

Sécurité vSphere

Update 2

Modifié le 27 avril 2022

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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

Copyright © 2009-2022 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

À propos de la sécurité de vSphere 13

Informations mises à jour 15

1 Sécurité dans l'environnement vSphere 17

Sécurisation de l'hyperviseur ESXi 17

Sécurisation des systèmes vCenter Server et services associés 19

Sécurisation des machines virtuelles 21

Sécurisation de la couche de mise en réseau virtuelle 22

Mots de passe dans votre environnement vSphere 23

Meilleures pratiques en matière de sécurité et ressources de sécurité 25

2 Authentification vSphere à l'aide de vCenter Single Sign-On 27

Comprendre vCenter Single Sign-On 28

Protection de votre environnement par vCenter Single Sign-On 28

Composants vCenter Single Sign-On 31

Incidence de vCenter Single Sign-On sur l'installation 32

Incidence de vCenter Single Sign-On sur les mises à niveau 32

Utilisation de vCenter Single Sign-On avec vSphere 35

Groupes du domaine vsphere.local 38

Exigences de mots de passe et comportement de verrouillage de vCenter Server 39

Configuration des sources d'identité vCenter Single Sign-On 40

Sources d'identité pour vCenter Server avec vCenter Single Sign-On 41

Définir le domaine par défaut de vCenter Single Sign-On 43

Ajouter une source d'identité de vCenter Single Sign-On 44

Paramètres de source d'identité Active Directory 45

Paramètres de source d'identité du serveur LDAP Active Directory et du serveur OpenLDAP 47

Modifier une source d'identité de vCenter Single Sign-On 48

Supprimer une source d'identité vCenter Single Sign-On 49

Utiliser vCenter Single Sign-On avec l'authentification de session Windows 50

Authentification à deux facteurs de vCenter Server 50

Configuration de l'authentification par carte à puce pour vCenter Single Sign-On 52

Utiliser la ligne de commande pour configurer l'authentification par carte à puce 52

Utiliser l'interface Web de Platform Services Controller pour gérer l'authentification par carte à puce 56

Définir les stratégies de révocation pour l'authentification par carte à puce 59

Configurer l'authentification RSA SecurID 61

Gérer la page de connexion	64
Utilisation de vCenter Single Sign-On comme fournisseur d'identité pour un autre fournisseur de services	65
Ajouter un fournisseur de services SAML	65
STS (Security Token Service)	67
Générer un nouveau certificat de signature STS sur le dispositif	67
Générer un nouveau certificat de signature STS dans une installation vCenter Windows	69
Actualiser le certificat STS	70
Déterminer la date d'expiration d'un certificat LDAPS SSL	72
Gestion des stratégies vCenter Single Sign-On	73
Modifier la stratégie de mot de passe de vCenter Single Sign-On	73
Modifier la stratégie de verrouillage de vCenter Single Sign-On	74
Modifier la stratégie des jetons de vCenter Single Sign-On	75
Gestion des utilisateurs et des groupes vCenter Single Sign-On	76
Ajouter des utilisateurs vCenter Single Sign-On	77
Désactiver et activer des utilisateurs de vCenter Single Sign-On	78
Supprimer un utilisateur vCenter Single Sign-On	79
Modifier un utilisateur de vCenter Single Sign-On	79
Ajouter un groupe vCenter Single Sign-On	80
Ajouter des membres à un groupe vCenter Single Sign-On	81
Supprimer des membres d'un groupe vCenter Single Sign-On	81
Supprimer des utilisateurs de la solution vCenter Single Sign-On	82
Changer le mot de passe de vCenter Single Sign-On	83
Recommandations en matière de sécurité pour vCenter Single Sign-On	84
Dépannage de vCenter Single Sign-On	84
Détermination de la cause d'une erreur Lookup Service	84
Impossible de se connecter à l'aide de l'authentification de domaine Active Directory	86
La connexion à vCenter Server échoue, car le compte utilisateur est verrouillé	87
La réplication du service d'annuaire VMware peut prendre longtemps	88

3 Certificats de sécurité vSphere 90

Exigences en matière de certificats pour les différents chemins d'accès aux solutions	91
Présentation de la gestion de certificats	96
Présentation du remplacement des certificats	99
Où vSphere 6.0 utilise des certificats	102
VMCA et VMware Core Identity Services	104
Présentation du magasin de certificats VMware Endpoint	105
Gestion de la révocation de certificat	108
Remplacement des certificats dans les déploiements à grande échelle	108
Gestion de certificats avec l'interface Web Platform Services Controller	111
Explorer les magasins de certificats à partir de l'interface Web Platform Services Controller	112

Remplacer les certificats par de nouveaux certificats signés par VMCA depuis l'interface Web de Platform Services Controller	113
Faire de VMCA une autorité de certification intermédiaire depuis l'interface web de Platform Services Controller	115
Configurer votre système pour utiliser des certificats personnalisés depuis Platform Services Controller	117
Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés)	117
Ajouter un certificat racine approuvé au magasin de certificats	119
Ajouter des certificats personnalisés à partir de Platform Services Controller	120
Gestion de certificats avec l'utilitaire vSphere Certificate Manager	121
Restaurer la dernière opération effectuée via la republication des anciens certificats	123
Réinitialiser tous les certificats	123
Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats	123
Faire de VMCA une autorité de certification intermédiaire (Certificate Manager)	124
Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire)	124
Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats	126
Remplacer le certificat SSL machine par un certificat VMCA (autorité de certification intermédiaire)	128
Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA (autorité de certification intermédiaire)	129
Remplacer tous les certificats par des certificats personnalisés (Certificate Manager)	130
Générer des demandes de signature de certificat avec vSphere Certificate Manager (certificats personnalisés)	130
Remplacer le certificat SSL de machine par un certificat personnalisé	132
Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés	133
Remplacement manuel de certificats	135
Règles générales de démarrage et d'arrêt des services	135
Remplacer les certificats existants signés par l'autorité de certification VMware (VMCA) par de nouveaux certificats	135
Générer un nouveau certificat racine signé par VMCA	136
Remplacer les certificats SSL de la machine par des certificats signés par VMCA	138
Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA	142
Remplacer le certificat VMware Directory Service dans des environnement en mode mixte	149
Utiliser VMCA en tant qu'autorité de certificat intermédiaire	150
Remplacer le certificat racine (autorité de certification intermédiaire)	151
Remplacer les certificats SSL de la machine (autorité de certification intermédiaire)	154
Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire)	157
Remplacer le certificat de service d'annuaire VMware	163
Remplacer le certificat VMware Directory Service dans des environnement en mode mixte	164

Utiliser des certificats tiers avec vSphere	165
Demander des certificats et importer un certificat racine personnalisé	166
Remplacer les certificats SSL de machine par des certificats personnalisés	168
Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés	170
Remplacer le certificat de service d'annuaire VMware	172
Remplacer le certificat VMware Directory Service dans des environnement en mode mixte	173
Gestion des certificats et des services avec les commandes de l'interface de ligne de commande	174
Privilèges requis pour les opérations de gestion de certificats	175
Modification de la configuration de certtool	176
Référence des commandes d'initialisation de certtool	177
Référence des commandes de gestion certtool	181
Référence des commandes vecs-cli	183
Référence des commandes dir-cli	188
Afficher les certificats vCenter dans vSphere Web Client	194
Définir le seuil pour les avertissements d'expiration du certificat vCenter	195

4 Tâches de gestion des utilisateurs et des autorisations de vSphere 196

Présentation des autorisations dans vSphere	197
Présentation du modèle d'autorisation vCenter Server	198
Héritage hiérarchique des autorisations	200
Paramètres d'autorisation multiples	202
Exemple 1 : Héritage d'autorisations multiples	203
Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent	204
Exemple 3 : Rôle d'utilisateur supprimant un rôle de groupe	204
Gestion des autorisations des composants vCenter	205
Ajouter une autorisation à un objet d'inventaire	206
Changer des autorisations	207
Supprimer les autorisations	207
Changer les paramètres de validation d'autorisation	208
Autorisations globales	209
Ajouter une autorisation globale	209
Autorisations sur les objets de balise	210
Utilisation des rôles pour assigner des privilèges	212
Rôles système de vCenter Server	213
Créer un rôle personnalisé	214
Cloner un rôle	215
Éditer un rôle	216
Meilleures pratiques pour les rôles et les autorisations	216
Privilèges requis pour les tâches courantes	217

5 Sécurisation des hôtes ESXi 221

- Utiliser des scripts pour gérer des paramètres de configuration d'hôte 222
- Configurer des hôtes ESXi avec des profils d'hôte 223
- Recommandations générales de sécurité pour ESXi 224
 - Verrouillage des mots de passe et des comptes ESXi 226
 - Recommandations de sécurité pour la mise en réseau d'ESXi 228
 - Désactiver le Managed Object Browser (MOB) 228
 - Désactiver les clés autorisées (SSH) 229
- Gestion de certificats pour les hôtes ESXi 229
 - Mises à niveau d'hôtes et certificats 232
 - Paramètres par défaut des certificats ESXi 232
 - Afficher les informations d'expiration de certificat pour plusieurs hôtes ESXi 234
 - Afficher les détails de certificat pour un hôte ESXi spécifique 235
 - Renouveler ou actualiser des certificats ESXi 236
 - Modifier les paramètres par défaut de certificat 236
 - Présentation des changements de mode de certificat 237
 - Changer le mode de certificat 239
 - Remplacement de certificats et de clés SSL pour ESXi 240
 - Configuration requise pour les demandes de signature de certificat ESXi 241
 - Remplacer le certificat et la clé par défaut dans ESXi Shell 241
 - Remplacer un certificat et une clé par défaut à l'aide de la commande vifs 242
 - Remplacer un certificat par défaut à l'aide de HTTPS PUT 243
 - Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) 244
 - Utiliser des certificats personnalisés avec Auto Deploy 244
 - Restaurer les fichiers de certificat et de clé ESXi 246
- Personnalisation des hôtes avec le profil de sécurité 247
 - Configuration du pare-feu ESXi 247
 - Gérer les paramètres du pare-feu ESXi 248
 - Ajouter des adresses IP autorisées pour un hôte ESXi 249
 - Ports de pare-feu entrants et sortants pour les hôtes ESXi 250
 - Comportement du pare-feu client NFS 253
 - Commandes de pare-feu ESXCLI d'ESXi 254
 - Personnalisation des services ESXi à partir du profil de sécurité 255
 - Activer ou désactiver un service dans le profil de sécurité 256
 - Mode verrouillage 257
 - Comportement du mode de verrouillage 259
 - Activation du mode verrouillage à l'aide de vSphere Web Client 261
 - Désactiver le mode de verrouillage à l'aide de vSphere Web Client 262
 - Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe 263

Spécification des comptes disposant de privilèges d'accès en mode de verrouillage	263
Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB	265
Affectation d'autorisations pour ESXi	267
Privilèges de l'utilisateur racine	268
Privilèges vpxuser	269
Privilèges de l'utilisateur dcui	269
Utilisation d'Active Directory pour gérer des utilisateurs ESXi	269
Installer ou mettre à niveau vSphere Authentication Proxy	270
Configurer un hôte pour utiliser Active Directory	271
Ajouter un hôte à un domaine de service d'annuaire	273
Afficher les paramètres du service d'annuaire	273
Utiliser vSphere Authentication Proxy	274
Installer ou mettre à niveau vSphere Authentication Proxy	274
Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification	276
Configuration de vSphere Authentication Proxy	277
Exporter le certificat de vSphere Authentication Proxy	277
Importer un certificat de serveur proxy dans ESXi	278
Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine	279
Remplacer le certificat du serveur proxy d'authentification de l'hôte ESXi	279
Meilleures pratiques de sécurité de ESXi	280
Périphériques PCI et PCIe et ESXi	281
Configuration de l'authentification par carte à puce pour ESXi	282
Activer l'authentification par carte à puce	282
Désactiver l'authentification par carte à puce	283
Authentification d'informations d'identification d'utilisateur en cas de problèmes de connectivité	283
Utilisation de l'authentification par carte à puce en mode de verrouillage	284
Clés SSH ESXi	284
Sécurité SSH	285
Charger une clé SSH à l'aide d'une commande vifs	285
Charger une clé SSH à l'aide de HTTPS PUT	286
Utilisation du ESXi Shell	287
Utiliser vSphere Web Client pour activer l'accès à ESXi Shell	288
Créer un délai d'attente de disponibilité pour ESXi Shell dans vSphere Web Client	289
Créer un délai d'expiration pour les sessions ESXi Shell inactives dans vSphere Web Client	289
Utiliser l'interface utilisateur de la console directe (DCUI) pour activer l'accès au service ESXi Shell	290
Créer un délai d'attente de disponibilité pour ESXi Shell dans l'interface utilisateur de console directe	291
Créer un délai d'expiration pour des sessions ESXi Shell inactives	291
Connexion au ESXi Shell pour une opération de dépannage	292
Modifier les paramètres proxy Web ESXi	292

Considérations relatives à la sécurité dans vSphere Auto Deploy	293
Gestion des fichiers journaux ESXi	294
Configurer Syslog sur des hôtes ESXi	294
Emplacements des fichiers journaux ESXi	296
Trafic de la journalisation de la tolérance aux pannes	296

6 Sécurisation des systèmes vCenter Server 298

Meilleures pratiques de sécurité de vCenter Server	298
Meilleures pratiques pour le contrôle d'accès à vCenter Server	298
Configurer la stratégie de mot de passe de vCenter Server	300
Protection de l'hôte Windows vCenter Server	301
Suppression de certificats expirés ou révoqués et de journaux d'installations ayant échoué	301
Limitation de la connectivité réseau vCenter Server	302
Envisager la restriction d'utilisation de clients Linux	302
Vérifier les plug-in installés	303
Meilleures pratiques en matière de sécurité de vCenter Server Appliance	304
Vérifier les empreintes des hôtes ESXi hérités	304
Vérifier que la validation des certificats SSL sur Network File Copy est activée	305
Ports TCP et UDP pour vCenter Server	306
Accès à l'outil de surveillance du matériel basé sur la surveillance CIM	307

7 Sécurisation des machines virtuelles 309

Limiter les messages d'information entre les machines virtuelles et les fichiers VMX	309
Empêcher la réduction de disque virtuel	310
Recommandations en matière de sécurité des machines virtuelles	311
Protection générale d'une machine virtuelle	311
Utiliser des modèles pour déployer des machines virtuelles	312
Réduire l'utilisation de la console de machine virtuelle	313
Empêcher les machines virtuelles de récupérer les ressources	313
Désactiver les fonctions inutiles à l'intérieur des machines virtuelles	314
Supprimer les périphériques matériels inutiles	314
Désactiver les fonctionnalités d'affichage inutilisées	315
Désactiver les fonctions non exposées	316
Désactiver les transferts de fichiers HGFS	317
Désactiver les opérations Copier et Coller entre le système d'exploitation client et la console distante	317
Limitation de l'exposition des données sensibles copiées dans le presse-papiers	318
Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle	318
Interdiction pour les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques	319
Modification de la limite de mémoire variable du système d'exploitation invité	320

Empêcher les processus du système d'exploitation invité d'envoyer des messages de configuration à l'hôte 321

Éviter d'utiliser des disques indépendants non persistants 321

8 Sécurisation de la mise en réseau vSphere 323

Introduction à la sécurité du réseau vSphere 323

Sécurisation du réseau avec des pare-feu 325

Pare-feux pour configurations avec vCenter Server 326

Connexion à vCenter Server via un pare-feu 327

Pare-feu pour configurations sans vCenter Server 327

Connexion des hôtes ESXi via des pare-feu 327

Connexion à la console de la machine virtuelle via un pare-feu 328

Sécuriser le commutateur physique 329

Sécurisation des ports du commutateur standard à l'aide de stratégies de sécurité 329

Sécuriser les commutateurs standard vSphere 330

Modifications d'adresse MAC 331

Transmissions forgées 332

Fonctionnement en mode promiscuité 332

Sécuriser les commutateurs distribués vSphere et les groupes de ports distribués 332

Sécurisation des machines virtuelles avec des VLAN 334

Considérations relatives à la sécurité pour les VLAN 335

Sécuriser les VLAN 336

Créer une DMZ réseau sur un hôte ESXi 336

Création de plusieurs réseaux sur un hôte ESXi 338

Sécurité du protocole Internet 340

Liste des associations de sécurité disponibles 341

Ajouter une association de sécurité IPsec 341

Supprimer une association de sécurité IPsec 342

Répertorier les stratégies de sécurité IPsec disponibles 342

Créer une stratégie de sécurité IPSec 343

Supprimer une stratégie de sécurité IPsec 344

Garantir une configuration SNMP appropriée 344

Utiliser des commutateurs virtuels avec l'API vSphere Network Appliance, uniquement si nécessaire 345

Meilleures pratiques en matière de sécurité de la mise en réseau vSphere 345

Recommandations générales de sécurité pour la mise en réseau 346

Étiquetage de composants de mise en réseau 347

Documenter et vérifier l'environnement VLAN vSphere 348

Adoption de solides pratiques d'isolation de réseau 348

9 Meilleures pratiques concernant plusieurs composants vSphere 351

Synchronisation des horloges sur le réseau vSphere 351

Synchroniser les horloges ESXi avec un serveur de temps réseau	352
Configuration des paramètres de synchronisation horaire dans vCenter Server Appliance	352
Utiliser la synchronisation de l'heure de VMware Tools	353
Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server Appliance	353
Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP	354
Meilleures pratiques en matière de sécurité du stockage	355
Sécurisation du stockage iSCSI	355
Sécurisation des périphériques iSCSI	355
Protection d'un SAN iSCSI	356
Masquage et zonage des ressources SAN	357
Utilisation d'informations d'identification Kerberos pour NFS 4.1	357
Vérifier que l'envoi des données de performances de l'hôte aux invités est désactivé	358
Configuration de délais d'expiration pour ESXi Shell et vSphere Web Client	359
10 Gestion de la Configuration du protocole TLS avec l'utilitaire de reconfiguration de TLS	360
Ports prenant en charge la désactivation des versions TLS	360
Désactivation des versions de TLS dans vSphere	362
Installer l'utilitaire de configuration de TLS	363
Effectuer une sauvegarde manuelle facultative	364
Désactiver les versions TLS sur les systèmes vCenter Server	366
Désactiver les versions de TLS sur les hôtes ESXi	367
Désactiver les versions TLS sur les systèmes Platform Services Controller	368
Restaurer les modifications de l'utilitaire de configuration TLS	370
Désactiver les versions de TLS sur vSphere Update Manager	371
Désactiver les précédentes versions de TLS pour Update Manager, port 9087	372
Désactiver les précédentes versions de TLS pour le port 8084 d'Update Manager	373
Réactiver les versions de TLS désactivées pour le port 9087 du service Update Manager	374
Réactiver les versions de TLS désactivées pour le port 8084 du service Update Manager	374
11 Privilèges définis	376
Privilèges d'alarmes	377
Privilèges Auto Deploy et privilèges de profil d'image	378
Privilèges de certificats	380
Privilèges de bibliothèque de contenu	380
Privilèges de centre de données	383
Privilèges de banque de données	384
Privilèges de cluster de banques de données	385
Privilèges de Distributed Switch	385
Privilèges de gestionnaire d'agent ESX	386
Privilèges d'extension	387

Privilèges de dossier	387
Privilèges globaux	388
Privilèges CIM d'hôte	389
Privilèges de configuration d'hôte	389
Inventaire d'hôte	391
Privilèges d'opérations locales d'hôte	392
Privilèges de réplication d'hôte vSphere	393
Privilèges de profil d'hôte	393
Privilèges du fournisseur Inventory Service	393
Privilèges de balisage Inventory Service	394
Privilèges de réseau	395
Privilèges de performances	395
Privilèges d'autorisations	396
Privilèges de stockage basé sur le profil	396
Privilèges de ressources	397
Privilèges de tâche planifiée	398
Privilèges de sessions	398
Privilèges de vues de stockage	399
Privilèges de tâches	399
Privilèges Transfer Service	400
Privilèges de règle de VRM	400
Privilèges de configuration de machine virtuelle	400
Privilèges d'opérations d'invité de machine virtuelle	402
Privilèges d'interaction de machine virtuelle	403
Privilèges d'inventaire de machine virtuelle	415
Privilèges de provisionnement de machine virtuelle	416
Privilèges de configuration de services de machine virtuelle	418
Privilèges de gestion des snapshots d'une machine virtuelle	419
Privilèges vSphere Replication de machine virtuelle	419
Privilèges du groupe dvPort	420
Privilèges de vApp	421
Privilèges vServices	422

À propos de la sécurité de vSphere

Sécurité vSphere fournit des informations sur la sécurisation de votre environnement vSphere® pour VMware® vCenter® Server et VMware ESXi.

