Authentification vSphere

Modifié le 29 novembre 2022
VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

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

https://docs.vmware.com/fr/

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Table des matières

À propos de *Authentification vSphere*

La documentation de *Authentification vSphere* fournit des informations pour vous aider à effectuer des tâches courantes telles que la gestion des certificats et la configuration de vCenter Single Sign-On.

VMware prend l'intégration au sérieux. Pour promouvoir ce principe au sein de notre communauté de clients, de partenaires et interne, nous créons du contenu à l'aide d'une langue inclusive.

Authentification vSphere explique comment vous pouvez gérer les certificats pour vCenter Server et les services associés et comment configurer l'authentification avec vCenter Single Sign-On.

Tableau 1-1. Faits saillants sur *Authentification vSphere*

Rubriques	Points forts du contenu
Démarrage avec l'authentification	■ Gestion des services d'authentification. ■ Gestion de vCenter Server à l'aide de l'interface de gestion de vCenter Server.
Certificats de sécurité vSphere	■ Modèle de certificat et options de remplacement des certificats. ■ Remplacer les certificats à partir de l'interface utilisateur (cas simples). ■ Remplacer les certificats à l'aide de l'utilitaire Certificate Manager. ■ Remplacer les certificats à l'aide de l'interface de ligne de commande (situations complexes). ■ Référence d'interface de ligne de commande de gestion des certificats.
Authentification vSphere à l'aide de vCenter Single Sign-On	■ Architecture du processus d'authentification. ■ Comment ajouter des sources d'identité pour que les utilisateurs de votre domaine puissent s'authentifier. ■ Authentification à deux facteurs. ■ Gestion des utilisateurs, groupes et stratégies. ■ Fédération de fournisseur d'identité vCenter Server

Qu'est-il arrivé à Platform Services Controller ?

À partir de vSphere 7.0, le déploiement d'une nouvelle instance de vCenter Server ou la mise à niveau vers vCenter Server 7.0 nécessite l'utilisation de vCenter Server Appliance, une machine virtuelle préconfigurée optimisée pour l'exécution de vCenter Server. La nouvelle instance de vCenter Server contient tous les services Platform Services Controller, en préservant

les fonctionnalités et les workflows, notamment l'authentification, la gestion des certificats, les balises et la gestion des licences. Il n'est plus nécessaire ni possible de déployer et d'utiliser une instance externe de Platform Services Controller. Tous les services Platform Services Controller sont consolidés dans vCenter Server, et le déploiement et l'administration sont simplifiés.

Comme ces services font désormais partie de vCenter Server, ils ne sont plus décrits comme partie intégrante de Platform Services Controller. Dans vSphere 7.0, la publication *Authentification vSphere* remplace la publication *Administration de Platform Services Controller* . La nouvelle publication contient des informations complètes sur l'authentification et la gestion des certificats. Pour plus d'informations sur la mise à niveau ou la migration de déploiements de vSphere 6.5 et 6.7 à l'aide d'une instance externe de Platform Services Controller existante vers vSphere 7.0 avec vCenter Server Appliance, consultez la documentation *Mise à niveau vSphere*.

Documentation connexe

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

Outre ces documents, VMware publie le *Guide de configuration de sécurité de vSphere* (nommé auparavant *Guide de sécurisation renforcée*) pour chaque version de vSphere, disponible à l'adresse https://core.vmware.com/security. Le *Guide de configuration de sécurité de vSphere* contient des instructions sur les paramètres de sécurité qui peuvent ou doivent être définis par le client, et sur les paramètres de sécurité fournis par VMware qui doit être vérifiés par le client afin de s'assurer qu'ils sont toujours définis sur les valeurs par défaut.

Public cible

Ces informations sont destinées aux administrateurs qui souhaitent configurer l'authentification vCenter Server et gérer les certificats. Elles sont destinées aux administrateurs système Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Informations mises à jour

Ce document *Authentification vSphere* est mis à jour avec chaque nouvelle version du produit ou lorsque cela s'avère nécessaire.

Ce tableau comporte l'historique des mises à jour de la documentation relative à la *Authentification vSphere*.

Révision	Description
29 novembre 2022	■ Mise à jour mineure dans Gérer vCenter Server à l'aide de l'interface de gestion. ■ Mise à jour mineure dans Référence des commandes dir-cli.
31 octobre 2022	■ Mise à jour mineure dans Paramètres d'Active Directory over LDAP et de la source d'identité du serveur OpenLDAP.
19 octobre 2022	■ Mise à jour mineure dans Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA à l'aide l'interface de ligne de commande.
11 octobre 2022	Version initiale.

Prise en main de la gestion des certificats vSphere et de l'authentification

1

vSphere fournit des services d'infrastructure communs pour gérer les certificats pour les composants vCenter Server et ESXi, et pour gérer l'authentification avec vCenter Single Sign-On.

Gestion des certificats vSphere

Par défaut, vSphere vous permet de provisionner des composants vCenter Server et des hôtes ESXi avec des certificats d'autorité de certification VMware (VMCA). Vous pouvez également utiliser des certificats personnalisés stockés dans VMware Endpoint Certificate Store (VECS) Pour plus d'informations, consultez Options de gestion des certificats vSphere.

Qu'est-ce que vCenter Single Sign-On

vCenter Single Sign-On permet aux composants vSphere de communiquer au moyen d'un mécanisme d'échange de jetons sécurisé. vCenter Single Sign-On utilise des termes et définitions spécifiques importants à comprendre.

Tableau 1-1. Glossaire de vCenter Single Sign-On

Terme	Définition
Principal	Entité pouvant être authentifiée, telle qu'un utilisateur.
Fournisseur d'identité	Service qui gère les sources d'identité et authentifie les principaux. Exemples : Microsoft Active Directory Federation Services (AD FS) et vCenter Single Sign-On.
Source d'identité (Directory Service)	Stocke et gère les principaux. Les principaux regroupent un ensemble d'attributs concernant un utilisateur ou un compte de service, tel que le nom, l'adresse, l'e-mail et l'appartenance à un groupe. Exemples : Microsoft Active Directory et VMware Directory Service (vmdir).
Authentification	Moyens utilisés afin de déterminer si quelqu'un ou quelque chose est effectivement celui ou ce qu'il déclare lui-même être. Par exemple, les utilisateurs sont authentifiés lorsqu'ils fournissent leurs informations d'identification, telles que les cartes à puce, le nom d'utilisateur et le mot de passe approprié, etc.
Autorisation	Processus de vérification des objets auxquels les principaux ont accès.

Tableau 1-1. Glossaire de vCenter Single Sign-On (suite)

Terme	Définition
Jeton	Ensemble de données signé contenant les informations d'identité d'un principal spécifique. Un jeton peut inclure non seulement des informations de base sur le principal, telles que l'adresse e-mail et le nom complet, mais également, selon le type de jeton, les groupes et les rôles du principal.
vmdir	VMware Directory Service. Référentiel LDAP interne (local) de vCenter Server qui contient des identités d'utilisateur, des groupes et des données de configuration.
OpenID Connect (OIDC)	Protocole d'authentification basé sur OAuth2. vCenter Server utilise les capacités OIDC lors de l'interaction avec Active Directory Federation Services (AD FS).

Présentation des types d'authentification vCenter Single Sign-On

vCenter Single Sign-On utilise différents types d'authentification, selon que le fournisseur d'identité vCenter Server intégré ou un fournisseur d'identité externe est impliqué.

Tableau 1-2. Types d'authentification vCenter Single Sign-On

Type d'authentification	Quel est le fournisseur d'identité utilisé ?	Est-ce que vCenter Server peut gérer le mot de passe ?	Description
Authentification basée sur des jetons	Fournisseur d'identité externe. Par exemple, AD FS.	Non	vCenter Server contacte le fournisseur d'identité externe via un protocole particulier et obtient un jeton qui représente l'identité d'un utilisateur particulier.
Authentification simple	vCenter Server	Oui	Le nom d'utilisateur et le mot de passe sont transmis directement à vCenter Server, ce qui valide les informations d'identification via ses sources d'identité.

Ce chapitre contient les rubriques suivantes :

- Gestion de certificats vCenter Server
- Gestion des services d'authentification de vCenter Server
- Gestion de vCenter Server

Gestion de certificats vCenter Server

Vous gérez des certificats vCenter Server depuis vSphere Client ou en utilisant une API, des scripts ou des interfaces de ligne de commande.

Le tableau suivant décrit les interfaces que vous pouvez utiliser pour gérer des certificats vCenter Server.

Tableau 1-3. Interfaces de gestion des certificats vSphere

Interface	Description
vSphere Client	Interface Web (client basé sur HTML5). Reportez-vous à la section Gestion des certificats avec vSphere Client.
API de vSphere Automation	Reportez-vous au *Guide de programmation des SDK de VMware vSphere Automation* à l'adresse https://developer.vmware.com/docs/11699/vmware-vsphere-automation-sdks-programming-guide
Utilitaire de gestion de certificats	Outil de ligne de commande prenant en charge la génération d'une demande de signature de certificat (CSR) et le remplacement des certificats. Reportez-vous à la section Gestion des certificats à l'aide de l'utilitaire vSphere Certificate Manager.
Interfaces de ligne de commande pour la gestion des services de certificat et d'annuaire	Ensemble de commandes pour la gestion des certificats, le magasin de certificats VMware Endpoint (VECS) et VMware Directory Service (vmdir). Reportez-vous à la section Chapitre 3 Référence des commandes CLI vSphere Certificates and Services.

Gestion des certificats vCenter Server avec vSphere Client

Vous pouvez gérer les certificats vCenter Server dans vSphere Client.

Procédure

1. Connectez-vous à une instance de vCenter Server en tant qu'utilisateur disposant de privilèges d'administrateur dans le domaine vCenter Single Sign-On local.

   Le domaine par défaut est vsphere.local.
2. Sélectionnez **Administration**.
3. Sous **Certificats**, cliquez sur **Gestion des certificats**.

   Des panneaux de certificat pour les différents types de certificats s'affichent.
4. Effectuez des tâches de certificat, telles que l'affichage des détails de certificat, le renouvellement du certificat SSL de la machine et l'ajout d'un certificat racine approuvé.

   Pour plus d'informations, consultez Gestion des certificats avec vSphere Client.

Gérer les certificats vCenter Server à l'aide des interfaces de ligne de commande

vCenter Server inclut des interfaces de ligne de commande pour la génération de demandes de signature de certificat (CSR), la gestion des certificats et la gestion des services.

Par exemple, vous pouvez utiliser la commande `certool` pour générer des demandes de signature de certificat et remplacer des certificats.

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

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

CLI	Description	Liens
`certool`	Génère et gère les certificats et les clés. Partie de VMCA (VMware Certificate Authority).	Référence des commandes d'initialisation de certool
`vecs-cli`	Gère les contenus des instances de VMware Certificate Store. Partie du démon VMAFD (VMware Authentication Framework Daemon)	Référence des commandes vecs-cli
`dir-cli`	Crée et met à jour les certificats dans le Vmware Directory Service. Fait partie de VMAFD.	Référence des commandes dir-cli
`sso-config`	Mettez à jour les certificats STS (Security Token Service).	Remplacer un certificat STS vCenter Server à l'aide de la ligne de commande
`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.

Conditions préalables

Activez la connexion SSH à vCenter Server. Vous pouvez utiliser l'onglet **Paramètres d'accès** de l'interface de gestion de vCenter Server (`https://vcenter_server_ip:5480`) pour l'activation et la désactivation de la connexion SSH.

Procédure

1 Connectez-vous à l'interpréteur de commande vCenter Server.

   Généralement, vous devez être l'utilisateur racine ou administrateur. Reportez-vous à Privilèges requis pour l'exécution des CLI vSphere 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. Vous êtes parfois invité à entrer le mot de passe deux fois à des fins de protection des informations sensibles.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

   La commande `service-control` n'impose pas l'entrée du chemin.

   Pour plus d'informations, consultez Remplacement manuel des certificats vSphere.

Gestion des services d'authentification de vCenter Server

Vous pouvez gérer les services d'authentification à partir de vSphere Client ou à l'aide de l'interface de ligne de commande. Vous pouvez également gérer le processus de configuration de la fédération de fournisseur d'identité vCenter Server à l'aide d'une API.

Vous pouvez gérer l'authentification de vCenter Server en utilisant différentes interfaces.

Tableau 1-5. Interfaces pour la gestion des services d'authentification de vCenter Server

Interface	Description
vSphere Client	Interface Web (client basé sur HTML5).
API	Gérez le processus de configuration de la fédération du fournisseur d'identité vCenter Server.
`sso-config`	Utilitaire de ligne de commande permettant de configurer le fournisseur d'identité intégré de vCenter Server.

Gérer les services d'authentification de vCenter Server avec vSphere Client

Vous pouvez gérer les services d'authentification de vCenter Server depuis vSphere Client.

Procédure

1 Connectez-vous à une instance de vCenter Server en tant qu'utilisateur disposant de privilèges d'administrateur dans le domaine vCenter Single Sign-On local.

   Le domaine par défaut est vsphere.local.

2 Sélectionnez **Administration**.

3 Sous **Single Sign On**, cliquez sur **Configuration** pour gérer les fournisseurs d'identité et configurer les stratégies de mot de passe et de verrouillage.

   Pour plus d'informations, consultez Chapitre 4 Authentification vSphere à l'aide de vCenter Single Sign-On.

Gérer les services d'authentification vCenter Server à l'aide de scripts

vCenter Server inclut un utilitaire, `sso-config`, pour la gestion des services d'authentification.

Utilisez l'utilitaire `sso-config` pour les tâches de gestion non prises en charge par vSphere Client ou pour créer des scripts personnalisés pour votre environnement.

Tableau 1-6. Interfaces de ligne de commande pour la gestion de l'authentification et des services associés

CLI	Description	Liens
`sso-config`	Utilitaire de ligne de commande permettant de configurer le fournisseur d'identité intégré de vCenter Server.	Consultez l'aide de `sso-config` en exécutant `sso-config.sh -help` ou consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/67304 pour obtenir des exemples d'utilisation.
`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. La commande `service-control` ne requiert pas de spécifier le chemin.

Conditions préalables

Activez la connexion SSH à vCenter Server. Vous pouvez utiliser l'onglet **Paramètres d'accès** de l'interface de gestion de vCenter Server (`https://vcenter_server_ip:5480`) pour l'activation et la désactivation de la connexion SSH.

Procédure

1. Connectez-vous à l'interpréteur de commande vCenter Server.

   Généralement, vous devez être l'utilisateur racine ou administrateur. Reportez-vous à Privilèges requis pour l'exécution des CLI vSphere pour plus de détails.

2. Accédez à l'utilitaire `sso-config` à l'emplacement par défaut suivant.

   ```
   /opt/vmware/bin/sso-config.sh
   ```

   Les privilèges requis dépendent de la tâche à effectuer. Vous êtes parfois invité à entrer le mot de passe deux fois à des fins de protection des informations sensibles.

Gestion de vCenter Server

Vous pouvez gérer l'instance de vCenter Server Appliance dans l'interface de gestion de vCenter Server ou de l'interpréteur de commande de vCenter Server.

Pour plus d'informations sur la gestion de vCenter Server, reportez-vous à la section *Configuration de vCenter Server*.

Tableau 1-7. Interfaces pour la gestion de vCenter Server

Interface	Description
Interface de gestion de vCenter Server	Utilisez cette interface pour reconfigurer les paramètres système. Reportez-vous à la section Gérer vCenter Server à l'aide de l'interface de gestion.
Interpréteur de commandes de vCenter Server	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 des certificats à l'aide de l'utilitaire vSphere Certificate Manager et Chapitre 3 Référence des commandes CLI vSphere Certificates and Services.

Gérer vCenter Server à l'aide de l'interface de gestion

Vous pouvez utiliser l'interface de gestion de vCenter Server pour configurer les paramètres système.

Les paramètres de l'interface de gestion vCenter Server 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.

Note Dans le volet **Mise en réseau**, la carte réseau virtuelle 0 est réservée au trafic de gestion. Vous ne pouvez pas réattribuer le trafic de la carte réseau 0 à une autre carte réseau. Si vous utilisez VCHA, ce trafic utilise la carte réseau 1. Vous pouvez ajouter des cartes réseau au vCenter Server Appliance. Consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/article/2147155.

Procédure

1. Dans un navigateur, accédez à l'interface Web à l'adresse `https://vcenter_server_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 votre entreprise et du navigateur utilisé.
3. Connectez-vous en tant qu'utilisateur racine.

   Le mot de passe racine par défaut est le mot de passe racine que vous définissez lors du déploiement de vCenter Server.

Résultats

La page Résumé de l'interface de gestion de vCenter Server s'affiche.

Gérer vCenter Server à l'aide du shell de vCenter Server

Vous pouvez utiliser les utilitaires de gestion des services et les CLI à partir du shell de vCenter Server. Vous pouvez utiliser TTY1 pour vous connecter à la console ou employer SSH pour vous connecter au shell.

Procédure

1 Activez la connexion SSH si nécessaire.

   a Connectez-vous à l'interface de gestion de vCenter Server à l'adresse https://*vcenter_server_ip*:5480.

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

   c Enclenchez l'option **Activer la connexion SSH**, puis cliquez sur **OK**.

   Vous pouvez suivre les mêmes instructions pour activer le shell de dépistage de l'instance de vCenter Server.

2 Accédez au shell.

   - Si vous avez un accès direct à la console de vCenter Server, 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 l'instance de vCenter Server.

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

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

Ajouter une instance de vCenter Server à un domaine Active Directory

Si vous souhaitez ajouter une source d'identité Active Directory à vCenter Server, vous devez joindre l'instance de vCenter Server à un domaine Active Directory.

Si vous ne pouvez pas utiliser la fédération de fournisseur d'identité vCenter Server ou Active Directory sur LDAPS, vCenter Server prend en charge l'authentification Windows intégrée (IWA). Pour utiliser IWA, vous devez lier vCenter Server à votre domaine Active Directory.

Procédure

1 À l'aide de vSphere Client, connectez-vous à vCenter Server en tant qu'utilisateur disposant de privilèges d'administrateur dans le domaine vCenter Single Sign-On local (vsphere.local par défaut).

2 Sélectionnez **Administration**.

3 Développez **Single Sign On** et cliquez sur **Configuration**.

4 Dans l'onglet **Fournisseur d'identité**, cliquez sur **Domaine Active Directory**.

5 Cliquez sur **Joindre AD**, entrez le domaine, une unité d'organisation éventuelle, ainsi qu'un nom d'utilisateur et un mot de passe, puis cliquez sur **Joindre**.

6 Redémarrez vCenter Server.

Étape suivante

Pour associer des utilisateurs et des groupes du domaine Active Directory joint, ajoutez le domaine joint en tant que source d'identité vCenter Single Sign-On. Reportez-vous à la section Ajouter ou modifier une source d'identité vCenter Single Sign-On.

Certificats de sécurité vSphere

2

vSphere fournit une sécurité en utilisant des certificats pour chiffrer les communications, authentifier des services et signer des jetons.

Utilisation des certificats par vSphere

vSphere utilise des certificats pour :

- Chiffrer les communications entre deux nœuds, comme une instance de vCenter Server et un hôte ESXi.
- Authentifiez les services vSphere.
- Effectuer des actions internes telles que la signature des jetons.

Présentation de VMware Certificate Authority

L'autorité de certification interne de vSphere, VMware Certificate Authority (VMCA), fournit tous les certificats nécessaires pour vCenter Server et ESXi. VMCA est installé sur chaque hôte vCenter Server, ce qui sécurise immédiatement la solution sans autre modification requise. Le maintien de cette configuration par défaut permet la surcharge opérationnelle la plus faible pour la gestion des certificats. vSphere fournit un mécanisme permettant de renouveler ces certificats s'ils arrivent à expiration.

vSphere fournit également un mécanisme pour remplacer certains certificats par vos propres certificats. Toutefois, remplacez uniquement le certificat SSL qui fournit un chiffrement entre les nœuds pour conserver une faible surcharge de gestion des certificats.

Options de gestion des certificats vSphere

Les options suivantes sont recommandées pour la gestion des certificats.

Tableau 2-1. Options recommandées pour la gestion des certificats vSphere

Mode	Description	Avantages
Certificats VMCA par défaut	VMCA fournit tous les certificats requis pour les hôtes vCenter Server et ESXi.	Surcharge la plus simple et la plus faible. VMCA peut gérer le cycle de vie des certificats de vCenter Server et des hôtes ESXi.
Certificats VMCA par défaut avec certificats SSL externes (mode hybride)	Vous remplacez les certificats SSL de vCenter Server et autorisez VMCA à gérer les certificats pour les utilisateurs de solution et les hôtes ESXi. Le cas échéant, pour les déploiements hautement sécurisés, vous pouvez également remplacer les certificats SSL de l'hôte ESXi.	Simple et sécurisée. VMCA gère les certificats internes, mais vous bénéficiez de l'utilisation de vos certificats SSL approuvés par l'entreprise et ces certificats sont approuvés par les navigateurs.

VMware ne recommande pas le remplacement des certificats d'utilisateur de solution ou STS, ni l'utilisation d'une autorité de certification subordonnée à la place de VMCA. Si vous choisissez une de ces options, vous vous exposez à plus de complexité et un risque potentiel pour votre sécurité, ce qui représente une augmentation inutile dans vos risques opérationnels. Pour plus d'informations sur la gestion des certificats dans un environnement vSphere, consultez le blog intitulé *Nouvelle procédure produit - Remplacement hybride des certificats SSL vSphere* à l'adresse http://vmware.com/go/hybridvmca.

Outils disponibles pour remplacer les certificats vSphere

Vous pouvez utiliser les options suivantes pour remplacer les certificats existants.

Tableau 2-2. Différentes approches du remplacement de certificats vSphere

Option	Reportez-vous au
Utilisez vSphere Client.	Gestion des certificats avec vSphere Client
Utilisez l'API de vSphere Automation pour gérer le cycle de vie des certificats.	*Guide de programmation des SDK de VMware vSphere Automation* à l'adresse https://developer.vmware.com/docs/11699/vmware-vsphere-automation-sdks-programming-guide
Utilisez l'utilitaire vSphere Certificate Manager à partir de la ligne de commande.	Gestion des certificats à l'aide de l'utilitaire vSphere Certificate Manager
Utilisez les commandes CLI pour remplacer des certificats manuellement.	Chapitre 3 Référence des commandes CLI vSphere Certificates and Services

Ce chapitre contient les rubriques suivantes :

- Exigences en matière de certificats pour les différents chemins d'accès aux solutions dans vSphere
- Présentation de la gestion des certificats vSphere

- Gestion des certificats avec vSphere Client
- Gestion des certificats à l'aide de l'utilitaire vSphere Certificate Manager
- Remplacement manuel des certificats vSphere

Exigences en matière de certificats pour les différents chemins d'accès aux solutions dans vSphere

Les exigences en matière de certificats varient si vous utilisez VMware Certificate Authority (VMCA) comme autorité de certification intermédiaire ou si vous utilisez des certificats personnalisés. Les exigences sont également différentes pour les certificats de machine.

Avant de commencer à modifier les certificats, assurez-vous que l'heure est synchronisée sur tous les nœuds de votre environnement vSphere.

Note vSphere déploie uniquement des certificats RSA pour l'authentification du serveur et ne prend pas en charge la génération de certificats ECDSA. vSphere vérifie les certificats ECDSA présentés par d'autres serveurs. Par exemple, si vSphere se connecte à un serveur Syslog et que le serveur Syslog dispose d'un certificat ECDSA, vSphere prend en charge la vérification de ce certificat.

Conditions requises pour tous les certificats vSphere importés

- Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque vous ajoutez des clés à VECS, elles sont converties en PKCS8.
- x509 version 3
- SubjectAltName doit contenir DNS Name=*machine_FQDN*
- Format CRT
- Contient les utilisations de clé suivantes : signature numérique, chiffrement de clé.
- Lors de l'exemption du certificat d'utilisateur de solution vpxd-extension, le champ Utilisation étendue de la clé peut être vide ou contenir la valeur du champ Authentification du serveur.

vSphere ne prend pas en charge les certificats suivants.

- Certificats comportant des caractères génériques.
- Les algorithmes md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 et sha1WithRSAEncryption ne sont pas pris en charge.

Conformité du certificat vSphere à la norme RFC 2253

Le certificat doit être conforme à la norme RFC 2253.

