le propriétaire du magasin peut exécuter toutes les opérations, y compris délivrer et retirer des permissions. L'administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut, possède tous les privilèges pour tous les magasins, y compris celui de délivrer et retirer des permissions.

Vous pouvez utiliser `vecs-cli get-permissions --name <store-name>` pour récupérer les paramètres actuels du magasin.

Option	Description
`--name <name>`	Nom du magasin de certificats.
`--user <username>`	Nom unique de l'utilisateur auquel les autorisations sont accordées.
`--grant [read|write]`	Autorisation à accorder : lecture (read) ou écriture (write).
`--revoke [read|write]`	Autorisation à révoquer : lecture (read) ou écriture (write). Commande non prise en charge actuellement.

vecs-cli store get-permissions

Retire les paramètres d'autorisation actifs pour le magasin.

Option	Description
`--name <name>`	Nom du magasin de certificats.
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

vecs-cli entry create

Crée une entrée dans VECS. Utilisez cette commande pour ajouter une clé privée ou un certificat à un magasin.

Option	Description
`--store <NameOfStore>`	Nom du magasin de certificats.
`--alias <Alias>`	Alias facultatif du certificat. Cette option est ignorée pour le magasin racine approuvé.
`--cert <certificate_file_path>`	Chemin complet du fichier de certificat.
`--key <key-file-path>`	Chemin complet de la clé correspondant au certificat. Facultatif.
`--password <password>`	Mot de passe facultatif pour le chiffrement de la clé privée.

Option	Description
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

vecs-cli entry list

Affiche la liste des entrées présentes dans un magasin spécifié.

Option	Description
`--store <NameOfStore>`	Nom du magasin de certificats.

vecs-cli entry getcert

Récupère un certificat de VECS. Vous pouvez envoyer le certificat vers un fichier de sortie ou l'afficher en tant que texte lisible par l'œil humain.

Option	Description
`--store <NameOfStore>`	Nom du magasin de certificats.
`--alias <Alias>`	Alias du certificat.
`--output <output_file_path>`	Fichier dans lequel écrire le certificat.
`--text`	Affiche une version du certificat lisible par l'œil humain.
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

vecs-cli entry getkey

Récupère une clé stockée dans VECS. Vous pouvez envoyer la clé vers un fichier de sortie ou l'afficher en tant que texte lisible par l'œil humain.

Option	Description
`--store <NameOfStore>`	Nom du magasin de certificats.
`--alias <Alias>`	Alias de la clé.
`--output <output_file_path>`	Fichier de sortie dans lequel écrire la clé.
`--text`	Affiche une version de la clé lisible par l'œil humain.

Option	Description
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

vecs-cli entry delete

Supprime une entrée dans un magasin de certificats. Si vous supprimez une entrée dans VECS, vous la supprimez définitivement de VECS. La seule exception est le certificat racine actuel. VECS interroge vmdir pour obtenir un certificat racine.

Option	Description
`--store <NameOfStore>`	Nom du magasin de certificats.
`--alias <Alias>`	Alias de l'entrée à supprimer.
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.
`-y`	Supprime l'invite de confirmation. Pour utilisateurs avancés uniquement.

vecs-cli force-refresh

Force l'actualisation de VECS. Par défaut, VECS interroge vmdir toutes les 5 minutes à la recherche de nouveaux fichiers de certificat racine. Utilisez cette commande pour mettre à jour VECS immédiatement à partir de vmdir.

Option	Description
`--server <server-name>`	Utilisé pour spécifier un nom de serveur si vous vous connectez à une instance distante de VECS.
`--upn <user-name>`	Nom principal de l'utilisateur utilisé pour se connecter à l'instance de serveur spécifiée par `--server <server-name>` . Lorsque vous créez un magasin, celui-ci est créé dans le contexte de l'utilisateur actuel. Par conséquent, le propriétaire du magasin est le contexte de l'utilisateur actuel et pas toujours l'utilisateur racine.