Pour vous aider à protéger votre environnement vSphere, cette documentation décrit les fonctionnalités de sécurité disponibles et les mesures à prendre pour protéger votre environnement des attaques.

Pour vous aider à protéger votre environnement vSphere, cette documentation décrit les fonctionnalités de sécurité disponibles et les mesures à prendre pour protéger votre environnement des attaques.

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

Rubriques	Points forts du contenu
Authentification avec vCenter Single Sign-On	<ul style="list-style-type: none">■ Fonctionnalités et services de vCenter Single Sign-On.■ Ajout et gestion des sources d'identité.■ Stratégies vCenter Single Sign-On.■ Utilisateurs et groupes.
Gestion des autorisations et des utilisateurs	<ul style="list-style-type: none">■ Modèle d'autorisations (rôles, groupes et objets).■ Création de rôles personnalisés.■ Définition des autorisations.■ Gestion des autorisations globales.
Gestion des certificats	<ul style="list-style-type: none">■ Gestion des certificats ESXi■ Gestion des certificats pour vCenter Server et services associés.<ul style="list-style-type: none">■ Gestion des certificats à l'aide de l'interface utilisateur.■ Gestion des certificats à l'aide de l'utilitaire Certificate Manager.■ Utilisation de la CLI pour la gestion manuelle des certificats (inclut des exemples).
Fonctionnalités relatives à la sécurité de l'hôte	<ul style="list-style-type: none">■ Mode de verrouillage et autres fonctionnalités de profil de sécurité.■ Authentification des hôtes par carte à puce.■ vSphere Authentication Proxy.

Tableau 1-1. Faits saillants sur *Sécurité vSphere* (suite)

Rubriques	Points forts du contenu
Meilleures pratiques en matière de sécurité et de sécurisation renforcée	<p>Meilleures pratiques et avis des experts en sécurité VMware.</p> <ul style="list-style-type: none"> ■ Sécurité de vCenter Server. ■ Sécurité de l'hôte. ■ Sécurité des machines virtuelles. ■ Sécurité de la mise en réseau.
Privilèges vSphere	Liste complète de tous les privilèges vSphere pris en charge dans cette version.

Documentation connexe

Outre ce document, VMware publie un *Guide de sécurisation renforcée* pour chaque version de vSphere. Ces guides sont disponibles à la page <http://www.vmware.com/security/hardening-guides.html>. Le *Guide de sécurisation renforcée* est une feuille de calcul comprenant des entrées pour différents problèmes potentiels de sécurité. Il offre des éléments pour trois profils de risque. Ce document *Sécurité vSphere* ne contient pas d'informations concernant le profil de risque 1 (environnement imposant une sécurité maximale, comme les installations gouvernementales top secrètes).

Public cible

Ces informations sont destinées aux administrateurs système Windows ou Linux expérimentés qui maîtrisent les technologies de machine virtuelle et les opérations de centre de données.

Informations mises à jour

Cette documentation relative à *Sécurité vSphere* est mise 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 *Sécurité vSphere*.

Révision	Description
27 avril 2022	■ Mise à jour mineure dans Privilèges de vues de stockage .
5 novembre 2021	■ Mise à jour mineure dans Meilleures pratiques de sécurité de ESXi . ■ Correction de Désactiver les versions de TLS sur les hôtes ESXi pour indiquer que vous êtes connecté à l'instance de vCenter Server.
14 août 2020	VMware prend l'intégration au sérieux. Pour encourager ce principe avec notre client, notre partenaire et notre communauté interne, nous remplaçons en partie la terminologie de notre contenu. Nous avons mis à jour ce guide pour supprimer des instances de langage non inclusif. ■ Mise à jour mineure dans Sécurisation des machines virtuelles .
4 octobre 2017	■ Mise à jour de la section Présentation des changements de mode de certificat pour indiquer qu'il est acceptable de passer les hôtes en mode de maintenance et de les déconnecter pour effectuer le basculement de mode. La suppression des hôtes n'est pas nécessaire.
FR-001949-07	■ Ajout d'une nouvelle rubrique, Exigences en matière de certificats pour les différents chemins d'accès aux solutions qui décrit en détail les exigences en matière de certificats. Suppression de l'ancienne rubrique, qui était moins détaillée. ■ Ajout du nouveau chapitre Chapitre 10 Gestion de la Configuration du protocole TLS avec l'utilitaire de reconfiguration de TLS .
FR-001949-06	■ Mise à jour de Utiliser la ligne de commande pour configurer l'authentification par carte à puce pour indiquer clairement que les espaces ne sont pas autorisés dans les listes séparées par des virgules des certificats. ■ Insertion de l'emplacement du script dans Utiliser la ligne de commande pour configurer l'authentification par carte à puce . ■ Clarification de la nécessité de la chaîne de certificats complète dans Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés . ■ Correction d'un problème dans l'introduction à Paramètres d'autorisation multiples .
FR-001949-05	■ Ajout d'informations pour la validation et la période de validation à Changer les paramètres de validation d'autorisation .
FR-001949-04	■ Correction d'erreur de nom de paramètre dans Vérifier que la validation des certificats SSL sur Network File Copy est activée . ■ Informations ajoutées sur l'emplacement de la commande <code>service-control</code> sous Windows dans Gestion des certificats et des services avec les commandes de l'interface de ligne de commande .

Révision	Description
FR-001949-03	<ul style="list-style-type: none"> ■ Ajout d'informations sur les autorisations de balise dans Autorisations sur les objets de balise. ■ Clarification de l'ordre de certificat dans Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire).
FR-001949-02	<ul style="list-style-type: none"> ■ Remarque sur la connexion avec vSphere Client ajoutée à Chapitre 2 Authentification vSphere à l'aide de vCenter Single Sign-On. ■ Clarification dans Paramètres de source d'identité Active Directory. Le système doit être joint à un nom Active Directory et le nom de domaine doit pouvoir être résolu par DNS.
FR-001949-01	<ul style="list-style-type: none"> ■ Correction de l'ordre des certificats dans Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine (autorité de certification intermédiaire). ■ Mis à jour Verrouillage des mots de passe et des comptes ESXi. Les phrases secrètes ne sont pas activées par défaut. ■ Étapes corrigées pour accéder à l'interpréteur de commandes dans Utiliser la ligne de commande pour configurer l'authentification par carte à puce. ■ Correction de Changer le mot de passe de vCenter Single Sign-On. Si votre mot de passe expire, vous devez contacter l'administrateur. ■ Mise à jour du script PowerCLI dans Utiliser des scripts pour gérer des paramètres de configuration d'hôte. ■ Informations mises à jour sur le nombre d'instances de vCenter Server dans Incidence de vCenter Single Sign-On sur l'installation. ■ Plusieurs mises à jour de Utiliser la ligne de commande pour configurer l'authentification par carte à puce, Utiliser l'interface Web de Platform Services Controller pour gérer l'authentification par carte à puce et Configurer l'authentification RSA SecurID. ■ Corrections dans Ports TCP et UDP pour vCenter Server. Par exemple les ports 903 et 5900-5964 sont utilisés sur l'hôte, pas sur le système vCenter Server et d'autres ports, comme le 9090, sont uniquement utilisés en interne. ■ Suppression d'informations concernant les clés DSA de Charger une clé SSH à l'aide d'une commande vifs. ■ Mise à jour de STS (Security Token Service) pour inclure la procédure pour générer un nouveau certificat de signature STS.
FR-001949-00	Version initiale.

Sécurité dans l'environnement vSphere

1

Les composants d'un environnement vSphere sont sécurisés d'origine par un nombre de fonctionnalités telles que les certificats, l'autorisation, un pare-feu sur chaque hôte ESXi, un accès limité, etc. Vous pouvez modifier la configuration par défaut de plusieurs manières, vous pouvez notamment définir des autorisations sur des objets vCenter, ouvrir des ports de pare-feu ou modifier les certificats par défaut. Ces interventions permettent de bénéficier d'une flexibilité maximale pour la sécurisation des systèmes vCenter Server, des hôtes ESXi et des machines virtuelles.

Une présentation à haut niveau de différents aspects de vSphere qui nécessitent une certaine attention vous aide à planifier votre stratégie de sécurité. Vous pouvez également tirer parti d'autres ressources de sécurité de vSphere sur le site Web VMware.

Ce chapitre contient les rubriques suivantes :

- [Sécurisation de l'hyperviseur ESXi](#)
- [Sécurisation des systèmes vCenter Server et services associés](#)
- [Sécurisation des machines virtuelles](#)
- [Sécurisation de la couche de mise en réseau virtuelle](#)
- [Mots de passe dans votre environnement vSphere](#)
- [Meilleures pratiques en matière de sécurité et ressources de sécurité](#)

Sécurisation de l'hyperviseur ESXi

L'hyperviseur ESXi est sécurisé par nature. Vous pouvez accroître la protection des hôtes ESXi en utilisant le mode de verrouillage et d'autres fonctionnalités intégrées. Si vous configurez un hôte de référence et apportez des modifications à tous les hôtes en fonction des profils d'hôte de cet hôte, ou si vous effectuez une gestion par scripts, vous renforcez la protection de votre environnement en veillant à ce que les modifications s'appliquent à tous les hôtes.

Utilisez les fonctionnalités suivantes (présentées en détail dans ce guide) pour renforcer la protection des hôtes ESXi gérés par vCenter Server. Reportez-vous également au livre blanc *Sécurité de VMware vSphere Hypervisor*.

Limiter l'accès à ESXi

Par défaut, les services ESXi Shell et SSH ne s'exécutent pas et seul l'utilisateur racine peut se connecter à l'interface utilisateur de la console directe (DCUI). Si vous décidez d'activer l'accès à ESXi ou SSH, vous pouvez définir des délais d'expiration pour limiter le risque d'accès non autorisé.

Les hôtes pouvant accéder à l'hôte ESXi doivent disposer d'autorisations de gestion de l'hôte. Ces autorisations se définissent sur l'objet hôte de vCenter Server qui gère l'hôte.

Utiliser des utilisateur nommés et le moindre privilège

Par défaut, l'utilisateur racine peut effectuer de nombreuses tâches. Au lieu d'autoriser les administrateurs à se connecter à l'hôte ESXi à l'aide du compte d'utilisateur racine, vous pouvez appliquer des privilèges de configuration de l'hôte différents à divers utilisateurs nommés à partir de l'interface de gestion des autorisations de vCenter Server. Vous pouvez créer des rôles personnalisés, attribuer des privilèges à un rôle et associer le rôle à un utilisateur nommé et à un objet hôte d'ESXi en utilisant vSphere Web Client.

Dans une configuration à hôte unique, vous gérez directement les utilisateurs. Consultez la documentation de *Administration de vSphere avec vSphere Client*.

Réduire le nombre de ports de pare-feu ESXi ouverts

Par défaut, les ports de pare-feu de votre hôte ESXi sont uniquement ouverts lorsque vous démarrez un service correspondant. Vous pouvez utiliser les commandes de vSphere Web Client, ESXCLI ou PowerCLI pour vérifier et gérer l'état des ports du pare-feu.

Reportez-vous à [Configuration du pare-feu ESXi](#).

Automatiser la gestion de l'hôte ESXi

Parce qu'il est souvent important que les différents hôtes d'un même centre de données soient synchronisés, utilisez l'installation basée sur scripts ou vSphere Auto Deploy pour provisionner les hôtes. Vous pouvez gérer les hôtes à l'aide de scripts. Les profils d'hôtes constituent une alternative à la gestion basée sur scripts. Vous configurez un hôte de référence, exportez le profil d'hôte et appliquez celui-ci à votre hôte. Vous pouvez appliquer le profil d'hôte directement ou dans le cadre du provisionnement avec Auto Deploy.

Consultez [Utiliser des scripts pour gérer des paramètres de configuration d'hôte](#) et *Installation et configuration de vSphere* pour plus d'informations sur vSphere Auto Deploy.

Exploiter le mode de verrouillage

En mode de verrouillage, les hôtes ESXi sont, par défaut, uniquement accessibles par le biais de vCenter Server. À partir de vSphere 6.0, vous avez le choix entre un mode de verrouillage strict et un mode de verrouillage normal. Vous pouvez également définir des utilisateurs exceptionnels pour permettre un accès direct aux comptes de service tels que les agents de sauvegarde.

Reportez-vous à [Mode verrouillage](#).

Vérifier l'intégrité du module VIB

Un niveau d'acceptation est associé à chaque module VIB. Vous pouvez ajouter un VIB à un hôte ESXi uniquement si son niveau d'acceptation est identique ou supérieur au niveau d'acceptation de l'hôte. Vous ne pouvez pas ajouter un VIB CommunitySupported ou PartnerSupported à un hôte à moins d'avoir explicitement modifié le niveau d'acceptation de l'hôte.

Reportez-vous à [Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB](#).

Gérer les certificats ESXi

Dans vSphere 6.0 et version ultérieure, l'autorité de certification VMware (VMCA) provisionne chaque hôte ESXi à l'aide d'un certificat signé dont l'autorité de certification racine par défaut est VMCA. Si la stratégie d'une entreprise l'exige, vous pouvez remplacer les certificats existants par des certificats signés par une autorité de certification tierce.

Reportez-vous à [Gestion de certificats pour les hôtes ESXi](#)

Authentification par carte à puce

À partir de vSphere 6.0, ESXi prend en charge l'option d'authentification par carte à puce plutôt que par nom d'utilisateur et mot de passe.

Reportez-vous à [Configuration de l'authentification par carte à puce pour ESXi](#).

Verrouillage de compte ESXi

À partir de vSphere 6.0, le verrouillage des comptes est pris en charge pour l'accès via SSH et vSphere Web Services SDK. L'interface de console directe (DCUI) et ESXi Shell ne prennent pas en charge le verrouillage de compte. Par défaut, un nombre maximal de dix tentatives de connexion échouées est autorisé avant le verrouillage du compte. Par défaut, le compte est déverrouillé au bout de deux minutes.

Reportez-vous à [Verrouillage des mots de passe et des comptes ESXi](#).

Les considérations de sécurité pour les hôtes autonomes sont identiques, bien que les tâches de gestion puissent différer. Consultez la documentation de *Administration de vSphere avec vSphere Client*.

Sécurisation des systèmes vCenter Server et services associés

Votre système vCenter Server et les services associés sont protégés par l'authentification via vCenter Single Sign-On, ainsi que par l'autorisation via le modèle d'autorisations vCenter Server. Vous pouvez modifier le comportement par défaut ou prendre des mesures supplémentaires pour protéger l'accès à votre environnement.

Lorsque vous protégez votre environnement vSphere, tenez compte du fait que tous les services associés aux instances de vCenter Server doivent être protégés. Dans certains environnements, vous pouvez protéger plusieurs instances de vCenter Server et une ou plusieurs instances de Platform Services Controller.

Renforcer toutes les machines hôtes vCenter

Pour protéger votre environnement vCenter, vous devez commencer par renforcer chaque machine qui exécute vCenter Server ou un service associé. Ceci s'applique aussi bien à une machine physique qu'à une machine virtuelle. Installez toujours les derniers correctifs de sécurité pour votre système d'exploitation et mettez en œuvre les meilleures pratiques standard de l'industrie pour protéger la machine hôte.

Découvrir le modèle de certificat vCenter

Par défaut, l'autorité de certification VMware provisionne chaque hôte ESXi, chaque machine de l'environnement et chaque utilisateur de solution à l'aide d'un certificat signé par VMCA (VMware Certificate Authority). L'environnement fourni est prêt à l'emploi, mais vous pouvez modifier le comportement par défaut si la stratégie de l'entreprise l'exige. Reportez-vous à [Chapitre 3 Certificats de sécurité vSphere](#).

Pour une protection supplémentaire, supprimez explicitement les certificats révoqués ou qui ont expiré, ainsi que les installations qui ont échoué.

Configurer vCenter Single Sign-On

vCenter Server et les services associés sont protégés par la structure d'authentification vCenter Single Sign-On. La première fois que vous installez le logiciel, vous spécifiez un mot de passe pour l'utilisateur administrator@vsphere.local, et seul ce domaine est disponible en tant que source d'identité. Vous pouvez ajouter d'autres sources d'identité (Active Directory ou LDAP) et définir une source d'identité par défaut. Dorénavant, les utilisateurs qui peuvent s'authentifier auprès d'une source d'identité ont la possibilité d'afficher des objets et d'effectuer des tâches, dans la mesure où ils y ont été autorisés. Reportez-vous à [Chapitre 2 Authentification vSphere à l'aide de vCenter Single Sign-On](#).

Attribuer des rôles aux utilisateurs ou aux groupes

Pour optimiser la journalisation, chaque autorisation octroyée pour un objet peut être associée à un utilisateur ou groupe nommé, ainsi qu'à un rôle prédéfini ou personnalisé. Le modèle d'autorisations vSphere 6.0 procure une grande flexibilité en offrant la possibilité d'autoriser les utilisateurs et les groupes de diverses façons. Reportez-vous à la section [Présentation des autorisations dans vSphere](#) et [Privilèges requis pour les tâches courantes](#).

Assurez-vous de limiter les privilèges d'administrateur et l'utilisation du rôle d'administrateur. Dans la mesure du possible, évitez d'utiliser l'utilisateur Administrateur anonyme.

Configurer NTP

Configurez NTP pour chaque nœud de votre environnement. L'infrastructure de certificats exige un horodatage précis et ne fonctionne correctement que si les nœuds sont synchronisés.

Reportez-vous à [Synchronisation des horloges sur le réseau vSphere](#).

Sécurisation des machines virtuelles

Pour sécuriser vos machines virtuelles, appliquez tous les correctifs appropriés aux systèmes d'exploitation invités et protégez votre environnement, de même que vous protégez votre machine physique. Pensez à désactiver toutes les fonctionnalités inutiles, à minimiser l'utilisation de la console de machine virtuelle et à suivre toute autre meilleure pratique.

Protéger le système d'exploitation invité

Pour protéger votre système d'exploitation invité, assurez-vous qu'il utilise les correctifs les plus récents et, le cas échéant, des applications de logiciel anti-espion et anti-programme malveillant. Reportez-vous à la documentation du fournisseur de votre système d'exploitation invité et, le cas échéant, à d'autres informations disponibles dans des manuels ou sur Internet pour ce système d'exploitation.

Désactiver les fonctionnalités inutiles

Vérifiez que toute fonctionnalité inutile est désactivée pour minimiser les points d'attaque potentiels. De nombreuses fonctionnalités peu utilisées sont désactivées par défaut. Supprimez le matériel inutile et désactivez certaines fonctionnalités, comme HFSG (host-guest filesystem) ou la fonction de copier/coller entre la machine virtuelle et une console distante.

Reportez-vous à la section [Désactiver les fonctions inutiles à l'intérieur des machines virtuelles](#).

Utiliser les modèles et la gestion basée sur des scripts

Les modèles de machine virtuelle vous permettent de configurer le système d'exploitation afin qu'il respecte des conditions requises spécifiques, puis de créer d'autres machines virtuelles avec les mêmes paramètres.

Pour modifier les paramètres de machine virtuelle après le déploiement initial, vous pouvez utiliser les scripts (PowerCLI, par exemple). Cette documentation explique comment effectuer des tâches à l'aide de l'interface utilisateur graphique. Vous pouvez utiliser des scripts au lieu de l'interface utilisateur graphique pour maintenir la cohérence de votre environnement. Dans les environnements de grande envergure, vous pouvez grouper les machines virtuelles dans des dossiers pour optimiser les scripts.

Pour plus d'informations sur les modèles, reportez-vous à la section [Utiliser des modèles pour déployer des machines virtuelles](#) et au document *Administration d'une machine virtuelle vSphere*. Pour plus d'informations sur PowerCLI, consultez la documentation de VMware PowerCLI.