Si vous ne générez pas de demande de signature de certificat à l'aide de vSphere Certificate Manager, assurez-vous que la demande comprend les champs suivants.

String	AttributeType X.500
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

Si vous générez des demandes de signature de certificat à l'aide de vSphere Certificate Manager, vous êtes invité à entrer les informations suivantes et vSphere Certificate Manager ajoute les champs correspondants dans le fichier CSR.

- Mot de passe de l'utilisateur administrator@vsphere.local ou de l'administrateur du domaine vCenter Single Sign-On auquel vous vous connectez.
- Informations que vSphere Certificate Manager enregistre 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.
  - 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 nœud vCenter Server sur lequel vous exécutez vSphere Certificate Manager.

Exigences en matière de certificats lorsque VMCA est utilisé comme autorité de certification intermédiaire

Lorsque vous utilisez VMCA comme autorité de certification intermédiaire, les certificats doivent répondre aux exigences suivantes.

Type de certificat	Exigences en matière de certificats

Certificat racine	■ Vous pouvez utiliser vSphere Certificate Manager pour générer la demande de signature de certificat. Reportez-vous à la section Générer une demande de signature de certificat avec Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire).
	■ Si vous préférez créer la demande de signature de certificat manuellement, le certificat envoyé pour signature doit satisfaire les conditions suivantes :
	■ Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (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
	■ L'extension d'autorité de certification doit être définie sur true pour les certificats racines et la signature de certification doit figurer dans la liste de conditions requises. Par exemple :
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ La signature CRL doit être activée.
	■ Le champ Utilisation étendue de la clé peut être vide ou contenir la valeur du champ Authentification du serveur.
	■ Aucune limite explicite à la longueur de la chaîne de certificats. VMCA utilise la valeur par défaut OpenSSL, qui est 10 certificats.
	■ Les certificats incluant des caractères génériques ou plusieurs noms DNS ne sont pas pris en charge.
	■ Vous ne pouvez pas créer d'autorités de certification filiales de VMCA.
	Reportez-vous à l'article « Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x » de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2112009 pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

Certificat SSL de machine	Vous pouvez utiliser vSphere Certificate Manager pour créer la demande de signature de certificat ou pour créer manuellement la demande de signature de certificat.

Type de certificat	Exigences en matière de certificats
	Si vous créez manuellement la demande de signature de certificat, elle doit répondre aux exigences répertoriées précédemment sous *Exigences pour tous les certificats vSphere importés*. Vous devez également spécifier le nom de domaine complet de l'hôte.
Certificat d'utilisateur de solution	Vous pouvez utiliser vSphere Certificate Manager pour créer la demande de signature de certificat ou pour créer manuellement la demande de signature de certificat. **Note** Vous devez utiliser une valeur différente pour le nom de chaque utilisateur de solution. Si vous générez le certificat manuellement, il peut s'afficher comme **CN** sous **Objet**, en fonction de l'outil que vous utilisez. Si vous utilisez vSphere Certificate Manager, l'outil vous invite à entrer les informations de certificat pour chaque utilisateur de solution. vSphere Certificate Manager stocke les informations dans `certool.cfg`. Pour l'utilisateur de solution vpxd-extension, vous pouvez laisser vide l'option Utilisation de clé étendue ou utiliser « Authentification client WWW TLS ».

Exigences lors de l'utilisation des certificats personnalisés

Lorsque vous voulez utiliser des certificats personnalisés, ils doivent répondre aux exigences suivantes.

Type de certificat	Exigences en matière de certificats
Certificat SSL de machine	Le certificat SSL de machine sur chaque nœud doit avoir un certificat distinct de votre autorité de certification d'entreprise ou tierce. ■ Vous pouvez générer la demande de signature de certificat à l'aide de vSphere Client ou vSphere Certificate Manager, ou en créer une manuellement. La demande de signature de certificat doit répondre aux exigences répertoriées précédemment sous *Exigences pour tous les certificats vSphere importés*. ■ 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.
Certificat d'utilisateur de solution	Chaque utilisateur de solution sur chaque nœud doit avoir un certificat distinct de votre autorité de certification d'entreprise ou tierce. ■ Vous pouvez générer les demandes de signature de certificat à l'aide de vSphere Certificate Manager ou en préparer une vous-même. La demande de signature de certificat doit répondre aux exigences répertoriées précédemment sous *Exigences pour tous les certificats vSphere importés*. ■ Si vous utilisez vSphere Certificate Manager, l'utilitaire vous invite à entrer les informations de certificat pour chaque utilisateur de solution. vSphere Certificate Manager stocke les informations dans `certool.cfg`. **Note** Vous devez utiliser une valeur différente pour le nom de chaque utilisateur de solution. Un certificat généré manuellement peut s'afficher comme **CN** sous **Objet**, en fonction de l'outil que vous utilisez. Lorsque vous remplacez ultérieurement les certificats d'utilisateurs de solution par des certificats personnalisés, indiquez la chaîne de certificats de signature complète de l'autorité de certification tierce. Pour l'utilisateur de solution vpxd-extension, vous pouvez laisser vide l'option Utilisation de clé étendue ou utiliser « Authentification client WWW TLS ».

Présentation de la gestion des certificats vSphere

La procédure à suivre pour la configuration ou la mise à jour de votre infrastructure de certificats vSphere dépend des exigences de votre environnement. Vous devez définir si vous effectuez une nouvelle installation ou une mise à niveau et si vous envisagez 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. VMware Certificate Authority (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 6.0 ou version ultérieure 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 votre 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 votre stratégie d'entreprise n'autorise pas les certificats intermédiaires dans la chaîne, vous pouvez remplacer les certificats de façon explicite. Vous pouvez utiliser vSphere Client, 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 VMware Certificate Endpoint Store (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 vous effectuez une actualisation des certificats à partir de vSphere Client, les certificats signés par VMCA remplacent les certificats personnalisés.
- Pour la mise à niveau d'une installation simple de vCenter Server vers un déploiement intégré, vCenter Server conserve les certificats personnalisés. Après la mise à niveau, votre environnement fonctionne comme auparavant. Les certificats vCenter Server et vCenter Single Sign-On existants 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. VMware ne recommande pas le remplacement des certificats d'utilisateur de solutions.

Interfaces de certificat vSphere

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

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

Interface	Utilisez
vSphere Client	Effectuez les tâches de certificat courantes à l'aide d'une interface utilisateur graphique.
API de vSphere Automation	Consultez le *Guide de programmation des SDK de VMware vSphere Automation*.
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 vSphere Certificate Management	Effectuez toutes les tâches de gestion de certificats avec `dir-cli`, `certool` et `vecs-cli`.
Utilitaire `sso-config`	Effectuez la gestion du certificat STS à partir de la ligne de commande de l'installation de vCenter Server.
PowerCLI 12.4 (requiert vSphere 7.0 ou version ultérieure)	Gérez des magasins de certificats approuvés, gérez des certificats SSL de machine vCenter Server et gérez des certificats SSL de machine ESXi.

Pour ESXi, effectuez la gestion des certificats à partir de vSphere 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 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.

Remplacement des certificats vSphere

Vous pouvez effectuer différents types de remplacement de certificats selon la stratégie et les besoins de votre entreprise pour le système que vous configurez. Vous pouvez effectuer un remplacement de certificat à l'aide de vSphere Client en utilisant l'utilitaire vSphere Certificate

Manager, ou le remplacer manuellement à l'aide des interfaces de ligne de commande incluses dans votre installation.

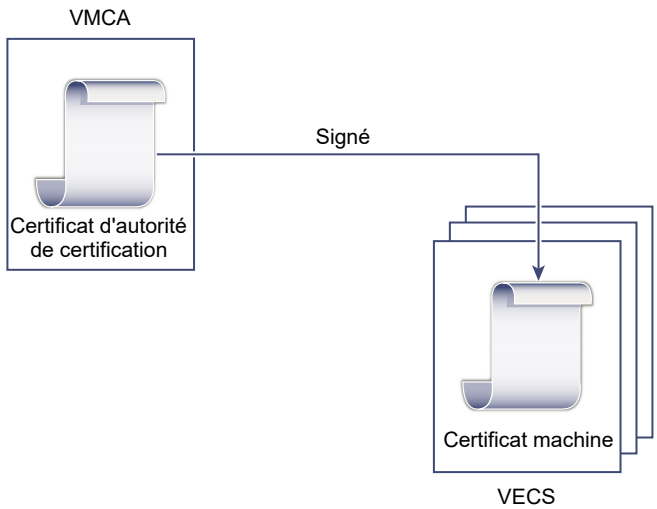
VMware Certificate Authority (VMCA) est inclus dans chaque déploiement de vCenter Server. VMCA provisionne chaque nœud, chaque utilisateur de solution vCenter Server et chaque hôte ESXi avec un certificat signé par VMCA en tant qu'autorité de certification.

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.

Remplacement des certificats 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 10 ans, et 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 10 ans.

Figure 2-1. 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

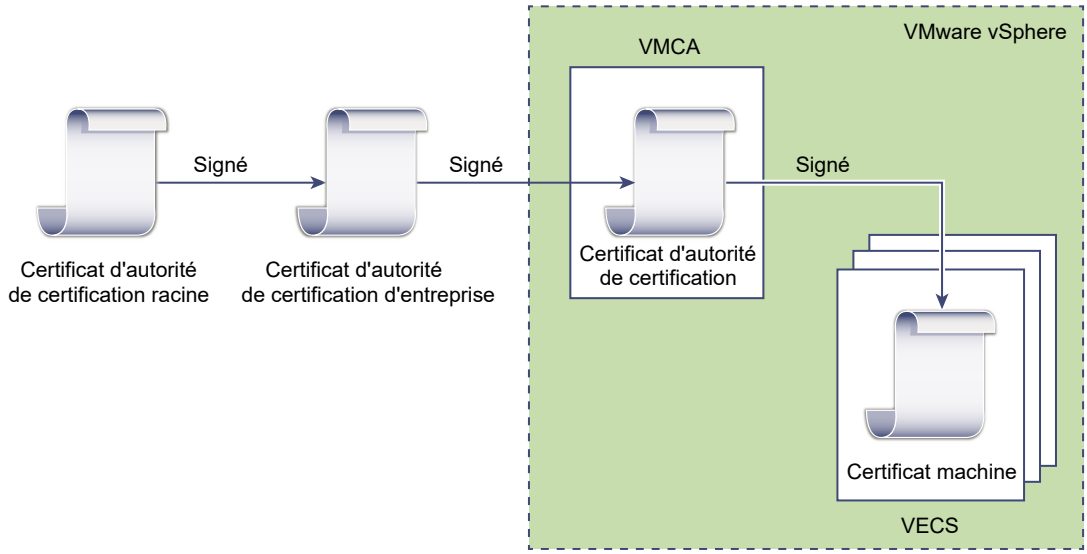
Pour le remplacement manuel de certificat, reportez-vous à Remplacer les certificats existants signés par VMCA par de nouveaux certificats signés par VMCA à l'aide de la CLI.

Faire de VMCA une autorité de certification intermédiaire

Vous pouvez remplacer le certificat racine VMCA par un certificat qui est signé par une autorité de certification (CA) 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.

Note Si vous effectuez une nouvelle installation avec un système vCenter Server, 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 2-2. 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 :

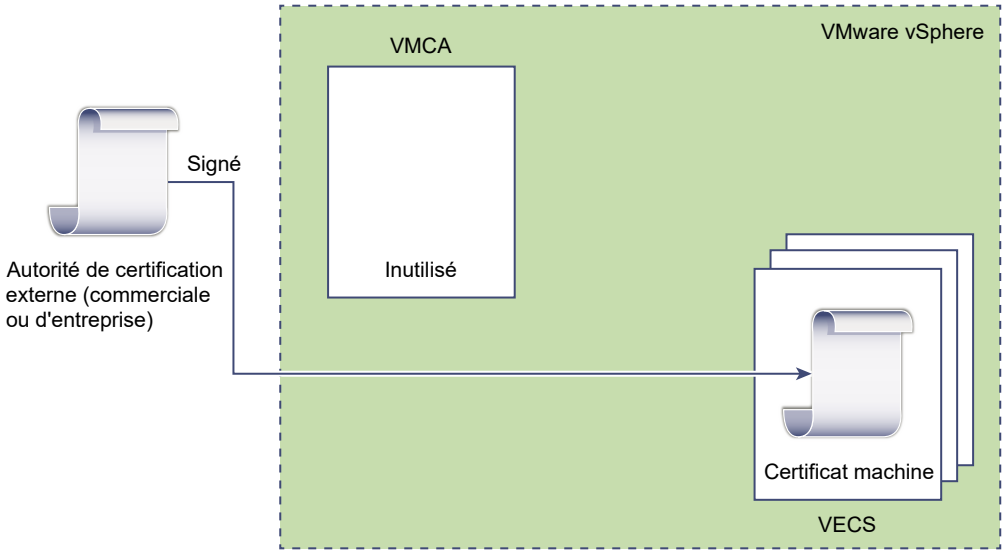
- Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats
- Remplacer le certificat SSL machine par un certificat VMCA (déploiement Enhanced Linked Mode multi-nœud)
- Remplacer le certificat d'utilisateurs de solution par un certificat VMCA (déploiement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

Pour le remplacement manuel de certificat, reportez-vous à Faire de VMCA une autorité de certification intermédiaire à l'aide de l'interface de ligne de commande.

Remplacement des certificats signés par VMCA par 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 2-3. 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 Remplacer les certificats par des certificats personnalisés à l'aide de l'interface de ligne de commande.

Vous pouvez également utiliser vSphere Client pour générer une demande de signature de certificat pour un certificat SSL de machine (personnalisé) et remplacer le certificat après son renvoi par l'autorité de certification. Reportez-vous à la section Générer une demande de signature de certificat pour un certificat SSL de machine à l'aide de vSphere Client (certificats personnalisés).

Utilisation de l'approche hybride pour le déploiement de certificats

Dans l'approche 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 Client. Pour plus d'informations, reportez-vous à la documentation *Sécurité vSphere*.

Tableau 2-4. Options de remplacement de certificat ESXi

Option	Description
Mode VMware Certificate Authority (par défaut)	Lorsque vous renouvelez des certificats à partir de vSphere 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	Permet de mettre à jour et d'utiliser manuellement 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.

Utilisation de certificats par vSphere

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 2-5. Certificats dans vSphere

Certificat	Alloué	Commentaires
Certificats ESXi	VMCA (par défaut)	Stockés localement sur l'hôte ESXi.
Certificats SSL de la machine	VMCA (par défaut)	Stocké dans VMware Endpoint Certificate Store (VECS).
Certificats d'utilisateurs de solutions	VMCA (par défaut)	Stockés dans VECS.
Certificat de signature SSL vCenter Single Sign-On	Provisionné au cours de l'installation.	Gérez ce certificat à partir de la ligne de commande. **Note** Ne modifiez pas ce certificat dans le système de fichiers pour éviter de provoquer des résultats imprévisibles.

Tableau 2-5. Certificats dans vSphere (suite)

Certificat	Alloué	Commentaires
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 en tant que certificat vmdir.
Certificats auto-signés SMS	Provisionné lors de l'enregistrement du fournisseur IOFilter.	Dans vSphere 7.0 et versions ultérieures, les certificats auto-signés SMS sont stockés dans `/etc/vmware/ssl/iofiltervp_castore.pem`. Avant vSphere 7.0, les certificats auto-signés SMS étaient stockés dans `/etc/vmware/ssl/gbe.pem`. En outre, le magasin SMS peut également stocker les certificats auto-signés du fournisseur VASA VVOL (version 4.0 et antérieures) lorsque retainVasaProviderCertificate=True.

Certificats 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. Pour plus d'informations, consultez la documentation *Sécurité vSphere*.

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 vCenter Server dispose de son propre certificat SSL de machine. Tous les services exécutés sur un nœud vCenter Server 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. Les connexions SSL vers des services vCenter individuels accèdent toujours au proxy inverse. Le trafic n'accède pas aux services eux-mêmes.
- Service vCenter Server (vpxd).
- VMware Directory Service (vmdir)

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 vSphere Client 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'utilisateur de solution suivants sont inclus dans VECS :

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

  Note 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 du démon de service vCenter (vpxd). vpxd utilise le certificat d'utilisateur de solution stocké dans ce magasin pour s'authentifier sur vCenter Single Sign-On.
- `vpxd-extension` : 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 Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance.
- `wcp`: VMware vSphere® avec le magasin VMware Tanzu™.

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.

Vous pouvez remplacer ce certificat dans l'interface de ligne de commande. Reportez-vous à la section Remplacer un certificat STS vCenter Server à l'aide de la ligne de commande.

Certificat SSL de VMware Directory Service

Dans vSphere 6.5 et versions ultérieures, le certificat SSL de machine est utilisé en tant que certificat VMware Directory. Pour les versions antérieures de vSphere, reportez-vous à la documentation correspondante.

Certificat de chiffrement des machines virtuelles vSphere

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

VMware Certificate Authority et VMware Core Identity Services

Les services d'identité de base font partie de chaque système vCenter Server. VMCA (VMware Certificate Authority) fait partie de chaque groupe de services d'identité de base VMware. Utilisez l'interface de ligne de commande de gestion et vSphere Client pour interagir avec ces services.

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

Tableau 2-6. Services d'identité de base

Service	Description
VMware Directory Service (vmdir)	Source d'identité qui assure la gestion des certificats SAML pour l'authentification auprès de vCenter Single Sign-On.
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.
Démon VMware Authentication Framework (VMAFD)	Inclut le magasin de certificats de point de terminaison VMware (VECS) et plusieurs autres services d'authentification. Les administrateurs VMware interagissent avec VECS. Les autres services sont utilisés en interne.

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 s'exécute sur chaque nœud de vCenter Server et 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 racine approuvé. Vous pouvez également gérer explicitement les certificats et les clés dans VECS à l'aide des commandes `vecs-cli`. Reportez-vous à la section Référence des commandes vecs-cli.

VECS inclut les magasins suivants.

Tableau 2-7. 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 le service VMware Directory Service (vmdir) sur chaque nœud vCenter Server. Tous les services de vSphere 6.0 ou versions ultérieures 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.
Magasins d'utilisateurs de solution ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	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. Les magasins de certificats d'utilisateur de solution suivants sont inclus dans VECS : ■ `machine` : utilisé par le serveur de licences et le service de journalisation. **Note** 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 du démon de service vCenter (vpxd). vpxd utilise le certificat d'utilisateur de solution stocké dans ce magasin pour s'authentifier sur vCenter Single Sign-On. ■ `vpxd-extension` : 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 Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance. ■ `wcp`: VMware vSphere® avec le magasin VMware Tanzu™. Chaque nœud vCenter Server comprend un certificat `machine`.
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.

Tableau 2-7. 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. **Note** 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 depuis l'interface de ligne de commande.

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.

Note 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 des certificats vSphere

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

vSphere prend en charge le remplacement des certificats, mais n'applique pas la révocation des certificats pour les hôtes ESXi ou 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 vSphere dans les grands déploiements

Lorsque vous remplacez des certificats dans des déploiements comportant un grand nombre d'hôtes vCenter Server, vous pouvez utiliser l'utilitaire de gestion des certificats vSphere ou remplacer les certificats manuellement à l'aide des interfaces de ligne de commande. Certaines pratiques recommandées guident le processus que vous choisissez.

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

Si votre environnement inclut plusieurs nœuds vCenter Server, vous pouvez remplacer les certificats SSL de la machine avec vSphere Client, l'utilitaire vSphere Certificate Manager ou manuellement avec des commandes de l'interface de ligne de commande.

vSphere Certificate Manager

Exécutez vSphere Certificate Manager sur chaque machine. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat. Consultez les rubriques suivantes pour plus d'informations :

- Remplacer le certificat racine VMCA par un certificat de signature personnalisé et Remplacer tous les certificats à l'aide de Certificate Manager
- Remplacer le certificat SSL de machine par un certificat VMCA (autorité de certification intermédiaire) à l'aide de Certificate Manager
- Remplacer les certificats d'utilisateur de solutions par des certificats VMCA (autorité de certification intermédiaire) à l'aide de Certificate Manager

Remplacement manuel de certificats

Pour le remplacement manuel des certificats, exécutez les commandes de l'interface de ligne de commande de remplacement des certificats sur chaque machine. Consultez les rubriques suivantes pour plus d'informations :

- Remplacer les certificats SSL de machine par des certificats signés par VMCA à l'aide de la CLI
- Remplacer les certificats SSL de machine (autorité de certification intermédiaire) à l'aide de la CLI
- Remplacer les certificats SSL de machine par des certificats personnalisés à l'aide de la CLI

Remplacement des certificats d'utilisateur de solution dans des environnements comportant plusieurs systèmes de vCenter Server en mode Enhanced Linked Mode

Si votre environnement inclut plusieurs systèmes vCenter Server en mode Enhanced Linked Mode, procédez comme suit pour le remplacement des certificats d'utilisateurs de solution.

Note 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. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat. Reportez-vous à la section Gestion des certificats à l'aide de l'utilitaire vSphere Certificate Manager.

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 chaque vCenter Server.
   - Un certificat pour chacun des utilisateurs de solutions suivants sur chaque nœud :
     - utilisateur de solution `vpxd`
     - utilisateur de solution `vpxd-extension`
     - utilisateur de solution `vsphere-webclient`
     - utilisateur de solution `wcp`
2. Utilisez les commandes de l'interface de ligne de commande pour remplacer les certificats sur chaque nœud. La précision de la procédure dépend du type de remplacement de certificat que vous effectuez.

   Consultez les rubriques suivantes pour plus d'informations :
   - Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA à l'aide l'interface de ligne de commande
   - Remplacer les certificats d'utilisateur de solutions (autorité de certification intermédiaire) à l'aide de la CLI
   - Remplacer les certificats d'utilisateurs de solutions par des certificats personnalisés à l'aide de Certificate Manager

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. Si vous remplacez le certificat SSL machine par défaut sur le système vCenter Server, 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. Pour plus d'informations, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2109074.

Gestion des certificats avec vSphere Client

Vous pouvez afficher et gérer des certificats à l'aide de vSphere Client.

vSphere Client vous permet d'effectuer ces tâches de gestion.

- Affichez les certificats SSL, racines VMCA (VMware Certificate Authority), racines approuvés et STS (Security Token Service) de la machine.
- Ajoutez de nouveaux certificats racines approuvés, puis renouvelez ou remplacez les certificats SSL et STS de machine existants.
- Générez une demande de signature de certificat (CSR) personnalisée pour un certificat SSL de machine et remplacez le certificat lorsque l'autorité de certification le renvoie.

Les workflows de remplacement de certificat sont en grande partie entièrement pris en charge à partir de vSphere Client. D'autres workflows de remplacement de certificat sont pris en charge par l'utilitaire vSphere Certificate Manager. Reportez-vous à la section Gestion des certificats à l'aide de l'utilitaire vSphere Certificate Manager.

Pour en savoir plus sur les options de remplacement des certificats par défaut, reportez-vous à la section Remplacement des certificats vSphere.

Note Si vous utilisez VMCA comme autorité de certification intermédiaire ou que vous utilisez des certificats personnalisés, vous vous exposez à plus de complexité et à un risque potentiel pour votre sécurité, ce qui représente une augmentation inutile dans vos risques opérationnels. Pour plus d'informations sur la gestion des certificats dans un environnement vSphere, consultez le blog intitulé *Nouvelle procédure produit - Remplacement hybride des certificats SSL vSphere* à l'adresse http://vmware.com/go/hybridvmca.

Explorer les magasins de certificats avec vSphere Client

Une instance du magasin de certificats VECS (VMware Endpoint Certificate Store) est incluse sur chaque nœud vCenter Server. Vous pouvez explorer les différents magasins dans le magasin de certificats de point de terminaison VMware depuis vSphere Client, y compris les certificats SSL de machine et racine approuvés.

Consultez la section Présentation du magasin de certificats VMware Endpoint pour plus d'informations sur les différents magasins dans VECS.

Conditions préalables

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. Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.
   a Dans le menu **Accueil**, sélectionnez **Administration**.
   b Sous **Certificats**, cliquez sur **Gestion des certificats**.
4 Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.
5 Explorez les certificats stockés dans VMware Endpoint Certificate Store (VECS).

   La rubrique Présentation du magasin de certificats VMware Endpoint décrit le contenu des magasins individuels.
6 Pour afficher les détails d'un certificat, sélectionnez celui-ci et cliquez sur **Afficher les détails**.
7 Utilisez le menu **Actions** pour renouveler ou remplacer les certificats.