Référence des commandes dir-cli

L'utilitaire `dir-cli` prend en charge la création et les mises à jour d'utilisateurs de solution, la gestion des comptes, et la gestion de certificats et de mots de passe dans VMware Directory Service (vmdir). Vous pouvez également utiliser `dir-cli` pour gérer et interroger le niveau fonctionnel de domaine d'instances de Platform Services Controller.

dir-cli nodes list

Répertorie tous les systèmes vCenter Server de l'instance de Platform Services Controller spécifiée.

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.
`--server <psc_ip_or_fqdn>`	Utilisez cette option si vous ne voulez pas cibler l'instance de Platform Services Controller rattachée par affinité. Spécifiez l'adresse IP ou le nom de domaine complet de l'instance de Platform Services Controller ;

dir-cli computer password-reset

Cette commande vous permet de réinitialiser le mot de passe du compte de la machine dans le domaine. Cette option est utile si vous devez restaurer une instance de Platform Services Controller.

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.
`--live-dc-hostname <server name>`	Nom actuel de l'instance de Platform Services Controller.

dir-cli service create

Crée un utilisateur de solution. Principalement utilisé par les solutions tierces.

Option	Description
`--name <name>`	Nom de l'utilisateur de solution à créer
`--cert <cert file>`	Chemin d'accès au fichier de certificat. Il peut s'agir d'un certificat signé par VMCA ou d'un certificat tiers.
`--ssogroups <comma-separated-groupnames>`	
`--wstrustrole <ActAsUser>`	
`--ssoadminrole <Administrator/User>`	

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli service list

Répertorie les utilisateurs de solutions que `dir-cli` connaît.

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli service delete

Supprime un utilisateur de solution dans vmdir. Lorsque vous supprimez l'utilisateur de solution, tous les services associés deviennent inaccessibles à tous les nœuds de gestion qui utilisent cette instance de vmdir.

Option	Description
`--name`	Nom de l'utilisateur de solution à supprimer.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli service update

Met à jour le certificat pour un utilisateur de solution spécifié, c'est-à-dire une collection de services. Après l'exécution de cette commande, VECS applique la modification 5 minutes plus tard ou vous pouvez utiliser `vecs-cli force-refresh` pour forcer une actualisation.

Option	Description
`--name <name>`	Nom de l'utilisateur de solution à mettre à jour.
`--cert <cert_file>`	Nom du certificat à attribuer au service.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli user create

Crée un utilisateur normal dans vmdir. Cette commande peut être employée pour des utilisateurs humains qui s'authentifient auprès de vCenter Single Sign-On avec un nom d'utilisateur et un mot de passe. Utilisez cette commande uniquement lors du test de prototypes.

Option	Description
`--account <name>`	Nom de l'utilisateur vCenter Single Sign-On à créer.
`--user-password <password>`	Mot de passe initial de l'utilisateur.
`--first-name <name>`	Prénom de l'utilisateur.
`--last-name <name>`	Nom de l'utilisateur.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli user modify

Supprime l'utilisateur spécifié dans vmdir.

Option	Description
`--account <name>`	Nom de l'utilisateur vCenter Single Sign-On à supprimer.
`--password-never-expires`	Définissez cette option sur true si vous créez un compte d'utilisateur pour des tâches automatisées devant s'authentifier dans Platform Services Controller, et que vous souhaitez vous assurer que les tâches ne s'arrêtent pas en raison de l'expiration du mot de passe. Utilisez cette option avec précaution.
`--password-expires`	Définissez cette option sur true si vous souhaitez inverser l'option `--password-never-expires`.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli user delete

Supprime l'utilisateur spécifié dans vmdir.

Option	Description
`--account <name>`	Nom de l'utilisateur vCenter Single Sign-On à supprimer.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli user find-by-name

Cette commande vous permet de trouver un utilisateur par nom dans vmdir. Les informations retournées par cette commande varient en fonction de ce que vous spécifiez dans l'option `--level`.

Option	Description
`--account <name>`	Nom de l'utilisateur vCenter Single Sign-On à supprimer.
`--level <info level 0|1|2>`	Renvoie les informations suivantes : ■ Niveau 0 - Compte et UPN ■ Informations de niveau 1 - niveau 0 + prénom et nom ■ Niveau 2 : niveau 0 + indicateur de compte désactivé, indicateur de compte verrouillé, indicateur mot de passe n'expire jamais, indicateur de mot de passe expiré et indicateur d'expiration de mot de passe. Le niveau par défaut est 0.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli group modify

Ajoute un utilisateur ou un groupe à un groupe déjà existant.