Minimiser l'utilisation de la console de machine virtuelle

La console de machine virtuelle joue, pour la machine virtuelle, le même rôle que le moniteur sur un serveur physique. Les utilisateurs qui ont accès à une console de machine virtuelle ont accès à la gestion d'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. Par conséquent, la console de machine virtuelle devient vulnérable aux attaques malveillantes sur une machine virtuelle.

Sécurisation de la couche de mise en réseau virtuelle

La couche de mise en réseau virtuelle comprend des adaptateurs réseau virtuels, des commutateurs virtuels, des commutateurs virtuels distribués, des ports et des groupes de ports. ESXi utilise la couche réseau virtuelle pour les communications entre les machines virtuelles et leurs utilisateurs. En outre, ESXi utilise cette couche pour communiquer avec les SAN iSCSI, le stockage NAS, etc.

vSphere offre toutes les fonctionnalités pour garantir une infrastructure de mise en réseau sécurisée. Vous pouvez sécuriser séparément chacun des éléments de l'infrastructure (commutateurs virtuels, commutateurs virtuels distribués ou adaptateurs réseau virtuels, par exemple). En outre, tenez compte des directives suivantes, détaillées dans la section [Chapitre 8 Sécurisation de la mise en réseau vSphere](#).

Isoler le trafic réseau

Pour assurer un environnement ESXi sécurisé, il est essentiel d'isoler le trafic réseau. Des réseaux différents requièrent un accès et un niveau d'isolation distincts. Un réseau de gestion isole le trafic client, le trafic de l'interface de ligne de commande ou de l'API ou le trafic des logiciels tiers du trafic normal. Ce réseau doit être accessible uniquement aux administrateurs système, réseau et sécurité.

Reportez-vous à [Recommandations de sécurité pour la mise en réseau d'ESXi](#).

Utiliser des pare-feu pour sécuriser les éléments du réseau virtuel

Vous pouvez ouvrir et fermer les ports de pare-feu et sécuriser les différents éléments du réseau virtuel séparément. Les règles de pare-feu associent les services avec les pare-feu correspondants et peuvent ouvrir et fermer le pare-feu ESXi en fonction de l'état du service.

Reportez-vous à [Configuration du pare-feu ESXi](#).

Étudier les stratégies de sécurité réseau

Une stratégie de sécurité de la mise en réseau assure la protection du trafic contre l'emprunt d'identité d'adresse MAC et l'analyse des ports indésirables. La règle de sécurité d'un commutateur standard ou distribué est mise en œuvre au niveau de la couche 2 (couche de liaison de données) de la pile de protocole réseau. Les trois éléments de la stratégie de sécurité sont le mode promiscuité, les changements d'adresse MAC et les Transmissions forgées.

Les instructions sont disponibles dans la documentation *Mise en réseau vSphere*.

Sécuriser la mise en réseau des machines virtuelles

Les méthodes utilisées pour sécuriser un réseau de machines virtuelles dépendent du système d'exploitation invité installé, de la présence ou non d'un environnement sécurisé, ainsi que d'un certain nombre d'autres facteurs. Les commutateurs virtuels et les commutateurs virtuels distribués offrent un niveau de protection élevé lorsqu'ils sont utilisés avec d'autres mesures de sécurité (installation de pare-feu, notamment).

Reportez-vous à [Chapitre 8 Sécurisation de la mise en réseau vSphere](#).

Envisager les VLAN pour protéger votre environnement

ESXi prend en charge les VLAN IEEE 802.1q. Vous pouvez donc les utiliser pour renforcer la protection du réseau de machines virtuelles ou la configuration de stockage. Les VLAN permettent de segmenter un réseau physique : ainsi, deux machines du même réseau physique peuvent s'envoyer mutuellement des paquets ou en recevoir (sauf s'ils se trouvent sur le même réseau VLAN).

Reportez-vous à [Sécurisation des machines virtuelles avec des VLAN](#).

Sécuriser les connexions du stockage virtualisé

Une machine virtuelle stocke les fichiers du système d'exploitation, les fichiers de programme et d'autres données sur un disque virtuel. Chaque disque virtuel apparaît sur la machine virtuelle en tant que lecteur SCSI connecté au contrôleur SCSI. Une machine virtuelle n'a pas accès aux détails du stockage ni aux informations relatives au LUN sur lequel réside son disque virtuel.

VMFS (Virtual Machine File System) combine un système de fichiers distribué et un gestionnaire de volumes qui présente les volumes virtuels à l'hôte ESXi. La sécurisation de la connexion avec le stockage relève de votre responsabilité. Par exemple, si vous utilisez un stockage iSCSI, vous pouvez configurer votre environnement pour qu'il utilise l'authentification CHAP et, si la stratégie de l'entreprise l'exige, l'authentification CHAP mutuelle, en exploitant vSphere Web Client ou des CLI.

Reportez-vous à [Meilleures pratiques en matière de sécurité du stockage](#).

Évaluer l'utilisation d'IPSec

ESXi prend en charge IPSec sur IPv6. Vous ne pouvez pas utiliser IPSec sur IPv4.

Reportez-vous à [Sécurité du protocole Internet](#).

De plus, déterminez si VMware NSX pour vSphere est une solution adéquate pour sécuriser la couche de mise en réseau dans votre environnement.

Mots de passe dans votre environnement vSphere

Les restrictions de mot de passe, le verrouillage et l'expiration dans votre environnement vSphere dépendent de plusieurs facteurs : système visé par l'utilisateur, identité de l'utilisateur et mode de définition des règles.

Mots de passe d'ESXi

Les restrictions de mot de passe ESXi sont déterminées par le module PAM Linux `pam_passwdqc`. Reportez-vous à [Verrouillage des mots de passe et des comptes ESXi](#).

Mots de passe pour vCenter Server et autres services de vCenter

vCenter Single Sign-On gère l'authentification pour tous les utilisateurs qui se connectent à vCenter Server et à d'autres services de vCenter. Les restrictions de mot de passe, le verrouillage et l'expiration dépendent du domaine de l'utilisateur et de l'identité de l'utilisateur.

administrator@vsphere.local

Le mot de passe de l'utilisateur `administrator@vsphere.local`, ou de l'utilisateur `administrator@mydomain` si vous avez sélectionné un domaine différent au cours de l'installation, n'expire pas et n'est pas soumis à la stratégie de verrouillage. À tous les autres niveaux, le mot de passe doit respecter les restrictions définies dans la stratégie de mot de passe vCenter Single Sign-On. Reportez-vous à [Modifier la stratégie de mot de passe de vCenter Single Sign-On](#).

Si vous oubliez le mot de passe de ces utilisateurs, recherchez dans le système de la base de connaissances VMware des informations sur la réinitialisation de ce mot de passe.

Autres utilisateurs de vsphere.local

Les mots de passe des autres utilisateurs de `vsphere.local` ou des utilisateurs du domaine local que vous avez spécifiés au cours de l'installation doivent respecter les restrictions définies par la stratégie de mot de passe et la stratégie de verrouillage de vCenter Single Sign-On. Reportez-vous à la section [Modifier la stratégie de mot de passe de vCenter Single Sign-On](#) et [Modifier la stratégie de verrouillage de vCenter Single Sign-On](#). Ces mots de passe expirent après 90 jours par défaut, bien que les administrateurs puissent modifier l'expiration dans le cadre de la stratégie de mot de passe.

Si un utilisateur oublie son mot de passe `vsphere.local`, un administrateur peut réinitialiser ce mot de passe à l'aide de la commande `dir-cli`.

Autres utilisateurs

Les restrictions de mot de passe, le verrouillage et l'expiration de tous les autres utilisateurs sont déterminés par le domaine (source d'identité) auprès duquel l'utilisateur peut s'authentifier.

vCenter Single Sign-On prend en charge une source d'identité par défaut et les utilisateurs peuvent se connecter à vSphere Client simplement avec leur nom d'utilisateur. Le domaine détermine les paramètres de mot de passe. Si des utilisateurs veulent se connecter en tant qu'utilisateur dans un domaine qui n'est pas le domaine par défaut, ils peuvent inclure le nom de domaine, c'est-à-dire spécifier *utilisateur@domaine* ou *domaine\utilisateur*. Les paramètres de mot de passe des domaines s'appliquent également dans ce cas.

Mots de passe pour les utilisateurs de l'interface utilisateur de la console directe de vCenter Server Appliance

vCenter Server Appliance est une machine virtuelle basée sur Linux préconfigurée et optimisée pour l'exécution de vCenter Server et des services associés sur Linux.

Lorsque vous déployez une instance de vCenter Server Appliance, vous spécifiez un mot de passe pour l'utilisateur racine du système d'exploitation Linux du dispositif et un mot de passe pour l'utilisateur `administrator@vsphere.local`. Vous pouvez modifier le mot de passe de l'utilisateur racine et effectuer d'autres tâches de gestion de l'utilisateur local vCenter Server Appliance depuis l'interface utilisateur de la console directe. Reportez-vous à *Configuration de vCenter Server Appliance*.

Meilleures pratiques en matière de sécurité et ressources de sécurité

Si vous suivez les meilleures pratiques, votre ESXi et vCenter Server peuvent être au moins aussi sûr qu'un environnement non virtualisé.

Ce manuel répertorie les meilleures pratiques pour les différents composants de votre infrastructure vSphere.

Tableau 1-1. Meilleures pratiques de sécurité

Composant de vSphere	Ressource
Hôte ESXi	Meilleures pratiques de sécurité de ESXi
Système vCenter Server	Meilleures pratiques de sécurité de vCenter Server
Machine virtuelle	Recommandations en matière de sécurité des machines virtuelles
Mise en réseau vSphere	Meilleures pratiques en matière de sécurité de la mise en réseau vSphere

Ce manuel ne représente que l'une des sources dont vous avez besoin pour assurer la sécurité de l'environnement.

Les ressources de sécurité VMware, notamment les alertes et les téléchargements de sécurité, sont disponibles en ligne.

Tableau 1-2. Ressources de sécurité VMware disponibles sur le Web

Rubrique	Ressource
Stratégie de sécurité VMware, alertes de sécurité à jour, téléchargements de sécurité et discussions sur des thèmes liés à la sécurité.	http://www.vmware.com/go/security
Politique de l'entreprise en matière de réponse sécuritaire	http://www.vmware.com/support/policies/security_response.html VMware s'engage à vous aider à maintenir un environnement sécurisé. Dans ce cadre, les problèmes de sécurité sont corrigés rapidement. La politique VMware en matière de réponse sécuritaire fait état de notre engagement lié à la résolution d'éventuelles vulnérabilités de nos produits.
Politique de support logiciel tiers	http://www.vmware.com/support/policies/ VMware prend en charge un grand nombre de systèmes de stockage et d'agents logiciels (tels que les agents de sauvegarde ou les agents de gestion système). Vous trouverez la liste des agents, outils et autres logiciels prenant en charge ESXi en cherchant sur http://www.vmware.com/vmtn/resources/ les guides de compatibilité ESXi. Il existe sur le marché un nombre de produits et de configurations tel quel VMware ne peut pas tous les tester. Si un produit ou une configuration spécifique ne figure pas dans l'un des guides de compatibilité, contactez le Support technique, qui pourra vous aider à résoudre les problèmes rencontrés ; en revanche, il ne pourra pas vous garantir que ce produit ou cette configuration peut être utilisé. Vous devez toujours évaluer les risques de sécurité liés aux produits ou aux configurations non pris en charge.
Standards de sécurité et de conformité, ainsi que solutions partenaires et contenu détaillé sur la virtualisation et la conformité	http://www.vmware.com/go/compliance
Informations sur les certifications et les validations de sécurité telles que CCEVS et FIPS pour les différentes versions des composants de vSphere.	https://www.vmware.com/support/support-resources/certifications.html
Guides de sécurisation renforcée pour les différentes versions de vSphere et d'autres produits VMware.	https://www.vmware.com/support/support-resources/hardening-guides.html
livre blanc <i>Sécurité de VMware vSphere Hypervisor</i>	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvrsr-uslet-101.pdf

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

2

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

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

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

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

Une fois qu'un utilisateur a pu s'authentifier dans vCenter Single Sign-On, vous pouvez l'autoriser à réaliser certaines tâches. Dans la plupart des cas, vous attribuez des privilèges vCenter Server, mais vSphere propose également d'autres modèles d'autorisation. Reportez-vous à [Présentation des autorisations dans vSphere](#).

Note Si vous souhaitez activer un utilisateur Active Directory pour vous connecter à une instance de vCenter Server en utilisant le vSphere Client avec SSPI, vous devez joindre l'instance vCenter Server au domaine Active Directory. Pour plus d'informations sur la jonction à un vCenter Server Appliance avec un Platform Services Controller externe à un domaine Active Directory, consultez l'article de la base de connaissances VMware suivant <http://kb.vmware.com/kb/2118543>.

Ce chapitre contient les rubriques suivantes :

- [Comprendre vCenter Single Sign-On](#)
- [Configuration des sources d'identité vCenter Single Sign-On](#)
- [Authentification à deux facteurs de vCenter Server](#)

- Utilisation de vCenter Single Sign-On comme fournisseur d'identité pour un autre fournisseur de services
- STS (Security Token Service)
- Gestion des stratégies vCenter Single Sign-On
- Gestion des utilisateurs et des groupes vCenter Single Sign-On
- Recommandations en matière de sécurité pour vCenter Single Sign-On
- Dépannage de vCenter Single Sign-On

Comprendre vCenter Single Sign-On

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



Domaines et sites vCenter Single Sign-On 6.0

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

Protection de votre environnement par vCenter Single Sign-On

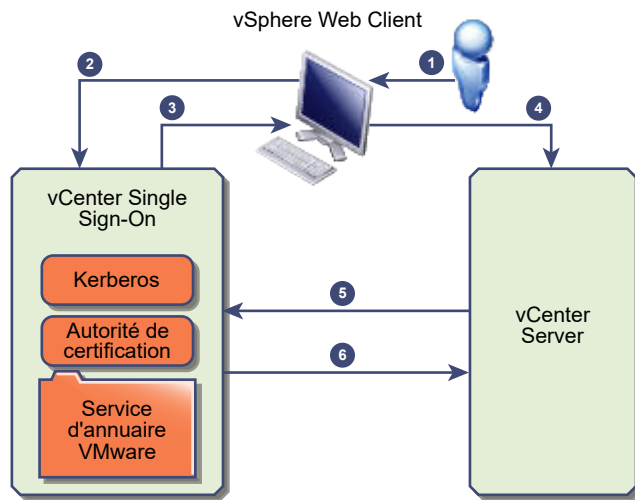
vCenter Single Sign-On permet aux composants vSphere de communiquer entre eux au moyen d'un mécanisme d'échange de jetons sécurisé au lieu d'obliger les utilisateurs à s'authentifier séparément pour chaque composant.

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

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

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

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



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

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

- 2 vSphere Web Client transmet les informations de connexion au service vCenter Single Sign-On. Celui-ci vérifie alors le jeton SAML de vSphere Web Client. Si vSphere Web Client dispose d'un jeton valide, vCenter Single Sign-On vérifie ensuite que l'utilisateur figure bien dans la source d'identité configurée (par exemple, Active Directory).
 - Si seul le nom d'utilisateur est employé, vCenter Single Sign-On vérifie dans le domaine par défaut.
 - Si un nom de domaine est inclus avec le nom d'utilisateur (*DOMAIN/user1* ou *user1@DOMAIN*), vCenter Single Sign-On vérifie ce domaine.
- 3 Si l'utilisateur peut s'authentifier auprès de la source d'identité, vCenter Single Sign-On renvoie un jeton qui représente l'utilisateur pour vSphere Web Client.
- 4 vSphere Web Client transmet le jeton au système vCenter Server.
- 5 vCenter Server vérifie auprès du serveur vCenter Single Sign-On que le jeton est valide et n'a pas expiré.
- 6 Le serveur vCenter Single Sign-On renvoie le jeton au système vCenter Server en exploitant la structure d'autorisation de vCenter Server pour autoriser l'accès de l'utilisateur.

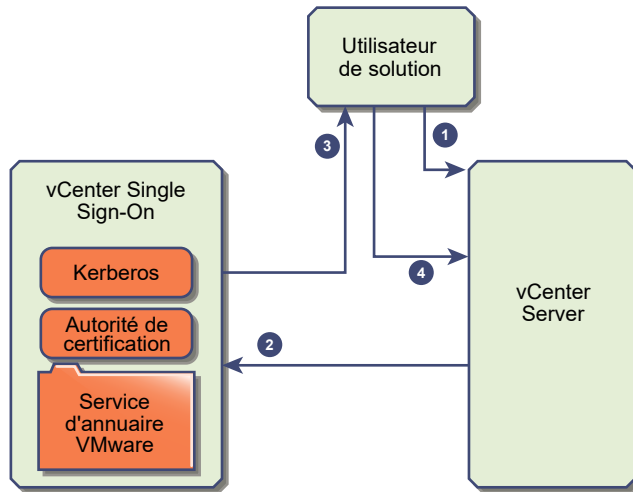
L'utilisateur peut désormais s'authentifier, puis afficher et modifier les objets pour lesquels il possède les privilèges pertinents.

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. Reportez-vous à la section [Ajouter une autorisation à un objet d'inventaire](#).

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

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

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



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

- 1 L'utilisateur de solution tente de se connecter à un service vCenter.
- 2 L'utilisateur de solution est redirigé vers vCenter Single Sign-On. Si l'utilisateur de solution est nouveau dans vCenter Single Sign-On, il doit présenter un certificat valide.
- 3 Si le certificat est valide, vCenter Single Sign-On attribue un jeton SAML (jeton de support) à l'utilisateur de solution. Le jeton est signé par vCenter Single Sign-On.
- 4 L'utilisateur de solution est ensuite redirigé vers vCenter Single Sign-On et peut effectuer des tâches, selon les autorisations qui lui sont attribuées.
- 5 La prochaine fois que l'utilisateur de solution devra s'authentifier, il pourra utiliser le jeton SAML pour se connecter à vCenter Server.

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

Composants vCenter Single Sign-On

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

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

STS (Security Token Service)

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

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

Serveur d'administration

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

VMware Directory Service (vmdir)

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

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

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

Identity Management Service

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

Incidence de vCenter Single Sign-On sur l'installation

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

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

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

L'ordre d'installation est important.

Première installation

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

Installations suivantes

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

Incidence de vCenter Single Sign-On sur les mises à niveau

Si vous mettez à niveau un environnement Simple Install vers un déploiement intégré vCenter Server 6, l'opération s'effectue en toute transparence. Lorsque vous mettez à niveau une installation personnalisée, le service vCenter Single Sign-On fait partie de Platform Services Controller après la mise à niveau. Les utilisateurs qui peuvent se connecter à vCenter Server après une mise à niveau varient selon la version à partir de laquelle vous procédez à la mise à niveau et la configuration du déploiement.

Au cours de la mise à niveau, vous pouvez définir un nom de domaine vCenter Single Sign-On différent, qui sera utilisé à la place de vsphere.local.

Chemins de mise à niveau

Le résultat de la mise à niveau dépend des options d'installation que vous avez sélectionnées et du modèle de déploiement vers lequel vous effectuez la mise à niveau.

Tableau 2-1. Chemins de mise à niveau

Source	Résultat
vSphere 5.5 et versions antérieures de Simple Install	vCenter Server avec Platform Services Controller intégré.
vSphere 5.5 et versions antérieures de Custom Install	<p>Si vCenter Single Sign-On était installé sur un nœud différent de vCenter Server, un autre environnement, avec un Platform Services Controller externe, est créé.</p> <p>Si vCenter Single Sign-On était installé sur le même nœud que vCenter Server, mais que d'autres services sont sur des nœuds différents, un autre environnement, avec un Platform Services Controller intégré, est créé.</p> <p>Si l'installation personnalisée comportait plusieurs serveurs vCenter Single Sign-On à réplication multiple, un autre environnement, avec plusieurs instances de Platform Services Controller à réplication multiple, est créé.</p>

Utilisateurs autorisés à se connecter après la mise à niveau d'une installation simple

Si vous mettez à niveau un environnement provisionné à l'aide de l'option d'installation simple (Simple Install), vous obtenez toujours une installation avec un Platform Services Controller intégré. Les utilisateurs autorisés à se connecter sont différents selon que l'environnement source contient ou non vCenter Single Sign-On.