   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.

Définir le seuil pour les avertissements d'expiration du certificat vCenter à l'aide de vSphere Client

vCenter Server surveille tous les certificats du magasin VECS (VMware Endpoint Certificate Store) et émet une alarme lorsqu'un certificat est à 30 jours ou moins de son expiration. Vous pouvez utiliser vSphere Client pour modifier le délai d'avertissement à l'aide de l'option avancée `vpxd.cert.threshold`.

Procédure

1 Connectez-vous à vSphere Client.
2 Sélectionnez l'objet vCenter Server et cliquez sur **Configurer**.
3 Cliquez sur **Paramètres avancés**.
4 Cliquez sur **Modifier les paramètres** et filtrez pour **`threshold`**.
5 Modifiez le paramètre de `vpxd.cert.threshold` en saisissant la valeur souhaitée et cliquez sur **Enregistrer**.

Renouveler les certificats VMCA par de nouveaux certificats signés par VMCA à l'aide de vSphere Client

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 une sélection ou l'ensemble des certificats de votre environnement depuis vSphere Client.

Conditions préalables

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. Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Certificats**, cliquez sur **Gestion des certificats**.
4. Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.
5. Renouvelez le certificat SSL de la machine signé par VMCA pour le système local.
   a. À partir de la vignette **Certificat SSL de machine**, cliquez sur **Actions > Renouveler**.
   b. Spécifiez la durée du certificat en jours.
   c. Cliquez sur **Renouveler**.

      Les services vCenter Server redémarrent automatiquement. Vous devez vous reconnecter, car le redémarrage des services met fin à la session de l'interface utilisateur.

Remplacer les certificats par des certificats personnalisés à l'aide de vSphere Client

Vous pouvez utiliser vSphere Client pour remplacer les certificats par défaut par des certificats personnalisés.

Vous pouvez utiliser vSphere Client pour générer des demandes de signature de certificat pour chaque machine et remplacer les certificats lorsque vous les recevez de votre autorité de certification interne ou tierce. 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 vSphere Client.

Générer une demande de signature de certificat pour un certificat SSL de machine à l'aide de vSphere Client (certificats personnalisés)

Le certificat SSL de machine est utilisé par le service de proxy inverse sur chaque nœud vCenter Server. Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Vous pouvez utiliser vSphere Client pour générer une demande de signature de certificat (CSR) pour le certificat SSL de machine et pour remplacer le certificat une fois qu'il est prêt.

Conditions préalables

Le certificat doit répondre à la configuration requise suivante :

- Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
- Format CRT
- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>.
- Contient les utilisations de clé suivantes : signature numérique, chiffrement de clé

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Certificats**, cliquez sur **Gestion des certificats**.
4. Entrez les informations d'identification de votre vCenter Server.

5 Générer la demande de signature de certificat.

a Sous la vignette **Certificat SSL de machine**, cliquez sur **Actions > Générer la demande de signature de certificat (CSR)**.

b Entrez vos informations de certificat et cliquez sur **Suivant**.

À partir de vSphere 8.0, 3 072 (bits) est la valeur par défaut pour la taille de clé. 2 048 n'est plus pris en charge lors de la génération d'une CSR à l'aide de vSphere Client. vCenter Server accepte toujours les certificats personnalisés ayant une longueur de clé de 2 048 bits. Toutefois, à partir de vSphere 8.0, vous pouvez uniquement générer des CSR à l'aide de vSphere Client avec une longueur de clé minimale de 3 072 bits.

Note Lorsque vous utilisez vCenter Server pour générer une demande de signature de certificat avec une taille de clé de 16 384 bits, la génération prend quelques minutes car cette opération est gourmande en CPU.

c Copiez ou téléchargez la demande de signature de certificat.

d Cliquez sur **Terminer**.

e Fournissez la demande de signature de certificat à votre autorité de certification.

Étape suivante

Lorsque l'autorité de certification renvoie le certificat, remplacez le certificat existant dans le magasin de certificats. Reportez-vous à la section Ajouter des certificats personnalisés avec vSphere Client.

Ajouter un certificat racine approuvé au magasin de certificats avec vSphere Client

Si vous souhaitez utiliser des certificats tiers dans votre environnement, vous devez ajouter un certificat racine approuvé au magasin de certificats. Pour cela, vous pouvez utiliser vSphere Client.

Conditions préalables

Obtenez le certificat racine personnalisé de votre autorité de certification (CA) tierce ou interne.

vSphere n'accepte que les certificats d'autorité de certification valides pour l'importation. Pour être valide, un certificat d'autorité de certification doit avoir le bit CA et le bit keyCertSign définis dans la contrainte de base et les extensions de certificat X.509 v3 d'utilisation de clé, respectivement. Cela signifie que le certificat est une autorité de certification et que son objectif est la signature de certificat. Pour plus d'informations, consultez le site Web https://www.rfc-editor.org/rfc/rfc5280.

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Certificats**, cliquez sur **Gestion des certificats**.

4 Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.

5 Sous **Certificats racines approuvés**, cliquez sur **Ajouter**.

6 Cliquez sur **Parcourir** et sélectionnez l'emplacement de la chaîne de certificats.

   Vous pouvez utiliser un fichier de type CER, PEM ou CRT.

7 Cliquez sur **Ajouter**.

   Le certificat est ajouté au magasin.

Ajouter des certificats personnalisés avec vSphere Client

Vous pouvez utiliser vSphere Client pour ajouter des certificats SSL de machine personnalisés au magasin de certificats.

Il suffit généralement de remplacer le certificat SSL de la machine pour chaque composant.

Conditions préalables

Générez des demandes de signature de certificat (CSR, Certificate Signing Request) pour chaque certificat que vous souhaitez remplacer. Reportez-vous à la section Générer une demande de signature de certificat pour un certificat SSL de machine à l'aide de vSphere Client (certificats personnalisés). Placez le certificat et la clé privée dans un emplacement accessible par vCenter Server.

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Certificats**, cliquez sur **Gestion des certificats**.

4 Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.

5 Dans la vignette **Certificat SSL de machine**, cliquez sur **Actions > Importer et remplacer le certificat**.

6 Cliquez sur l'option de remplacement de certificat appropriée, puis sur **Suivant**.

Option	Description
Remplacer par VMCA	Crée une CSR générée par VMCA pour remplacer le certificat actuel.
Remplacer par un certificat généré à partir de l'instance de vCenter Server	Utilisez un certificat signé à l'aide d'une CSR générée par l'instance de vCenter Server pour remplacer le certificat actuel.
Remplacer le certificat d'autorité de certification externe (requiert une clé privée)	Utilisez un certificat signé par une autorité de certification externe pour remplacer le certificat actuel.

7 Entrez les informations de la demande CSR ou téléchargez les certificats appropriés.

8 Cliquez sur **Remplacer**.

Les services vCenter Server redémarrent automatiquement.

Gestion des certificats à l'aide de 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.

Pour en savoir plus sur les options de remplacement des certificats par défaut, reportez-vous à la section Remplacement des certificats vSphere.

Note Si vous utilisez VMCA comme autorité de certification intermédiaire ou que vous utilisez des certificats personnalisés, vous vous exposez à plus de complexité et à un risque potentiel pour votre sécurité, ce qui représente une augmentation inutile dans vos risques opérationnels. Pour plus d'informations sur la gestion des certificats dans un environnement vSphere, consultez le blog intitulé *Nouvelle procédure produit - Remplacement hybride des certificats SSL vSphere* à l'adresse http://vmware.com/go/hybridvmca.

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.

Vous exécutez les options de vSphere 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. Avant d'exécuter vSphere Certificate Manager, veillez à bien comprendre le processus de remplacement et procurez-vous les certificats que vous souhaitez utiliser.

Attention 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 vSphere Certificate Manager

L'utilitaire vSphere Certificate Manager se trouve à l'adresse suivant :

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

Note Lors de l'exécution de vSphere Certificate Manager, certaines options vous invitent comme suit :

```
Enter proper value for VMCA 'Name':
```

Répondez à cette invite en entrant le nom de domaine complet de la machine sur laquelle la configuration du certificat est en cours d'exécution.

Présentation des workflows dans l'utilitaire vSphere Certificate Manager

Le tableau suivant présente une vue d'ensemble des workflows de remplacement des certificats que vous pouvez effectuer à l'aide de l'utilitaire vSphere Certificate Manager.

Tableau 2-8. Workflows de l'utilitaire de gestion des certificats vSphere

Workflow	Description	Reportez-vous au
Remplacement du certificat racine VMCA par un certificat de signature personnalisé et remplacement de tous les certificats	Pour générer le certificat racine VMCA et remplacer tous les certificats, utilisez l'option 4, Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats.	Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats à l'aide de Certificate Manager
Faire de VMCA une autorité de certification intermédiaire	Pour faire de VMCA une autorité de certification intermédiaire, vous devez exécuter l'utilitaire vSphere Certificate Manager plusieurs fois et utiliser plusieurs options. Ce workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions.	Faire de VMCA une autorité de certification intermédiaire à l'aide de Certificate Manager

Tableau 2-8. Workflows de l’utilitaire de gestion des certificats vSphere (suite)

Workflow	Description	Reportez-vous au
Remplacement de tous les certificats par des certificats personnalisés	Pour remplacer tous les certificats par des certificats personnalisés, vous devez exécuter l’utilitaire vSphere Certificate Manager plusieurs fois et utiliser plusieurs options. Ce workflow fournit l'intégralité des étapes de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions.	Remplacer tous les certificats par un certificat personnalisé à l'aide de Certificate Manager
Restauration de la dernière opération effectuée	Pour restaurer la dernière opération de certificat effectuée et revenir à l'état précédent, utilisez l'option 7, Restaurer la dernière opération effectuée en republiant les anciens certificats.	Restaurer la dernière opération effectuée en republiant les anciens certificats à l'aide de Certificate Manager
Réinitialisation de tous les certificats	Pour remplacer tous les certificats vCenter existants par des certificats signés par VMCA. Utilisez l'option 8, Réinitialiser tous les certificats.	Réinitialiser tous les certificats à l'aide de Certificate Manager

Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats à l'aide de Certificate Manager

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour régénérer le certificat racine VMCA et remplacer le certificat SSL de machine locale, ainsi que les certificats d'utilisateur de la solution locale par des certificats signés par VMCA. Lorsque plusieurs instances de vCenter Server sont connectées dans une configuration Enhanced Linked Mode, vous devez remplacer les certificats sur chaque vCenter Server.

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 vCenter Server, 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 de vCenter Server
- Nom VMCA, c'est-à-dire le nom de domaine complet de la machine sur laquelle la configuration de certificat est en cours d'exécution.

Conditions préalables

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. Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Sélectionnez l'option 4. Régénérer un nouveau certificat racine VMCA et remplacez tous les certificats.
3. Entrez le nom de l'utilisateur administrateur et le mot de passe.
4. Répondez aux invites.

   vSphere Certificate Manager génère un nouveau certificat racine VMCA basé sur votre entrée et remplace tous les certificats sur le système où vous exécutez vSphere Certificate Manager. Le processus de remplacement est terminé après le redémarrage des services par vSphere Certificate Manager.
5. Pour remplacer le certificat SSL de machine, exécutez vSphere Certificate Manager avec l'option 3, Remplacer le certificat SSL de machine par un certificat VMCA.
6. Pour remplacer les certificats d'utilisateurs de solutions, exécutez Certificate Manager avec l'option 6, Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA.

Faire de VMCA une autorité de certification intermédiaire à l'aide de Certificate Manager

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour faire de VMCA une autorité de certification intermédiaire. À la fin du processus, VMCA signe tous les nouveaux certificats avec

la chaîne complète. Si vous le souhaitez, vous pouvez utiliser vSphere Certificate Manager pour remplacer tous les certificats existants par de nouveaux certificats signés par VMCA.

VMware ne recommande pas d'utiliser VMCA en tant qu'autorité de certification subordonnée (ou intermédiaire). Si vous choisissez cette option, vous vous exposez à plus de complexité et à un risque potentiel pour votre sécurité, ce qui représente une augmentation inutile dans vos risques opérationnels. Pour plus d'informations sur la gestion des certificats dans un environnement vSphere, consultez le blog intitulé *Nouvelle procédure produit - Remplacement hybride des certificats SSL vSphere* à l'adresse http://vmware.com/go/hybridvmca.

Pour faire de VMCA une autorité de certification intermédiaire, vous devez exécuter vSphere Certificate Manager plusieurs fois. Les étapes générales de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions sont notamment :

1 Lancement de l'utilitaire vSphere Certificate Manager.

2 Génération d'une demande de signature de certificat par l'exécution de 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. Lorsque vous êtes invité à entrer à nouveau une option, sélectionnez l'option 1, Générer une ou plusieurs demandes de signature de certificat et une ou plusieurs clés pour le certificat de signature racine VMCA.

3 Soumission de 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.

4 Combinaison du certificat racine VMCA au certificat racine de l'autorité de certification et enregistrement du fichier.

5 Remplacement des certificats par l'exécution de l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats, et réponse aux invites. Ce processus remplace tous les certificats sur la machine locale.

6 (Facultatif) Remplacement des certificats sur chaque nœud lorsque plusieurs instances de vCenter Server sont connectées dans une configuration Enhanced Linked Mode par :

   a En premier lieu le remplacement du certificat SSL de machine par le (nouveau) certificat VMCA (option 3, Remplacer le certificat SSL de machine par un certificat VMCA).

   b Ensuite le remplacement des certificats d'utilisateurs de solutions par le (nouveau) certificat VMCA (option 6, Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA).

Générer une demande de signature de certificat avec Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire)

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR). 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.

  Note À partir de vSphere 8.0, si vous utilisez vCenter Server pour générer la demande de signature de certificat, la taille de la clé est modifiée par défaut à 3 072 bits au lieu de 2 048.

- Si vous préférez créer la demande de signature de certificat manuellement, le certificat envoyé pour signature doit satisfaire les conditions suivantes :
  - Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (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
  - L'extension d'autorité de certification doit être définie sur true pour les certificats racines et la signature de certification doit figurer dans la liste de conditions requises. Par exemple :

    ```
    basicConstraints        = critical,CA:true
    keyUsage                = critical,digitalSignature,keyCertSign
    ```

  - La signature CRL doit être activée.
  - Le champ Utilisation étendue de la clé peut être vide ou contenir la valeur du champ Authentification du serveur.
  - Aucune limite explicite à la longueur de la chaîne de certificats. VMCA utilise la valeur par défaut OpenSSL, qui est 10 certificats.
  - Les certificats incluant des caractères génériques ou plusieurs noms DNS ne sont pas pris en charge.
  - Vous ne pouvez pas créer d'autorités de certification filiales de VMCA.

    Reportez-vous à l'article « Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x » de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2112009 pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

Conditions préalables

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 Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Sélectionnez l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats.

Initialement, vous utilisez cette option pour générer la demande de signature de certificat, pas pour remplacer des certificats.

3 Entrez le nom de l'utilisateur administrateur et le mot de passe.

4 Sélectionnez l'option 1, Générer une ou plusieurs demandes de signature de certificat et une ou plusieurs clés pour le certificat de signature racine VMCA, pour générer la CSR et répondre aux invites.

Dans le cadre du processus, vous devez fournir un répertoire. vSphere Certificate Manager place le certificat à signer (fichier `*.csr`) et le fichier de clés correspondant (fichier `*.key`) dans le répertoire.

5 Nom de la demande de signature de certificat (CSR) `root_signing_cert.csr`.

6 Envoyez la demande CSR à votre entreprise ou à l'autorité de certification externe pour obtenir la signature et nommez le certificat signé `root_signing_cert.cer`.

7 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-----
```

8 Enregistrez le fichier en tant que `root_signing_chain.cer`.

Étape suivante

Remplacez le certificat racine existant par le certificat racine chaîné. Reportez-vous à la section Remplacer le certificat racine VMCA par un certificat de signature personnalisé et Remplacer tous les certificats à l'aide de Certificate Manager.

Remplacer le certificat racine VMCA par un certificat de signature personnalisé et Remplacer tous les certificats à l'aide de Certificate Manager

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour générer une demande de signature de certificat et l'envoyer à une autorité de certification tierce ou d'entreprise pour la signature. Vous pouvez ensuite remplacer le certificat racine VMCA par un certificat de signature

personnalisé et remplacer tous les certificats existants par des certificats signés par l'autorité de certification personnalisée.

Exécutez vSphere Certificate Manager sur une instance externe de vCenter Server pour remplacer le certificat racine VMCA par un certificat de signature personnalisé.

Conditions préalables

- 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 Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire) pour les conditions requise des certificats et le processus de combinaison des certificats.
- Rassemblez les informations qui vous sont nécessaires.
  - Mot de passe pour administrator@vsphere.local
  - Certificat personnalisé valide pour Root (fichier `.crt`)
  - Clé personnalisée valide pour l'utilisateur racine (fichier `.key`)

Procédure

1. Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Sélectionnez l'option 2, Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats.
3. Entrez le nom de l'utilisateur administrateur et le mot de passe.
4. Sélectionnez l'option 2, Importer un ou plusieurs certificats et clés personnalisés pour remplacer le certificat de signature racine VMCA existant, puis 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`.

Remplacer le certificat SSL de machine par un certificat VMCA (autorité de certification intermédiaire) à l'aide de Certificate Manager

Lorsque vous utilisez VMCA comme autorité de certification intermédiaire, vous pouvez explicitement remplacer le certificat SSL de machine à l'aide de l'utilitaire vSphere Certificate

Manager. Tout d'abord, vous remplacez le certificat racine VMCA sur vCenter Server, puis vous pouvez remplacer le certificat SSL de machine, qui sera signé par la nouvelle racine du VMCA. 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 vCenter Server, 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 de vCenter Server
- Nom VMCA, c'est-à-dire le nom de domaine complet de la machine sur laquelle la configuration de certificat est en cours d'exécution.

Conditions préalables

- Vous devez connaître les informations suivantes pour exécuter 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.
  - Nom d'hôte ou adresse IP du système vCenter Server.

Procédure

1 Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Sélectionnez l'option 3, Remplacer le certificat SSL de machine par un certificat VMCA.

3 Entrez le nom de l'utilisateur administrateur et le mot de passe.

4 Répondez aux invites.

vSphere Certificate Manager stocke les informations dans le fichier `certool.cfg`.

Résultats

vSphere Certificate Manager remplace le certificat machine SSL.

Remplacer les certificats d'utilisateur de solutions par des certificats VMCA (autorité de certification intermédiaire) à l'aide de Certificate Manager

Lorsque vous utilisez VMCA comme autorité de certification intermédiaire, vous pouvez explicitement remplacer le certificat d'utilisateur de solution à l'aide de l'utilitaire vSphere Certificate Manager. Tout d'abord, vous remplacez le certificat racine VMCA sur vCenter Server, puis vous pouvez remplacer le certificat d'utilisateur de solution, qui sera signé par la nouvelle racine du VMCA. Vous pouvez également utiliser cette option pour remplacer les certificats de solutions qui sont altérés ou sur le point d'expirer.

Conditions préalables

- Redémarrez tous les nœuds vCenter Server explicitement si vous avez remplacé le certificat racine VMCA dans un déploiement constitué de plusieurs instances de vCenter Server dans une configuration Enhanced Linked Mode.
- Vous devez connaître les informations suivantes pour exécuter vSphere Certificate Manager avec cette option.
  - Mot de passe pour administrator@vsphere.local
  - Nom d'hôte ou adresse IP du système vCenter Server

Procédure

1 Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Sélectionnez l'option 6, Remplacer les certificats d'utilisateur de solutions par des certificats VMCA.

3 Entrez le nom de l'utilisateur administrateur et le mot de passe.

4 Répondez aux invites.

Pour plus d'informations, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2112281.

Résultats

vSphere Certificate Manager remplace tous les certificats d'utilisateurs de solutions.

Remplacer tous les certificats par un certificat personnalisé à l'aide de 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 vSphere Client, l'utilitaire vSphere Certificate Manager ou des interfaces 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 l'utilitaire vSphere Certificate Manager plusieurs fois. Les étapes générales de remplacement des certificats SSL de machine et des certificats d'utilisateurs de solutions sont notamment :

1 Lancement de l'utilitaire vSphere Certificate Manager.

2 Génération des demandes de signature de certificat pour le certificat SSL de 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 machine, sélectionnez l'option 1, Remplacer le certificat SSL de machine par un certificat personnalisé. Lorsque vous êtes invité à nouveau à choisir une option, sélectionnez l'option 1, Générer une ou plusieurs demandes de signature de certificat et une ou plusieurs clés pour le certificat SSL de machine.

   b Si la stratégie de l'entreprise n'autorise pas un déploiement hybride, sélectionnez l'option 5, Remplacer les certificats d'utilisateurs de solutions par un certificat personnalisé.

3 Soumission de 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.

4 Après avoir reçu les certificats signés et le certificat racine de votre autorité de certification, remplacez le certificat SSL de machine sur chaque machine à l'aide de l'option 1, Remplacer le certificat SSL de machine par un certificat personnalisé.

5 Si vous souhaitez également remplacer les certificats d'utilisateurs de solutions, sélectionnez l'option 5, Remplacer les certificats d'utilisateurs de solutions par un certificat personnalisé.

6 Enfin, lorsque plusieurs instances de vCenter Server sont connectées dans une configuration Enhanced Linked Mode, vous devez répéter le processus sur chaque nœud.

Générer des demandes de signature de certificat avec Certificate Manager (certificats personnalisés)

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR) 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.

Conditions préalables

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.
- Vous êtes invité à saisir le nom d'hôte ou l'adresse IP de vCenter Server.
- 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.

  Note À partir de vSphere 8.0, si vous utilisez vCenter Server pour générer la demande de signature de certificat, la taille de la clé est modifiée par défaut à 3 072 bits au lieu de 2 048.

Procédure

1 Connectez-vous à chaque vCenter Server (le shell vCenter Server) dans votre environnement et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Option 1 : remplacer le certificat SSL de machine par un certificat personnalisé.

3 Entrez le nom de l'utilisateur administrateur et le mot de passe.

4 Sélectionnez l'option 1, Générer une ou plusieurs demandes de signature de certificat et une ou plusieurs clés pour le certificat SSL de machine, pour générer la CSR, répondre aux invites et quitter vSphere Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. vSphere Certificate Manager place les fichiers de certificat et de clé dans le répertoire.

5 Si vous souhaitez également remplacer tous les certificats d'utilisateurs de solutions, redémarrez vSphere Certificate Manager et sélectionnez l'option 5, Remplacer les certificats d'utilisateurs de solutions par un certificat personnalisé.

6 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de vCenter Server, si vous y êtes invité.

7 Sélectionnez l'option 1, Générer une ou plusieurs demandes de signature de certificat et une ou plusieurs clés pour les certificats d'utilisateurs de solutions afin de générer les CSR, répondre aux invites et quitter vSphere Certificate Manager.

   Dans le cadre du processus, vous devez fournir un répertoire. Certificate Manager place le certificat et les fichiers clés dans le répertoire.

Étape suivante

Pour effectuer le remplacement des certificats, reportez-vous à la section Remplacer le certificat SSL de machine par un certificat personnalisé à l'aide de Certificate Manager.

Remplacer le certificat SSL de machine par un certificat personnalisé à l'aide de Certificate Manager

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour remplacer le certificat SSL de machine sur chaque nœud par un certificat personnalisé. Le certificat SSL de machine est utilisé par le service de proxy inverse sur chaque nœud vCenter Server. Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services.

Conditions préalables

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 Certificate Manager (certificats personnalisés).

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 : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
   - Format CRT
   - x509 version 3
   - SubjectAltName doit contenir DNS Name=<machine_FQDN>.
   - Contient les utilisations de clé suivantes : signature numérique, chiffrement de clé

Reportez-vous également à l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2112014, Obtention de certificats vSphere depuis une autorité de certification Microsoft.

Procédure

1 Connectez-vous à vCenter Server et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Option 1 : remplacer le certificat SSL de machine par un certificat personnalisé.

3 Entrez le nom de l'utilisateur administrateur et le mot de passe.

4 Sélectionnez l'option 2, Importer un ou plusieurs certificats personnalisés et une ou plusieurs clés pour remplacer le certificat SSL de machine existant, 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`)
   - Adresse IP de vCenter Server

Remplacer les certificats d'utilisateurs de solutions par des certificats personnalisés à l'aide de Certificate Manager

Bon nombre d'entreprises demandent uniquement à ce que vous remplaciez les certificats de services accessibles de façon externe. Toutefois, l'utilitaire vSphere Certificate Manager prend également en charge le remplacement des certificats d'utilisateurs de solutions. Les utilisateurs de solution sont des ensembles de services, par exemple, tous les services associés à vSphere Client.

Lorsque vous êtes invité à indiquer un certificat d'utilisateur de solution, fournissez la chaîne de certificat de signature complète de l'autorité de certification tierce.

Le format est semblable à l'exemple suivant.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

Conditions préalables

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 Certificate Manager (certificats personnalisés).

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 : de 2 048 bits (minimum) à 16 384 bits (maximum) (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, chiffrement de clé

Reportez-vous également à l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2112014, Obtention de certificats vSphere depuis une autorité de certification Microsoft.

Procédure

1 Connectez-vous à vCenter Server et démarrez vSphere Certificate Manager.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

2 Sélectionnez l'option 5, Remplacer les certificats d'utilisateurs de solutions par un certificat personnalisé.

3 Entrez le nom de l'utilisateur SSO et le mot de passe.

4 Sélectionnez l'option 2, Importer un ou plusieurs certificats personnalisés et une ou plusieurs clés pour remplacer les certificats d'utilisateurs de solutions existants, puis répondez 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
   - Le certificat et la clé (`vpxd.crt` et `vpxd.key`) pour l'utilisateur de solution de machine

- L'ensemble complet de certificats et de clés (`vpxd.crt` et `vpxd.key`) pour tous les utilisateurs de solution

Restaurer la dernière opération effectuée en republiant les anciens certificats à l'aide de Certificate Manager

Lorsque vous effectuez une opération de gestion de certificats en utilisant l'utilitaire 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.

Note 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.

Procédure

1. Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Sélectionnez l'option 7, Restaurer la dernière opération effectuée en republiant les anciens certificats.
3. Entrez le nom de l'utilisateur administrateur et le mot de passe.
4. Pour continuer, entrez **`Y`**.

Réinitialiser tous les certificats à l'aide de Certificate Manager

Vous pouvez utiliser l'utilitaire vSphere Certificate Manager pour 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 VMware Endpoint Certificate Store (VECS) sont remplacés.

vSphere Certificate Manager peut remplacer tous les certificats. Les certificats remplacés dépendent des options que vous sélectionnez.

Procédure

1. Connectez-vous au shell vCenter Server et démarrez vSphere Certificate Manager.

   ```
   /usr/lib/vmware-vmca/bin/certificate-manager
   ```

2. Sélectionnez l'option 8. Réinitialiser tous les certificats.
3. Entrez le nom de l'utilisateur administrateur et le mot de passe.
4. Lorsque vous y êtes invité, entrez vos informations de certificat.

Étape suivante

Une fois les certificats remplacés et les services redémarrés, vérifiez vos informations de certificat.

Remplacement manuel des certificats vSphere

Pour certains cas spéciaux de remplacement de certificats, vous ne pouvez pas utiliser l'utilitaire vSphere Certificate Manager. En revanche, vous pouvez utiliser les interfaces de ligne de commande incluses dans votre installation pour le remplacement de certificat.

Instructions relatives à l'arrêt et au démarrage des services vCenter Server

Pour certaines parties du remplacement manuel de certificat, vous devez arrêter tous les services vCenter Server, 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.

Vous devez arrêter et démarrer les services dans le cadre du processus de remplacement des certificats. Vous pouvez utiliser la commande `service-control` pour démarrer et arrêter les services. Vous pouvez démarrer et arrêter tous les services ou les services individuels. Pour plus d'informations, consultez l'aide relative à la ligne de commande.

Suivez ces instructions.

- 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 des problèmes avec vos hôtes.
- Si votre environnement inclut plusieurs administrateurs, arrêtez les services avant d'ajouter un nouveau certificat racine et redémarrez-les après l'ajout d'un nouveau certificat.
- Arrêtez les services juste avant de supprimer un certificat SSL de machine dans VECS (VMware Endpoint Certificate Store).

Remplacer les certificats existants signés par VMCA par de nouveaux certificats signés par VMCA à l'aide de la CLI

Si le certificat racine VMware Certificate Authority (VMCA) expire dans un avenir proche ou si vous voulez le remplacer pour d'autres raisons, vous pouvez utiliser la CLI pour 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.

Conditions préalables

Seul l'utilisateur administrator@vsphere.local ou d'autres utilisateurs du groupe peuvent effectuer des tâches de gestion de certificats. Reportez-vous à la section Ajouter des membres à un groupe vCenter Single Sign-On.

Générer un nouveau certificat racine signé par VMCA à l'aide de la CLI

Vous pouvez générer de nouveaux certificats signés par VMCA avec la CLI `certool` et les publier dans vmdir.

Procédure

1 Dans vCenter Server, 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.