Option	Description
`--name <name>`	Nom du groupe dans vmdir.
`--add <user_or_group_name>`	Nom de l'utilisateur ou du groupe à ajouter.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli group list

Répertorie un groupe vmdir spécifié.

Option	Description
`--name <name>`	Nom facultatif du groupe dans vmdir. Cette option permet de vérifier l'existence d'un groupe spécifique.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli ssogroup create

Crée un groupe dans le domaine local (vsphere.local par défaut).

Utilisez cette commande si vous souhaitez créer des groupes pour gérer des autorisations d'utilisateurs pour le domaine vCenter Single Sign-On. Par exemple, si vous créez un groupe, puis l'ajoutez au groupe d'administrateurs du domaine vCenter Single Sign-On, tous les utilisateurs que vous avez ajoutés à ce groupe disposent d'autorisations d'administrateur pour le domaine.

Il est également possible d'octroyer des autorisations à des objets d'inventaire vCenter à des groupes du domaine vCenter Single Sign-On. Consultez la documentation de *Sécurité vSphere*.

Option	Description
`--name <name>`	Nom du groupe dans vmdir. La longueur maximale est de 487 caractères.
`--description <description>`	Description facultative pour le groupe.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli trustedcert publish

Publie un certificat racine approuvé dans vmdir.

Option	Description
`--cert <file>`	Chemin d'accès au fichier de certificat.
`--crl <file>`	Cette option n'est pas prise en charge par VMCA.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.
`--chain`	Spécifiez cette option si vous publiez un certificat chaîné. Aucune valeur d'option n'est requise.

dir-cli trustedcert publish

Publie un certificat racine approuvé dans vmdir.

Option	Description
`--cert <file>`	Chemin d'accès au fichier de certificat.
`--crl <file>`	Cette option n'est pas prise en charge par VMCA.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.
`--chain`	Spécifiez cette option si vous publiez un certificat chaîné. Aucune valeur d'option n'est requise.

dir-cli trustedcert unpublish

Annule la publication d'un certificat racine actuellement approuvé dans vmdir. Utilisez cette commande, par exemple, si vous avez ajouté un autre certificat racine à vmdir qui est maintenant le certificat racine de tous les autres certificats de votre environnement. L'annulation de la publication de certificats qui ne sont plus utilisés s'inscrit dans le renforcement de votre environnement.

Option	Description
`--cert-file <file>`	Chemin d'accès au fichier de certificat dont vous souhaitez annuler la publication
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli trustedcert list

Répertorie tous les certificats racines approuvés et leurs ID correspondants. Vous avez besoin des ID de certificats pour récupérer un certificat avec `dir-cli trustedcert get`.

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli trustedcert get

Récupère un certificat racine approuvé dans vmdir et l'écrit dans un fichier spécifié.

Option	Description
`--id <cert_ID>`	ID du certificat à récupérer. La commande `dir-cli trustedcert list` affiche l'ID.
`--outcert <path>`	Chemin d'écriture du fichier de certificat.
`--outcrl <path>`	Chemin d'écriture du fichier de CRL. Actuellement inutilisé.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli password create

Crée un mot de passe aléatoire qui répond aux exigences en matière de mot de passe. Cette commande peut être utilisée par des utilisateurs de solutions tierces.

Option	Description
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli password reset

Permet à un administrateur de réinitialiser le mot de passe d'un utilisateur. Si vous êtes un utilisateur non-administrateur et souhaitez réinitialiser un mot de passe, utilisez plutôt la commande`dir-cli password change`.

Option	Description
`--account`	Nom du compte auquel attribuer un nouveau mot de passe.
`--new`	Nouveau mot de passe de l'utilisateur spécifié.
`--login <admin_user_id>`	Administrateur du domaine vCenter Single Sign-On local, administrator@vsphere.local par défaut.
`--password <admin_password>`	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli password change

Permet à un utilisateur de modifier son mot de passe. Vous devez être l'utilisateur qui possède le compte pour apporter cette modification. Les administrateurs peuvent employer `dir-cli password reset` pour réinitialiser n'importe quel mot de passe.