Tableau 2-2. Privilèges de connexion après la mise à niveau d'un environnement d'installation simple

Version source	Accès pour	Remarques
vSphere 5.0	Utilisateurs de systèmes d'exploitation locaux administrator@vsphere.local	Vous pourrez être invité à indiquer l'administrateur du dossier racine dans la hiérarchie de l'inventaire vSphere pendant l'installation, en raison de modifications dans les magasins de l'utilisateur. Si votre installation précédente prenait en charge les utilisateurs Active Directory, vous pouvez ajouter le domaine Active Directory comme source d'identité.
vSphere 5.1	Utilisateurs de systèmes d'exploitation locaux administrator@vsphere.local Admin@SystemDomain	Depuis vSphere 5.5, vCenter Single Sign-On prend en charge une seule source d'identité par défaut. Vous pouvez définir la source d'identité par défaut. Les utilisateurs d'un domaine non défini par défaut peuvent spécifier le domaine au moment de leur connexion (<i>DOMAIN\user</i> ou <i>user@DOMAIN</i>).
vSphere 5.5	administrator@vsphere.local ou l'administrateur du domaine que vous avez spécifié lors de la mise à niveau. Tous les utilisateurs de toutes les sources d'identité peuvent se connecter comme précédemment.	

Si vous effectuez la mise à niveau à partir de vSphere 5.0, qui n'intègre pas vCenter Single Sign-On, vers une version qui comprend vCenter Single Sign-On, les utilisateurs de systèmes d'exploitation locaux deviennent beaucoup moins importants que les utilisateurs d'un service d'annuaire tel qu'Active Directory. En conséquence, il n'est pas toujours possible, voire même souhaitable, de conserver les utilisateurs du système d'exploitation local comme utilisateurs authentifiés.

Utilisateurs autorisés à se connecter après la mise à niveau d'une installation personnalisée

Si vous mettez à niveau un environnement provisionné à l'aide de l'option d'installation personnalisée (Custom Install), le résultat dépend de vos choix initiaux :

- Si vCenter Single Sign-On était installé sur le même nœud que le système vCenter Server, le résultat est une installation avec un Platform Services Controller intégré.

- Si vCenter Single Sign-On était installé sur un autre nœud que le système vCenter Server, le résultat est une installation avec un Platform Services Controller externe.
- Si vous avez effectué la mise à niveau à partir de vSphere 5.0, vous pouvez sélectionner un Platform Services Controller externe ou intégré au cours de la mise à niveau.

Les privilèges de connexion après la mise à niveau dépendent de plusieurs facteurs.

Tableau 2-3. Privilèges de connexion après une mise à niveau d'un environnement d'installation personnalisé

Version source	Accès pour	Remarques
vSphere 5.0	<p>vCenter Single Sign-On reconnaît les utilisateurs de systèmes d'exploitation locaux de la machine sur laquelle est installé le Platform Services Controller, mais pas la machine sur laquelle est installé vCenter Server.</p> <p>Note Le recours à des utilisateurs de systèmes d'exploitation locaux pour l'administration n'est pas recommandé, notamment dans les environnements fédérés.</p> <p>administrator@vsphere.local peut se connecter à vCenter Single Sign-On et à chaque instance de vCenter Server en tant qu'utilisateur administrateur.</p>	<p>Si votre installation 5.0, possible issue in final view gérât les utilisateurs Active Directory, ces utilisateurs n'ont plus accès après la mise à niveau. Vous pouvez ajouter le domaine Active Directory comme source d'identité.</p>
vSphere 5.1 ou vSphere 5.5	<p>vCenter Single Sign-On reconnaît les utilisateurs de systèmes d'exploitation locaux de la machine sur laquelle est installé le Platform Services Controller, mais pas la machine sur laquelle est installé vCenter Server.</p> <p>Note Le recours à des utilisateurs de systèmes d'exploitation locaux pour l'administration n'est pas recommandé, notamment dans les environnement fédérés.</p> <p>administrator@vsphere.local peut se connecter à vCenter Single Sign-On et à chaque instance de vCenter Server en tant qu'utilisateur administrateur.</p> <p>Pour les mises à niveau à partir de vSphere 5.1, Admin@SystemDomain possède les mêmes privilèges qu'administrator@vsphere.local.</p>	<p>Depuis vSphere 5.5, vCenter Single Sign-On prend en charge une seule source d'identité par défaut.</p> <p>Vous pouvez définir la source d'identité par défaut.</p> <p>Les utilisateurs d'un domaine non défini par défaut peuvent spécifier le domaine au moment de leur connexion (<i>DOMAIN\user</i> ou <i>user@DOMAIN</i>).</p>

Utilisation de vCenter Single Sign-On avec vSphere

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

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

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

Les objets visibles par l'utilisateur et les actions que celui-ci peut effectuer sont généralement déterminés par les paramètres d'autorisation vCenter Server. Les administrateurs vCenter Server attribuent ces autorisations depuis l'interface **Gérer > Permissions** de vSphere Web Client, et non via vCenter Single Sign-On. Reportez-vous à [Chapitre 4 Tâches de gestion des utilisateurs et des autorisations de vSphere](#).

Utilisateurs de vCenter Single Sign-On et de vCenter Server

À l'aide de vSphere Web Client, les utilisateurs s'authentifient auprès de vCenter Single Sign-On en entrant leurs informations d'identification sur la page de connexion de vSphere Web Client. Une fois connectés à vCenter Server, les utilisateurs authentifiés peuvent afficher toutes leurs instances de vCenter Server ou d'autres objets vSphere pour lesquels leur rôle leur accorde des privilèges. Aucune autre authentification n'est requise. Reportez-vous à [Chapitre 4 Tâches de gestion des utilisateurs et des autorisations de vSphere](#).

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

Tous les utilisateurs pouvant s'authentifier auprès de vCenter Single Sign-On ont la possibilité de réinitialiser leur mot de passe, même si celui-ci a expiré, à condition qu'ils le connaissent. Reportez-vous à [Changer le mot de passe de vCenter Single Sign-On](#). 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 Web 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 Web Client. Après authentification, cet utilisateur peut accéder à l'interface d'administration de vCenter Single Sign-On à partir de vSphere Web Client et gérer les sources d'identité et les domaines par défaut, spécifier les stratégies de mot de passe et effectuer d'autres tâches d'administration. Reportez-vous à [Configuration des sources d'identité vCenter Single Sign-On](#).

Note Vous ne pouvez pas renommer l'utilisateur `administrator@vsphere.local`. Pour une sécurité accrue, envisagez de créer des utilisateurs nommés supplémentaires dans le domaine `vsphere.local` et de leur attribuer des privilèges d'administration. Vous pouvez ensuite cesser d'utiliser `administrator@vsphere.local`.

Authentification dans différentes versions de vSphere

Si un utilisateur se connecte à un système vCenter Server version 5.0 ou version antérieure, vCenter Server authentifie l'utilisateur en le validant par rapport à un domaine Active Directory ou à la liste des utilisateurs du système d'exploitation local. Dans vCenter Server 5.1 et les versions ultérieures, les utilisateurs sont authentifiés par l'intermédiaire de vCenter Single Sign-On.

Note Vous ne pouvez pas utiliser vSphere Web Client pour gérer vCenter Server version 5.0 ou versions antérieures. Mettez à niveau vCenter Server vers la version 5.1 ou une version ultérieure.

Utilisateurs ESXi

ESXi n'est pas intégré à vCenter Single Sign-On. Vous ajoutez explicitement l'hôte ESXi à un domaine Active Directory. Reportez-vous à [Configurer un hôte pour utiliser Active Directory](#).

Vous pouvez toujours créer des utilisateurs ESXi locaux avec vSphere Client, vCLI ou PowerCLI. vCenter Server ne reconnaît pas les utilisateurs qui sont locaux à ESXi et ESXi ne reconnaît pas les utilisateurs de vCenter Server.

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

Comment se connecter aux composants de vCenter Server

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

- Les utilisateurs qui se trouvent dans le domaine par défaut peuvent se connecter avec leurs nom d'utilisateur et mot de passe.
- Les utilisateurs qui se trouvent dans un domaine qui a été ajouté à vCenter Single Sign-On en tant que source d'identité, mais qui n'est pas le domaine par défaut, peuvent se connecter à vCenter Server, mais ils doivent spécifier le domaine de l'une des manières suivantes.
 - En incluant un préfixe de nom de domaine : par exemple, `MONDOMAINE\utilisateur1`
 - En incluant le domaine : par exemple, `utilisateur1@mondomaine.com`

- Les utilisateurs qui se trouvent dans un domaine qui n'est pas une source d'identité vCenter Single Sign-On ne peuvent pas se connecter à vCenter Server. Si le domaine que vous ajoutez à vCenter Single Sign-On fait partie d'une hiérarchie de domaines, Active Directory détermine si les utilisateurs des autres domaines de la hiérarchie sont ou non authentifiés.

Note 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 vsphere.local

Le domaine vsphere.local comprend plusieurs groupes prédéfinis. Attribuez les utilisateurs à l'un de ces groupes pour leur permettre d'effectuer les actions correspondantes.

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

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

Les groupes suivants sont prédéfinis dans vsphere.local.

Note 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.

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

Tableau 2-4. Groupes du domaine vsphere.local

Privilège	Description
Utilisateurs	Utilisateurs du domaine vsphere.local.
SolutionUsers	Utilisateurs de solution. Ce groupe contient les services vCenter. Chaque utilisateur de solution s'authentifie individuellement auprès de vCenter Single Sign-On avec un certificat. Par défaut, VMCA provisionne les utilisateurs de solution à l'aide de certificats. N'ajoutez aucun membre à ce groupe explicitement.
CAAdmins	Les membres du groupe CAAdmins possèdent des privilèges d'administration pour VMCA. En général, il est déconseillé d'ajouter des membres à ces groupes.

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

Privilège	Description
DCAdmins	<p>Les membres du groupe DCAdmins peuvent exercer des actions d'administrateur de contrôleur de domaine sur le service d'annuaire VMware.</p> <p>Note Ne gérez pas le contrôleur de domaine directement. Utilisez plutôt la CLI <code>vmdir</code> ou vSphere Web Client pour effectuer les tâches correspondantes.</p>
SystemConfiguration.BashShellAdministrators	<p>Ce groupe est disponible uniquement pour les déploiements de vCenter Server Appliance.</p> <p>Tout utilisateur appartenant à ce groupe peut activer et désactiver l'accès à l'interpréteur de commandes de dépistage. Par défaut, tout utilisateur qui se connecte à vCenter Server Appliance à l'aide de SSH peut uniquement accéder aux commandes disponibles dans le shell restreint. Les utilisateurs de ce groupe peuvent accéder à l'interpréteur de commandes de dépistage.</p>
ActAsUsers	Les membres de ce groupe sont autorisés à recevoir des jetons actas de vCenter Single Sign-On.
ExternalIPDUsers	Ce groupe n'est pas utilisé par vSphere. Il est nécessaire en conjonction avec VMware vCloud Air.
SystemConfiguration.Administrators	Les membres du groupe SystemConfiguration.Administrators peuvent afficher et gérer la configuration du système dans vSphere Web Client. Ces utilisateurs peuvent afficher, démarrer, redémarrer et dépanner les services et consulter et gérer les nœuds disponibles.
DCClients	<p>Ce groupe est utilisé en interne pour permettre aux nœuds de gestion d'accéder aux données qui se trouvent dans le service d'annuaire VMware.</p> <p>Note Ne modifiez pas ce groupe. Toute modification pourrait compromettre votre infrastructure de certificats.</p>
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 du service d'annuaire VMware (vmdir). Les membres de ce groupe peuvent effectuer des tâches d'administration vCenter Single Sign-On. En général, il est déconseillé d'ajouter des membres à ce groupe.

Exigences de mots de passe et comportement de verrouillage de vCenter Server

Pour gérer votre environnement, vous devez connaître la stratégie de mot de passe vCenter Single Sign-On, les mots de passe vCenter Server et le comportement de verrouillage.

Mot de passe d'administrateur vCenter Single Sign-On

Le mot de passe d'administrator@vsphere.local doit satisfaire les exigences suivantes :

- Au moins 8 caractères
- Au moins un caractère minuscule
- Au moins un caractère numérique
- Au moins un caractère spécial

Le mot de passe d'administrator@vsphere.local ne peut pas comporter plus de 20 caractères. Seuls les caractères ASCII visibles sont autorisés. Cela signifie, par exemple, que vous ne pouvez pas utiliser le caractère espace.

Mots de passe d'vCenter Server

Dans vCenter Server, les exigences en matière de mot de passe sont dictées par vCenter Single Sign-On ou par la source d'identité configurée qui peut être Active Directory, OpenLDAP ou le système d'exploitation local du serveur vCenter Single Sign-On (non recommandé).

Comportement de verrouillage

Les utilisateurs sont verrouillés après un nombre prédéfini de tentatives de connexion infructueuses successives. Par défaut, les utilisateurs sont verrouillés après cinq tentatives infructueuses successives en trois minutes et un compte verrouillé est déverrouillé automatiquement après cinq minutes. Vous pouvez modifier ces valeurs par défaut à l'aide de la stratégie de verrouillage. Reportez-vous à [Modifier la stratégie de verrouillage de vCenter Single Sign-On](#).

À partir de vSphere 6.0, l'administrateur du domaine système, administrator@vsphere.local par défaut, n'est pas affecté par la stratégie de verrouillage.

N'importe quel utilisateur peut modifier son mot de passe à l'aide de la commande `dir-cli password change`. Si un utilisateur oublie le mot de passe, l'administrateur peut réinitialiser le mot de passe à l'aide de la commande `dir-cli password reset`.

Reportez-vous à [Verrouillage des mots de passe et des comptes ESXi](#) pour une description des mots de passe des utilisateurs locaux d'ESXi.

Configuration des sources d'identité vCenter Single Sign-On

Lorsqu'un utilisateur se connecte, vCenter Single Sign-On vérifie dans la source d'identité par défaut si cet utilisateur peut s'authentifier. 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 Web 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. Par défaut, seul l'utilisateur administrator@vsphere.local possède les privilèges d'administrateur sur le serveur vCenter Single Sign-On dans une nouvelle installation.

- [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.

- [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.

- [Ajouter une source d'identité de vCenter Single Sign-On](#)

Les utilisateurs peuvent se connecter à vCenter Server uniquement s'ils se trouvent 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 à partir de vSphere Web Client.

- [Modifier une source d'identité de vCenter Single Sign-On](#)

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

- [Supprimer une source d'identité vCenter Single Sign-On](#)

Les utilisateurs vSphere sont définis dans une source d'identité. Vous pouvez supprimer une source d'identité de la liste des sources d'identité enregistrées.

- [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). Pour que la case à cocher soit disponible sur la page de connexion, le plug-in d'intégration du client doit être installé.

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

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

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

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

Types de sources d'identité

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

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

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

- Utilisateurs du système vCenter Single Sign-On Lorsque vous installez vCenter Single Sign-On, une seule source d'identité système, nommée `vsphere.local`, est créée. Cette source d'identité est nommée **vsphere.local** dans vSphere Web Client.

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 (*DOMAINE\user*) pour s'authentifier.

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

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

Définir le domaine par défaut de vCenter Single Sign-On

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

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

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine `vsphere.local`.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.

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

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

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

Les utilisateurs peuvent se connecter à vCenter Server uniquement s'ils se trouvent 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 à partir de vSphere Web Client.

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

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

localos

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

vsphere.local

Contient les utilisateurs internes de vCenter Single Sign-On.

Conditions préalables

Le domaine que vous souhaitez ajouter comme source d'identité doit être accessible par la machine sur laquelle vCenter Single Sign-On s'exécute. Si vous utilisez vCenter Server Appliance, reportez-vous à la documentation de *Configuration de vCenter Server Appliance*.

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.
- 3 Dans l'onglet **Sources d'identité**, cliquez sur l'icône **Ajouter source d'identité**.

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

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

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. Il s'agit de la configuration du domaine Active Directory par défaut pour ce qui est des autorisations d'authentification. VMware recommande l'utilisation d'un utilisateur spécial de service.

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

Étape suivante

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

Paramètres de source d'identité Active Directory

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

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

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

- Pour une installation Windows, joignez la machine Windows au domaine Active Directory.
- Pour vCenter Server Appliance, suivez les instructions de la documentation *Configuration de vCenter Server Appliance*.

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, reportez-vous à l'article [2070433](#) de la base de connaissances VMware.

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

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

Tableau 2-5. 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. Si vous utilisez vCenter Server Appliance, utilisez les informations sur la configuration des paramètres réseau pour mettre à jour les paramètres de serveur DNS.
Utiliser un compte d'ordinateur	Sélectionnez cette option pour utiliser le compte de l'ordinateur local en tant que SPN. Lorsque vous sélectionnez cette option, vous spécifiez uniquement le nom de domaine. Si vous prévoyez de renommer l'ordinateur, ne sélectionnez pas cette option.
Utiliser le nom de principal du service (SPN)	Sélectionnez cette option si vous prévoyez de renommer l'ordinateur local. Vous devez spécifier un SPN, un utilisateur pouvant s'authentifier auprès de la source d'identité et un mot de passe pour cet utilisateur.

Tableau 2-5. 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 (<code>STS/example.com</code> , par exemple). Le SPN doit être unique dans le domaine. L'exécution de la commande <code>setspn -S</code> permet de vérifier qu'aucun doublon n'est créé. Pour obtenir des informations sur l'outil de ligne de commande <code>setspn</code> , 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 (<code>jchin@mydomain.com</code> , par exemple). Vous pouvez vérifier le nom d'utilisateur principal (UPN, User Principal Name) dans l'éditeur ASDI (Active Directory Service Interfaces Editor).

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

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

Si vous configurez une source d'identité OpenLDAP, consultez l'article [2064977](#) de la base de connaissances VMware pour connaître les conditions préalables supplémentaires.

Tableau 2-6. Active Directory en tant que serveur LDAP et paramètres OpenLDAP

Champ	Description
Nom	Nom de la source d'identité.
Nom de domaine (DN) de base des utilisateurs	Nom unique de base pour les utilisateurs.
Nom de domaine	Nom de domaine complet du domaine, par exemple, <code>exemple.com</code> . N'entrez pas une adresse IP dans ce champ.
Alias du domaine	Pour les sources d'identité Active Directory, le nom NetBIOS du domaine. Ajoutez le nom NetBIOS du domaine Active Directory en tant qu'alias de la source d'identité si vous utilisez les authentifications SSPI. Pour les sources d'identité OpenLDAP, le nom du domaine en lettres majuscules est ajouté si vous ne spécifiez pas d'alias.
DN de base des groupes	Nom unique de base pour les groupes.

Tableau 2-6. Active Directory en tant que serveur LDAP et paramètres OpenLDAP (suite)

Champ	Description
URL du serveur principal	<p>Serveur LDAP du contrôleur de domaine principale du domaine.</p> <p>Utilisez le format suivant : ldap://hostname:port ou ldaps://hostname:port. Le port est généralement 389 pour ldap: connections et 636 pour ldaps: connections. Pour les déploiements de contrôleurs multi-domaines Active Directory, le port est généralement 3268 pour ldap: connections et 3269 pour ldaps: connections.</p> <p>Un certificat qui établit la confiance du point terminal LDAP du serveur Active Directory est requis lorsque vous utilisez ldaps:// dans l'URL LDAP principale ou secondaire.</p>
URL secondaire du serveur	Adresse du serveur LDAP d'un contrôleur de domaine secondaire utilisé pour le basculement.
Choisir un certificat	Si vous souhaitez utiliser LDAPS avec la source d'identité de votre serveur LDAP Active Directory et OpenLDAP, le bouton Choisir un certificat devient disponible une fois que vous avez tapé ldaps:// dans le champ d'URL. Aucune URL secondaire n'est requise.
Nom d'utilisateur	ID d'un utilisateur du domaine qui dispose au minimum d'un accès en lecture seule au nom de domaine (DN) de base pour les utilisateurs et les groupes.
Mot de passe	Mot de passe de l'utilisateur spécifié par Nom d'utilisateur.

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

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.
- 3 Cliquez sur l'onglet **Sources d'identité**.
- 4 Cliquez avec le bouton droit sur la source d'identité dans le tableau et sélectionnez **Modifier la source d'identité**.

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

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

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

Supprimer une source d'identité vCenter Single Sign-On

Les utilisateurs vSphere sont définis dans une source d'identité. Vous pouvez supprimer une source d'identité de la liste des sources d'identité enregistrées.