```
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) Dans vCenter Server, affichez le certificat racine VMCA pour vous assurer qu'il se trouve dans le magasin de certificats.

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

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.

```
/usr/lib/vmware-vmafd/bin/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).

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/
certool.cfg
```

Remplacer les certificats SSL de machine par des certificats signés par VMCA à l'aide de la CLI

Une fois que vous avez généré un nouveau certificat racine signé par VMCA, vous pouvez utiliser la commande `vecs-cli` pour 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. Lorsque plusieurs instances de vCenter Server sont connectées dans une configuration Enhanced Linked Mode, vous devez exécuter les commandes de génération de certificat SSL de machine sur chaque nœud.

Conditions préalables

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 trouver le fichier `certool.cfg` dans le répertoire `/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.

   ```
   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.crt
   --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-<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. Dans un déploiement de plusieurs instances de vCenter Server connectées dans une configuration Enhanced Linked Mode, exécutez cette commande sur chaque nœud vCenter Server.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

Le fichier `new-vmca-ssl.crt` est créé dans le répertoire actuel.

4 (Facultatif) Répertoriez le contenu de VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Exemple de sortie sur vCenter Server :

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
```

```
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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 chaque instance de vCenter Server, exécutez les commandes suivantes 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.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Étape suivante

Vous pouvez également remplacer les certificats de vos hôtes ESXi. Consultez la publication *Sécurité vSphere*.

Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA à l'aide l'interface de ligne de commande

Après avoir remplacé les certificats SSL de la machine, vous pouvez utiliser la commande `dir-cli` pour 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.

Vous remplacez le certificat d'utilisateur de solution de machine et le certificat d'utilisateur de solution sur chaque système vCenter Server.

Note 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.

Conditions préalables

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.

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
   4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
   5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
   6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
   ```

   Dans un déploiement de plusieurs instances de vCenter Server connectées dans une configuration Enhanced Linked Mode, la sortie de `dir-cli service list` inclut 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.

   ```
   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
```

Note 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/privée pour chaque utilisateur de solution sur chaque nœud vCenter Server dans une configuration Enhanced Linked Mode. Cela inclut une paire pour la solution de machine et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Générez une paire de clés pour l'utilisateur de solution de machine.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Générez une paire de clés pour l'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Générez une paire de clés pour l'utilisateur de solution vpxd-extension sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d Générez une paire de clés pour l'utilisateur de solution vsphere-webclient sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

e Générez une paire de clés pour l'utilisateur de solution wcp sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Générez des certificats d'utilisateurs de solutions qui sont signés par le nouveau certificat racine VMCA pour l'utilisateur de solution de machine et pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient, wcp) sur chaque nœud vCenter Server.

Note 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 pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Générez un certificat pour l'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Générez un certificat pour l'utilisateur de solution vpxd-extensions sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Générez un certificat pour l'utilisateur de solution vsphere-webclient sur chaque nœud en exécutant la commande suivante.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Générez un certificat pour l'utilisateur de solution wcp sur chaque nœud en exécutant les commandes suivantes.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

3 Remplacez les certificats d'utilisateurs de solutions dans VECS par les nouveaux certificats d'utilisateurs de solutions.

Note Les paramètres `--store` et `--alias` doivent correspondre exactement aux noms par défaut des services.

a Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud :

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Remplacez le certificat d'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Remplacez le certificat d'utilisateur de solution vpxd-extension sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Remplacez le certificat d'utilisateur de solution wcp sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 exécutez cette commande sur un système vCenter Server.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
```

```
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Note 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 chaque nœud vCenter Server. Par exemple, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'utilisateur de solution de machine sur vCenter Server, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Remplacez le certificat d'utilisateur de solution vpxd dans vmdir sur chaque nœud. Par exemple, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Remplacez le certificat d'utilisateur de solution vpxd-extension dans vmdir sur chaque nœud. Par exemple, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd-extension, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud. Par exemple, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vsphere-webclient, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Remplacez le certificat d'utilisateur de solution wcp sur chaque nœud. Par exemple, si wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e correspond à l'ID d'utilisateur de solution wcp, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Étape suivante

Redémarrez tous les services sur chaque nœud vCenter Server.

Faire de VMCA une autorité de certification intermédiaire à l'aide de l'interface de ligne de commande

Vous utilisez l'interface de ligne de commande pour 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.

Si vous utilisez VMCA comme autorité de certification intermédiaire ou que vous utilisez des certificats personnalisés, vous vous exposez à plus de complexité et un risque potentiel pour votre sécurité, ce qui représente une augmentation inutile dans vos risques opérationnels. Pour plus d'informations sur la gestion des certificats dans un environnement vSphere, consultez le blog intitulé *Nouvelle procédure produit - Remplacement hybride des certificats SSL vSphere* à l'adresse http://vmware.com/go/hybridvmca.

Remplacer le certificat racine (autorité de certification intermédiaire) à l'aide de la CLI

La première étape du remplacement des certificats VMCA par des certificats personnalisés génère une demande de signature de certificat, qui est envoyée pour être signée. Vous pouvez ensuite utiliser la CLI pour ajouter le 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 : de 2 048 bits (minimum) à 16 384 bits (maximum) (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
- L'extension d'autorité de certification doit être définie sur true pour les certificats racines et la signature de certification doit figurer dans la liste de conditions requises. Par exemple :

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- La signature CRL doit être activée.
- Le champ Utilisation étendue de la clé peut être vide ou contenir la valeur du champ Authentification du serveur.
- Aucune limite explicite à la longueur de la chaîne de certificats. VMCA utilise la valeur par défaut OpenSSL, qui est 10 certificats.

- Les certificats incluant des caractères génériques ou plusieurs noms DNS ne sont pas pris en charge.
- Vous ne pouvez pas créer d'autorités de certification filiales de VMCA.

  Reportez-vous à l'article « Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x » de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2112009 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 (minimum) à 16 384 bits (maximum)
- 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 signé par VMCA et la chaîne d'autorité de certification complète de votre autorité de certification tierce ou d'entreprise. Enregistrez le fichier, par exemple en tant que `rootca1.crt`.

   Vous pouvez effectuer cette étape en copiant tous les certificats de l'autorité de certification au format PEM dans un fichier unique. Vous démarrez avec le certificat racine VMCA et terminez avec le certificat racine de l'autorité de certification au format 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.

   ```
   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, si le certificat dispose d'un seul certificat dans la chaîne :

```
dir-cli trustedcert publish --cert rootca1.crt
```

Si le certificat dispose de plusieurs certificats dans la chaîne :

```
dir-cli trustedcert publish --cert rootcal.crt --chain
```

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`.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/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.

Étape suivante

Vous pouvez supprimer le certificat racine VMCA initial du magasin de certificats si la stratégie de votre entreprise l'exige. Dans ce cas, vous devez remplacer le certificat de signature de vCenter Single Sign-On. Reportez-vous à la section Remplacer un certificat STS vCenter Server à l'aide de la ligne de commande.

Remplacer les certificats SSL de machine (autorité de certification intermédiaire) à l'aide de la CLI

Après avoir reçu le certificat signé de l'autorité de certification, vous pouvez utiliser la CLI pour en faire le certificat racine VMCA et 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. Lorsque plusieurs instances de vCenter Server sont connectées dans une configuration Enhanced Linked Mode, vous devez exécuter les commandes de génération de certificat SSL de machine sur chaque nœud.

Conditions préalables

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.

   Le fichier `certool.cfg` se trouve dans le répertoire `/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.

```
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-<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. Dans un déploiement de plusieurs instances de vCenter Server connectées dans une configuration Enhanced Linked Mode, exécutez cette commande sur chaque nœud vCenter Server.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

Le fichier `new-vmca-ssl.crt` est créé dans le répertoire actuel.

4 (Facultatif) Répertoriez le contenu de VECS.

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- Exemple de sortie sur vCenter Server :

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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 chaque instance de vCenter Server, exécutez les commandes suivantes 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.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Remplacer les certificats d'utilisateur de solutions (autorité de certification intermédiaire) à l'aide de la CLI

Après avoir remplacé les certificats SSL de machine, vous pouvez utiliser la CLI pour remplacer les certificats d'utilisateurs de solutions.

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.

Vous remplacez le certificat d'utilisateur de solution de machine et le certificat d'utilisateur de solution sur chaque système vCenter Server.

Note 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.

Conditions préalables

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.

   ```
   dir-cli service list
   Enter password for administrator@vsphere.local:
   1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
   2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
   3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
   4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
   5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
   6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
   ```

Dans un déploiement de plusieurs instances de vCenter Server connectées dans une configuration Enhanced Linked Mode, la sortie de `dir-cli service list` inclut 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.

```
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
```

Note 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/privée pour chaque utilisateur de solution sur chaque nœud vCenter Server dans une configuration Enhanced Linked Mode. Cela inclut une paire pour la solution de machine et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient, wcp).

a Générez une paire de clés pour l'utilisateur de solution de machine.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b Générez une paire de clés pour l'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c Générez une paire de clés pour l'utilisateur de solution vpxd-extension sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --
pubkey=vpxd-extension-key.pub
```

d Générez une paire de clés pour l'utilisateur de solution vsphere-webclient sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

e Générez une paire de clés pour l'utilisateur de solution wcp sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 Générez des certificats d'utilisateurs de solutions qui sont signés par le nouveau certificat racine VMCA pour l'utilisateur de solution de machine et pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient, wcp) sur chaque nœud vCenter Server.

Note 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 pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

```
/usr/lib/vmware-vmca/bin/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.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

c Générez un certificat pour l'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd
```

d Générez un certificat pour l'utilisateur de solution vpxd-extensions sur chaque nœud.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

e Générez un certificat pour l'utilisateur de solution vsphere-webclient sur chaque nœud en exécutant la commande suivante.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

f Générez un certificat pour l'utilisateur de solution wcp sur chaque nœud en exécutant les commandes suivantes.

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```

3 Remplacez les certificats d'utilisateurs de solutions dans VECS par les nouveaux certificats d'utilisateurs de solutions.

Note Les paramètres `--store` et `--alias` doivent correspondre exactement aux noms par défaut des services.

a Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud :

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b Remplacez le certificat d'utilisateur de solution vpxd sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c Remplacez le certificat d'utilisateur de solution vpxd-extension sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e Remplacez le certificat d'utilisateur de solution wcp sur chaque nœud.

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 exécutez cette commande sur un système vCenter Server.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

Note 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 chaque nœud vCenter Server. Par exemple, si machine-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'utilisateur de solution de machine sur vCenter Server, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c Remplacez le certificat d'utilisateur de solution vpxd dans vmdir sur chaque nœud. Par exemple, si vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d Remplacez le certificat d'utilisateur de solution vpxd-extension dans vmdir sur chaque nœud. Par exemple, si vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vpxd-extension, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e Remplacez le certificat d'utilisateur de solution vsphere-webclient sur chaque nœud. Par exemple, si vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 correspond à l'ID d'utilisateur de solution vsphere-webclient, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f Remplacez le certificat d'utilisateur de solution wcp sur chaque nœud. Par exemple, si wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e correspond à l'ID d'utilisateur de solution wcp, exécutez la commande suivante :

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

Remplacer les certificats par des certificats personnalisés à l'aide de l'interface de ligne de commande

Si la stratégie de votre entreprise l'exige, vous pouvez utiliser l'interface de ligne de commande pour 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. vCenter Server utilise des certificats d'utilisateur de solution uniquement pour la communication interne. Les certificats d'utilisateur de solution ne sont pas utilisés pour la communication externe.

Note Si vous ne souhaitez pas utiliser VMCA, vous devrez remplacer vous-même tous les certificats, fournir de nouveaux composants avec des certificats et suivre l'expiration des certificats.

Même si vous décidez d'utiliser des certificats personnalisés, vous pouvez toujours utiliser l'utilitaire VMware Certificate Manager pour le remplacement des certificats. Reportez-vous à la section Remplacer tous les certificats par un certificat personnalisé à l'aide de Certificate Manager.

Si vous rencontrez des problèmes avec vSphere Auto Deploy après le remplacement des certificats, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2000988.

Demander des certificats et importer un certificat racine personnalisé à l'aide de la CLI

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, puis à utiliser la CLI pour importer les certificats racines dans le magasin de certificats VMware Endpoint (VECS).

Conditions préalables

Le certificat doit répondre à la configuration requise suivante :

- Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (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, chiffrement de 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 (CSR) 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 (DNS NAME=*FQDN_machine*).
   - Le cas échéant, cinq certificats d'utilisateur de solution pour chaque nœud. Les certificats d'utilisateurs de solutions n'ont pas besoin d'inclure d'adresse IP, de nom d'hôte ou d'adresse e-mail. Chaque certificat doit avoir un sujet de certificat différent.

   En général, le résultat est un fichier PEM pour la chaîne d'approbation, plus les certificats SSL signés pour chaque nœud vCenter Server.
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, consultez 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.

```
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
```

Étape suivante

Vous pouvez supprimer le certificat racine VMCA initial du magasin de certificats si la stratégie de votre entreprise l'exige. Dans ce cas, vous devez actualiser le certificat vCenter Single Sign-On. Reportez-vous à la section Remplacer un certificat STS vCenter Server à l'aide de la ligne de commande.

Remplacer les certificats SSL de machine par des certificats personnalisés à l'aide de la CLI

Après avoir reçu les certificats personnalisés, vous pouvez utiliser la CLI pour remplacer chaque certificat de machine.

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 valide pour Root (fichier `.crt`)

Conditions préalables

Vous devez avoir reçu de votre autorité de certification tierce ou d'entreprise un certificat pour chaque machine.

- Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
- Format CRT
- x509 version 3

- SubjectAltName doit contenir DNS Name=<machine_FQDN>.
- Contient les utilisations de clé suivantes : signature numérique, chiffrement de 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 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 Mettez à jour le point de terminaison d'enregistrement de Lookup Service.

```
/usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/
lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --
password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
```

4 Redémarrez tous les services.

```
service-control --start --all
```

Référence des commandes CLI vSphere Certificates and Services

3

Vous pouvez gérer les certificats VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store), VMware Directory Service (vmdir) et Security Token Service (STS) à l'aide d'un groupe d'interfaces de ligne de commande. 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.

Vous accédez normalement aux outils d'interface de ligne de commande affectés à la gestion des certificats et des services associés via une connexion SSH au Shell du dispositif. Pour plus d'informations, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2100508.

La section Remplacement manuel des certificats vSphere fournit des exemples de remplacement de certificats à l'aide des commandes CLI.

Tableau 3-1. Outils CLI vSphere de gestion des certificats et des services associés

CLI	Description	Reportez-vous au
`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
`vecs-cli`	Gère les contenus des instances de VMware Certificate Store. Partie du démon VMAFD (VMware Authentication Framework Daemon)	Référence des commandes vecs-cli
`dir-cli`	Crée et met à jour les certificats dans le Vmware Directory Service. Fait partie de VMAFD.	Référence des commandes dir-cli
`sso-config.sh`	Gère les certificats STS.	Aide relative à la ligne de commande. La saisie de `sso-config.sh` sans options affiche l'aide relative à la ligne de commande.
`service-control`	Démarrez ou arrêtez les services, par exemple faisant partie d'un workflow de remplacement de certificat.	Exécutez cette commande pour arrêter les services avant d'exécuter d'autres commandes d'interface de ligne de commande.

Emplacements des CLI vSphere

Par défaut, les emplacements des interfaces de ligne de commande sont les suivants.

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

Note La commande `service-control` ne requiert pas de spécifier le chemin.

Privilèges requis pour l'exécution des CLI vSphere

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 du groupe Administrateurs disposent de privilèges d'accès permanents.

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 dans le répertoire `/usr/lib/VMware-Vmca/share/config/` par défaut.

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.
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
- Remplacez les valeurs individuelles sur la ligne de commande. Par exemple, pour remplacer Locality, exécutez la commande suivante :

  ```
  /usr/lib/vmware-vmca/bin/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.

Ce chapitre contient les rubriques suivantes :

- Référence des commandes d'initialisation de certool
- Référence des commandes de gestion certool
- Référence des commandes vecs-cli
- Référence des commandes dir-cli

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 VMware Certificate Authority (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 la section Modification des options de configuration de certool. Vous trouverez des exemples d'utilisation à la section Remplacer les certificats existants signés par VMCA par de nouveaux certificats signés par VMCA à l'aide de la CLI. 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
`--gencsr`	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 --gencsr --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 la section Faire de VMCA une autorité de certification intermédiaire à l'aide de l'interface de ligne de commande.

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.
`--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 du fichier de certificat.
`--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.
`--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. 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.
`--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 vos services d'authentification.

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 3-2. 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 le service VMware Directory Service (vmdir) sur chaque nœud vCenter Server. Tous les services de vSphere 6.0 ou versions ultérieures 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.
Magasins d'utilisateurs de solution ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	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. Les magasins de certificats d'utilisateur de solution suivants sont inclus dans VECS : ■ `machine` : utilisé par le serveur de licences et le service de journalisation. **Note** 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 du démon de service vCenter (vpxd). vpxd utilise le certificat d'utilisateur de solution stocké dans ce magasin pour s'authentifier sur vCenter Single Sign-On. ■ `vpxd-extension` : 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 Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance. ■ `wcp`: VMware vSphere® avec le magasin VMware Tanzu™. Chaque nœud vCenter Server comprend un certificat `machine`.
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.

Tableau 3-2. 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. **Note** 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.

Note N'utilisez pas cette commande pour ajouter des certificats racines au magasin TRUSTED_ROOTS. Utilisez plutôt la commande `dir-cli` pour publier des certificats racines.

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.
`--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 utiliser `dir-cli` pour gérer et interroger le niveau fonctionnel de domaine d'instances de vCenter Server.

dir-cli nodes list

Répertorie tous les systèmes vCenter Server connectés avec le mode Enhanced Linked Mode.

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 pour vous connecter à une autre instance de vCenter Server pour afficher ses partenaires de réplication.

dir-cli computer password-reset

Cette commande vous permet de réinitialiser le mot de passe du compte de la machine dans le domaine.

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 vCenter Server.

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>`	Définit l'utilisateur de solution en tant que membre des groupes spécifiés.
`--wstrustrole <ActAsUser>`	Définit l'utilisateur de solution en tant que membre du groupe des administrateurs ou des utilisateurs intégré. En d'autres termes, détermine si l'utilisateur de solution dispose des privilèges d'administration.
`--ssoadminrole <Administrator/User>`	Définit l'utilisateur de solution en tant que membre du groupe ActAsUser. Le rôle ActAsUser permet à des utilisateurs d'agir pour le compte d'autres utilisateurs.
`--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 avoir exécuté cette commande, mettez à jour l'entrée de certificat d'utilisateur de solution dans VECS en exécutant la commande `vecs-cli entry create`. Reportez-vous à la section Référence des commandes vecs-cli.

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

Modifie l'utilisateur spécifié dans vmdir.

Option	Description
`--account <name>`	Nom de l'utilisateur vCenter Single Sign-On à modifier.
`--password-never-expires`	Définissez cette option sur true si vous modifiez un compte d'utilisateur pour des tâches automatisées devant s'authentifier dans vCenter Server, 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 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. Après l'exécution de cette commande, VECS récupère la modification du certificat après une minute, ou vous pouvez exécuter la commande `vecs-cli force-refresh` pour synchroniser immédiatement le certificat.

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.

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

4

vCenter Single Sign-On est un broker d'authentification et une infrastructure d'échange de jetons de sécurité. vCenter Single Sign-On émet un jeton lorsqu'un utilisateur s'authentifie. L'utilisateur peut utiliser le jeton pour s'authentifier sur les services vCenter Server. 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.