Option	Description
`--account`	Nom du compte.
`--current`	Mot de passe actuel de l'utilisateur qui possède le compte.
`--new`	Nouveau mot de passe de l'utilisateur qui possède le compte.

Dépannage de Platform Services Controller 5

Les rubriques suivantes fournissent un point de départ pour résoudre les problèmes de Platform Services Controller. Recherchez des pointeurs supplémentaires dans ce centre de documentation et dans le système de base de connaissances VMware.

Ce chapitre aborde les rubriques suivantes :

Détermination de la cause d'une erreur Lookup Service

L'installation de vCenter Single Sign-On affiche un message d'erreur relatif à vCenter Server ou vSphere Web Client.

Problème

Les programmes d'installation de vCenter Server et de Web Client affichent le message d'erreur `Could not contact Lookup Service. Please check VM_ssoreg.log...`.

Cause

Ce problème a plusieurs causes, notamment des horloges non synchronisées sur les machines hôte, un blocage provenant du pare-feu et des services qui doivent être démarrés.

Solution

1. Vérifiez si les horloges des ordinateurs hôte sur lesquels vCenter Single Sign-On, vCenter Server et Web Client sont actifs sont synchronisées.
2. Consultez le journal spécifique qui figure dans le message d'erreur.

   Dans le message, le dossier temporaire système se rapporte à `%TEMP%`.

3 Dans le fichier journal, recherchez les messages suivants.

Le fichier journal contient un sortie de toutes les tentatives d'installation. Situez le dernier message qui affiche `Initializing registration provider...`

Message	Cause et solution
java.net.ConnectException: La connexion a expiré : connect	L'adresse IP est erronée, un pare-feu bloque l'accès à vCenter Single Sign-On, ou vCenter Single Sign-On est surchargé. Assurez-vous qu'aucun pare-feu ne bloque le port vCenter Single Sign-On (par défaut 7444) et que l'ordinateur sur lequel vCenter Single Sign-On est installé dispose de suffisamment de capacité de CPU, d'E/S et de RAM.
java.net.ConnectException: Connection refused: connect	L'adresse IP ou le nom de domaine complet est erroné(e) et le service vCenter Single Sign-On n'a pas démarré ou a démarré au cours de la minute écoulée. Vérifiez que vCenter Single Sign-On fonctionne en contrôlant l'état du service vCenter Single Sign-On (sous Windows) et du daemon vmware-sso (sous Linux). Redémarrez le service. Si cette procédure ne résout pas le problème, consultez la section récupération du Guide de dépannage de vSphere.
Code d'état inattendu : 404. Échec du serveur SSO lors de l'initialisation	Redémarrez vCenter Single Sign-On. Si cette procédure ne résout pas le problème, consultez la section Récupération du *Guide de dépannage de vSphere*.
Le message d'erreur qui s'affiche dans l'interface utilisateur commence par `Could not connect to vCenter Single Sign-on`.	Vous pouvez également voir le code de retour `SslHandshakeFailed`. Il s'agit d'une erreur inhabituelle. Elle indique que l'adresse IP ou le FQDN qui assure la résolution vers l'hôte vCenter Single Sign-On n'est pas celle/celui que voues avez utilisé(e) pendant l'installation de vCenter Single Sign-On. Dans `%TEMP%\VM_ssoreg.log`, recherchez la ligne qui contient le message suivant. `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>`, A étant le nom de domaine complet que vous avez entré pendant l'installation de vCenter Single Sign-On, B et C étant des alternatives autorisées générées par le système. Corrigez la configuration pour utiliser le FQDN à droite du signe != dans le fichier journal. Dans la plupart des cas, utilisez le FQDN que vous avez spécifié pendant l'installation de vCenter Single Sign-On . Si aucune des alternatives n'est possible dans votre configuration réseau, récupérez votre configuration vCenter Single Sign-On SSL.

Impossible de se connecter à l'aide de l'authentification de domaine Active Directory

Vous vous connectez à un composant de vCenter Server dans vSphere Web Client. Vous utilisez votre nom d'utilisateur et mot de passe Active Directory. L'authentification échoue.