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- Accédez à **Administration > Single Sign-On > Configuration**.
- Dans l'onglet **Sources d'identité**, sélectionnez une source d'identité et cliquez sur l'icône **Supprimer une source d'identité**.
- Cliquez sur **Oui** lorsque vous êtes invité à confirmer.

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

Vous pouvez utiliser vCenter Single Sign-On avec l'authentification de session Windows (SSPI). Pour que la case à cocher soit disponible sur la page de connexion, le plug-in d'intégration du client doit être installé.

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

Conditions préalables

Votre domaine Windows doit être correctement configuré. Reportez-vous à l'article [2064250](#) de la base de connaissances VMware.

Procédure

- 1 Accédez à la page de connexion de vSphere Web Client.
- 2 Si la case à cocher **Utiliser l'authentification de session Windows** n'est pas disponible, cliquez sur **Télécharger le plug-in d'intégration de client** en bas de la page de connexion.
- 3 Si le navigateur bloque l'installation en émettant des erreurs de certificat ou en exécutant un bloqueur de fenêtres contextuelles, suivez les instructions d'aide du navigateur pour résoudre le problème.

- 4 Fermez les autres navigateurs si vous y êtes invité.

Après l'installation, le plug-in est disponible pour tous les navigateurs. Si votre navigateur le requiert, vous devrez peut-être autoriser le plug-in pour des sessions individuelles ou pour toutes les sessions.

- 5 Quittez et redémarrez le navigateur.

Après le redémarrage, vous pouvez sélectionner la case à cocher **Utiliser l'authentification de session Windows**.

Authentification à deux facteurs de vCenter Server

vCenter Single Sign-On vous permet de vous authentifier en utilisant le nom et le mot de passe d'un utilisateur dans une source d'identité connue par vCenter Single Sign-On, ou en utilisant l'authentification de session Windows pour les sources d'identité Active Directory. À partir de vSphere 6.0 Update 2, vous pouvez également vous authentifier en utilisant une carte à puce (Carte d'accès commun ou CAC basée sur UPN), ou en utilisant un jeton RSA SecurID.

Méthodes d'authentification à deux facteurs

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

Authentification par carte d'accès commun (CAC)

L'authentification CAC permet un accès uniquement aux utilisateurs qui attachent une carte physique au lecteur USB de l'ordinateur sur lequel ils se connectent. Si la PKI est déployée de telle sorte que les certificats de carte à puce sont les seuls certificats clients qui sont émis par l'autorité de certification, seuls les certificats de carte à puce sont présentés à l'utilisateur. L'utilisateur sélectionne un certificat et est ensuite 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 SecureID, votre environnement doit inclure une instance de RSA Authentication Manager correctement configurée. Si Platform Services Controller est configuré pour pointer vers le serveur RSA et que l'authentification RSA SecurID est activée, les utilisateurs peuvent se connecter avec leur nom d'utilisateur et leur jeton.

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

Les administrateurs peuvent effectuer la configuration à partir de l'interface Web de Platform Services Controller ou en utilisant le script `sso-config` (`sso-config.bat` sur Windows et `sso-config.sh` sur le dispositif).

- Pour une authentification CAC, vous configurez votre navigateur Web à l'aide du script `sso-config` et vous pouvez effectuer la configuration de vCenter Single Sign-On à partir de l'interface Web de Platform Services Controller ou en utilisant `sso-config`. La configuration inclut l'activation de l'authentification CAC, la configuration de stratégies de révocation de certificat et la configuration d'une page de connexion.
- Pour RSA SecureID, vous utilisez le script `sso-config` pour configurer RSA Authentication Manager pour le domaine et pour activer l'authentification par jeton RSA. La méthode d'authentification s'affiche dans l'interface Web de Platform Services Controller si elle est activée, mais vous ne pouvez pas configurer l'authentification RSA SecureID à partir de l'interface Web.

Combinaison de différentes méthodes d'authentification

Vous pouvez activer ou désactiver chaque méthode d'authentification séparément à l'aide de `sso-config`. Il convient, par exemple, de maintenir l'authentification par nom d'utilisateur et par mot de passe initialement activée pendant que vous testez l'une des méthodes d'authentification à deux facteurs, et de définir ensuite une seule méthode d'authentification comme étant activée.

Configuration de l'authentification par carte à puce pour vCenter Single Sign-On

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

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 CAC est utilisée dans les environnements dans lesquels chaque machine dispose d'un lecteur de carte à puce et où sont préinstallés des pilotes de matériel de carte à puce qui gèrent ce type de carte.

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

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

Note Dans la plupart des cas, il convient 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 la connexion par nom d'utilisateur et par mot de passe en se connectant directement à Platform Services Controller.

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

Vous pouvez employer l'utilitaire `sso-config` pour configurer 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.

Lorsque vous configurez l'authentification par carte à puce à partir de la ligne de commande, configurez toujours Platform Services Controller en utilisant la commande `sso-config` en premier. Puis, vous pouvez effectuer d'autres tâches à l'aide de l'interface Web de Platform Services Controller.

- 1 Configurez Platform Services Controller afin que le navigateur Web demande l'envoi du certificat par carte à puce lorsque l'utilisateur se connecte.
- 2 Configurez la stratégie d'authentification. Vous pouvez configurer la stratégie en utilisant le script `sso-config` ou l'interface Web de Platform Services Controller. La configuration des types d'authentification et des paramètres de révocation pris en charge est stockée dans VMware Directory Service et est répliquée dans toutes les instances de Platform Services Controller d'un domaine vCenter Single Sign-On.

Si l'authentification par 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 la connexion depuis vSphere Web Client ne fonctionne pas, et que l'authentification par nom d'utilisateur et par mot de passe est désactivée, un utilisateur racine ou administrateur peut réactiver l'authentification par nom d'utilisateur et par mot de passe depuis la ligne de commande de Platform Services Controller en exécutant la commande suivante. L'exemple concerne Windows ; pour Linux, utilisez `sso-config.sh`.

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

Vous trouverez le script `sso-config` aux emplacements suivants :

Windows C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat

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

Conditions préalables

- Vérifiez que votre environnement utilise Platform Services Controller version 6.0 Update 2 ou ultérieure, et que vCenter Server version 6.0 ou ultérieure est bien installé. Mettez à niveau les nœuds de version 5.5 vers la version 6.0.
- 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) qui correspond à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).
 - L'authentification du client doit être spécifiée dans le champ Stratégie d'application ou Utilisation avancée de la clé d'un certificat, sinon le navigateur n'affiche pas ce certificat.
- Vérifiez que l'interface Web de Platform Services Controller est approuvée par la station de travail de l'utilisateur final ; sinon, le navigateur ne tente pas l'authentification.

- Configurez une source d'identité Active Directory et ajoutez-la à vCenter Single Sign-On en tant que source d'identité.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent alors s'authentifier, car ils font partie du groupe Active Directory et ils ont des privilèges d'administrateur de vCenter Server. L'utilisateur administrator@vsphere.local ne peut pas effectuer d'authentification par carte à puce.
- Si vous souhaitez utiliser la solution haute disponibilité (HA, High Availability) de Platform Services Controller dans votre environnement, configurez HA avant de configurer l'authentification par carte à puce. Consultez l'article de la base de connaissances VMware [2112085](#) (Windows) ou [2113315](#) (vCenter Server Appliance).

Procédure

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

Option	Description
Windows	Connectez-vous à l'installation Windows de Platform Services Controller et utilisez WinSCP ou un utilitaire similaire pour copier les fichiers.
Dispositif	<ol style="list-style-type: none"> a Connectez-vous à la console du dispositif, soit directement soit à l'aide de SSH. b Activez l'interpréteur de commande du dispositif de la façon suivante. <div data-bbox="683 1054 1075 1159" data-label="Text"> <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </div> c Utilisez WinSCP ou un utilitaire similaire pour copier les certificats dans le dossier <code>/usr/lib/vmware-sso/vmware-sts/conf</code> dans Platform Services Controller. d Vous pouvez éventuellement désactiver l'interpréteur de commande du dispositif de la façon suivante. <div data-bbox="683 1381 1075 1404" data-label="Text"> <pre>chsh -s "bin/appliancesh" root</pre> </div>

- 2 Sur chaque nœud Platform Services Controller, configurez les paramètres d'authentification par carte à puce en utilisant l'interface de ligne de commande de `sso-config`.

- a Accédez au répertoire dans lequel le script `sso-config` se trouve.

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

- b Exécutez la commande suivante :

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

Par exemple :

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer -t vsphere.local
```

- c Redémarrez la machine virtuelle ou physique.

```
service-control --stop vmware-std
service-control --start vmware-std
```

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

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

Par exemple :

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

Si vous spécifiez plusieurs certificats, les espaces ne sont pas autorisés entre ces certificats.

- 4 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
```

Vous pouvez utiliser ces commandes pour activer et désactiver différentes méthodes d'authentification en fonction des besoins.

- 5 (Facultatif) Pour définir une liste verte des stratégies de certificat, exécutez la commande suivante.

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

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

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

Cette liste 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.

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

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

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

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

Lorsque vous configurez l'authentification par carte à puce à partir de la ligne de commande, configurez toujours Platform Services Controller en utilisant la commande `sso-config` en premier. Puis, vous pouvez effectuer d'autres tâches à l'aide de l'interface Web de Platform Services Controller.

- 1 Configurez Platform Services Controller afin que le navigateur Web demande l'envoi du certificat par carte à puce lorsque l'utilisateur se connecte.
- 2 Configurez la stratégie d'authentification. Vous pouvez configurer la stratégie en utilisant le script `sso-config` ou l'interface Web de Platform Services Controller. La configuration des types d'authentification et des paramètres de révocation pris en charge est stockée dans VMware Directory Service et est répliquée dans toutes les instances de Platform Services Controller d'un domaine vCenter Single Sign-On.

Si l'authentification par 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 la connexion depuis vSphere Web Client ne fonctionne pas, et que l'authentification par nom d'utilisateur et par mot de passe est désactivée, un utilisateur racine ou administrateur peut réactiver l'authentification par nom d'utilisateur et par mot de passe depuis la ligne de commande de Platform Services Controller en exécutant la commande suivante. L'exemple concerne Windows ; pour Linux, utilisez `sso-config.sh`.

```
sso-config.bat -set_authn_policy -pwdAuthn true
```


Conditions préalables

- Vérifiez que votre environnement utilise Platform Services Controller version 6.0 Update 2 ou ultérieure, et que vCenter Server version 6.0 ou ultérieure est bien installé. Mettez à niveau les nœuds de version 5.5 vers la version 6.0.
- 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) qui correspond à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).
 - L'authentification du client doit être spécifiée dans le champ Stratégie d'application ou Utilisation avancée de la clé d'un certificat, sinon le navigateur n'affiche pas ce certificat.
- Vérifiez que l'interface Web de Platform Services Controller est approuvée par la station de travail de l'utilisateur final ; sinon, le navigateur ne tente pas l'authentification.
- Configurez une source d'identité Active Directory et ajoutez-la à vCenter Single Sign-On en tant que source d'identité.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent alors s'authentifier, car ils font partie du groupe Active Directory et ils ont des privilèges d'administrateur de vCenter Server. L'utilisateur administrator@vsphere.local ne peut pas effectuer d'authentification par carte à puce.
- Si vous souhaitez utiliser la solution haute disponibilité (HA, High Availability) de Platform Services Controller dans votre environnement, configurez HA avant de configurer l'authentification par carte à puce. Consultez l'article de la base de connaissances VMware [2112085](#) (Windows) ou [2113315](#) (vCenter Server Appliance).

Procédure

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

Option	Description
Windows	Connectez-vous à l'installation Windows de Platform Services Controller et utilisez WinSCP ou un utilitaire similaire pour copier les fichiers.
Dispositif	<ol style="list-style-type: none"> a Connectez-vous à la console du dispositif, soit directement soit à l'aide de SSH. b Activez l'interpréteur de commande du dispositif de la façon suivante. <pre> shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root </pre> c Utilisez WinSCP ou un utilitaire similaire pour copier les certificats dans le dossier <code>/usr/lib/vmware-sso/vmware-sts/conf</code> dans Platform Services Controller. d Vous pouvez éventuellement désactiver l'interpréteur de commande du dispositif de la façon suivante. <pre> chsh -s "bin/appliancesh" root </pre>

- 2 Sur chaque nœud Platform Services Controller, configurez les paramètres d'authentification par carte à puce en utilisant l'interface de ligne de commande de `sso-config`.
 - a Accédez au répertoire dans lequel le script `sso-config` se trouve.

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

- b Exécutez la commande suivante :

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

Par exemple :

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer,MySmartCA2.cer
-t vsphere.local
```

Séparez les certificats par des virgules, mais n'insérez pas d'espace après la virgule.

- c Redémarrez la machine virtuelle ou physique.