Les utilisateurs et les comptes de service s'authentifient avec un jeton ou un nom d'utilisateur et un mot de passe. Les utilisateurs de solution s'authentifient avec un certificat. Pour plus d'informations sur le remplacement des certificats des utilisateurs de solution, consultez Chapitre 2 Certificats de sécurité vSphere.

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 contient les rubriques suivantes :

Protection de votre environnement par vCenter Single Sign-On

vCenter Single Sign-On permet aux composants vSphere de communiquer au moyen d'un mécanisme d'échange de jetons sécurisé.

vCenter Single Sign-On utilise les services suivants.

- Authentification des utilisateurs par le biais d'une fédération de fournisseur d'identité externe ou du fournisseur d'identité intégré de vCenter Server. Le fournisseur d'identité intégré prend en charge les comptes locaux, Active Directory ou OpenLDAP, l'authentification Windows intégrée (IWA) et divers mécanismes d'authentification (carte à puce, RSA SecurID et l'authentification de session Windows).
- Authentification des utilisateurs de solution par le biais des certificats.
- STS (Security Token Service).
- SSL pour sécuriser le trafic.

Présentation du fournisseur d'identité

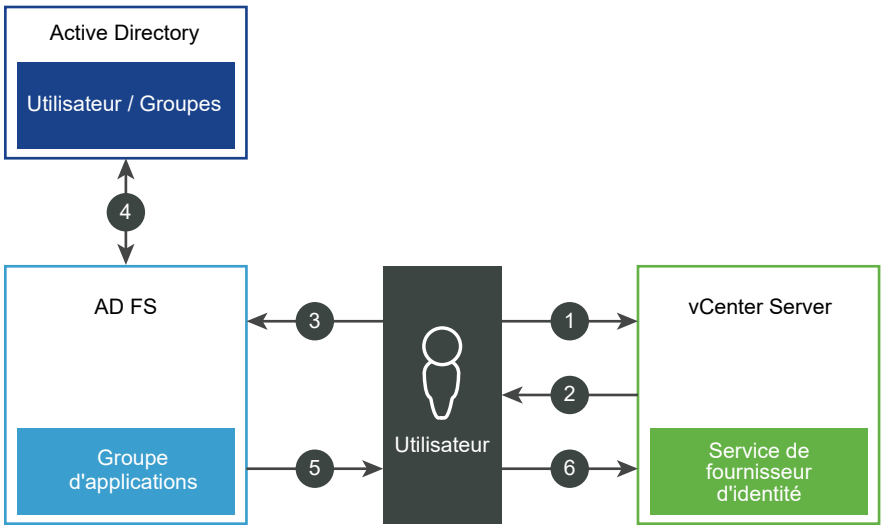
Avant vSphere 7.0, vCenter Server comprenait un fournisseur d'identité intégré. Par défaut, vCenter Server utilise le domaine vsphere.local comme source d'identité, mais vous pouvez la modifier lors de l'installation. Vous pouvez configurer le fournisseur d'identité intégré de vCenter Server pour utiliser Active Directory (AD) comme source d'identité à l'aide de LDAP/S, OpenLDAP/S et de l'authentification Windows intégrée (IWA). De telles configurations permettent aux clients de se connecter à l'instance de vCenter Server à l'aide de leurs comptes AD.

À partir de vSphere 7.0, vous pouvez configurer l'instance de vCenter Server pour un fournisseur d'identité externe à l'aide de l'authentification fédérée. Dans une telle configuration, vous remplacez vCenter Server comme fournisseur d'identité. Actuellement, vSphere prend en charge Active Directory Federation Services (AD FS) en tant que fournisseur d'identité externe. Dans cette configuration, AD FS interagit avec les sources d'identité au nom de l'instance de vCenter Server.

Connexion de l'utilisateur avec l'authentification fédérée du fournisseur d'identité vCenter Server

La figure suivante montre le flux de connexion de l'utilisateur pour la fédération de fournisseur d'identité vCenter Server.

Figure 4-1. Connexion de l'utilisateur de la fédération de fournisseur d'identité vCenter Server



vCenter Server, AD FS et Active Directory interagissent de la façon suivante :

1 L'utilisateur démarre sur la page d'accueil de vCenter Server en entrant un nom d'utilisateur.

2 Si le nom d'utilisateur est destiné à un domaine fédéré, vCenter Server redirige la demande d'authentification vers AD FS.

3 Si nécessaire, AD FS invite l'utilisateur à se connecter avec des informations d'identification Active Directory.

4 AD FS authentifie l'utilisateur avec Active Directory.

5 AD FS émet un jeton de sécurité avec les informations de groupe d'Active Directory.

6 vCenter Server utilise le jeton pour connecter l'utilisateur.

L'utilisateur est désormais authentifié et peut afficher et modifier les objets pour lesquels il possède les privilèges pertinents.

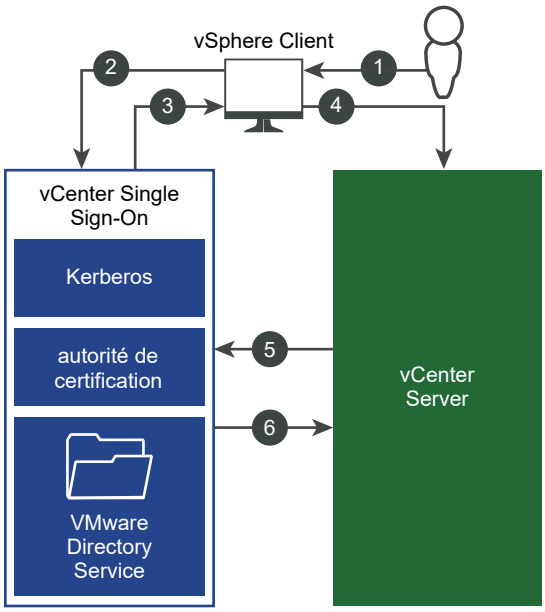
Note Le rôle Aucun accès est attribué initialement à chaque utilisateur. Pour qu'un utilisateur puisse se connecter, un administrateur vCenter Server doit au moins lui attribuer le rôle Lecture seule. Consultez la documentation de *Sécurité vSphere*.

Si le fournisseur d'identité externe est inaccessible, le processus de connexion revient à la page de destination de vCenter Server et affiche un message d'information approprié. Les utilisateurs peuvent toujours se connecter à l'aide de leurs comptes locaux dans la source d'identité vsphere.local.

Connexion de l'utilisateur avec le fournisseur d'identité intégré de vCenter Server

La figure suivante illustre le flux de connexion de l'utilisateur lorsque vCenter Server agit comme le fournisseur d'identité.

Figure 4-2. Connexion de l'utilisateur avec le fournisseur d'identité intégré de vCenter Server



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

   Lorsque l'authentification Windows intégrée (IWA) a été configurée, les utilisateurs peuvent également se connecter sans avoir à entrer de nouveau leur mot de passe Windows en cochant la case **Utiliser l'authentification de session Windows**.

2 vSphere Client transmet les informations de connexion au service vCenter Single Sign-On. Celui-ci vérifie alors le jeton SAML de vSphere Client. Si vSphere 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 Client.

4 vSphere 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 utilisant la structure d'autorisation de vCenter Server pour autoriser l'accès de l'utilisateur.

L'utilisateur est désormais authentifié et peut afficher et modifier les objets pour lesquels il possède les privilèges pertinents.

Note 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*.

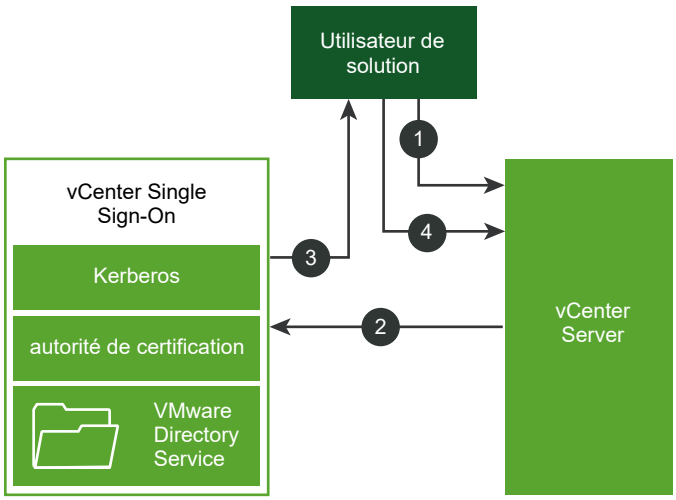
Connexion pour les utilisateurs de solution

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

Note L'instance de vCenter Server utilise des certificats d'utilisateur de solution uniquement pour la communication interne. Les certificats d'utilisateur de solution ne sont pas utilisés pour la communication externe.

La figure suivante illustre le flux de connexion des utilisateurs de solution.

Figure 4-3. Connexion pour les utilisateurs de solution



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

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.

   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 votre stratégie d'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 la section Remplacer les certificats par des certificats personnalisés à l'aide de l'interface de ligne de commande.

Chiffrement pris en charge

Le chiffrement AES, qui est le niveau de chiffrement le plus élevé, est pris en charge. Le chiffrement pris en charge affecte également la sécurité lorsque vCenter Single Sign-On utilise Active Directory comme source d'identité.

Cela affecte également la sécurité chaque fois qu'un hôte ESXi ou vCenter Server est associé à Active Directory.

Comprendre la fédération de fournisseur d'identité vCenter Server

À partir de vSphere 7.0, vCenter Server prend en charge l'authentification fédérée pour se connecter à vCenter Server.

Pour activer l'authentification fédérée sur vCenter Server, vous devez configurer une connexion à un fournisseur d'identité externe. L'instance de fournisseur d'identité que vous configurez remplace vCenter Server en tant que fournisseur d'identité. Actuellement, vCenter Server prend en charge uniquement Active Directory Federation Services (AD FS) en tant que fournisseur d'identité externe.

Note VMware vous encourage à utiliser l'authentification fédérée, car vSphere se dirige vers l'authentification basée sur des jetons. vCenter Server continue d'avoir des comptes locaux, destinés à l'accès administratif et à la récupération d'erreur.

Fonctionnement de la fédération de fournisseur d'identité vCenter Server

La fédération de fournisseur d'identité vCenter Server vous permet de configurer un fournisseur d'identité externe pour l'authentification fédérée. Dans cette configuration, le fournisseur d'identité externe interagit avec la source d'identité au nom de l'instance de vCenter Server.

Principes de base de la fédération de fournisseur d'identité vCenter Server

À partir de vSphere 7.0, vCenter Server prend en charge l'authentification fédérée. Dans ce scénario, lorsqu'un utilisateur se connecte au système vCenter Server, vCenter Server redirige la connexion de l'utilisateur vers le fournisseur d'identité externe. Les informations d'identification de l'utilisateur ne sont plus fournies directement à l'instance de vCenter Server. Au lieu de cela, l'utilisateur fournit des informations d'identification au fournisseur d'identité externe. L'instance

de vCenter Server approuve le fournisseur d'identité externe pour effectuer l'authentification. Dans le modèle de fédération, les utilisateurs ne fournissent jamais d'informations d'identification directement à un service ou à une application, mais uniquement au fournisseur d'identité. Par conséquent, vous « fédérez » vos applications et services, tels que vCenter Server, avec votre fournisseur d'identité.

Avantages de la fédération de fournisseur d'identité vCenter Server

La fédération de fournisseur d'identité vCenter Server offre les avantages suivants.

- Vous pouvez utiliser Single Sign-On avec une infrastructure et des applications fédérées existantes.
- Vous pouvez améliorer la sécurité du centre de données, car le système vCenter Server ne gère jamais les informations d'identification de l'utilisateur.
- Vous pouvez utiliser les mécanismes d'authentification, tels que l'authentification multifacteur, pris en charge par le fournisseur d'identité externe.

Composants de la fédération de fournisseur d'identité vCenter Server

Les composants suivants comprennent une configuration de fédération de fournisseur d'identité vCenter Server qui utilise Microsoft Active Directory Federation Services (AD FS) :

- Une instance de vCenter Server
- Un service de fournisseur d'identité configuré sur l'instance de vCenter Server
- Un serveur AD FS et le domaine Microsoft Active Directory associé
- Un groupe d'applications AD FS
- Les groupes et utilisateurs Active Directory mappés aux groupes et utilisateurs de l'instance de vCenter Server

Note Actuellement, vCenter Server prend en charge uniquement les services AD FS en tant que fournisseur d'identité externe.

Architecture de la fédération de fournisseur d'identité vCenter Server

Dans la fédération de fournisseur d'identité vCenter Server, vCenter Server utilise le protocole OpenID Connect (OIDC) pour recevoir un jeton d'identité qui authentifie l'utilisateur avec vCenter Server.

Pour établir une relation d'approbation de partie de confiance entre vCenter Server et un fournisseur d'identité, vous devez établir les informations d'identification et un secret partagé entre eux. Dans AD FS, vous devez créer une configuration OIDC appelée groupe d'applications, qui se compose d'une application serveur et d'une API Web. Les deux composants spécifient les informations que l'instance de vCenter Server utilise pour approuver le serveur AD FS et communiquer avec lui. Vous créez également un fournisseur d'identité correspondant dans l'instance de vCenter Server. Enfin, vous configurez des appartenances de groupe dans l'instance de vCenter Server pour autoriser les connexions des utilisateurs dans le domaine AD FS.

L'administrateur AD FS doit fournir les informations suivantes pour créer la configuration du fournisseur d'identité vCenter Server :

- Identificateur de client : chaîne de l'UUID générée par l'assistant Groupe d'applications AD FS qui identifie le groupe d'applications.
- Secret partagé : secret généré par l'assistant Groupe d'applications AD FS qui est utilisé pour authentifier l'instance de vCenter Server dans AD FS.
- Adresse OpenID : URL du point de terminaison de découverte de fournisseur OpenID du serveur AD FS, spécifiant une adresse connue qui est généralement le point de terminaison de l'émetteur concaténé au chemin « `/.well-known/openid-configuration` ». Par exemple : `https://webserver.example.com/adfs/.well-known/openid-configuration`.

Fédération de fournisseur d'identité vCenter Server et Enhanced Linked Mode

Lorsque vous activez la fédération de fournisseur d'identité dans des environnements vCenter Server à l'aide du mode Enhanced Linked Mode, l'authentification et les workflows continuent de fonctionner comme avant.

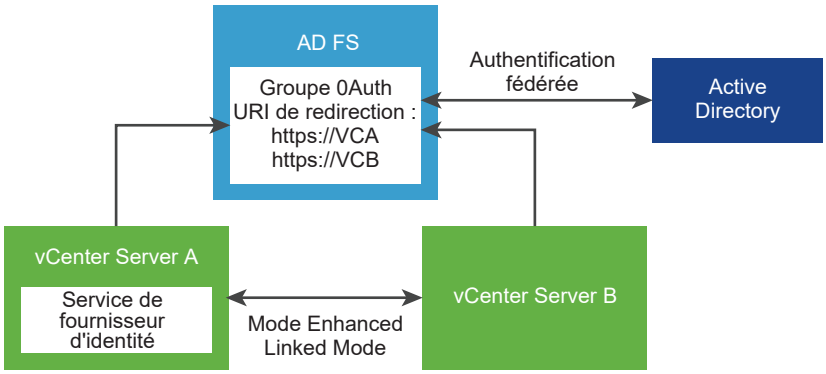
Si vous utilisez la configuration Enhanced Linked Mode, notez ce qui suit lors de la connexion à vCenter Server à l'aide de l'authentification fédérée.

- Les utilisateurs continuent à voir le même inventaire et peuvent effectuer les mêmes actions, en fonction du modèle d'autorisations et de rôles de vCenter Server.
- Les hôtes vCenter Server en mode Enhanced Linked Mode ne doivent pas nécessairement avoir accès à leurs fournisseurs d'identité entre eux. Prenons par exemple deux systèmes vCenter Server A et B qui utilisent le mode Enhanced Linked Mode. Une fois que le système vCenter Server A autorise un utilisateur, celui-ci est également autorisé sur le système vCenter Server B.

Workflow d'authentification avec Enhanced Linked Mode et une fédération de fournisseur d'identité vCenter Server

L'illustration suivante présente le workflow d'authentification avec Enhanced Linked Mode et la fédération de fournisseur d'identité vCenter Server.

Figure 4-4. Enhanced Linked Mode et fédération de fournisseur d'identité vCenter Server



1 Deux nœuds vCenter Server sont déployés dans une configuration Enhanced Linked Mode.

2 La configuration AD FS a été configurée sur le système vCenter Server A à l'aide de l'assistant de modification du fournisseur d'identité dans vSphere Client. Des appartenances et des autorisations de groupe ont également été établies pour les utilisateurs ou les groupes AD FS.

3 Le système vCenter Server A réplique la configuration AD FS sur le système vCenter Server B.

4 Tous les URI de redirection des deux nœuds vCenter Server sont ajoutés au groupe d'applications OAuth dans AD FS. Un seul groupe d'applications OAuth est créé.

5 Lorsqu'un utilisateur se connecte au système vCenter Server A et est autorisé par celui-ci, l'utilisateur est également autorisé sur le système vCenter Server B. Il en va de même si l'utilisateur se connecte d'abord au système vCenter Server B.

Le mode Enhanced Linked Mode de vCenter Server prend en charge les scénarios de configuration suivants pour la fédération de fournisseur d'identité. Dans cette section, les termes « Paramètres AD FS » et « Configuration AD FS » font référence aux paramètres que vous configurez dans vSphere Client à l'aide de l'assistant Changer le fournisseur d'identité, ainsi que des appartenances aux groupes ou des autorisations que vous avez établies pour les utilisateurs ou les groupes AD FS.

Activer AD FS sur une configuration Enhanced Linked Mode existante

Étapes de haut niveau :

1 Déployez N nœuds vCenter Server dans la configuration Enhanced Linked Mode.

2 Configurez AD FS sur l'un des nœuds vCenter Server liés.

3 La configuration AD FS est répliquée sur tous les autres nœuds vCenter Server (N-1).

4 Ajoutez tous les URI de redirection pour la totalité des N nœuds vCenter Server au groupe d'applications OAuth configuré dans AD FS.

Lier une nouvelle instance de vCenter Server à une configuration AD FS Enhanced Linked Mode existante

Étapes de haut niveau :

1 (Condition préalable) Configurez AD FS sur une configuration Enhanced Linked Mode à N nœuds vCenter Server.

2 Déployez un nouveau nœud vCenter Server indépendant.

3 Redirigez le nouveau nœud vCenter Server vers le domaine Enhanced Linked Mode AD FS à N nœuds, en utilisant l'un des *N* nœuds comme partenaire de réplication.

4 Tous les paramètres AD FS de la configuration Enhanced Linked Mode existante sont répliqués vers le nouveau nœud vCenter Server.

   Les paramètres AD FS qui se trouvent dans le domaine Enhanced Linked Mode AD FS à N nœuds remplacent tous les paramètres AD FS existants sur le nœud vCenter Server récemment lié.

5 Ajoutez tous les URI de redirection du nouveau nœud vCenter Server au groupe d'applications OAuth configuré existant dans AD FS.

Annuler le lien d'une instance de vCenter Server à une configuration AD FS Enhanced Linked Mode

Étapes de haut niveau :

1 (Condition préalable) Configurez AD FS sur une configuration Enhanced Linked Mode vCenter Server à N nœuds.

2 Annulez l'enregistrement de l'un des hôtes vCenter Server dans la configuration à N nœuds et redirigez-le vers un nouveau domaine pour le dissocier de la configuration à N nœuds.

3 Le processus de redirection du domaine ne conserve pas les paramètres SSO, de sorte que tous les paramètres AD FS sur le nœud vCenter Server dont le lien est annulé sont restaurés et perdus. Pour continuer à utiliser AD FS sur ce nœud vCenter Server non lié, vous devez reconfigurer AD FS depuis le début ou vous devez relier le nœud vCenter Server à une configuration Enhanced Linked Mode dans laquelle AD FS est déjà configuré.

Restrictions et interopérabilité de la fédération de fournisseurs d'identité vCenter Server

La fédération de fournisseurs d'identité vCenter Server peut interagir avec de nombreuses autres fonctionnalités VMware.

Lors de la planification de votre stratégie de fédération de fournisseurs d'identité vCenter Server, tenez compte des éventuelles limitations d'interopérabilité.

Mécanismes d'authentification

Dans une configuration de fédération de fournisseur d'identité vCenter Server, le fournisseur d'identité externe gère les mécanismes d'authentification (mots de passe, MFA, biométrie, etc.).

Prise en charge d'un domaine Active Directory unique

Lorsque vous configurez la fédération de fournisseurs d'identité vCenter Server, l'assistant Configurer le fournisseur d'identité principal vous invite à entrer les informations LDAP pour le domaine AD contenant les utilisateurs et les groupes pour lesquels vous souhaitez qu'ils puissent accéder à vCenter Server. vCenter Server dérive le domaine AD à utiliser pour l'autorisation, ainsi que les autorisations à partir du nom unique de base de l'utilisateur que vous spécifiez dans l'assistant. Vous pouvez ajouter des autorisations sur des objets vSphere uniquement pour les utilisateurs et les groupes de ce domaine AD. Les utilisateurs ou les groupes de domaines enfants AD ou d'autres domaines de la forêt AD ne sont pas pris en charge par la fédération de fournisseurs d'identité vCenter Server.

Stratégies vCenter Server

Lorsque le système vCenter Server est utilisé comme fournisseur d'identité, vous contrôlez les stratégies de mot de passe, de verrouillage et de jeton de vCenter Server pour le domaine vsphere.local. Lors de l'utilisation de l'authentification fédérée avec le système vCenter Server, le fournisseur d'identité externe contrôle les stratégies de mot de passe, de verrouillage et de jeton pour les comptes stockés dans la source d'identité, tels qu'Active Directory.

Audit et conformité

Lors de l'utilisation de la fédération de fournisseurs d'identité vCenter Server, le système vCenter Server continue de créer des entrées de journal pour les connexions utilisateur réussies. Toutefois, le fournisseur d'identité externe est responsable du suivi et de la journalisation des actions, telles que les tentatives d'entrée de mot de passe et les verrouillages de compte d'utilisateur. Le système vCenter Server ne journalise pas ces événements, car ils ne sont plus visibles pour vCenter Server. Par exemple, lorsque AD FS est le fournisseur d'identité, il suit et journalise les erreurs des connexions fédérées. Lorsque le système vCenter Server est le fournisseur d'identification des connexions locales, vCenter Server surveille et journalise les erreurs de ces connexions. Dans une configuration fédérée, le système vCenter Server continue de consigner les actions de l'utilisateur après la connexion.

Intégration de produits VMware existants

Les produits VMware intégrés à l'instance de vCenter Server (par exemple, VMware vRealize Operations, VMware vSAN™, VMware NSX®, etc.) continuent de fonctionner comme auparavant.

Produits qui intègrent la post-connexion

Les produits qui intègrent la post-connexion (c'est-à-dire qu'ils n'ont pas besoin d'une connexion distincte) continuent de fonctionner comme avant.

Authentification simple pour l'accès aux API, SDK et CLI

Les scripts, produits et autres fonctionnalités existantes qui reposent sur des commandes d'API, de SDK ou d'interface de ligne de commande qui utilisent l'authentification simple (c'est-à-dire nom d'utilisateur et mot de passe) continuent de fonctionner comme avant. En interne, l'authentification s'effectue en transmettant le nom d'utilisateur et le mot de passe. Cette transmission du nom d'utilisateur et du mot de passe compromet certains des avantages de l'utilisation de la fédération d'identité, car elle expose le mot de passe à vCenter Server (et à vos scripts). Envisagez de migrer vers l'authentification basée sur des jetons, lorsque c'est possible.

Interface de gestion de vCenter Server

Si l'utilisateur est membre du groupe administrateurs, l'accès à l'interface de gestion de vCenter Server (anciennement appelée interface de gestion de dispositif vCenter Server ou interface VAMI) est pris en charge.