Problème

Vous ajoutez une source d'identité Active Directory à vCenter Single Sign-On, mais les utilisateurs ne parviennent pas à se connecter à vCenter Server.

Cause

Les utilisateurs se connectent à leur domaine par défaut à l'aide de leur nom d'utilisateur et mot de passe. Pour tous les autres domaines, ils doivent inclure le nom de domaine (utilisateur@domaine ou DOMAINE\utilisateur).

Si vous utilisez vCenter Server Appliance d'autres problèmes peuvent se produire.

Solution

Pour tous les déploiements de vCenter Single Sign-On, vous pouvez modifier la source d'identité par défaut. Une fois la modification effectuée, les utilisateurs peuvent se connecter à la source d'identité par défaut à l'aide de leur nom d'utilisateur et mot de passe uniquement.

Pour configurer votre source d'identité d'authentification Windows intégrée avec un domaine enfant dans votre forêt Active Directory, reportez-vous à l'article 2070433 de la base de connaissances VMware. Par défaut, l'authentification Windows intégrée utilise le domaine racine de votre forêt Active Directory.

Si vous utilisez vCenter Server Appliance et que la modification de la source d'identité par défaut ne résout pas le problème, effectuez l'une des interventions de dépannage supplémentaires suivantes.

1 Synchronisez les horloges entre vCenter Server Appliance et les contrôleurs de domaine Active Directory.

2 Vérifiez que chaque contrôleur de domaine dispose d'un enregistrement de pointeur (PTR) dans le service DNS du domaine Active Directory et que les informations de l'enregistrement PTR correspondent au nom DNS du contrôleur. Lors de l'utilisation de vCenter Server Appliance, vous pouvez exécuter les commandes suivantes pour effectuer la tâche :

   a Pour répertorier les contrôleurs de domaine, exécutez la commande suivante :

   ```
   # dig SRV _ldap._tcp.my-ad.com
   ```

   Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

   ```
   ;; ANSWER SECTION:
   _ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
   ...
   ```

   b Pour chaque contrôleur de domaine, vérifiez la résolution directe et inverse en exécutant la commande suivante :

   ```
   # dig my-controller.my-ad.com
   ```

   Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

   ```
   ;; ANSWER SECTION:
   my-controller.my-ad.com (...) IN A controller IP address
   ...
   ```

   ```
   # dig -x <controller IP address>
   ```

   Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

   ```
   ;; ANSWER SECTION:
   IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
   ...
   ```

3 Si cela ne résout pas le problème, supprimez vCenter Server Appliance du domaine Active Directory, puis rejoignez le domaine. Consultez la documentation de *Configuration de vCenter Server Appliance*.

4 Fermez toutes les sessions de navigateur connectées à vCenter Server Appliance et redémarrez tous les services.

```
/bin/service-control --restart --all
```

La connexion à vCenter Server échoue, car le compte d'utilisateur est verrouillé

Lorsque vous vous connectez à vCenter Server à partir de la page de connexion de vSphere Web Client, une erreur indique que le compte est verrouillé.

Problème

Après plusieurs tentatives infructueuses, vous ne parvenez pas à vous connecter à vSphere Web Client à l'aide de vCenter Single Sign-On. Vous voyez un message indiquant que votre compte est verrouillé.

Cause

Vous avez dépassé le nombre maximal d'échecs de tentative de connexion.

Solution

- Si vous avez essayé de vous connecter en tant qu'utilisateur du domaine système (vsphere.local par défaut), demandez à votre administrateur de vCenter Single Sign-On de déverrouiller votre compte. Si le verrouillage est réglé pour expirer dans la règle de verrouillage, vous pouvez attendre que votre compte soit déverrouillé. Les administrateurs vCenter Single Sign-On peuvent utiliser des interfaces de lignes de commande pour déverrouiller leur compte.
- Si vous vous connectez en tant qu'un utilisateur d'un domaine Active Directory ou LDAP, demandez à votre administrateur Active Directory ou LDAP de déverrouiller votre compte.