```
service-control --stop vmware-std
service-control --start vmware-std
```

- 3 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

- 4 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`.

- 5 Accédez à **Single Sign-On > Configuration**.

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

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

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

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

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 où vCenter Single Sign-On recherche des informations sur les certificats révoqués.

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

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

OCSP uniquement

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

CRL uniquement

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

OSCP et CRL

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

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

URL OSCP

Par défaut, vCenter Single Sign-On vérifie l'emplacement du répondeur OCSP qui est défini dans le certificat en cours de validation. Vous pouvez explicitement spécifier un emplacement si l'extension d'accès aux informations de l'autorité est absente du certificat ou si vous souhaitez la remplacer (par exemple, parce qu'elle n'est pas disponible dans votre environnement).

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 lorsque l'extension du point de distribution CRL est absente du certificat et si vous souhaitez remplacer la valeur par défaut.

Emplacement de la liste de révocation des certificats

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

En outre, vous pouvez limiter les certificats que vCenter Single Sign-On accepte en ajoutant une stratégie de certificat.

Conditions préalables

- Vérifiez que votre environnement utilise Platform Services Controller version 6.0 Update 2 ou version ultérieure, et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Mettez à niveau les nœuds de version 5.5 vers la version 6.0.
- 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) qui correspond à un compte Active Directory dans l'extension du nom de remplacement du sujet (SAN, Subject Alternative Name).

- L'authentification du client doit être spécifiée dans le champ Stratégie d'application ou Utilisation avancée de la clé d'un certificat, sinon le navigateur n'affiche pas ce certificat.
- Vérifiez que l'interface Web de Platform Services Controller est approuvée par la station de travail de l'utilisateur final ; sinon, le navigateur ne tente pas l'authentification.
- Configurez une source d'identité Active Directory et ajoutez-la à vCenter Single Sign-On en tant que source d'identité.
- Attribuez le rôle Administrateur vCenter Server à un ou plusieurs utilisateurs dans la source d'identité Active Directory. Ces utilisateurs peuvent alors s'authentifier, car ils font partie du groupe Active Directory et ils ont des privilèges d'administrateur de vCenter Server. L'utilisateur administrator@vsphere.local ne peut pas effectuer d'authentification par carte à puce.
- Si vous souhaitez utiliser la solution HA de Platform Services Controller dans votre environnement, effectuez toute la configuration HA avant de configurer l'authentification par carte à puce. Reportez-vous à l'article [2113085](#) (Windows) ou [2113315](#) (vCenter Server Appliance) de la base de connaissances VMware.

Procédure

- 1 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Accédez à **Single Sign-On > Configuration**.
- 4 Cliquez sur **Paramètres de révocation de certificats**, et activez ou désactivez la vérification de la révocation.
- 5 Si des stratégies de certificat sont en vigueur dans votre environnement, vous pouvez ajouter une stratégie dans le volet **Stratégies de certificat acceptées**.

Configurer l'authentification RSA SecurID

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

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

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 utilise Platform Services Controller version 6.0 Update 2 ou version ultérieure, et que vous utilisez vCenter Server version 6.0 ou version ultérieure. Mettez à niveau les nœuds de version 5.5 vers la version 6.0.
- Vérifiez que votre environnement dispose d'une instance de RSA Authentication Manager correctement configurée et que les utilisateurs disposent de jetons RSA. RSA Authentication Manager version 8.0 ou version ultérieure est requis.
- Vérifiez que la source d'identité qui est utilisée par RSA Manager a été ajoutée à vCenter Single Sign-On. Reportez-vous à [Ajouter une source d'identité de vCenter Single Sign-On](#).
- Vérifiez que le système RSA Authentication Manager peut résoudre le nom d'hôte de Platform Services Controller et que le système Platform Services Controller peut résoudre le nom d'hôte de RSA Authentication Manager.
- Exportez le fichier `sdconf.rec` depuis RSA Manager en sélectionnant **Accès > Agents d'authentification > Générer le fichier de configuration**. Décompressez le fichier `AM_Config.zip` résultant pour trouver le fichier `sdconf.rec`.
- Copiez le fichier `sdconf.rec` sur le nœud de Platform Services Controller.

Procédure

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

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

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

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

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

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

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

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

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

Par exemple :

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

Vous pouvez spécifier les options suivantes :

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

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

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

La valeur par défaut est généralement appropriée, par exemple :

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

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

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

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

Par exemple :

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

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

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

Résultats

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

Gérer la page de connexion

À partir de vSphere 6.0 Update 2, vous pouvez inclure une page de connexion dans votre environnement. Vous pouvez afficher du texte ou exiger que l'utilisateur clique sur une case à cocher (par exemple, pour indiquer qu'il accepte les conditions générales. Vous pouvez activer et désactiver la page de connexion, et vous pouvez exiger que les utilisateurs cliquent sur une case à cocher de consentement explicite.

Procédure

- 1 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Sous Single Sign-On, sélectionnez **Configuration**, puis cliquez sur l'onglet **Page de connexion**.
- 4 Cliquez sur **Modifier** et configurez la page de connexion.

Option	Description
État	Cliquez sur la case à cocher Activé pour activer la page de connexion. Vous ne pouvez pas modifier les autres champs tant que vous n'avez pas cliqué sur cette case à cocher.
Consentement explicite	Cliquez sur la case à cocher Consentement explicite 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.
Titre	Titre de la page. Par défaut, le texte de la page de connexion est <i>I agree to the</i> . Vous pouvez ajouter des informations à ce message, par exemple <i>Terms and Conditions</i> .
Message	Message que l'utilisateur voit lorsqu'il clique sur la page. Par exemple, le texte des termes et conditions. Le message est requis si vous utilisez le consentement explicite.

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

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

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

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

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

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

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

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

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

Ajouter un fournisseur de services SAML

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

connectent au fournisseur de services, ce dernier authentifie ces utilisateurs avec vCenter Single Sign-On.

Utilisez ce processus si vous souhaitez intégrer la solution Single Sign-On incluse avec VMware vRealize Automation 7.0 et versions ultérieures avec le fournisseur d'identité vCenter Single Sign-On ou si vous travaillez avec un autre fournisseur de services SAML externe.

Ce processus implique l'importation des métadonnées de votre fournisseur de services SAML dans vCenter Single Sign-On et l'importation des métadonnées vCenter Single Sign-On dans votre fournisseur de services SAML afin que les deux fournisseurs partagent toutes les données.

Conditions préalables

Le service cible doit entièrement prendre en charge la norme SAML 2.0.

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

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

Actuellement, vous ne pouvez pas importer des métadonnées SAML IDP à partir de vSphere Web Client.

Procédure

- 1 Exportez les métadonnées de votre fournisseur de services dans un fichier.
- 2 Importez les métadonnées du fournisseur de services dans vCenter Single Sign-On.
 - a Connectez-vous à vSphere Web Client en tant qu'administrator@vsphere.local ou un autre utilisateur disposant de privilèges d'administrateur de vCenter Single Sign-On.
Les utilisateurs disposant des privilège d'administrateur de vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.
 - b Accédez à **Single Sign-On > Configuration**.
 - c Sélectionnez l'onglet **Fournisseurs de service SAML**.
 - d Dans le champ **Métadonnées de votre fournisseur de services SAML**, cliquez sur **Importer** et collez les chaînes XML dans la boîte de dialogue ou cliquez sur **Importer à partir du fichier** pour importer un fichier, puis cliquez sur **Importer**.
- 3 Exportez des métadonnées vCenter Single Sign-On.
 - a Dans le champ **Métadonnées pour votre fournisseur de services SAML**, cliquez sur **Télécharger**.
 - b Spécifiez un emplacement du fichier.

- 4 Accédez au fournisseur de services SAML, par exemple VMware vRealize Automation 7.0 ou versions ultérieures, puis suivez les instructions de votre fournisseur de services SAML pour ajouter les métadonnées vCenter Single Sign-On à ce fournisseur de services.

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

STS (Security Token Service)

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

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

Utilisateur

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

Utilisateur d'application

Certificat valide.

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

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

Générer un nouveau certificat de signature STS sur le dispositif

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

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

Reportez-vous à la section [Générer un nouveau certificat de signature STS dans une installation vCenter Windows](#) si vous exécutez une installation Windows de Platform Services Controller.

Procédure

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

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

- 2 Copiez le fichier `certtool.cfg` dans un nouveau répertoire.

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

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

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

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

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

- 4 Générez la clé.

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

- 5 Générez le certificat.

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

- 6 Convertissez le certificat au format PK12.

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

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

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.pl2 -srcstoretype pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword

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

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

Étape suivante

Vous pouvez à présent importer le nouveau certificat. Reportez-vous à [Actualiser le certificat STS](#).

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

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

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

Si vous utilisez un dispositif virtuel, consultez [Générer un nouveau certificat de signature STS sur le dispositif](#).

Procédure

- 1 Créez un répertoire pour contenir le nouveau certificat.

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

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

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

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

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

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

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

4 Générez la clé.

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

5 Générez le certificat.

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

6 Convertissez le certificat au format PK12.

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

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

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

Étape suivante

Vous pouvez à présent importer le nouveau certificat. Reportez-vous à [Actualiser le certificat STS](#).

Actualiser le certificat STS

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

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

Utilisateur de solution

Certificat valide

Autres utilisateurs

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

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

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

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

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

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

Conditions préalables

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

Dispositif Platform Services Controller

`certificate_location/keys/root-trust.jks` Par exemple : `/keys/root-trust.jks`

Par exemple :

`/root/newsts/keys/root-trust.jks`

Installation Windows

`certificate_location\root-trust.jks`

Par exemple :

C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

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

- 3 Ajoutez le certificat.

- a Cliquez sur **Parcourir** pour accéder au fichier JKS du magasin de clés qui contient le nouveau certificat, puis cliquez sur **Ouvrir**.
- b Tapez le mot de passe lorsque vous y êtes invité.
- c Cliquez sur le haut de la chaîne d'alias STS, puis cliquez sur **OK**.
- d Retapez le mot de passe lorsque vous y êtes invité.

- 4 Cliquez sur **OK**.

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

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

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

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

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.

- 3 Cliquez sur l'onglet **Certificats**, puis sur le sous-onglet **Magasin d'approbations des sources d'identité**.
- 4 Recherchez le certificat et vérifiez la date d'expiration dans la zone de texte **Date de fin de validité**.

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

Gestion des stratégies vCenter Single Sign-On

Les stratégies vCenter Single Sign-On permettent d'appliquer les règles de sécurité au sein de votre environnement. Vous pouvez afficher et modifier les mots de passe, les stratégies de verrouillage et les stratégies de 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 de vCenter Single Sign-On est un ensemble de règles et de restrictions sur le format et l'expiration des mots de passe d'utilisateurs de vCenter Single Sign-On. La stratégie de mot de passe s'applique uniquement aux utilisateurs inclus dans le domaine vCenter Single Sign-On (vsphere.local).

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.
- 3 Cliquez sur l'onglet **Politiques** et sélectionnez **Stratégies des mots de passe**.
- 4 Cliquez sur **Modifier**.
- 5 Modifiez les paramètres de la stratégie de mot de passe.

Option	Description
Description	Description de la stratégie de mot de passe.
Durée de vie maximale	Nombre maximal de jours d'existence d'un mot de passe au terme duquel l'utilisateur doit le changer.
Restreindre la réutilisation	Nombre de mots de passe précédents de l'utilisateur qui ne peuvent être sélectionnés. Par exemple, si un utilisateur ne peut réutiliser aucun des six derniers mots de passe, tapez « 6 ».
Longueur maximale	Nombre maximal de caractères autorisés dans le mot de passe.

Option	Description
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	<p>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 :</p> <ul style="list-style-type: none"> ■ Spéciaux : & # % ■ Alphabétiques : A b c D ■ Majuscules : A B C ■ Minuscules : a b c ■ Numériques : 1 2 3 <p>Le nombre minimal de caractères alphabétiques ne doit pas être inférieur aux exigences combinées de lettres majuscules et minuscules.</p> <p>Dans vSphere 6.0 et versions ultérieures, les caractères non-ASCII sont pris en charge dans les mots de passe. Dans les versions précédentes de vCenter Single Sign-On, les caractères pris en charge sont plus limités.</p>
Caractères identiques adjacents	Nombre maximal de caractères adjacents identiques autorisés dans le mot de passe. Le nombre doit être supérieur à 0. Par exemple, si vous entrez 1, le mot de passe suivant n'est pas autorisé : p@\$\$word.

6 Cliquez sur **OK**.

Modifier la stratégie de verrouillage de vCenter Single Sign-On

Une stratégie de verrouillage de vCenter Single Sign-On spécifie les conditions dans lesquelles le compte vCenter Single Sign-On d'un utilisateur est verrouillé lorsque ce dernier tente de se connecter avec des informations d'identification incorrectes. Vous pouvez modifier la règle 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 vous permet de spécifier le nombre maximal de tentatives de connexion infructueuses et le délai entre deux tentatives. 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 à vSphere Web Client en tant qu'administrator@vsphere.local ou un autre utilisateur disposant des privilèges vCenter Single Sign-On.

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Accédez à **Administration > Single Sign-On > Configuration**.
- 3 Cliquez sur l'onglet **Règles** et sélectionnez **Règle de verrouillage**.

- 4 Cliquez sur **Edit**.
- 5 Modifiez les paramètres.

Option	Description
Description	Description facultative de la stratégie de verrouillage.
Nombre maximal de tentatives de connexion échouées	Nombre maximal de tentatives de connexion infructueuses autorisées avant que le compte soit verrouillé.
Intervalle 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.

- 6 Cliquez sur **OK**.

Modifier la stratégie des jetons de vCenter Single Sign-On

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

Procédure

- 1 Connectez-vous à vSphere Web Client.
- 2 Sélectionnez **Administration > Single Sign-On**, puis **Configuration**.
- 3 Cliquez sur l'onglet **Règles** et sélectionnez **Règle des jetons**.

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

- 4 Modifiez les paramètres de configuration de la stratégie des jetons.

Option	Description
Tolérance de l'horloge	Différence de temps, en millisecondes, que vCenter Single Sign-On tolère entre l'horloge d'un client et l'horloge du contrôleur de domaine. Si la différence de temps est supérieure à la valeur spécifiée, vCenter Single Sign-On déclare que le jeton n'est pas valide.
Nombre maximum de renouvellements de jetons	Nombre maximal de fois qu'un jeton peut être renouvelé. Une fois le nombre maximal de tentatives de renouvellement atteint, un nouveau jeton de sécurité est nécessaire.
Nombre maximum de délégations de jetons	Des jetons détenteurs de clé peuvent être délégués à des services de l'environnement vSphere. Un service qui utilise un jeton délégué s'exécute de la part du principal qui a fourni le jeton. Une demande de jeton spécifie une identité DelegateTo. La valeur de DelegateTo peut être un jeton de solution ou une référence à un jeton de solution. Cette valeur indique le nombre de fois qu'un jeton détenteur de clé peut être délégué.

Option	Description
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	<p>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 vCenter Server obtient des jetons délégués de la part d'un utilisateur et les utilise pour effectuer des opérations.</p> <p>Cette valeur détermine la durée de vie d'un jeton détenteur de clé avant que celui-ci soit marqué comme non valide.</p>

5 Cliquez sur **OK**.

Gestion des utilisateurs et des groupes vCenter Single Sign-On

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

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

- [Ajouter des utilisateurs vCenter Single Sign-On](#)

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

- [Désactiver et activer des utilisateurs de vCenter Single Sign-On](#)

Lorsqu'un compte d'utilisateur vCenter Single Sign-On est désactivé, l'utilisateur ne peut pas ouvrir de session sur le serveur vCenter Single Sign-On tant que le compte n'est pas réactivé par un administrateur. Vous pouvez désactiver et activer des utilisateurs dans l'interface vSphere Web Client.

- [Supprimer un utilisateur vCenter Single Sign-On](#)

Vous pouvez supprimer des utilisateurs qui se trouvent dans le domaine vsphere.local à partir de vCenter Single Sign-On. En revanche, vous ne pouvez pas supprimer de vSphere Web Client des utilisateurs du système d'exploitation local ou d'un autre domaine.

- [Modifier un utilisateur de vCenter Single Sign-On](#)

Vous pouvez modifier le mot de passe ou d'autres informations d'un utilisateur de vCenter Single Sign-On à partir de vSphere Web Client. Vous ne pouvez pas renommer d'utilisateurs dans le domaine vsphere.local. Vous ne pouvez donc pas renommer administrator@vsphere.local.

- **Ajouter un groupe vCenter Single Sign-On**

Dans vCenter Single Sign-On, les groupes répertoriés dans l'onglet **Groupes** sont internes à vCenter Single Sign-On. Un groupe permet de créer un conteneur pour un ensemble de membres d'un groupe (principaux).

- **Ajouter des membres à un groupe vCenter Single Sign-On**

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

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

Vous pouvez supprimer des membres d'un groupe vCenter Single Sign-On dans vSphere Web Client. Lorsque vous supprimez un membre (utilisateur ou groupe) d'un groupe local, vous ne devez pas supprimer le membre du système.

- **Supprimer des utilisateurs de la solution vCenter Single Sign-On**

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

- **Changer le mot de passe de vCenter Single Sign-On**

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

Ajouter des utilisateurs vCenter Single Sign-On

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

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 l'interface de gestion de vCenter Single Sign-On de vSphere Web Client.

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.

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

Vous ne pouvez pas ajouter des utilisateurs aux autres domaines.

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

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

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

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

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

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

- 8 Cliquez sur **OK**.

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 des utilisateurs de vCenter Single Sign-On

Lorsqu'un compte d'utilisateur vCenter Single Sign-On est désactivé, l'utilisateur ne peut pas ouvrir de session sur le serveur vCenter Single Sign-On tant que le compte n'est pas réactivé par un administrateur. Vous pouvez désactiver et activer des utilisateurs dans l'interface vSphere Web Client.

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 utilisateurs dans la page Utilisateurs et groupes vCenter.

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 à vSphere Web Client en tant qu'`administrator@vsphere.local` ou un autre utilisateur disposant des privilèges vCenter Single Sign-On.

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine `vsphere.local`.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Sélectionnez un utilisateur, cliquez sur l'icône **Désactiver**, puis cliquez sur **Oui** lorsque vous y êtes invité.
- 4 Pour réactiver l'utilisateur, cliquez avec le bouton droit sur l'utilisateur, sélectionnez **Activer**, puis cliquez sur **Oui** lorsque vous y êtes invité.

Supprimer un utilisateur vCenter Single Sign-On

Vous pouvez supprimer des utilisateurs qui se trouvent dans le domaine `vsphere.local` à partir de vCenter Single Sign-On. En revanche, vous ne pouvez pas supprimer de vSphere Web Client des utilisateurs du système d'exploitation local ou d'un autre domaine.

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 à vSphere Web Client en tant qu'`administrator@vsphere.local` ou un autre utilisateur disposant des privilèges vCenter Single Sign-On.

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine `vsphere.local`.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Sélectionnez l'onglet **Utilisateurs**, puis le domaine `vsphere.local`.
- 4 Dans la liste des utilisateurs, sélectionnez celui que vous souhaitez supprimer et cliquez sur l'icône **Supprimer**.

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

Modifier un utilisateur de vCenter Single Sign-On

Vous pouvez modifier le mot de passe ou d'autres informations d'un utilisateur de vCenter Single Sign-On à partir de vSphere Web Client. Vous ne pouvez pas renommer d'utilisateurs dans le domaine `vsphere.local`. Vous ne pouvez donc pas renommer `administrator@vsphere.local`.

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

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

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Cliquez sur l'onglet **Users**.
- 4 Cliquez-droit sur l'utilisateur et sélectionnez **Modifier l'utilisateur**.
- 5 Effectuez les modifications sur l'utilisateur.

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

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

- 6 Cliquez sur **OK**.

Ajouter un groupe vCenter Single Sign-On

Dans vCenter Single Sign-On, les groupes répertoriés dans l'onglet **Groupes** sont internes à vCenter Single Sign-On. Un groupe permet de créer un conteneur pour un ensemble de membres d'un groupe (principaux).

Lorsque vous ajoutez un groupe vCenter Single Sign-On dans l'interface d'administration de vSphere Web Client, le groupe est ajouté au domaine vsphere.local.

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Sélectionnez l'onglet **Groupes** et cliquez sur l'icône **Nouveau groupe**.
- 4 Entrez le nom et la description du groupe.

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

- 5 Cliquez sur **OK**.

Étape suivante

- Ajoutez des membres au groupe.

Ajouter des membres à un groupe vCenter Single Sign-On

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

Vous pouvez ajouter des membres de groupes Microsoft Active Directory ou OpenLDAP à un groupe vCenter Single Sign-On. Vous ne pouvez pas ajouter de groupes de sources d'identité externes à un groupe vCenter Single Sign-On.

Les groupes répertoriés dans l'onglet **Groupes** de vSphere Web Client appartiennent au domaine vsphere.local. Reportez-vous à [Groupes du domaine vsphere.local](#).

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Cliquez sur l'onglet **Groupes** et cliquez sur le groupe (par exemple, Administrateurs).
- 4 Dans la zone Membres du groupe, cliquez sur l'icône **Ajouter des membres**.
- 5 Sélectionnez la source d'identité contenant le membre à ajouter au groupe.
- 6 (Facultatif) Entrez un terme de recherche et cliquez sur **Rechercher**.
- 7 Sélectionnez le membre et cliquez sur **Ajouter**.

Vous pouvez ajouter plusieurs membres simultanément.

- 8 Cliquez sur **OK**.

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

Vous pouvez supprimer des membres d'un groupe vCenter Single Sign-On dans vSphere Web Client. Lorsque vous supprimez un membre (utilisateur ou groupe) d'un groupe local, vous ne devez pas supprimer le membre du système.

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Sélectionnez l'onglet **Groupes** et cliquez sur le groupe.
- 4 Dans la liste des membres du groupe, sélectionnez l'utilisateur ou le groupe à supprimer et cliquez sur l'icône **Supprimer un membre**.
- 5 Cliquez sur **OK**.

Résultats

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

Supprimer des utilisateurs de la solution vCenter Single Sign-On

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

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

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

Procédure

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

Les utilisateurs disposant des privilèges d'administrateur vCenter Single Sign-On font partie du groupe Administrateurs du domaine vsphere.local.

- 2 Cliquez sur **Page d'accueil**, puis accédez à **Administration > Single Sign-On > Utilisateurs et groupes**.
- 3 Cliquez sur l'onglet **Utilisateurs de la solution**, puis sur le nom d'utilisateur de solution.
- 4 Cliquez sur l'icône **Supprimer un utilisateur de la solution**.

5 Cliquez sur **Oui**.

Résultats

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

Changer le mot de passe de vCenter Single Sign-On

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

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

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 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

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

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

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

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

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

6 Cliquez sur **OK**.

Recommandations en matière de sécurité pour vCenter Single Sign-On

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

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

Vérifier l'expiration du mot de passe

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

Configurer NTP

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

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

Dépannage de vCenter Single Sign-On

Le processus de configuration de vCenter Single Sign-On peut être complexe.

Les rubriques suivantes fournissent un point de départ pour résoudre les problèmes de vCenter Single Sign-On. Recherchez des pointeurs supplémentaires dans ce centre de documentation et dans le système de base de connaissances VMware.

Détermination de la cause d'une erreur Lookup Service

L'installation de vCenter Single Sign-On affiche un message d'erreur relatif à vCenter Server ou vSphere Web Client.

Problème

Les programmes d'installation de vCenter Server et de Web Client affichent le message d'erreur `Could not contact Lookup Service. Please check VM_ssoreg.log....`

Cause

Ce problème a plusieurs causes, notamment des horloges non synchronisées sur les machines hôte, un blocage provenant du pare-feu et des services qui doivent être démarrés.

Solution

- 1 Vérifiez si les horloges des ordinateurs hôte sur lesquels vCenter Single Sign-On, vCenter Server et Web Client sont actifs sont synchronisées.
- 2 Consultez le journal spécifique qui figure dans le message d'erreur.

Dans le message, le dossier temporaire système se rapporte à %TEMP%.

- 3 Dans le fichier journal, recherchez les messages suivants.

Le fichier journal contient un sortie de toutes les tentatives d'installation. Situez le dernier message qui affiche `Initializing registration provider...`

Message	Cause et solution
java.net.ConnectException: La connexion a expiré : connect	L'adresse IP est erronée, un pare-feu bloque l'accès à vCenter Single Sign-On, ou vCenter Single Sign-On est surchargé. Assurez-vous qu'aucun pare-feu ne bloque le port vCenter Single Sign-On (par défaut 7444) et que l'ordinateur sur lequel vCenter Single Sign-On est installé dispose de suffisamment de capacité de CPU, d'E/S et de RAM.
java.net.ConnectException: Connection refused: connect	L'adresse IP ou le nom de domaine complet est erroné(e) et le service vCenter Single Sign-On n'a pas démarré ou a démarré au cours de la minute écoulée. Vérifiez que vCenter Single Sign-On fonctionne en contrôlant l'état du service vCenter Single Sign-On (sous Windows) et du daemon vmware-ssso (sous Linux). Redémarrez le service. Si cette procédure ne résout pas le problème, consultez la section récupération du Guide de dépannage de vSphere.
Code d'état inattendu : 404. Échec du serveur SSO lors de l'initialisation	Redémarrez vCenter Single Sign-On. Si cette procédure ne résout pas le problème, consultez la section Récupération du <i>Guide de dépannage de vSphere</i> .
Le message d'erreur qui s'affiche dans l'interface utilisateur commence par <code>Could not connect to vCenter Single Sign-on.</code>	Vous pouvez également voir le code de retour <code>SslHandshakeFailed</code> . Il s'agit d'une erreur inhabituelle. Elle indique que l'adresse IP ou le FQDN qui assure la résolution vers l'hôte vCenter Single Sign-On n'est pas celle/celui que vous avez utilisé(e) pendant l'installation de vCenter Single Sign-On. Dans %TEMP%\VM_ssoreg.log, recherchez la ligne qui contient le message suivant. <code>host name in certificate did not match: <install-configured FQDN or IP> != <A> or or <C></code> , A étant le nom de domaine complet que vous avez entré pendant l'installation de vCenter Single Sign-On, B et C étant des alternatives autorisées générées par le système. Corrigez la configuration pour utiliser le FQDN à droite du signe != dans le fichier journal. Dans la plupart des cas, utilisez le FQDN que vous avez spécifié pendant l'installation de vCenter Single Sign-On. Si aucune des alternatives n'est possible dans votre configuration réseau, récupérez votre configuration vCenter Single Sign-On SSL.

Impossible de se connecter à l'aide de l'authentification de domaine Active Directory

Vous vous connectez à un composant de vCenter Server dans vSphere Web Client. Vous utilisez votre nom d'utilisateur et mot de passe Active Directory. L'authentification échoue.

Problème

Vous ajoutez une source d'identité Active Directory à vCenter Single Sign-On, mais les utilisateurs ne parviennent pas à se connecter à vCenter Server.

Cause

Les utilisateurs se connectent à leur domaine par défaut à l'aide de leur nom d'utilisateur et mot de passe. Pour tous les autres domaines, ils doivent inclure le nom de domaine (utilisateur@domaine ou DOMAINE\utilisateur).

Si vous utilisez vCenter Server Appliance d'autres problèmes peuvent se produire.

Solution

Pour tous les déploiements de vCenter Single Sign-On, vous pouvez modifier la source d'identité par défaut. Une fois la modification effectuée, les utilisateurs peuvent se connecter à la source d'identité par défaut à l'aide de leur nom d'utilisateur et mot de passe uniquement.

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

Si vous utilisez vCenter Server Appliance et que la modification de la source d'identité par défaut ne résout pas le problème, effectuez l'une des interventions de dépannage supplémentaires suivantes.

- 1 Synchronisez les horloges entre vCenter Server Appliance et les contrôleurs de domaine Active Directory.
- 2 Vérifiez que chaque contrôleur de domaine dispose d'un enregistrement de pointeur (PTR) dans le service DNS du domaine Active Directory et que les informations de l'enregistrement PTR correspondent au nom DNS du contrôleur. Lors de l'utilisation de vCenter Server Appliance, vous pouvez exécuter les commandes suivantes pour effectuer la tâche :
 - a Pour répertorier les contrôleurs de domaine, exécutez la commande suivante :

```
# dig SRV _ldap._tcp.my-ad.com
```

Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

```
;; ANSWER SECTION:
_ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
...
```

- b Pour chaque contrôleur de domaine, vérifiez la résolution directe et inverse en exécutant la commande suivante :

```
# dig my-controller.my-ad.com
```

Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...
```

```
# dig -x <controller IP address>
```

Les adresses appropriées sont situées dans « answer section », comme dans l'exemple suivant :

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

- 3 Si cela ne résout pas le problème, supprimez vCenter Server Appliance du domaine Active Directory, puis rejoignez le domaine. Consultez la documentation de *Configuration de vCenter Server Appliance*.
- 4 Fermez toutes les sessions de navigateur connectées à vCenter Server Appliance et redémarrez tous les services.

```
/bin/service-control --restart --all
```

La connexion à vCenter Server échoue, car le compte utilisateur est verrouillé

Lorsque vous vous connectez à vCenter Server à partir de la page de connexion de vSphere Web Client, une erreur indique que le compte est verrouillé.