Entrée du texte du nom d'utilisateur sur la page de connexion AD FS

La page de connexion AD FS ne prend pas en charge la transmission de texte pour préremplir la zone de texte de nom d'utilisateur. Par conséquent, lors des connexions fédérées avec AD FS, après l'entrée de votre nom d'utilisateur sur la page de lancement de vCenter Server et redirection vers la page de connexion AD FS, vous devez entrer de nouveau votre nom d'utilisateur sur la page de connexion AD FS. Le nom d'utilisateur que vous entrez sur la page de lancement de vCenter Server est nécessaire pour rediriger la connexion vers le fournisseur d'identité approprié, et le nom d'utilisateur sur la page de connexion AD FS est nécessaire pour s'authentifier auprès d'AD FS. Cette incapacité à transmettre le nom d'utilisateur à la page de connexion AD FS constitue une limite d'AD FS. Vous ne pouvez pas configurer ou modifier ce comportement directement dans vCenter Server.

Cycle de vie de la fédération de fournisseurs d'identité vCenter Server

Lorsque vous gérez le cycle de vie de la fédération de fournisseurs d'identité vCenter Server, des éléments spécifiques doivent être pris en compte.

Vous pouvez gérer le cycle de vie de la fédération de fournisseurs d'identité vCenter Server de l'une des manières suivantes.

Migration d'Active Directory vers AD FS

Si vous utilisez Active Directory comme source d'identité pour vCenter Server, la migration vers l'utilisation d'AD FS est directe. Si vos groupes et rôles Active Directory correspondent à vos groupes et rôles AD FS, vous n'avez pas besoin d'effectuer d'autres actions. Lorsque les groupes et les rôles ne correspondent pas, vous devez effectuer des tâches supplémentaires. Si vCenter Server est membre du domaine, envisagez de le supprimer du domaine, car il n'est pas requis ou utilisé pour la fédération d'identité.

Redirection et migration inter-domaines

La fédération de fournisseur d'identité de vCenter Server prend en charge la redirection inter-domaines, c'est-à-dire le déplacement d'une instance de vCenter Server d'un domaine vSphere SSO vers un autre. L'instance de vCenter Server redirigée reçoit la configuration AD FS répliquée depuis le système vCenter Server ou les systèmes sur lesquels elle était dirigée.

En général, il n'est pas nécessaire d'effectuer une reconfiguration AD FS supplémentaire pour une redirection inter-domaines, sauf si l'une des conditions suivantes est vraie.

1 La configuration AD FS de l'instance de vCenter Server redirigée diffère de la configuration AD FS de l'instance de vCenter Server sur laquelle elle était dirigée.

2 C'est la première fois que l'instance de vCenter Server redirigée reçoit une configuration AD FS.

Dans ces cas-là, vous devez ajouter les URI de redirection du système vCenter Server au groupe d'applications correspondant sur le serveur AD FS. Par exemple, si vCenter Server 1 avec le groupe d'applications AD FS A (ou aucune configuration AD FS) est redirigé vers vCenter Server 2 avec le groupe d'applications AD FS B, vous devez ajouter les URI de redirection de vCenter Server 1 au groupe d'applications B.

Configuration de la Fédération de fournisseurs d'identité vCenter Server

Après avoir initialement déployé vCenter Server, vous pouvez configurer un fournisseur d'identité externe pour l'authentification fédérée.

Vous configurez Fédération de fournisseurs d'identité de vCenter Server à partir de vSphere Client ou de l'API. Vous devez également effectuer une configuration sur votre fournisseur d'identité externe. Pour configurer Fédération de fournisseurs d'identité vCenter Server, 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.

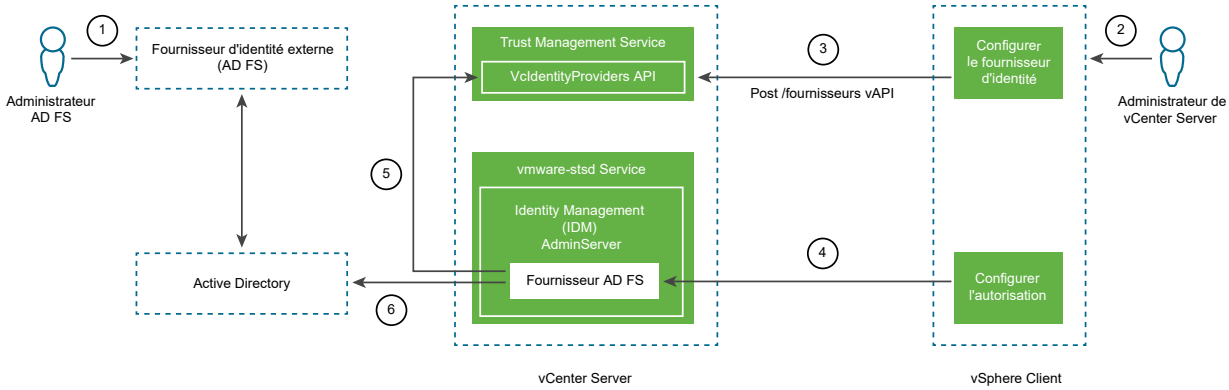
Flux de configuration de la fédération de fournisseur d'identité vCenter Server

Pour configurer la fédération de fournisseur d'identité vCenter Server efficacement, vous devez comprendre les flux de communication qui se produisent.

Flux de configuration de la fédération de fournisseur d'identité vCenter Server

La figure suivante illustre le flux de configuration de la fédération de fournisseur d'identité vCenter Server.

Figure 4-5. Flux de configuration de la fédération de fournisseur d'identité vCenter Server



vCenter Server, AD FS et Active Directory interagissent de la manière suivante.

1 L'administrateur AD FS configure une application OAuth AD FS pour vCenter Server.

2 L'administrateur vCenter Server se connecte à l'instance de vCenter Server à l'aide de vSphere Client.

3 L'administrateur vCenter Server ajoute un fournisseur d'identité AD FS à l'instance de vCenter Server et entre également des informations sur le domaine Active Directory.

   vCenter Server a besoin de ces informations pour établir une connexion LDAP au domaine Active Directory du serveur AD FS. À l'aide de cette connexion, l'instance de vCenter Server recherche des utilisateurs et des groupes, et les ajoute aux groupes locaux vCenter Server à l'étape suivante. Pour plus d'informations, consultez la section intitulée « Recherche dans le domaine Active Directory » ci-dessous.

4 L'administrateur vCenter Server configure les autorisations d'autorisation dans l'instance de vCenter Server pour les utilisateurs AD FS.

5 Le fournisseur AD FS interroge l'API VcIdentityProviders pour obtenir les informations de connexion LDAP pour la source Active Directory.

6 Le fournisseur AD FS recherche dans Active Directory les utilisateurs ou les groupes interrogés pour terminer la configuration de l'autorisation.

Recherche dans le domaine Active Directory

Vous pouvez configurer AD FS en tant que fournisseur d'identité externe dans l'instance de vCenter Server à l'aide de l'assistant Configurer le fournisseur d'identité principal dans vSphere Client. Dans le cadre du processus de configuration, vous devez entrer les informations sur votre domaine Active Directory, y compris les informations de nom unique d'utilisateur et de groupe. La configuration d'AD FS pour l'authentification nécessite ces informations de connexion Active Directory. Cette connexion est nécessaire pour rechercher et mapper des noms d'utilisateurs et des groupes Active Directory à des rôles et des autorisations dans vCenter Server, alors qu'AD FS

est utilisé pour l'authentification de l'utilisateur. Cette étape de l'assistant Configurer le fournisseur d'identité principal ne crée pas une source d'identité Active Directory sur LDAP. vCenter Server utilise plutôt ces informations pour établir une connexion compatible avec la recherche valide à votre domaine Active Directory pour y rechercher des utilisateurs et des groupes.

Prenons un exemple utilisant les entrées de nom unique suivantes :

- Nom unique de base pour les utilisateurs : cn=Users,dc=corp,dc=local
- Nom unique de base pour les groupes : dc=corp,dc=local
- Nom d'utilisateur : cn=Administrator,cn=Users,dc=corp,dc=local

Si l'utilisateur AdfsUser@corp.local est membre du groupe ADGroup@corp.local, la saisie de ces informations dans l'assistant permet à un administrateur vCenter Server de rechercher le groupe ADGroup@corp.local et de l'ajouter au groupe Administrators@vsphere.local de vCenter Server. Par conséquent, l'utilisateur AdfsUser@corp.local se voit accorder des privilèges d'administration dans vCenter Server lors de la connexion.

vCenter Server utilise également ce processus de recherche lorsque vous configurez des autorisations globales pour des utilisateurs et des groupes Active Directory. Dans les deux cas, qu'il s'agisse de configurer des autorisations globales ou d'ajouter un utilisateur ou un groupe, vous sélectionnez le domaine que vous avez saisi pour votre fournisseur d'identité AD FS dans le menu déroulant **Domaine** pour rechercher et sélectionner des utilisateurs et des groupes dans votre domaine Active Directory.

Utiliser le magasin de certificats racines approuvés au lieu du truststore JRE

Si vous avez importé un certificat d'autorité de certification racine par votre propre autorité de certification interne dans le truststore JRE dans vSphere 7.0, à partir de vSphere 7.0 Update 1, vous pouvez enregistrer le certificat dans le magasin de certificats racines approuvés.

Pour configurer la fédération de fournisseurs d'identité vCenter Server dans vSphere 7.0 avec un certificat d'autorité de certification racine émis par votre propre autorité de certification interne, vous deviez l'importer dans le truststore JRE. À partir de vSphere 7.0 Update 1, vous pouvez enregistrer le certificat dans le magasin de certificats racines approuvés. Cette modification signifie que vous devez ajouter le certificat d'autorité de certification racine émis par votre propre autorité de certification interne au magasin de certificats racines approuvés (également appelé magasin de certificats de point de terminaison VMware ou VECS). Les certificats dans le truststore JRE continuent de fonctionner, mais vCenter Server est en cours de normalisation sur l'utilisation du magasin de certificats racines approuvés.

Procédure

1. Connectez-vous avec vSphere Client à l'instance de vCenter Server.
2. Accédez à **Administration > Certificats > Gestion des certificats**.
3. En regard de **Certificats racine approuvés**, cliquez sur **Ajouter**.

4 Recherchez le certificat racine AD FS, puis cliquez sur **Ajouter**.

Le certificat est ajouté dans un panneau sous **Certificats racines approuvés**.

Configurer la fédération de fournisseurs d'identité vCenter Server pour AD FS

Après l'installation ou la mise à niveau vers vSphere 7.0 ou version ultérieure, vous pouvez configurer la fédération du fournisseur d'identité vCenter Server.

vCenter Server ne prend en charge qu'un seul fournisseur d'identité externe configuré (une source) et la source d'identité vsphere.local. Vous ne pouvez pas utiliser plusieurs fournisseurs d'identité externes. La Fédération de fournisseur d'identité vCenter Server utilise OpenID Connect (OIDC) pour la connexion de l'utilisateur à vCenter Server.

Cette tâche décrit comment ajouter un groupe AD FS au groupe d'administrateurs vSphere comme moyen de contrôle des autorisations. Vous pouvez également configurer des privilèges à l'aide de l'autorisation AD FS par le biais d'autorisations globales ou d'objets dans l'instance de vCenter Server. Pour plus d'informations sur l'ajout d'autorisations, consultez la documentation de *Sécurité vSphere*.

Attention Si vous utilisez une source d'identité Active Directory que vous avez précédemment ajoutée à vCenter Server pour votre source d'identité AD FS, ne supprimez pas cette source d'identité existante de vCenter Server. Cela entraîne une régression avec des rôles et des appartenances à un groupe précédemment attribués. L'utilisateur AD FS avec des autorisations globales et des utilisateurs ajoutés au groupe d'administrateurs ne pourra pas se connecter.

Solution : si vous n'avez pas besoin des rôles et des appartenances de groupes précédemment attribués, et que vous souhaitez supprimer la source d'identité Active Directory précédente, supprimez la source d'identité avant de créer le fournisseur AD FS et de configurer les appartenances de groupe dans vCenter Server.

Conditions préalables

Conditions requises pour les services de fédération Active Directory :

- AD FS pour Windows Server 2016 ou version ultérieure doit déjà être déployé.
- FS AD doit être connecté à Active Directory.
- Un groupe d'applications pour vCenter Server doit être créé dans AD FS dans le cadre du processus de configuration. Consultez l'article de la base de connaissances de VMware à l'adresse https://kb.vmware.com/s/article/78029.
- Un certificat d'autorité de certification racine AD FS ajouté au magasin de certificats racines approuvés (également appelé magasin de certificats VMware).
- Vous avez créé un groupe d'administrateurs vCenter Server dans AD FS qui contient les utilisateurs auxquels vous souhaitez accorder des privilèges d'administrateur vCenter Server.

Pour plus d'informations sur la configuration d'AD FS, consultez la documentation Microsoft.

vCenter Server et autres conditions requises :

- vSphere 7.0 ou version ultérieure
- vCenter Server doit pouvoir se connecter au point de terminaison de détection AD FS, de même que l'autorisation, le jeton, la déconnexion, JWKS et tout autre point de terminaison dans les métadonnées du point de terminaison de détection.
- Vous avez besoin du privilège **VcIdentityProviders.Gérer** pour créer, mettre à jour ou supprimer un fournisseur d'identité vCenter Server requis pour l'authentification fédérée. Pour limiter un utilisateur à l'affichage des informations de configuration du fournisseur d'identité uniquement, attribuez le privilège **VcIdentityProviders.Lire**.

Procédure

1. Connectez-vous avec vSphere Client à l'instance de vCenter Server.
2. Ajoutez votre certificat d'autorité de certification racine AD FS au magasin de certificats racines approuvés.
   a. Accédez à **Administration > Certificats > Gestion des certificats**.
   b. En regard de **Magasin de certificats racine approuvés**, cliquez sur **Ajouter**.
   c. Recherchez le certificat racine AD FS, puis cliquez sur **Ajouter**.

      Le certificat est ajouté dans un panneau sous **Certificats racines approuvés**.
3. Accédez à l'interface utilisateur de configuration.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Configuration**.
4. Sélectionnez l'onglet **Fournisseur d'identité** et obtenez les URI de redirection.
   a. Cliquez sur l'**icône** « i » d'information en regard du lien « Modifier le fournisseur d'identité ».

      Deux URI de redirection sont affichés dans la bannière contextuelle.
   b. Pour configurer le serveur AD FS, copiez les deux URI dans un fichier ou notez-les pour une utilisation ultérieure dans les étapes suivantes.
   c. Fermez la bannière contextuelle.
5. Créez une configuration OpenID Connect dans AD FS et configurez-la pour vCenter Server.

   Pour établir une relation d'approbation de partie de confiance entre vCenter Server et un fournisseur d'identité, vous devez établir les informations d'identification et un secret partagé entre eux. Dans AD FS, vous devez créer une configuration OpenID Connect appelée groupe d'applications, qui se compose d'une application serveur et d'une API Web. Les deux composants spécifient les informations que l'instance de vCenter Server utilise pour approuver le serveur AD FS et communiquer avec lui. Pour activer OpenID Connect dans AD FS, reportez-vous à l'article de la base de connaissances VMware sur https://kb.vmware.com/s/article/78029.

Notez ce qui suit lorsque vous créez le groupe d'applications AD FS.

- Vous avez besoin des deux URI de redirection que vous avez obtenus et enregistrés à partir de l'étape précédente.
- Copiez les informations suivantes dans un fichier ou notez-les pour les utiliser lors de la configuration du fournisseur d'identité vCenter Server à l'étape suivante.
  - Identificateur de client
  - Secret partagé
  - Adresse OpenID du serveur AD FS

6 Création d'un fournisseur d'identité sur vCenter Server.

a Revenez à l'onglet **Fournisseur d'identité** dans vSphere Client.

b Cliquez sur le lien « Modifier le fournisseur d'identité ».

L'Assistant Configurer le fournisseur d'identité principal s'ouvre.

c Sélectionnez **Microsoft ADFS** et cliquez sur **Suivant**.

Entrez les informations que vous avez collectées précédemment pour les zones de texte suivantes :

- Identificateur de client
- Secret partagé
- Adresse OpenID du serveur AD FS

d Cliquez sur **Suivant**.

e Entrez les informations d'utilisateur et de groupe pour la connexion Active Directory via LDAP pour rechercher des utilisateurs et des groupes.

vCenter Server dérive le domaine AD à utiliser pour les autorisations à partir du nom unique de base pour les utilisateurs. Vous pouvez ajouter des autorisations sur des objets vSphere uniquement pour les utilisateurs et les groupes de ce domaine AD. Les utilisateurs ou les groupes de domaines enfants AD ou d'autres domaines de la forêt AD ne sont pas pris en charge par la fédération de fournisseurs d'identité vCenter Server.

Option	Description
Nom unique de base pour les utilisateurs	Nom unique de base pour les utilisateurs.
Nom unique de base pour les groupes	Nom unique de base pour les groupes.
Nom d'utilisateur	ID d'un utilisateur du domaine qui dispose au minimum d'un accès en lecture seule au nom unique de base pour les utilisateurs et les groupes.
Mot de passe	ID d'un utilisateur du domaine qui dispose au minimum d'un accès en lecture seule au nom unique de base pour les utilisateurs et 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 les connexions LDAP et 636 pour les connexions LDAPS. Pour les déploiements de contrôleurs multi-domaines Active Directory, le port est généralement 3268 pour les connexions LDAP et 3269 pour les connexions LDAPS. Un certificat qui établit la confiance du point de terminaison LDAPS 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.
certificats SSL	Si vous souhaitez utiliser LDAPS avec votre source d'identité du serveur Active Directory LDAP ou OpenLDAP, cliquez sur **`Parcourir`** pour sélectionner un certificat.

f Cliquez sur **Suivant**, vérifiez les informations, puis cliquez sur **Terminer**.

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

a Dans le menu **Accueil**, sélectionnez **Administration**.

b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.

8 Configurez l'appartenance au groupe vCenter Server pour l'autorisation AD FS.

a Cliquez sur l'onglet **Groupes**.

b Cliquez sur le groupe **Administrateurs**, puis sur **Ajouter des membres**.

c Sélectionnez le domaine dans le menu déroulant.

d Dans la zone de texte située sous le menu déroulant, entrez les premiers caractères du groupe AD FS que vous souhaitez ajouter, puis attendez que la sélection déroulante s'affiche.

L'affichage de la sélection peut prendre plusieurs secondes, car vCenter Server établit la connexion et recherche Active Directory.

e Sélectionnez le groupe AD FS et ajoutez-le au groupe d'administrateurs.

f Cliquez sur **Enregistrer**.

9 Vérifiez que vous vous connectez à vCenter Server avec un utilisateur Active Directory.

Comprendre vCenter Single Sign-On

Si vous n'utilisez pas de fournisseur d'identité externe, vous devez comprendre l'architecture sous-jacente du fournisseur d'identité intégré (vCenter Single Sign-On) et son incidence sur l'installation et les mises à niveau.

Composants vCenter Single Sign-On

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

Lors de l'installation, les composants suivants sont déployés dans le cadre d'un déploiement de vCenter Server.

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 Server. Les jetons SAML permettent aux utilisateurs interactifs, de scripts et de services (notamment les utilisateurs de solution) 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 Client. Au départ, seul l'utilisateur administrator@*your_domain_name* dispose de ces privilèges. Vous pouvez modifier le domaine vSphere lorsque vous installez vCenter Server. Attribuez au domaine un nom différent que celui du domaine Microsoft Active Directory ou OpenLDAP.

VMware Directory Service (vmdir)

Le service VMware Directory Service (vmdir) est associé au domaine que vous indiquez lors de l'installation. Il est inclus dans chaque déploiement de vCenter Server. Ce service est un service d'annuaire mutualisé et à réplication d'homologue qui met à disposition un annuaire LDAP sur le port 389. Il stocke et gère également les comptes d'utilisateur et les mots de passe vCenter Single Sign-On qui sont sécurisés par l'algorithme de hachage SHA-512.

Si votre environnement inclut plusieurs instances de vCenter Server configurées en mode lié, une mise à jour du contenu vmdir d'une seule instance de vmdir est propagée à toutes les autres instances de vmdir.

Le service VMware Directory Service stocke les informations de certificat, en plus des informations de vCenter Single Sign-On.

Identity Management Service

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

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 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 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

Les utilisateurs s'authentifient auprès de vCenter Single Sign-On en entrant leurs informations d'identification sur la page de connexion. 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.

Tous les utilisateurs pouvant s'authentifier auprès de vCenter Single Sign-On peuvent réinitialiser leur mot de passe. Reportez-vous à la section Changer le mot de passe de vCenter Single Sign-On . 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 d'administration de vCenter Single Sign-On est accessible à partir de vSphere Client.

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 Client. Après authentification, cet utilisateur peut accéder à l'interface d'administration de vCenter Single Sign-On à partir de vSphere 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.

Note 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.

Autres comptes d'utilisateurs

Les comptes d'utilisateurs suivants sont créés automatiquement dans vCenter Server dans le domaine vsphere.local (ou le domaine par défaut que vous avez créé lors de l'installation). Ces comptes d'utilisateurs sont des comptes shell. La stratégie de mot de passe de vCenter Single Sign-On ne s'applique pas à ces comptes.

Tableau 4-1. Autres comptes d'utilisateurs vSphere

Compte	Description
K/M	Pour la gestion des clés Kerberos.
krbtgt/VSPHERE.LOCAL	Pour la compatibilité avec l'authentification Windows intégrée.
waiter-*random_string*	Pour Auto Deploy.

Utilisateurs ESXi

Les hôtes ESXi autonomes ne sont pas intégrés à vCenter Single Sign-On. 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 VMware Host Client, ESXCLI ou PowerCLI, vCenter Server ne reconnaît pas 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.

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

Comment se connecter aux composants de vCenter Server

Vous pouvez ouvrir une session en vous connectant à l'instance de vSphere Client.

Lorsqu'un utilisateur se connecte à un système vCenter Server à partir de vSphere Client, le comportement de connexion varie selon que l'utilisateur se trouve ou non dans le domaine qui est défini comme la 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.

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 la section Gestion des utilisateurs et des groupes vCenter Single Sign-On.

Pour tous les objets de la hiérarchie de vCenter Server, vous pouvez attribuer des autorisations 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, l'appartenance à un des groupes vCenter Single Sign-On détermine les privilèges. Par exemple, tout utilisateur qui est membre du groupe Administrateurs 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. 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.

Attention 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 4-2. Groupes du domaine vsphere.local

Privilège	Description
Utilisateurs	Les utilisateurs du domaine vCenter Single Sign-On (par défaut, vsphere.local).
SolutionUsers	Groupe d'utilisateurs de solution pour 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. N'ajoutez pas de membres à ce groupe, sauf en cas de force majeure.
DCAdmins	Les membres du groupe DCAdmins peuvent exercer des actions d'administrateur de contrôleur de domaine sur VMware Directory Service. **Note** Ne gérez pas le contrôleur de domaine directement. Utilisez plutôt la CLI `vmdir` ou vSphere Client pour effectuer les tâches correspondantes.
SystemConfiguration.BashShellAdministrators	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 à l'aide de SSH peut uniquement accéder aux commandes disponibles dans l'interpréteur de commandes 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 Act-As de vCenter Single Sign-On.
ExternalIDPUsers	vSphere n'utilise pas ce groupe interne. VMware vCloud Air requiert ce groupe.

Tableau 4-2. Groupes du domaine vsphere.local (suite)

Privilège	Description
SystemConfiguration.Administrators	Les membres du groupe SystemConfiguration.Administrators peuvent afficher et gérer la configuration du système dans vSphere 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. **Note** 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. N'ajoutez pas de membres à ce groupe, sauf en cas de force majeure et si vous en comprenez les conséquences.
TrustedAdmins	Les membres de ce groupe peuvent effectuer des tâches de configuration et d'administration de l'autorité d'approbation vSphere™ VMware®. Par défaut, ce groupe ne contient aucun membre. Vous devez ajouter un membre à ce groupe afin de pouvoir effectuer des tâches de l'autorité d'approbation vSphere.
AutoUpdate	Ce groupe est utilisé en interne pour vCenter Cloud Gateway.
SyncUsers	Ce groupe est utilisé en interne pour vCenter Cloud Gateway.
vSphereClientSolutionUsers	Ce groupe est utilisé en interne pour vSphere Client.
ServiceProviderUsers	Les membres de ce groupe peuvent gérer l'infrastructure vSphere with Tanzu et VMware Cloud on AWS.
NsxAdministrators	Ce groupe est utilisé pour VMware NSX.
WorkloadStorage	Groupe de stockage de charge de travail.