La réplication du service d'annuaire VMware peut prendre longtemps

Si votre environnement comprend plusieurs instances de Platform Services Controller et si l'une des instances de Platform Services Controller devient indisponible, votre environnement continue à fonctionner. Lorsque le Platform Services Controller devient à nouveau disponible, les données de l'utilisateur et les autres informations sont généralement répliquées dans les 60 secondes. Dans certains cas particuliers, cependant, la réplication peut prendre du temps.

Problème

Dans certaines situations, par exemple lorsque votre environnement comprend plusieurs instances de Platform Services Controller en différents lieux, et que vous apportez des modifications significatives pendant qu'une instance de Platform Services Controller est indisponible, vous ne voyez pas immédiatement la réplication entre les instances du service d'annuaire VMware. Ainsi, vous ne voyez pas un nouvel utilisateur ajouté à l'instance de Platform Services Controller disponible dans l'autre instance tant que la réplication n'est pas terminée.

Cause

Pendant le fonctionnement normal, les modifications apportées à une instance du service d'annuaire VMware (vmdir) dans une instance de Platform Services Controller (nœud) s'affichent dans son partenaire de réplication direct approximativement dans les 60 secondes suivantes. Selon la topologie de réplication, les modifications apportées à un nœud devront peut-être se propager sur des nœuds intermédiaires avant de parvenir à chaque instance de vmdir sur chaque nœud. Les informations répliquées sont celles concernant les utilisateurs, les certificats, les licences pour les machines virtuelles créées, clonées ou migrées avec VMware VMotion, etc.

Lorsque le lien de réplication est rompu, par exemple à cause d'une panne du réseau ou de l'indisponibilité d'un nœud, il n'y a pas de convergence des modifications apportées à la fédération. Un fois le nœud indisponible restauré, chaque nœud tente de récupérer l'ensemble des modifications. Par la suite, toutes les instances de vmdir convergent vers un état cohérent, mais l'obtention de cet état cohérent peut prendre un certain temps si de nombreuses modifications ont eu lieu pendant qu'un nœud était indisponible.

Solution

Votre environnement fonctionne normalement pendant que la réplication a lieu. Ne tentez pas de résoudre le problème, sauf s'il persiste pendant plus d'une heure.

Exporter un bundle de support de Platform Services Controller

Vous ne pouvez pas exporter un bundle de support qui contient les fichiers journaux des services Platform Services Controller. Après l'exportation, vous pouvez explorer les journaux localement ou envoyer le bundle au support VMware.

Prérequis

Vérifiez que le dispositif virtuel Platform Services Controller est déployé et en cours d'exécution.

Procédure

1 Dans un navigateur Web, connectez-vous à l'interface de gestion de Platform Services Controller à l'adresse https://*platform_services_controller_ip*:5480

2 Connectez-vous en tant qu'utilisateur racine pour le dispositif virtuel.

3 Cliquez **Créer un bundle de support**.

4 Sauf si les paramètres du navigateur empêchent un téléchargement immédiat, le bundle de support est enregistré sur votre machine locale.

Référence des journaux de service de Platform Services Controller

Les services Platform Services Controller utilisent syslog pour la journalisation. Vous pouvez examiner les fichiers de journaux afin de déterminer les causes des défaillances.

Tableau 5-1. Journaux de service

Service	Description
VMware Directory Service	Par défaut, la journalisation vmdir est conservée dans le fichier `/var/log/messages` ou `/var/log/vmware/vmdird/`. Pour les problèmes au moment du déploiement, `/var/log/vmware/vmdir/vmafdvmdirclient.log` peut également contenir des données de dépannage utile.
VMware Single Sign-On	La journalisation vCenter Single Sign-On est conservée dans le fichier `/var/log/vmware/sso/`.
VMWare Certificate Authority (VMCA)	Le journal de service VMCA est conservé dans le fichier `/var/log/vmware/vmcad/vmcad-syslog.log`.
VECS (VMware Endpoint Certificate Store)	Le journal de service VECS est conservé dans le fichier `var/log/vmware/vmafdd/vmafdd-syslog.log`.
VMware Lookup Service	Le journal Lookup Service est conservé dans le fichier `/var/log/vmware/sso/lookupServer.log`,

Index

S

T

U

V

W