Problème

Après plusieurs tentatives infructueuses, vous ne parvenez pas à vous connecter à vSphere Web Client à l'aide de vCenter Single Sign-On. Vous voyez un message indiquant que votre compte est verrouillé.

Cause

Vous avez dépassé le nombre maximal d'échecs de tentative de connexion.

Solution

- ◆ Si vous vous connectez en tant qu'un utilisateur du domaine système (vsphere.local), demandez à votre administrateur de vCenter Single Sign-On de déverrouiller votre compte. Vous pouvez également attendre que votre compte soit déverrouillé, si l'expiration du verrouillage est prévue dans la stratégie de mot de passe. Les administrateurs vCenter Single Sign-On peuvent utiliser des commandes d'interface de ligne de commande pour déverrouiller votre compte.
- ◆ Si vous vous connectez en tant qu'un utilisateur d'un domaine Active Directory ou LDAP, demandez à votre administrateur Active Directory ou LDAP de déverrouiller votre compte.

La réplication du service d'annuaire VMware peut prendre longtemps

Si votre environnement comprend plusieurs instances de Platform Services Controller et si l'une des instances de Platform Services Controller devient indisponible, votre environnement continue à fonctionner. Lorsque le Platform Services Controller devient à nouveau disponible, les données de l'utilisateur et les autres informations sont généralement répliquées dans les 60 secondes. Dans certains cas particuliers, cependant, la réplication peut prendre du temps.

Problème

Dans certaines situations, par exemple lorsque votre environnement comprend plusieurs instances de Platform Services Controller en différents lieux, et que vous apportez des modifications significatives pendant qu'une instance de Platform Services Controller est indisponible, vous ne voyez pas immédiatement la réplication entre les instances du service d'annuaire VMware. Ainsi, vous ne voyez pas un nouvel utilisateur ajouté à l'instance de Platform Services Controller disponible dans l'autre instance tant que la réplication n'est pas terminée.

Cause

Pendant le fonctionnement normal, les modifications apportées à une instance du service d'annuaire VMware (vmdir) dans une instance de Platform Services Controller (nœud) s'affichent dans son partenaire de réplication direct approximativement dans les 60 secondes suivantes. Selon la topologie de réplication, les modifications apportées à un nœud devront peut-être se propager sur des nœuds intermédiaires avant de parvenir à chaque instance de vmdir sur chaque nœud. Les informations répliquées sont celles concernant les utilisateurs, les certificats, les licences pour les machines virtuelles créées, clonées ou migrées avec VMware VMotion, etc.

Lorsque le lien de réplication est rompu, par exemple à cause d'une panne du réseau ou de l'indisponibilité d'un nœud, il n'y a pas de convergence des modifications apportées à la fédération. Un fois le nœud indisponible restauré, chaque nœud tente de récupérer l'ensemble des modifications. Par la suite, toutes les instances de vmdir convergent vers un état cohérent, mais l'obtention de cet état cohérent peut prendre un certain temps si de nombreuses modifications ont eu lieu pendant qu'un nœud était indisponible.

Solution

Votre environnement fonctionne normalement pendant que la réplication a lieu. Ne tentez pas de résoudre le problème, sauf s'il persiste pendant plus d'une heure.

Certificats de sécurité vSphere

3

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

Les certificats sont également utilisés par les services vCenter Server, tels que vSphere Web Client, pour l'authentification initiale auprès de vCenter Single Sign-On. vCenter Single Sign-On provisionne chaque composant avec un jeton SAML que le composant utilise pour l'authentification ultérieure.

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

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

Tableau 3-1. Différentes approches du remplacement de certificat

Option	Reportez-vous au
Utilisez l'interface web Platform Services Controller (vSphere 6.0 Update 1 et ultérieur).	Gestion de certificats avec l'interface Web Platform Services Controller
Utilisez l'utilitaire vSphere Certificate Manager à partir de la ligne de commande.	Gestion de certificats avec l'utilitaire vSphere Certificate Manager
Utilisez les commandes CLI pour remplacer des certificats manuellement.	Gestion des certificats et des services avec les commandes de l'interface de ligne de commande



Gestion des certificats vSphere

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

Ce chapitre contient les rubriques suivantes :

- [Exigences en matière de certificats pour les différents chemins d'accès aux solutions](#)
- [Présentation de la gestion de certificats](#)
- [Gestion de certificats avec l'interface Web Platform Services Controller](#)
- [Gestion de certificats avec l'utilitaire vSphere Certificate Manager](#)

- Remplacement manuel de certificats
- Gestion des certificats et des services avec les commandes de l'interface de ligne de commande
- Afficher les certificats vCenter dans vSphere Web Client
- Définir le seuil pour les avertissements d'expiration du certificat vCenter

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

Les exigences en matière de certificats varient si vous utilisez VMCA comme autorité de certification intermédiaire ou si vous utilisez des certificats personnalisés. Les exigences sont également différentes pour les certificats de machine et pour les certificats d'utilisateur de solution.

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

Exigences pour tous les certificats importés

- Taille de clé : 2 048 bits ou plus (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, non-répudiation, chiffrement de clé.
- L'authentification du client et l'authentification du serveur ne peuvent pas se trouver sous Utilisation avancée de la clé.

VMCA ne prend pas en charge les certificats suivants.

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

Conformité du certificat à 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 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 Certificate Manager, vous êtes invité à entrer les informations suivantes, et 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.
- Si vous générez une demande de signature de certificat dans un environnement avec une instance de Platform Services Controller externe, vous êtes invité à entrer le nom d'hôte ou l'adresse IP de Platform Services Controller.
- Informations que Certificate Manager enregistre dans le fichier `certtool.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.
 - Si vous exécutez la commande sur un nœud vCenter Server (gestion), l'adresse IP de Platform Services Controller

Exigences 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	<ul style="list-style-type: none"> ■ Vous pouvez utiliser vSphere Certificate Manager pour générer la demande de signature de certificat. Reportez-vous à Générer une demande de signature de certificat avec vSphere 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 : <ul style="list-style-type: none"> ■ Taille de clé : 2 048 bits ou plus ■ Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8 ■ x509 version 3 ■ Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises. ■ La signature CRL doit être activée. ■ L'utilisation avancée de la clé ne doit impliquer ni authentification client ni authentification 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. <p>Reportez-vous à l'article 2112009 de la base de connaissances de VMware, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0, pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.</p>
Certificat SSL de machine	<p>Vous pouvez utiliser vSphere Certificate Manager pour créer la demande de signature de certificat ou pour créer manuellement la demande de signature de certificat.</p> <p>Si vous créez manuellement la demande de signature de certificat, elle doit répondre aux exigences répertoriées sous <i>Exigences pour tous les certificats importés</i> ci-dessus. Vous devez également spécifier le nom de domaine complet de l'hôte.</p>
Certificat d'utilisateur de solution	<p>Vous pouvez utiliser vSphere Certificate Manager pour créer la demande de signature de certificat ou pour créer manuellement la demande de signature de certificat.</p>

Type de certificat	Exigences en matière de certificats
	<p>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.</p> <p>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 <code>certtool.cfg</code>. Consultez la section <i>Informations requises par Certificate Manager</i>.</p>

Exigences pour les 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	<p>Le certificat SSL de machine sur chaque nœud doit avoir un certificat distinct de votre autorité de certification d'entreprise ou tierce.</p> <ul style="list-style-type: none"> ■ Vous pouvez générer les demandes de signature de certificat à l'aide de vSphere Certificate Manager ou en créer une manuellement. La demande de signature de certificat doit répondre aux exigences répertoriées sous <i>Exigences pour tous les certificats importés</i>. ■ 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 <code>certtool.cfg</code>. Consultez la section <i>Informations requises par Certificate Manager</i>. ■ 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	<p>Chaque utilisateur de solution sur chaque nœud doit avoir un certificat distinct de votre autorité de certification d'entreprise ou tierce.</p> <ul style="list-style-type: none"> ■ 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 sous <i>Exigences pour tous les certificats importés</i>. ■ 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 <code>certtool.cfg</code>. Consultez la section <i>Informations requises par Certificate Manager</i>. <p>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.</p> <p>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.</p>

Note N'utilisez pas les points de distribution CRL, l'accès aux informations de l'autorité ni les informations de modèle de certificat dans les certificats personnalisés.

Présentation de la gestion de certificats

L'impact de la nouvelle infrastructure de certificats dépend des exigences de votre environnement, selon que vous effectuez une installation nouvelle ou une mise à niveau et selon que vous envisagez ESXi ou vCenter Server.

Administrateurs qui ne remplacent pas les certificats VMware

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

Administrateurs qui remplacent les certificats VMware par des certificats personnalisés

Pour les installations nouvelles, les administrateurs disposent de ces choix si la stratégie de l'entreprise exige des certificats signés par une autorité de certification tierce ou de l'entreprise ou demande des informations de certificats personnalisées.

- Remplacez le certificat racine VMCA par un certificat signé par une autorité de certification. Dans ce scénario, le certificat VMCA est un certificat intermédiaire de cette autorité de certification tierce. VMCA fournit aux composants de vCenter Server et aux hôtes ESXi des certificats qui incluent la chaîne complète de certificats.
- Si la stratégie d'une entreprise n'autorise pas les certificats intermédiaires dans la chaîne, vous devez remplacer les certificats de façon explicite. Vous pouvez utiliser 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 des certificats.

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

Après la mise à niveau de vCenter Server, les administrateurs peuvent définir le mode de certification sur Personnalisé (voir [Changer le mode de certificat](#)). Si le mode de certificat est VMCA (valeur par défaut) et si l'utilisateur effectue une actualisation des certificats à partir de vSphere Web Client, les certificats signés par l'autorité de certification VMware (VMCA) remplacent les certificats personnalisés.

- Pour les composants vCenter Server, ce qui se produit dépend de l'environnement existant.
 - Si vous effectuez la mise à niveau d'une installation simple vers un déploiement intégré, les certificats personnalisés de vCenter Server sont conservés. Après la mise à niveau, votre environnement fonctionne comme auparavant.
 - Si vous mettez à niveau un déploiement multi-site dans lequel vCenter Single Sign-On se trouve sur une machine différente des autres composants vCenter Server, le processus de mise à niveau crée un déploiement à plusieurs nœuds qui inclut un nœud Platform Services Controller et un ou plusieurs nœuds de gestion.

Dans ce scénario, les certificats existants de vCenter Server et de vCenter Single Sign-On sont conservés en tant que certificats SSL de la machine. VMCA attribue un certificat signé par VMCA à chaque utilisateur de solution (collection de services vCenter). Un utilisateur de solution n'utilise ce certificat que pour s'authentifier auprès de vCenter Single Sign-On, de sorte qu'il peut ne pas être nécessaire de remplacer les certificats d'utilisateurs de solutions.

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

Interfaces de certificat vCenter

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

Utilitaire vSphere Certificate Manager

Effectuez toutes les tâches courantes de remplacement de certificat à partir de la ligne de commande.

Interfaces de ligne de commande de gestion de certificats

Effectuez toutes les tâches de gestion de certificats avec `dir-cli`, `certool` et `vecs-cli`.

Gestion des certificats vSphere Web Client

Affichez les certificats, y compris les informations d'expiration.

Pour ESXi, effectuez la gestion des certificats à partir de vSphere Web Client. Les certificats sont provisionnés par VMCA et ne sont stockés localement que sur l'hôte ESXi, non pas dans vmdir ou VECS. Reportez-vous à [Gestion de certificats pour les hôtes ESXi](#).

Certificats vCenter pris en charge

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

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

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

Présentation du remplacement des certificats

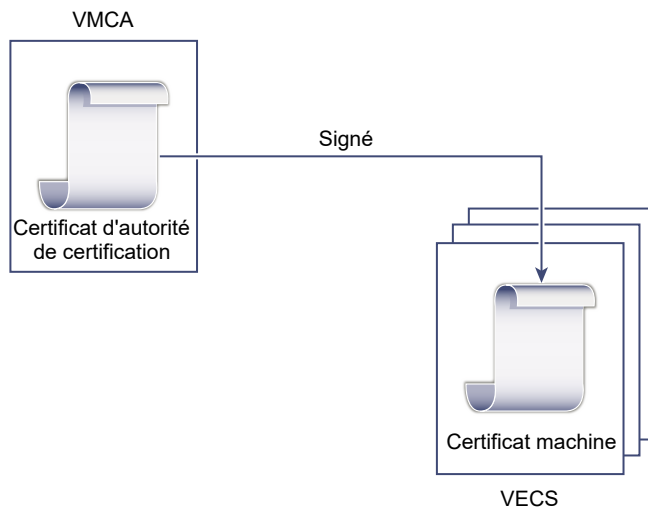
Vous pouvez effectuer différents types de remplacement de certificats selon la stratégie et les besoins de l'entreprise pour le système que vous configurez. Vous pouvez effectuer chaque remplacement avec l'utilitaire vSphere Certificate Manager ou manuellement à l'aide des interfaces de ligne de commande incluses avec votre installation.

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

Remplacer par des certificats signés par VMCA

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

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

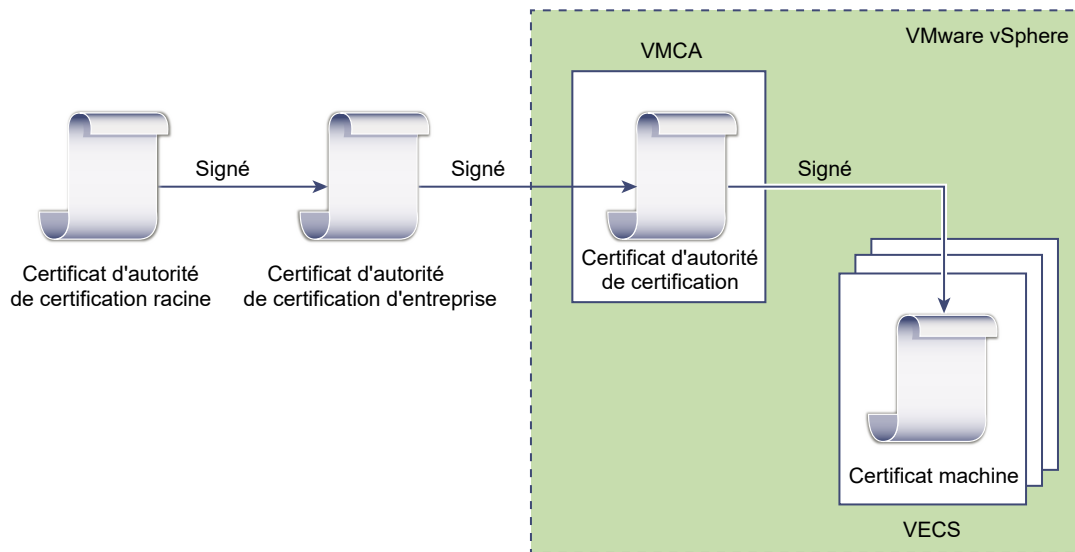


Faire de VMCA une autorité de certificat intermédiaire

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

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

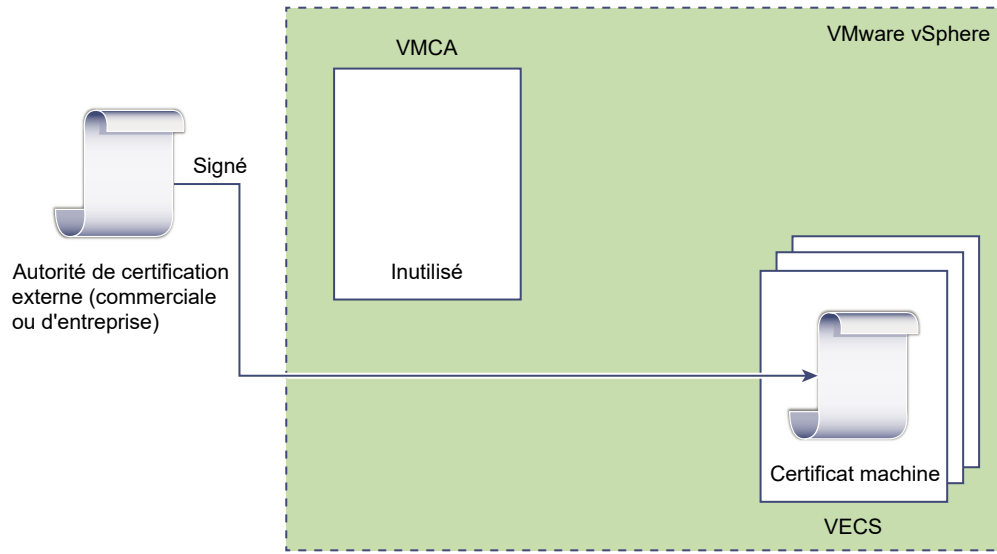
Figure 3-2. Les certificats signés par une autorité de certification tierce ou d'entreprise utilisent VMCA comme autorité de certification intermédiaire



Ne pas utiliser VMCA, provisionner avec des certificats personnalisés

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

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



Déploiement hybride

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

Remplacement des certificats ESXi

Pour les hôtes ESXi, vous pouvez modifier le comportement de provisionnement de certificats à partir de vSphere Web Client.

Mode d'autorité de certification VMware (par défaut)

Lorsque vous renouvelez des certificats à partir de vSphere Web Client, VMCA émet les certificats pour les hôtes. Si vous modifiez le certificat racine VMCA de manière à inclure une chaîne de certificats, les certificats hôtes incluent la chaîne complète.

Mode d'autorité de certification personnalisée

Vous permet de manuellement mettre à jour et d'utiliser des certificats qui ne sont pas signés ou émis par VMCA.

Mode d'empreinte

Peut être utilisé pour conserver les certificats 5.5 pendant l'actualisation. Utilisez ce mode uniquement temporairement dans des situations de débogage.

Où vSphere 6.0 utilise des certificats

Dans vSphere 6.0 et version ultérieure, l'autorité de certification VMware (VMCA) provisionne votre environnement avec des certificats. Ceci inclut les certificats SSL de la machine pour les connexions sécurisées, les certificats d'utilisateurs de solutions pour l'authentification à vCenter Single Sign-On et les certificats pour les hôtes ESXi qui sont ajoutés à vCenter Server.

Les certificats suivants sont utilisés.

Tableau 3-2. Certificats dans vSphere 6.0

Certificat	Provisionné par	Stocké
Certificats ESXi	VMCA (par défaut)	Localement sur l'hôte ESXi
Certificats SSL de la machine	VMCA (par défaut)	VECS
Certificats d'utilisateurs de solutions	VMCA (par défaut)	VECS
Certificat de signature SSL vCenter Single Sign-On	Provisionné au cours de l'installation.	Gérez ce certificat dans vSphere Web Client. Avertissement Ne modifiez pas ce certificat dans le système de fichiers pour éviter de provoquer des résultats imprévisibles.
Certificat SSL du service d'annuaire VMware (vmdir)	Provisionné au cours de l'installation.	Dans certains cas marginaux, il se peut que vous deviez remplacer ce certificat. Reportez-vous à Remplacer le certificat de service d'annuaire VMware .