Tableau 4-2. Groupes du domaine vsphere.local (suite)

Privilège	Description
RegistryAdministrators	Les membres de ce groupe peuvent gérer le registre.
NsxAuditors	Ce groupe est utilisé pour VMware NSX.
NsxViAdministrators	Ce groupe est utilisé pour VMware NSX.
SystemConfiguration.SupportUsers	Les membres du groupe SystemConfiguration.SupportUsers peuvent accéder à l'API du bundle de support.
SystemConfiguration.ReadOnly	Les membres de ce groupe peuvent accéder aux opérations en lecture seule de vCenter Server Appliance.

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.

La configuration de vCenter Single Sign-On s'effectue dans vSphere Client. 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.

Note Dans vSphere 7.0 Update 2, vous pouvez activer FIPS sur vCenter Server. Consultez la documentation de *Sécurité vSphere*. AD sur LDAP et IWA ne sont pas pris en charge lorsque FIPS est activé. Utilisez la fédération de fournisseurs d'identité externe en mode FIPS. Reportez-vous à la section Configuration de la Fédération de fournisseurs d'identité vCenter Server.

Un administrateur 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.

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.

Note 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 pour s'authentifier. Le nom de domaine se présente sous la forme :

```
DOMAIN\user
```

Les sources d'identité suivantes sont disponibles.

- Active Directory sur LDAP. vCenter Single Sign-On prend en charge plusieurs sources d'identité Active Directory sur LDAP.
- Active Directory (authentification Windows intégrée) versions 2003 et ultérieures. 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.
- OpenLDAP 2.4 et versions ultérieures. vCenter Single Sign-On prend en charge plusieurs sources d'identité OpenLDAP.

Note Une prochaine mise à jour de Microsoft Windows modifiera le comportement par défaut d'Active Directory pour exiger une authentification renforcée et un chiffrement fort. Cette modification aura un impact sur la manière dont vCenter Server s'authentifie avec Active Directory. Si vous utilisez Active Directory comme source d'identité pour vCenter Server, vous devez prévoir d'activer LDAPS. Pour plus d'informations sur cette mise à jour de sécurité Microsoft, consultez https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 et https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

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 Client, le comportement de connexion varie selon que l'utilisateur se trouve ou non dans le domaine qui est défini comme la 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. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Configuration**.
4. Sous l'onglet **Fournisseur d'identité**, cliquez sur **Sources d'identité**, sélectionnez une source d'identité, puis cliquez sur **Définir comme valeur par défaut**.
5. Cliquez sur **OK**.

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

Ajouter ou modifier une source d'identité 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 ou modifier les paramètres des sources d'identité qu'ils ont ajoutées.

Une source d'identité peut être une source d'identité Active Directory sur LDAP, un domaine Active Directory natif (authentification Windows intégrée) ou un service d'annuaire OpenLDAP. Reportez-vous à la section Sources d'identité pour vCenter Server avec vCenter Single Sign-On.

Immédiatement après l'installation, le domaine vsphere.local (ou le domaine spécifié lors de l'installation) comportant les utilisateurs internes de vCenter Single Sign-On est disponible.

Note Si vous avez mis à jour ou remplacé votre certificat SSL Active Directory, vous devez supprimer et rajouter la source d'identité dans vCenter Server.

Conditions préalables

Si vous ajoutez une source d'identité Active Directory (authentification Windows intégrée), l'instance de vCenter Server doit être dans le domaine Active Directory. Reportez-vous à la section Ajouter une instance de vCenter Server à un domaine Active Directory.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Configuration**.
4. Dans l'onglet **Fournisseur d'identité**, cliquez sur **Sources d'identité**, puis sur **Ajouter**.
5. Sélectionnez la 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 la section Paramètres de source d'identité Active Directory.
Active Directory sur LDAP	Cette option nécessite la spécification du contrôleur de domaine et d'autres informations. Reportez-vous à la section Paramètres d'Active Directory over LDAP et de la source d'identité du serveur OpenLDAP.
OpenLDAP	Utilisez cette option pour une source d'identité OpenLDAP. Reportez-vous à la section Paramètres d'Active Directory over LDAP et de la source d'identité du serveur OpenLDAP.

   Note 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. Cliquez sur **Ajouter**.

Étape suivante

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*.

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

La source d'identité d'Active Directory over LDAP est préférable à l'option Active Directory (authentification Windows intégrée). 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 de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2064977 pour connaître les exigences supplémentaires.

Note Une prochaine mise à jour de Microsoft Windows modifiera le comportement par défaut d'Active Directory pour exiger une authentification renforcée et un chiffrement fort. Cette modification aura un impact sur la manière dont vCenter Server s'authentifie avec Active Directory. Si vous utilisez Active Directory comme source d'identité pour vCenter Server, vous devez prévoir d'activer LDAPS. Pour plus d'informations sur cette mise à jour de sécurité Microsoft, consultez https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 et https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html.

Tableau 4-3. Paramètres d'Active Directory over LDAP et du serveur OpenLDAP

Option	Description
Nom	Nom de la source d'identité.
Nom unique de base des utilisateurs	Nom unique de base pour les utilisateurs. Entrez le nom de domaine (DN) à partir duquel lancer les recherches d'utilisateurs. Par exemple, cn=Users, dc=myCorp, dc=com.
Nom unique de base des groupes	Nom unique de base pour les groupes. Entrez le nom unique à partir duquel lancer les recherches de groupes. Par exemple, cn=Groups, dc=myCorp, dc=com.
Nom de domaine	Nom de domaine complet du domaine.
Alias de 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.
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. L'ID peut être dans l'un des formats suivants : ■ UPN (user@domain.com) ■ NetBIOS (DOMAIN/user) ■ DN (cn=user,cn=Users,dc=domain,dc=com) Le nom d'utilisateur doit être complet. L'entrée « user » ne fonctionne pas.

Tableau 4-3. Paramètres d'Active Directory over LDAP et du serveur OpenLDAP (suite)

Option	Description
Mot de passe	Mot de passe de l'utilisateur spécifié par **Nom d'utilisateur**.
Connexion à	Contrôleur de domaine auquel se connecter. Il peut s'agir de n'importe quel contrôleur dans le domaine ou de contrôleurs spécifiques.
URL du serveur principal	Serveur LDAP du contrôleur de domaine principale du domaine. Vous pouvez utiliser le nom d'hôte ou l'adresse IP. Utilisez le format **`ldap://hostname_or_IPaddress:port`** ou **`ldaps://hostname_or_IPaddress:port`**. Le port est généralement 389 pour les connexions LDAP et 636 pour les connexions LDAPS. Pour les déploiements de contrôleurs multi-domaines Active Directory, le port est généralement 3268 pour les connexions LDAP et 3269 pour les connexions LDAPS. Un certificat qui établit la confiance du point de terminaison LDAPS 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. Vous pouvez utiliser le nom d'hôte ou l'adresse IP.
Certificats (pour LDAPS)	Si vous souhaitez utiliser LDAPS avec votre source d'identité du serveur Active Directory LDAP ou OpenLDAP , cliquez sur **`Parcourir`** pour sélectionner un certificat qui a été exporté à partir du contrôleur de domaine spécifié dans l'URL LDAPS. (Notez que le certificat utilisé ici n'est pas un certificat d'autorité de certification racine.) Pour exporter le certificat à partir de Active Directory, consultez la documentation Microsoft.

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 (authentification Windows intégrée)

Vous pouvez configurer vCenter Single Sign-On pour utiliser une source d'identité Active Directory (authentification Windows intégrée) uniquement si cette source d'identité est disponible. Suivez les instructions de la documentation *Configuration de vCenter Server*.

Note 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, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2070433.

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.

Si vous avez activé la journalisation des événements de diagnostic dans votre annuaire Active Directory pour identifier vos besoins en sécurisation renforcée, vous pouvez voir un événement de journal avec l'ID d'événement 2889 sur ce serveur d'annuaire. L'ID d'événement 2889 est généré comme une anomalie plutôt qu'un risque de sécurité lorsque vous utilisez l'authentification Windows intégrée. Pour plus d'informations sur l'ID d'événement 2889, consultez l'article de la base de connaissances VMware https://kb.vmware.com/s/article/78644.

Tableau 4-4. Ajouter des paramètres de source d'identité

Zone de texte	Description
Nom de domaine	Nom de domaine complet du nom de domaine, par exemple mondomaine.com. Ne fournissez pas une adresse IP. Ce nom de domaine doit pouvoir être résolu par DNS par le système vCenter Server
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.

Tableau 4-4. Ajouter des paramètres de source d'identité (suite)

Zone de texte	Description
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).

Ajouter ou supprimer une source d'identité à l'aide de l'interface de ligne de commande

Vous pouvez utiliser l'utilitaire `sso-config` pour ajouter ou supprimer une source d'identité.

Une source d'identité peut être un domaine Active Directory natif (authentification Windows intégrée), AD sur LDAP, AD sur LDAP avec LDAPS (LDAP sur SSL) ou OpenLDAP. Reportez-vous à la section Sources d'identité pour vCenter Server avec vCenter Single Sign-On. Vous pouvez également utiliser l'utilitaire `sso-config` pour configurer l'authentification par carte à puce et RSA SecurID.

Conditions préalables

Si vous ajoutez une source d'identité Active Directory, l'instance de vCenter Server doit être dans le domaine Active Directory. Reportez-vous à la section Ajouter une instance de vCenter Server à un domaine Active Directory.

Activez la connexion SSH. Reportez-vous à la section Gérer vCenter Server à l'aide du shell de vCenter Server.

Procédure

1. Utilisez SSH ou une autre connexion de console à distance pour démarrer une session sur le système vCenter Server.
2. Connectez-vous en tant qu'utilisateur racine.
3. Modifiez vers le répertoire dans lequel l'utilitaire `sso-config` réside.

```
cd /opt/vmware/bin
```

4 Consultez l'aide de `sso-config` en exécutant `sso-config.sh -help` ou consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/67304 pour obtenir des exemples d'utilisation.

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 vCenter Server à un domaine Active Directory avant de pouvoir utiliser SSPI.

Conditions préalables

- Joindre vCenter Server à un domaine Active Directory Reportez-vous à la section Ajouter une instance de vCenter Server à un domaine Active Directory.
- Vérifiez que le domaine est correctement configuré. Consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2064250.
- Vérifiez que le plug-in d'authentification étendue est installé. Voir *Installation et configuration de vCenter Server*.

Note Lorsque vous configurez vCenter Server pour utiliser l'authentification fédérée avec Active Directory Federation Services, le plug-in d'authentification étendue ne s'applique qu'aux configurations où vCenter Server est le fournisseur d'identité (Active Directory sur LDAP, Authentification Windows intégrée et configurations OpenLDAP).

Procédure

1 Naviguer à la page de connexion de vSphere 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.

Gestion du service STS (Security Token Service) de vCenter Server

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

En tant qu'émetteur de jeton, STS utilise une clé privée pour signer les jetons et publie les certificats publics pour que les services vérifient la signature du jeton. vCenter Server gère les certificats de signature STS et les stocke dans VMware Directory Service (vmdir). Les jetons peuvent avoir une durée de vie significative et être signés de manière historique par n'importe quelle clé.

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

Tableau 4-5. Utilisateurs STS et informations d'identification

Type d'utilisateur	Informations d'identification principales
Utilisateur de solution	Certificat valide.
Autres utilisateurs	Nom d'utilisateur et mot de passe disponibles dans une source d'identité vCenter Single Sign-On.

STS authentifie l'utilisateur en fonction des informations d'identification principales et crée un jeton SAML contenant les attributs de l'utilisateur.

Par défaut, VMware Certificate Authority (VMCA) génère le certificat de signature STS. Vous pouvez actualiser le certificat de signature STS avec un nouveau certificat VMCA. Vous pouvez également importer et remplacer le certificat de signature STS par défaut par un certificat de signature STS généré personnalisé ou tiers. Ne remplacez pas le certificat de signature STS, sauf si la stratégie de sécurité de votre entreprise nécessite le remplacement de tous les certificats.

Vous pouvez utiliser vSphere Client pour :

- Actualiser les certificats STS
- Importer et remplacer des certificats STS personnalisés et générés par des tiers
- Afficher les détails du certificat STS, tels que la date d’expiration

Vous pouvez également utiliser la ligne de commande pour remplacer des certificats STS personnalisés et tiers.

Durée et expiration du certificat STS

Une nouvelle installation de vSphere 7.0 Update 1 et versions ultérieures crée un certificat de signature STS d'une durée de 10 ans. Lorsqu'un certificat de signature STS arrive à expiration, une alarme vous avertit à partir de 90 jours avant l'expiration, une fois par semaine, puis quotidiennement à partir de 7 jours avant l'expiration.

Note Dans certaines circonstances, le remplacement de vos certificats de signature STS peut modifier la durée des certificats. Lors du remplacement des certificats, soyez attentif aux dates d'émission et d'expiration.

Renouvellement automatique de certificat STS

À partir de vSphere 8.0, vCenter Single Sign-On renouvelle automatiquement un certificat de signature STS généré par VMCA. Le renouvellement automatique se produit avant l'expiration du certificat de signature STS et avant le déclenchement de l'alarme d'expiration de 90 jours. Si le renouvellement automatique échoue, vCenter Single Sign-On crée un message d'erreur dans le fichier journal. Si nécessaire, vous pouvez actualiser manuellement le certificat de signature STS.

Note vCenter Single Sign-On n'effectue pas de renouvellement automatique des certificats de signature STS personnalisés ou tiers.

Actualisation ou importation et remplacement des certificats STS

À partir de la version 8.0, l'actualisation ou l'importation et le remplacement des certificats de signature STS ne nécessitent pas le redémarrage de vCenter Server, évitant ainsi toute interruption de service. En outre, dans une configuration liée, l'actualisation ou l'importation et le remplacement des certificats de signature STS sur un seul vCenter Server met à jour les certificats STS sur tous les systèmes vCenter Server liés.

Note Dans certaines circonstances, une actualisation ou une importation et un remplacement de certificats de signature STS peuvent nécessiter le redémarrage manuel des systèmes vCenter Server.

Actualiser un certificat STS vCenter Server à l'aide de vSphere Client

Vous pouvez actualiser vos certificats de signature STS vCenter Server à l'aide de vSphere Client. Le VMware Certificate Authority (VMCA) émet un nouveau certificat et remplace le certificat actuel.

Lorsque vous actualisez les certificats de signature STS, VMware Certificate Authority (VMCA) émet un nouveau certificat et remplace le certificat actuel dans VMware Directory Service (vmdir). STS commence à utiliser le nouveau certificat pour émettre de nouveaux jetons. Dans une configuration Enhanced Linked Mode, vmdir charge le nouveau certificat du système vCenter Server émetteur vers tous les systèmes vCenter Server liés. Lorsque vous actualisez les certificats de signature STS, vous n'avez pas besoin de redémarrer le système vCenter Server ni tout autre système vCenter Server faisant partie d'une configuration Enhanced Linked Mode.

Si vous utilisez un certificat de signature STS généré personnalisé ou tiers, l'actualisation remplace ce certificat par un certificat émis par VMCA. Pour mettre à jour des certificats de signature STS générés personnalisés ou tiers, utilisez l'option Importer et remplacer. Reportez-vous à la section Importer et remplacer un certificat STS de vCenter Server à l'aide de vSphere Client.

Le certificat de signature STS émis par VMCA est valable 10 ans et n'est pas un certificat externe. Ne remplacez pas ce certificat, sauf si la stratégie de sécurité de votre entreprise l'exige.

Conditions préalables

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, il vous faut également fournir les informations d'identification de vCenter Single Sign-On pour un utilisateur possédant des privilèges d'administration sur le système vCenter Server.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Certificats**, cliquez sur **Gestion des certificats**.
4. Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.
5. Sous **Certificat de signature STS**, cliquez sur **Actions > Actualiser avec le certificat vCenter**.

   Si vous utilisez un certificat de signature STS généré personnalisé ou tiers, l'action d'actualisation remplace ce certificat par un certificat généré par VMCA.

   Note Si vous utilisiez des certificats tiers pour des raisons de conformité, l'actualisation risque de rendre vos systèmes vCenter Server non conformes. En outre, si vous utilisez un certificat de signature STS généré personnalisé ou tiers, le service de jetons de sécurité n'utilise plus ce certificat personnalisé ou tiers pour la signature de jeton.
6. Cliquez sur **Actualiser**.

   VMCA actualise le certificat de signature STS sur ce système vCenter Server et sur tous les systèmes vCenter Server liés.
7. (Facultatif) Si le bouton **Forcer l'actualisation** s'affiche, vCenter Single Sign-On a détecté un problème. Avant de cliquer sur **Forcer l'actualisation**, tenez compte des résultats potentiels suivants.
   - Si tous les systèmes vCenter Server affectés n'exécutent pas au moins vSphere 7.0 Update 3, ils ne prennent pas en charge l'actualisation des certificats.

- Si vous sélectionnez **Forcer l'actualisation**, vous devez redémarrer tous les systèmes vCenter Server. Ces systèmes peuvent devenir non opérationnels tant que vous ne le faites pas.

a Si vous n'êtes pas sûr de l'impact, cliquez sur **Annuler** et effectuez des recherches sur votre environnement.

b Si vous êtes sûr de l'impact, cliquez sur **Forcer l'actualisation** pour procéder à l'actualisation, puis redémarrez manuellement vos systèmes vCenter Server.

Importer et remplacer un certificat STS de vCenter Server à l'aide de vSphere Client

Vous pouvez importer et remplacer le certificat STS de vCenter Server par un certificat généré personnalisé ou tiers à l'aide de vSphere Client.

Pour importer et remplacer le certificat de signature STS par défaut, vous devez d'abord générer un nouveau certificat. Lorsque vous importez et remplacez des certificats de signature STS, VMware Directory Service (vmdir) charge le nouveau certificat à partir du système vCenter Server émetteur vers tous les systèmes vCenter Server liés.

Le certificat STS n'est pas un certificat externe. Ne remplacez pas ce certificat, sauf si la stratégie de sécurité de votre entreprise l'exige.

Conditions préalables

Pour la gestion des certificats, vous devez fournir le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut). Vous devez également fournir les informations d'identification de vCenter Single Sign-On pour un utilisateur disposant des privilèges d'administrateur sur le système vCenter Server.

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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 gestion de certificat.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Certificats**, cliquez sur **Gestion des certificats**.

4 Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.

5 Sous **Certificat de signature STS**, cliquez sur **Actions > Importer et remplacer**.

6 Sélectionnez le fichier PEM.

Le fichier PEM inclut la chaîne de certificat de signature et la clé privée.

7 Cliquez sur **Remplacer**.

Le certificat de signature STS est remplacé sur ce système vCenter Server et sur tous les systèmes vCenter Server liés. Sauf indication contraire, vous n'avez pas besoin de redémarrer les systèmes vCenter Server.

Remplacer un certificat STS vCenter Server à l'aide de la ligne de commande

Vous pouvez remplacer le certificat STS vCenter Server par un certificat généré personnalisé ou tiers à l'aide de l'interface de ligne de commande.

Pour utiliser un certificat requis par une société ou pour actualiser un certificat proche de l'expiration, vous pouvez remplacer le certificat de signature STS existant. Pour remplacer le certificat de signature STS par défaut, vous devez d'abord générer un nouveau certificat.

Le certificat STS n'est pas un certificat externe. Ne remplacez pas ce certificat, sauf si la stratégie de sécurité de votre entreprise l'exige.

Attention Vous devez utiliser les procédures décrites ici. Ne remplacez pas le certificat directement dans le système de fichiers.

Conditions préalables

Activez la connexion SSH à vCenter Server. Reportez-vous à la section Gérer vCenter Server à l'aide du shell de vCenter Server.

Procédure

1 Connectez-vous au shell vCenter Server en tant qu'utilisateur racine.

2 Créez un certificat.

a 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/newsts
```

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

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

c À l'aide d'un éditeur de ligne de commande tel que VIM, ouvrez votre copie du fichier `certool.cfg` et modifiez-la afin d'utiliser l'adresse IP locale et le nom d'hôte de l'instance de vCenter Server. 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
```

d Générez la clé.

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

e 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
```

f Créez un fichier PEM avec la chaîne de certificats et la clé privée.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 Mettez à jour le certificat de signature STS, par exemple :

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

VMCA actualise le certificat de signature STS sur ce système vCenter Server et sur tous les systèmes vCenter Server liés.

Afficher la chaîne de certificats de signature STS vCenter Server active à l'aide de vSphere Client

Vous pouvez utiliser vSphere Client pour afficher la chaîne de certificats de signature STS vCenter Server active.

Vous pouvez afficher les informations suivantes sur le certificat STS actif.

- Date « Valide jusqu'au »

- Une coche verte pour un certificat valide et une coche d'avertissement orange pour un certificat ayant expiré
- Un lien **Afficher les détails** pour afficher la chaîne de certificats active

Procédure

1. Connectez-vous avec vSphere Client à l'instance de vCenter Server.
2. Entrez le nom d'utilisateur et le mot de passe d'un utilisateur ayant au minimum des privilèges de lecture.
3. Accédez à l'interface utilisateur de gestion de certificat.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Certificats**, cliquez sur **Gestion des certificats**.
4. Si le système vous y invite, entrez les informations d'identification de votre instance de vCenter Server.
5. Pour afficher les détails du certificat STS actif, cliquez sur **Afficher les détails**.

Déterminer la date d'expiration d'un certificat SSL LDAPS à l'aide de la ligne de commande

Lors de l'utilisation d'Active Directory sur LDAPS, vous pouvez télécharger un certificat SSL pour le trafic LDAP. Les certificats SSL expirent après une durée de vie prédéfinie. Vous pouvez utiliser la commande `sso-config.sh` pour afficher la date d'expiration du certificat pour savoir s'il convient de remplacer ou de renouveler le certificat avant son expiration.

vCenter Server vous alerte lorsqu'un certificat SSL LDAP actif est proche de sa date d'expiration.

Les informations d'expiration des certificats s'affichent uniquement si vous utilisez Active Directory sur LDAP ou une source d'identité OpenLDAP et que vous spécifiez une URL `ldaps://` pour le serveur.

Conditions préalables

Activez la connexion SSH à vCenter Server. Reportez-vous à la section Gérer vCenter Server à l'aide du shell de vCenter Server.

Procédure

1. Connectez-vous à l'instance de vCenter Server en tant qu'utilisateur racine.
2. Exécutez la commande suivante.

   ```
   /opt/vmware/bin/sso-config.sh -get_identity_sources
   ```

   Ignorez les messages SLF4J.
3. Pour déterminer la date d'expiration, affichez les détails du certificat SSL et vérifiez le champ `NotAfter`.

Gestion des stratégies vCenter Single Sign-On

Les stratégies de vCenter Single Sign-On appliquent les règles de sécurité pour les comptes locaux et les jetons en général. 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 détermine le format de mot de passe et l'expiration de mot de passe. 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 compte d'utilisateur intégrés à vCenter Single Sign-On expirent après 90 jours. vSphere Client vous envoie un rappel lorsque votre mot de passe est sur le point d'expirer.

Reportez-vous à la section Changer le mot de passe de vCenter Single Sign-On .

Note Le compte d'administrateur (administrator@vsphere.local) n'est pas verrouillé et son mot de passe n'expire pas. Une bonne pratique de sécurité consiste à auditer les connexions de ce compte et à renouveler le mot de passe régulièrement.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Configuration**.
4. Cliquez sur l'onglet **Comptes locaux**.
5. Cliquez sur **Modifier** pour la ligne **Stratégie de mot de passe**.
6. Modifiez 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. Le nombre maximal de jours que vous pouvez entrer est 999 999 999. Une valeur zéro (0) signifie que le mot de passe n'expire jamais.

Option	Description
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 ■ Adjacents identiques : le nombre doit être supérieur à 0. Par exemple, si vous entrez 1, le mot de passe suivant n'est pas autorisé : p@$$word. Le nombre minimal de caractères alphabétiques ne doit pas être inférieur aux caractères combinés de lettres majuscules et minuscules. 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.

7 Cliquez sur **Enregistrer**.

Modifier la stratégie de verrouillage de vCenter Single Sign-On

Si un utilisateur tente de se connecter avec des informations d'identification incorrectes, une stratégie de verrouillage vCenter Single Sign-On précise quand le compte vCenter Single Sign-On de l'utilisateur est verrouillé. 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.

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

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Configuration**.

4 Cliquez sur l'onglet **Comptes locaux**.

5 Cliquez sur **Modifier** pour la ligne **Stratégie de verrouillage**.

   Vous devrez éventuellement effectuer un défilement vers le bas pour voir la ligne **Stratégie de verrouillage**.

6 Modifiez les paramètres.

Option	Description
Description	Description facultative de la stratégie de verrouillage.
Nombre maximal de tentatives de connexion infructueuses	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 **Enregistrer**.

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 Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Configuration**.

4 Cliquez sur l'onglet **Comptes locaux**.

5 Cliquez sur **Modifier** pour la ligne **Fiabilité des jetons**.

   Vous devrez éventuellement effectuer un défilement vers le bas pour voir la ligne **Fiabilité des jetons**.

6 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 maximal 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 maximal 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.

7 Cliquez sur **Enregistrer**.

Modifier la notification d'expiration du mot de passe pour les utilisateurs Active Directory (authentification Windows intégrée)

La notification d'expiration du mot de passe Active Directory est distincte de l'expiration du mot de passe SSO de vCenter Server. La notification de l'expiration du mot de passe par défaut pour un utilisateur Active Directory est de 30 jours, mais le délai d'expiration de mot de passe réel

dépend du système Active Directory. Le vSphere Client contrôle la notification d'expiration. Vous pouvez modifier la notification d'expiration par défaut afin de respecter les normes de sécurité de votre entreprise.

Conditions préalables

- Activez la connexion SSH à vCenter Server. Reportez-vous à la section Gérer vCenter Server à l'aide du shell de vCenter Server.

Procédure

1. Connectez-vous au shell de vCenter Server en tant qu'utilisateur disposant des privilèges d'administrateur.

   L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

2. Modifiez le répertoire et accédez à l'emplacement du fichier vSphere Client `webclient.properties`.

   ```
   cd /etc/vmware/vsphere-ui
   ```

3. Ouvrez le fichier `webclient.properties` à l'aide d'un éditeur de texte.

4. Modifiez la variable suivante.

   ```
   sso.pending.password.expiration.notification.days = 30
   ```

5. Redémarrez vSphere Client.

   ```
   service-control --stop vsphere-ui
   service-control --start vsphere-ui
   ```

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 Client.

vSphere Client présente une vue des utilisateurs et des groupes de votre domaine vSphere (vsphere.local par défaut). À partir de cette vue, vous pouvez ajouter, modifier et désactiver des utilisateurs. Vous pouvez également ajouter des groupes et gérer l'appartenance à un groupe.

Ajouter des utilisateurs vCenter Single Sign-On

Les utilisateurs répertoriés dans l'onglet **Utilisateurs** de vSphere 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. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4. Si vsphere.local n'est pas le domaine actuellement sélectionné, sélectionnez-le dans le menu déroulant.

   Vous ne pouvez pas ajouter des utilisateurs aux autres domaines.
5. Sous l'onglet **Utilisateurs**, cliquez sur **Ajouter**.
6. Entrez un nom d'utilisateur et un mot de passe pour le nouvel utilisateur.

   Le nombre maximal de caractères autorisés pour le nom d'utilisateur est de 300.

   Vous ne pouvez pas modifier le nom d'utilisateur après sa création. Le mot de passe doit répondre aux exigences des stratégies de mot de passe du système.
7. (Facultatif) Entrez le prénom et le nom du nouvel utilisateur.
8. (Facultatif) Entrez une adresse e-mail et une description pour l'utilisateur.
9. Cliquez sur **Ajouter**.

Résultats

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

Étape suivante

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 la section Ajouter des membres à un groupe vCenter Single Sign-On.

Désactiver et activer les utilisateurs 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 sur la page vCenter Server **Utilisateurs et groupes**.

Conditions préalables

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

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4. Sélectionnez un nom d'utilisateur, puis cliquez sur **Plus** et sur **Désactiver**.
5. Cliquez sur **OK**.
6. Pour activer à nouveau l'utilisateur, cliquez sur **Plus**, cliquez sur **Activer**, puis cliquez sur **OK**.

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.

Attention 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. Connectez-vous avec vSphere Client à l'instance 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.
   a Dans le menu **Accueil**, sélectionnez **Administration**.
   b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4 Sélectionnez l'option **Utilisateurs**, puis sélectionnez le domaine vsphere.local dans le menu déroulant.
5 Dans la liste des utilisateurs, sélectionnez celui que vous souhaitez supprimer.
6 Cliquez sur **Supprimer**.

   Soyez prudent lorsque vous effectuez cette opération, car elle est irréversible.
7 Cliquez sur **Supprimer**.

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 Client. Connectez-vous en tant qu'administrator@vsphere.local et dans le menu **Administration**, sélectionnez **Configuration > Comptes locaux > Stratégie de mot de passe**.

Voir aussi Modifier la stratégie de mot de passe de vCenter Single Sign-On.

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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.
   a Dans le menu **Accueil**, sélectionnez **Administration**.
   b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4 Cliquez sur **Utilisateurs**.
5 Sélectionnez l'utilisateur et cliquez sur **Modifier**.

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 stratégies de mot de passe du système.

7 Cliquez sur **Enregistrer**.

Ajouter un groupe vCenter Single Sign-On

L'onglet Groupes de vCenter Single Sign-On 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 Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.

4 Sélectionnez l'option **Groupes**, puis cliquez sur **Ajouter**.

5 Entrez le nom et la description du groupe.

   Le nombre maximal de caractères autorisés pour le nom de groupe est de 300. Vous ne pouvez pas modifier le nom du groupe après l'avoir créé.

6 Dans le menu déroulant **Ajouter des membres**, sélectionnez la source d'identité qui contient le membre à ajouter au groupe.

   Si vous avez configuré un fournisseur d'identité externe tel qu'AD FS, le domaine de ce fournisseur d'identité peut être sélectionné dans le menu déroulant **Ajouter des membres**.

7 Entrez un terme à rechercher.

8 Sélectionnez le membre.

   Vous pouvez ajouter plusieurs membres.

9 Cliquez sur **Ajouter**.

Étape suivante

Reportez-vous à la section Ajouter des membres à un groupe vCenter Single Sign-On.

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 Client.

Pour des informations générales, consultez l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2095342.

Les groupes répertoriés dans l'onglet **Groupes** de l'interface Web appartiennent au domaine vsphere.local. Reportez-vous à la section Groupes du domaine vCenter Single Sign-On.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4. Cliquez sur **Groupes** et cliquez sur le groupe (par exemple, Administrateurs).
5. Dans le menu déroulant **Ajouter des membres**, sélectionnez la source d'identité qui contient le membre à ajouter au groupe.

   Si vous avez configuré un fournisseur d'identité externe tel qu'AD FS, le domaine de ce fournisseur d'identité peut être sélectionné dans le menu déroulant **Ajouter des membres**.
6. Entrez un terme à rechercher.
7. Sélectionnez le membre.

   Vous pouvez ajouter plusieurs membres.
8. Cliquez sur **Enregistrer**.

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

Vous pouvez supprimer des membres d'un groupe vCenter Single Sign-On à l'aide de vSphere Client. Lorsque vous supprimez un membre (utilisateur ou groupe) d'un groupe, vous ne devez pas supprimer le membre du système.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
4. Sélectionnez **Groupes** et cliquez sur un groupe.
5. Dans la liste des membres du groupe, sélectionnez l'utilisateur ou le groupe à supprimer et cliquez sur l'icône représentant trois points verticaux.
6. Cliquez sur **Supprimer un membre**.
7. Cliquez sur **Supprimer**.

Résultats

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

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 de vSphere Client. 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.

Note Vous pouvez modifier un mot de passe uniquement s'il n'a pas expiré.

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. Connectez-vous avec vSphere Client à l'instance 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, cliquez sur votre nom d'utilisateur pour dérouler le menu, puis sélectionnez l'option **Modifier le mot de passe**.

4 Entrez votre mot de passe actuel.

5 Entrez 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 **Confirmer**.

   Vous pouvez également sélectionner **Single Sign-On > Utilisateurs et groupes**, puis sélectionnez l'utilisateur et cliquez sur **Modifier**.

Comprendre les autres options d'authentification vSphere

Dans vSphere 7.0 et versions ultérieures, la fédération de fournisseurs d'identité externes est la méthode d'authentification recommandée pour vCenter Server. Vous pouvez également vous authentifier en utilisant l'authentification de session Windows (SSPI), une carte à puce (carte d'accès commun ou CAC basée sur UPN) ou 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.

Fédération de fournisseurs d'identité externe

Avec la fédération de fournisseurs d'identité externe, vous pouvez utiliser les mécanismes d'authentification pris en charge par le fournisseur d'identité externe, notamment l'authentification à plusieurs facteurs.

Authentification par carte à puce

L'authentification par carte à puce permet un accès uniquement aux utilisateurs qui attachent un lecteur de carte physique à 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 vCenter Server 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.

Note 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 de vCenter Server

Les administrateurs peuvent configurer une méthode d'authentification autre que la méthode par défaut à partir de vSphere Client 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 vSphere Client ou à l'aide de `sso-config`. La configuration inclut l'activation de l'authentification par carte à puce et la configuration de stratégies de révocation des certificats.
- 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 vSphere Client. Cependant, si vous activez l'authentification RSA SecurID, cette méthode d'authentification figure dans vSphere Client.

Combinaison des méthodes d'authentification de vCenter Server

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.

Note Dans vSphere 7.0 Update 2, vous pouvez activer FIPS sur vCenter Server. Consultez la documentation de *Sécurité vSphere*. Les méthodes d'authentification RSA SecureID et CAC ne sont pas prises en charge lorsque FIPS est activé. Utilisez la fédération de fournisseurs d'identité externe pour l'authentification MFA. Reportez-vous à la section Configuration de la Fédération de fournisseurs d'identité vCenter Server.

Les utilisateurs qui se connectent à un système vCenter Server sont invités à s'authentifier avec une combinaison de carte à puce et de code PIN, de la façon suivante.

1. Lorsqu'un utilisateur insère la carte à puce dans le lecteur de carte à puce, le navigateur lit les certificats présents sur la carte.
2. Le navigateur 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 présent sur la carte à puce est connu. Si la vérification de révocation est activée, vCenter Single Sign-On vérifie également si le certificat est révoqué.
4. Si le certificat est connu par vCenter Single Sign-On et s'il n'est pas révoqué, l'utilisateur est authentifié et peut effectuer des tâches pour lesquelles il détient les autorisations.

Note 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 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 vCenter Server.

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 à partir de vSphere Client.

La configuration de l'authentification par carte à puce implique d'abord la configuration du proxy inverse, puis l'activation et la configuration de l'authentification par carte à puce en elle-même. Vous pouvez utiliser l'utilitaire `sso-config` pour gérer l'authentification par carte à puce.

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 vCenter Server.

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

La configuration utilise le port 3128, qui est défini et ouvert automatiquement.

Conditions préalables

Copiez les certificats de l'autorité de certification (CA) dans le système vCenter Server.

Note vCenter Server 7.0 prend en charge le protocole HTTP/2. Tous les navigateurs et toutes les applications modernes, y compris vSphere Client, se connectent à vCenter Server à l'aide de HTTP/2. Toutefois, l'authentification par carte à puce nécessite l'utilisation du protocole HTTP/1.1. L'activation de l'authentification par carte à puce désactive la négociation de protocole de couche application (ALPN, https://tools.ietf.org/html/rfc7301) pour HTTP/2, ce qui empêche efficacement le navigateur d'utiliser HTTP/2. Les applications qui utilisent uniquement HTTP/2, sans compter sur ALPN, continuent de fonctionner.

Procédure

1. Connectez-vous à l'interpréteur de commande vCenter Server en tant qu'utilisateur racine.
2. Créez un magasin d'autorités de certification de client approuvé.

   Ce magasin contient les certificats approuvés émis par l'autorité de certification 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 vCenter Server.

   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 `/etc/vmware-rhttpproxy/config.xml` qui inclut la définition du proxy inverse et ouvrez le fichier `config.xml` dans un éditeur.
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 certains de ces éléments. Supprimez les commentaires, effectuez une mise à jour ou ajoutez les éléments selon vos besoins.

5 Redémarrez le service STS.

```
service-control --restart sts
```

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.

Vous trouverez le script `sso-config` à l'emplacement suivant :

```
/opt/vmware/bin/sso-config.sh
```

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 vCenter Server 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 vCenter Server. La commande suivante active l'authentification par nom d'utilisateur et mot de passe :

```
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.

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

Conditions préalables

- 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 étendue de la clé, sinon le navigateur n'affiche pas le certificat.

- 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.
- Assurez-vous d'avoir configuré le proxy inverse et redémarré la machine physique ou virtuelle.

Procédure

1. Obtenez les certificats et copiez-les dans un dossier que l'utilitaire `sso-config` peut voir.
   a. Connectez-vous à la console du dispositif, soit directement soit à l'aide de SSH.
   b. Activez le shell 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 vCenter Server.
   d. Éventuellement, désactivez le shell de la façon suivante.

   ```
   chsh -s "/bin/appliancesh" root
   ```

2. Pour activer l'authentification par carte à puce, exécutez la commande suivante.

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

   Par exemple :

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

   Séparez les certificats par des virgules, mais n'insérez pas d'espace après la virgule.

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

   ```
   sso-config.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 verte des stratégies de certificat, exécutez la commande suivante.

   ```
   sso-config.sh -set_authn_policy -certPolicies policies
   ```

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

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

Cette liste verte spécifie les ID d'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.sh  -set_authn_policy -t tenantName  -useOcsp true
```

b Si le lien du répondeur OCSP n'est pas fourni par 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 pour chaque site vCenter Single Sign-On. Vous pouvez spécifier plusieurs répondeurs OCSP de remplacement pour votre site vCenter Single Sign-On pour permettre le basculement.

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

Note 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.

Prenez l'exemple suivant.

```
 .sso-config.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 responder 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.sh -t tenantName -get_alt_ocsp]
```

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

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

Utiliser vSphere Client 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 vSphere Client.

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 vCenter Server. La commande suivante active l'authentification par nom d'utilisateur et mot de passe :

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

Conditions préalables

- 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 étendue de la clé, sinon le navigateur n'affiche pas le certificat.
- 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.

- Assurez-vous d'avoir configuré le proxy inverse et redémarré la machine physique ou virtuelle.

Procédure

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

   a Connectez-vous à la console vCenter Server, soit directement soit à l'aide de SSH.

   b Désactivez le shell comme suit.

```
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 répertoire `/usr/lib/vmware-sso/vmware-sts/conf` sur vCenter Server.

   d Éventuellement, désactivez le shell du dispositif de la façon suivante.

```
chsh -s "/bin/appliancesh" root
```

2 Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Configuration**.

5 Dans l'onglet **Fournisseur d'identité**, cliquez sur **Authentification par carte à puce**, puis sur **Modifier**.

6 Sélectionnez ou désélectionnez les méthodes d'authentification et cliquez sur **Enregistrer**.

   Vous pouvez choisir l'authentification par carte à puce uniquement ou l'authentification par carte à puce et mot de passe et l'authentification de session Windows.

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

   La liste **Certificats d'autorité de certification approuvés** s'affiche.

7 Sous l'onglet **Certificats d'autorité de certification approuvés**, cliquez sur **Ajouter** et sur **Parcourir**.

8 Sélectionnez tous les certificats provenant d'autorités de certification approuvées, puis cliquez sur **Ajouter**.

Étape suivante

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 vCenter Server 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 la section Utiliser la ligne de commande pour gérer l'authentification par carte à puce.

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 vSphere Client 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 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 dépend de la configuration de 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 **Liste de révocation de certificats 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. Si l'extension de l'accès aux informations de l'autorité est absente du certificat ou si vous souhaitez la remplacer, vous pouvez spécifier explicitement un emplacement.

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 de certificats à partir du certificat** 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.

Conditions préalables

- 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 étendue de la clé, sinon le navigateur n'affiche pas le certificat.
- Vérifiez que le certificat vCenter Server est approuvé par le poste 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.

Procédure

1. Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Configuration**.

4 Sous l'onglet **Fournisseur d'identité**, cliquez sur **Authentification par carte à puce**.

5 Cliquez sur **Révocation des certificats** et sur **Modifier** pour activer ou désactiver la vérification de la révocation.

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

Configurer l'authentification RSA SecurID

Vous pouvez configurer votre environnement pour exiger que les utilisateurs se connectent avec un jeton RSA SecurID. 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.

Note 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.

Conditions préalables

- 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 la section Ajouter ou modifier une source d'identité vCenter Single Sign-On.
- Vérifiez que le système RSA Authentication Manager peut résoudre le nom d'hôte de vCenter Server et que le système vCenter Server 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**. Pour trouver le fichier `sdconf.rec`, décompressez le fichier `AM_Config.zip` obtenu.
- Copiez le fichier `sdconf.rec` sur le nœud de vCenter Server.

Procédure

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

```
/opt/vmware/bin
```

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

```
sso-config.sh -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 d'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 -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 -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. (Pris en charge uniquement avec les sources d'identité Active Directory sur LDAP.)

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

```
sso-config.sh -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
```

Résultats

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

Note Utilisez le format de nom d'utilisateur ***userID@domainName*** ou ***userID@domain_upn_suffix***.

Gestion du message de connexion à la page de connexion de vSphere Client

Vous pouvez créer un message qui s'affiche sur la page de connexion de vSphere Client.

Vous pouvez définir un message, une clause de non-responsabilité ou des conditions générales. En outre, vous pouvez configurer le message afin d'exiger une validation avant de se connecter.

Gérer le message de connexion à la page de connexion de vSphere Client

Vous pouvez ajouter un message de connexion à la page de connexion vSphere Client. Vous pouvez également configurer un message de connexion personnalisé et fournir une case à cocher pour recueillir le consentement de l'utilisateur.

Procédure

1 Connectez-vous avec vSphere Client à l'instance 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.

   a Dans le menu **Accueil**, sélectionnez **Administration**.

   b Sous **Single Sign-On**, cliquez sur **Configuration**.

4 Cliquez sur l'onglet **Message de connexion**.

5 Cliquez sur **Modifier** et configurez le message de connexion.

Option	Description
Afficher le message de connexion	Sélectionnez l'option **Afficher le message de connexion** pour activer le message de connexion. Vous ne pouvez pas modifier le message de connexion, sauf si vous pouvez basculer sur ce commutateur.
Message de connexion	Titre du message. Par défaut, lorsque l'option **Case à cocher Consentement** est sélectionnée, le texte du message de connexion est `I agree to Terms and Conditions`. Vous devez remplacer `Terms and Conditions` par votre propre texte. Si **Consentement par case à cocher** est désactivé, `Login message` s'affiche, sur lequel vous saisissez votre message.
Case à cocher Consentement	Sélectionnez l'option **Case à cocher Consentement** pour exiger que l'utilisateur clique sur une case à cocher avant de se connecter. Vous pouvez également afficher un message sans case à cocher.
Détails du message de connexion	Message affiché pour l'utilisateur lorsqu'il clique sur le message de connexion, par exemple, le texte des conditions générales. Vous devez entrer des détails dans cette zone de texte.

6 Cliquez sur **Enregistrer**.

Meilleures pratiques de sécurité de vCenter Single Sign-On

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

L'infrastructure d'authentification vSphere améliore 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. Après 90 jours, le mot de passe expire, et vous ne pouvez plus vous connecter. Vérifiez l'expiration et actualisez les mots de passe régulièrement dans les délais impartis.

Configurer le protocole de temps réseau

Utilisez le protocole NTP (Network Time Protocol) afin de vous assurer 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.

Reportez-vous à la documentation *Sécurité vSphere* pour obtenir des instructions sur la configuration de la synchronisation de l'heure à l'aide du protocole NTP.

Dépannage de l'authentification de vCenter Server

5

Les rubriques suivantes fournissent un point de départ pour résoudre les problèmes d'authentification de vCenter Server. Recherchez des pointeurs supplémentaires dans ce centre de documentation et dans le système de base de connaissances VMware.

Ce chapitre contient les rubriques suivantes :

Détermination de la cause d'une erreur Lookup Service

Le programme d'installation de vCenter Single Sign-On affiche un message d'erreur relatif à vCenter Server ou à vSphere Client.

Problème

Les programmes d'installation de vCenter Server et 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. Recherchez le dernier message qui indique `Initializing registration provider...`

Message	Cause et solution
`java.net.ConnectException: Connection timed out: 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'un pare-feu ne bloque pas le port vCenter Single Sign-On (par défaut, 7444). Assurez-vous également que la machine sur laquelle est installé vCenter Single Sign-On dispose de capacités de CPU, d'E/S et de RAM suffisantes.
`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 de vCenter Single Sign-On daemon vmware-sso. Redémarrez le service. Si le redémarrage ne résout pas le problème, consultez la section Récupération du *Guide de dépannage de vSphere*.
`Unexpected status code: 404. SSO Server failed during initialization`	Redémarrez vCenter Single Sign-On. Si le redémarrage ne résout pas le problème, consultez la section Récupération du *Guide de dépannage de vSphere*.
L'erreur indiquée dans l'interface utilisateur commence par `Could not connect to vCenter Single Sign-On`	Vous pouvez également voir le code de retour `SslHandshakeFailed`. Cette erreur indique que l'adresse IP ou le nom de domaine complet qui assure la résolution vers l'hôte vCenter Single Sign-On n'est pas l'adresse que vous avez utilisée pendant l'installation de vCenter Single Sign-On. Dans `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>` où A était le nom de domaine complet que vous avez entré lors de l'installation de vCenter Single Sign-On et B et C sont des alternatives admissibles générées par le système. Corrigez la configuration pour utiliser le nom de domaine complet à droite du signe `!=` dans le fichier journal. Dans la plupart des cas, utilisez le nom de domaine complet 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 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).

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, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2070433. Par défaut, l'authentification Windows intégrée utilise le domaine racine de votre forêt Active Directory.

Si 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 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.

   Vérifiez que les informations d'enregistrement PTR pour le contrôleur de domaine correspondent au nom DNS du contrôleur. Lors de l'utilisation de vCenter Server, exécutez 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 adresse IP de contrôleur
...
```

```
# 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 du domaine Active Directory, puis rejoignez le domaine. Consultez la documentation de *Configuration de vCenter Server*.

4 Fermez toutes les sessions de navigateur connectées à vCenter Server 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 Client, une erreur indique que le compte est verrouillé.

Problème

Après plusieurs tentatives infructueuses, vous ne parvenez pas à vous connecter à vSphere 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 du temps

Si votre environnement comprend plusieurs instances de vCenter Server connectées en mode Enhanced Linked Mode et si l'une des instances de vCenter Server devient indisponible, votre environnement continue à fonctionner. Lorsque le vCenter Server devient à nouveau disponible, les données de l'utilisateur et les autres informations sont généralement répliquées dans les 30 secondes avec des partenaires connectés en mode Enhanced Linked Mode. Dans certains cas, cependant, la réplication peut prendre du temps.

Problème

Dans certaines situations, par exemple lorsque votre environnement comprend plusieurs instances de vCenter Server en différents lieux, et que vous apportez des modifications significatives pendant qu'une instance de vCenter Server 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 vCenter Server disponible dans l'autre instance tant que la réplication n'est pas terminée. La réplication peut prendre un certain temps, selon votre topologie Enhanced Linked Mode.

Cause

Pendant le fonctionnement normal, les modifications apportées à une instance du service d'annuaire VMware (vmdir) dans une instance de vCenter Server (nœud) s'affichent dans son partenaire de réplication direct approximativement dans les 30 secondes. 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 vCenter Server

Vous pouvez exporter un bundle de support qui contient les fichiers journaux pour les services vCenter Server depuis vSphere Client ou à l'aide d'une API. Après l'exportation, vous pouvez explorer les journaux localement ou envoyer le bundle au support VMware.

Pour plus d'informations sur l'API, consultez *Guide de programmation de gestion de vCenter Server*.

Conditions préalables

Vérifiez que vCenter Server est déployé et en cours d'exécution.

Procédure

1. Dans un navigateur Web, connectez-vous à l'interface de gestion de la configuration de vCenter Server à l'adresse https://*platform_services_controller_ip*:5480.
2. Connectez-vous en tant qu'utilisateur racine pour l'instance de vCenter Server.
3. Dans le menu **Actions**, sélectionnez **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 des services d'authentification de vCenter Server

Les services d'authentification vCenter Server utilisent Syslog pour la journalisation. Vous pouvez examiner les fichiers de journaux afin de déterminer les causes des défaillances.

Tableau 5-1. Journaux des services d'authentification de vCenter Server

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`,