ESXi

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

Certificats SSL de la machine

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

Tous les services communiquent par l'intermédiaire du proxy inverse. Pour des raisons de compatibilité, les services qui étaient disponibles dans les versions précédentes de vSphere utilisent également des ports spécifiques. Par exemple, le service vpxd utilise MACHINE_SSL_CERT pour exposer son point de terminaison.

Chaque nœud (déploiement intégré, nœud de gestion ou Platform Services Controller) a son propre certificat SSL de machine. Tous les services exécutés sur ce nœud utilisent ce certificat SSL de machine pour exposer leurs points de terminaison.

Le certificat SSL de la machine s'utilise de la façon suivante :

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

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

Certificats d'utilisateurs de solutions

Un utilisateur de solution encapsule un ou plusieurs services vCenter Server et utilise les certificats pour s'authentifier auprès de vCenter Single Sign-On par l'intermédiaire de l'échange de jetons SAML. Chaque utilisateur de solution doit être authentifié auprès de vCenter Single Sign-On.

Les certificats d'utilisateurs de solutions sont utilisés pour l'authentification auprès de vCenter Single Sign-On. 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 Web 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'utilisateurs de solutions sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré :

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

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

Le magasin de machines est également inclus sur chaque nœud Platform Services Controller.

Certificats vCenter Single Sign-On

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

Certificat de signature vCenter Single Sign-On

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

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

Vous pouvez remplacer ce certificat dans vSphere Web Client. Reportez-vous à [Actualiser le certificat STS](#).

Certificat SSL du service d'annuaire VMware

Si vous utilisez des certificats personnalisés, il se peut que vous deviez remplacer le certificat SSL du service d'annuaire VMware de façon explicite. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

VMCA et VMware Core Identity Services

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

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

Tableau 3-3. Services d'identité de base

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

Présentation du magasin de certificats VMware Endpoint

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

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

VECS interroge périodiquement le service d'annuaire de VMware (vmdir) en vue d'éventuelles mises à jour du magasin TRUSTED_ROOTS. Vous pouvez également gérer explicitement les certificats et les clés dans VECS à l'aide des commandes `vecs-cli`. Reportez-vous à [Référence des commandes vecs-cli](#).

VECS inclut les magasins suivants.

Tableau 3-4. Magasins dans VECS

Magasin	Description
Magasin de certificats SSL de la machine (MACHINE_SSL_CERT)	<ul style="list-style-type: none">■ Utilisé par le service de proxy inverse sur chaque nœud vSphere.■ Utilisé par le service d'annuaire VMware (vmdir) sur les déploiements intégrés et sur chaque nœud Platform Services Controller. <p>Tous les services de vSphere 6.0 communiquent par l'intermédiaire d'un proxy inversé qui utilise le certificat SSL de machine. Pour la compatibilité descendante, les services 5.x utilisent toujours des ports spécifiques. En conséquence, certains services tels que vpxd ont toujours leur port ouvert.</p>
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.

Tableau 3-4. Magasins dans VECS (suite)

Magasin	Description
Magasins d'utilisateurs de solution	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).
■ virtuelle	Les certificats d'utilisateurs de solutions sont utilisés pour l'authentification avec vCenter Single Sign-On. vCenter Single Sign-On vérifie que le certificat est valide, mais ne vérifie pas d'autres attributs de certificat. Dans un déploiement intégré, tous les certificats d'utilisateur de la solution se trouvent sur le même système.
■ vpxd	Les magasins de certificats d'utilisateurs de solutions sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré :
■ vpxd-extensions	■ <code>machine</code> : Utilisé par le gestionnaire de composants, le serveur de licences et le service de journalisation.
■ vsphere-webclient	<p>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.</p> <p>■ <code>vpxd</code> : Magasin du démon de service vCenter (vpxd) sur les nœuds de gestion et les déploiements intégrés. vpxd utilise le certificat d'utilisateur de solution de ce magasin pour s'authentifier auprès de vCenter Single Sign-On.</p> <p>■ <code>vpxd-extensions</code> : Magasin d'extensions vCenter. Inclut le service Auto Deploy, Inventory Service et d'autres services ne faisant pas partie d'autres utilisateurs de solution.</p> <p>■ <code>vsphere-webclient</code> : Magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance.</p> <p>Le magasin de machines est également inclus sur chaque nœud Platform Services Controller.</p>

Tableau 3-4. 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	<p>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 la base de connaissances VMware vous y invite.</p> <p>Note Les CRLS ne sont pas pris en charge dans vSphere 6.0. Néanmoins, 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.</p>

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

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.

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

Gestion de la révocation de certificat

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

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

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

Remplacement des certificats dans les déploiements à grande échelle

Le remplacement des certificats dans les déploiements qui incluent plusieurs nœuds de gestion et un ou plusieurs nœuds Platform Services Controller est semblable au remplacement dans les déploiements intégrés. Dans les deux cas, vous pouvez utiliser l'utilitaire de gestion des certificats

vSphere ou remplacer les certificats manuellement. Certaines pratiques recommandées guident le processus de remplacement.

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

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

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

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

vSphere Certificate Manager

Exécutez vSphere Certificate Manager sur chaque machine. Sur les nœuds de gestion, vous êtes invité à fournir l'adresse IP de Platform Services Controller. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat.

Remplacement manuel de certificats

Pour le remplacement manuel des certificats, exécutez les commandes de remplacement des certificats sur chaque machine. Sur les nœuds de gestion, vous devez spécifier le Platform Services Controller avec le paramètre `--server`. Consultez les rubriques suivantes pour plus d'informations :

- [Remplacer les certificats SSL de la machine par des certificats signés par VMCA](#)
- [Remplacer les certificats SSL de la machine \(autorité de certification intermédiaire\)](#)
- [Remplacer les certificats SSL de machine par des certificats personnalisés](#)

Remplacement des certificats d'utilisateurs de solutions dans les environnements qui incluent plusieurs nœuds de gestion

Si votre environnement comporte plusieurs nœuds de gestion et un seul Platform Services Controller, suivez la procédure ci-dessous pour remplacer des certificats.

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. Sur les nœuds de gestion, vous êtes invité à fournir l'adresse IP de Platform Services Controller. Selon la tâche, vous êtes également invité à fournir les informations relatives au certificat.

Remplacement manuel de certificats

- 1 Générez ou demandez un certificat. Vous devez disposer des certificats suivants :
 - Un certificat d'utilisateur de solution de machine sur Platform Services Controller.
 - Un certificat d'utilisateur de solution de machine sur chaque nœud de gestion.
 - Un certificat pour chacun des utilisateurs de solutions suivants sur chaque nœud de gestion :
 - utilisateur de solution vpxd
 - utilisateur de solution vpxd-extension
 - utilisateur de solution vsphere-webclient
- 2 Remplacez les certificats sur chaque nœud. La précision de la procédure dépend du type de remplacement de certificat que vous effectuez. Reportez-vous à [Gestion de certificats avec l'utilitaire vSphere Certificate Manager](#)

Consultez les rubriques suivantes pour plus d'informations :

- [Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA](#)
- [Remplacer les certificats d'utilisateurs de solution \(autorité de certification intermédiaire\)](#)
- [Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés](#)

Si la stratégie d'une entreprise exige que vous remplaciez tous les certificats, vous devez également remplacer le certificat du service d'annuaire VMware (vmdir) sur Platform Services Controller. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

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 le système vCenter Server ou Platform Services Controller. Si vous remplacez le certificat SSL machine par défaut sur le système vCenter Server ou Platform Services Controller, une erreur de connexion se produit si la solution tente de se connecter au système vCenter Server.

Vous pouvez exécuter le script `ls_update_certs` pour résoudre le problème. Reportez-vous à [l'article 2109074 de la base de connaissances VMware](#) pour obtenir plus de détails.

Gestion de certificats avec l'interface Web Platform Services Controller

Vous pouvez afficher et gérer des certificats en vous connectant à l'interface Web Platform Services Controller. Vous pouvez réaliser de nombreuses tâches de gestion de certificats via l'utilitaire vSphere Certificate Manager ou à l'aide de cette interface Web.

L'interface Web Platform Services Controller vous permet de réaliser ces tâches de gestion.

- Affichez les magasins de certificats actuels, et ajoutez et supprimez des entrées de magasin de certificats.
- Explorez l'instance de VMware Certificate Authority (VMCA) associée à cette instance de Platform Services Controller.
- Affichez les certificats générés par VMware Certificate Authority.
- Renouvelez les certificats existants ou remplacez des certificats.

Les workflows de remplacement de certificat sont en grande partie entièrement pris en charge à partir de l'interface Web de Platform Services Controller. Pour générer des demandes de signature de certificat, vous pouvez employer l'utilitaire vSphere Certificate Manager.

Workflows pris en charge

Après l'installation d'une instance de Platform Services Controller, VMware Certificate Authority sur ce nœud provisionne tous les autres nœuds de l'environnement avec des certificats par défaut. Vous pouvez utiliser l'un des workflows suivants pour renouveler ou remplacer des certificats.

Renouveler les certificats

Vous pouvez demander à VMCA de générer un nouveau certificat racine et de renouveler tous les certificats de votre environnement depuis l'interface Web de Platform Services Controller.

Faire de VMCA une autorité de certificat intermédiaire

Vous pouvez générer une demande de signature de certificat à l'aide de l'utilitaire vSphere Certificate Manager, modifier le certificat que vous avez reçu de CSR pour ajouter VMCA à la chaîne, puis ajouter la chaîne de certificats et la clé privée à votre environnement. Lorsque vous renouvelez tous les certificats, VMCA provisionne toutes les machines et tous les utilisateurs de solutions avec des certificats qui sont signés par la chaîne complète.

Remplacer des certificats par des certificats personnalisés

Si vous ne souhaitez pas utiliser VMCA, vous pouvez générer des demandes de signature de certificat pour les certificats que vous souhaitez remplacer. L'autorité de certification renvoie un certificat racine et un certificat signé pour chaque demande de signature de certificat. Vous pouvez télécharger le certificat racine et les certificats personnalisés à partir de Platform Services Controller.

Si vous devez remplacer le certificat racine de VMware Directory Service (vmdir) ou si la stratégie d'entreprise exige que vous remplaciez le certificat vCenter Single Sign-On dans un environnement en mode mixte, vous pouvez utiliser des commandes de ligne de commande pour remplacer les autres certificats. Reportez-vous aux sections [Remplacer le certificat de service d'annuaire VMware](#) et [Remplacer le certificat VMware Directory Service dans des environnement en mode mixte](#).

Explorer les magasins de certificats à partir de l'interface Web Platform Services Controller

Une instance du magasin de certificats VECS (VMware Endpoint Certificate Store) est incluse sur chaque nœud Platform Services Controller et chaque nœud vCenter Server. Vous pouvez explorer les différents magasins compris dans VMware Endpoint Certificate Store à partir de l'interface Web Platform Services Controller.

Consultez la section [Présentation du magasin de certificats VMware Endpoint](#) 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 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Sous Certificats, cliquez sur **Magasin de certificats** et explorez le magasin.
- 4 Sélectionnez le magasin dans le magasin VECS (VMware Endpoint Certificate Store) que vous souhaitez explorer à partir du menu déroulant.

La section [Présentation du magasin de certificats VMware Endpoint](#) décrit le contenu des magasins individuels.

- 5 Pour afficher les détails d'un certificat, sélectionnez celui-ci et cliquez sur l'icône **Afficher les détails**.
- 6 Pour supprimer une entrée du magasin sélectionné, cliquez sur l'icône **Supprimer une entrée**.
Par exemple, si vous remplacez le certificat existant, vous pouvez ensuite supprimer l'ancien certificat racine. Supprimez des certificats uniquement si vous êtes sûr qu'ils ne sont plus utilisés.

Remplacer les certificats par de nouveaux certificats signés par VMCA depuis l'interface Web de Platform Services Controller

Vous pouvez remplacer tous les certificats signés par VMCA par de nouveaux certificats signés par VMCA ; ce processus se nomme renouvellement de certificat. Vous pouvez renouveler les certificats sélectionnés ou tous les certificats de votre environnement depuis l'interface web Platform Services Controller.

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 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.
- 4 Renouvelez le certificat SSL de la machine pour le système local.
 - a Cliquez sur l'onglet **Certificats de machine**.
 - b Sélectionnez le certificat, cliquez sur **Renouveler**, puis répondez **Oui** à l'invite.
- 5 (facultatif) Renouvelez les certificats d'utilisateur de solution pour le système local.
 - a Cliquez sur l'onglet **Certificats d'utilisateur de solution**.
 - b Sélectionnez un certificat, puis cliquez sur **Renouveler** pour renouveler les certificats individuels sélectionnés ou cliquez sur **Renouveler tout** pour renouveler tous les certificats d'utilisateur de solution.
 - c Répondez **Oui** à l'invite.
- 6 Si votre environnement inclut un Platform Services Controller externe, vous pouvez renouveler les certificats pour chaque système vCenter Server.
 - a Cliquez sur le bouton **Se déconnecter** dans le panneau Gestion des certificats.
 - b Lorsque vous y êtes invité, spécifiez l'adresse IP ou le nom de domaine du système vCenter Server ainsi que le nom d'utilisateur et le mot de passe d'un administrateur vCenter Server pouvant s'authentifier auprès de vCenter Single Sign-On.
 - c Renouvelez le certificat SSL de la machine dans vCenter Server et, si vous le souhaitez, chaque certificat d'utilisateur de solution.
 - d Si votre environnement comprend plusieurs systèmes vCenter Server, répétez la procédure pour chaque système.

Étape suivante

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement

`VCENTER_INSTALL_PATH\bin.`

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Faire de VMCA une autorité de certification intermédiaire depuis l'interface web de Platform Services Controller

Vous pouvez faire signer le certificat VMCA par une autre autorité de certification afin que VMCA devienne par la suite une autorité de certification intermédiaire. Tous les certificats générés par VMCA incluent la chaîne complète.

Vous pouvez réaliser cette configuration en utilisant l'utilitaire vSphere Certificate Manager, les CLI ou l'interface web Platform Services Controller.

Conditions préalables

- 1 Générer la demande de signature de certificat.
- 2 Modifiez le certificat que vous recevez et placez le certificat racine VMCA actuel en bas.

[Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine \(autorité de certification intermédiaire\)](#) explique les deux étapes.

Procédure

- 1 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Pour remplacer le certificat existant par le certificat chaîné, procédez comme suit :
 - a Dans Certificats, cliquez sur **Autorité de certification** et sélectionnez l'onglet **Certificat racine**.
 - b Cliquez sur **Remplacer le certificat**. Ajoutez le fichier de clé privée et le fichier de certificat (chaîne complète), puis cliquez sur **OK**.
 - c Dans la boîte de dialogue **Remplacer le certificat racine**, cliquez sur **Parcourir** et sélectionnez la clé privée, cliquez de nouveau sur **Parcourir** et sélectionnez le certificat, puis cliquez sur **OK**.

Par la suite, VMCA signe tous les certificats qu'il émet avec le nouveau certificat racine chaîné.

- 4 Renouvelez le certificat SSL de la machine pour le système local.
 - a Sous Certificats, cliquez sur **Gestion des certificats**, puis cliquez dans l'onglet **Certificats de la machine**.
 - b Sélectionnez le certificat, cliquez sur **Renouveler**, puis répondez **Oui** à l'invite.

VMCA remplace le certificat de la machine SSL par le certificat signé par la nouvelle autorité de certification.

- 5 (Facultatif) Renouvelez les certificats d'utilisateur de solution pour le système local.
 - a Cliquez sur l'onglet **Certificats d'utilisateur de solution**.
 - b Sélectionnez un certificat, puis cliquez sur **Renouveler** pour renouveler des certificats individuels sélectionnés ou cliquez sur **Renouveler tout** pour remplacer tous les certificats et répondez **Oui** à l'invite.

VMCA remplace le certificat d'utilisateur de solution ou tous les certificats d'utilisateur de solution par des certificats signés par la nouvelle autorité de certification.

- 6 Si votre environnement inclut un Platform Services Controller externe, vous pouvez renouveler les certificats pour chaque système vCenter Server.
 - a Cliquez sur le bouton **Se déconnecter** dans le panneau Gestion des certificats.
 - b Lorsque vous y êtes invité, spécifiez l'adresse IP ou le nom de domaine du système vCenter Server ainsi que le nom d'utilisateur et le mot de passe d'un administrateur vCenter Server pouvant s'authentifier auprès de vCenter Single Sign-On.
 - c Renouvelez le certificat SSL de la machine dans vCenter Server et, si vous le souhaitez, chaque certificat d'utilisateur de solution.
 - d Si votre environnement comprend plusieurs systèmes vCenter Server, répétez la procédure pour chaque système.

Étape suivante

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement `VCENTER_INSTALL_PATH\bin.`

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Configurer votre système pour utiliser des certificats personnalisés depuis Platform Services Controller

Vous pouvez utiliser Platform Services Controller pour configurer votre environnement de manière à utiliser des certificats personnalisés.

Vous pouvez générer des demandes de signature de certificat (CSR, Certificate Signing Requests) pour chaque machine et pour chaque utilisateur de solution employant l'utilitaire Certificate Manager. Lorsque vous soumettez les demandes de signature de certificat à votre autorité de certification interne ou tierce, l'autorité de certification renvoie les certificats signés et le certificat racine. Vous pouvez télécharger le certificat racine et les certificats signés à partir de l'interface utilisateur de Platform Services Controller.

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

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR, Certificate Signing Request) que vous pouvez ensuite utiliser avec votre autorité de certification d'entreprise ou envoyer à une autorité de certification externe. Vous pouvez utiliser les certificats avec les différents processus de remplacement de certificat pris en charge.

Vous pouvez exécuter l'outil Certificate Manager sur la ligne de commande comme suit :

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

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.
- Si vous générez une demande de signature de certificat dans un environnement avec une instance de Platform Services Controller externe, vous êtes invité à entrer le nom d'hôte ou l'adresse IP de Platform Services Controller.
- Pour générer une demande de signature du certificat SSL d'une machine, vous êtes invité à entrer les propriétés du certificat, qui sont stockées dans le fichier `certtool.cfg`. Pour la plupart des champs, vous pouvez accepter les valeurs par défaut ou entrer des valeurs spécifiques au site. Le FQDN de la machine est requis.

Procédure

- 1 Sur chaque machine de votre environnement, démarrez vSphere Certificate Manager et sélectionnez l'option 1.
- 2 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
- 3 Sélectionnez l'option 1 pour générer la demande de signature de certificat, répondez aux invites et quittez Certificate Manager.

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

- 4 Si vous souhaitez remplacer tous les certificats d'utilisateurs de solutions, redémarrez Certificate Manager.
- 5 Sélectionnez l'option 5.
- 6 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.

- 7 Sélectionnez l'option 1 pour générer les demandes de signature de certificat, répondez aux invites et quittez Certificate Manager.

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

Sur chaque nœud de Platform Services Controller, Certificate Manager génère un certificat et une paire de clés. Sur chaque nœud vCenter Server, Certificate Manager génère quatre certificats et paires de clés.

Étape suivante

Effectuez le remplacement de certificats.

Ajouter un certificat racine approuvé au magasin de certificats

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

Conditions préalables

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

Procédure

- 1 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.

- 4 Sélectionnez **Certificats racines approuvés**, puis cliquez sur **Ajouter un certificat**.

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

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

Étape suivante

Remplacez les certificats SSL de la machine et, facultativement, les certificats d'utilisateur de solution par des certificats signés par cette autorité de certification.

Ajouter des certificats personnalisés à partir de Platform Services Controller

Vous pouvez ajouter des certificats SSL de la machine et des certificats d'utilisateur de solution personnalisés au magasin de certificats à partir de Platform Services Controller.

Dans la plupart des cas, il suffit de remplacer le certificat SSL de la machine pour chaque composant. Le certificat de l'utilisateur de solution reste derrière un proxy.

Conditions préalables

Générez des demandes de signature de certificat (CSR, Certificate Signing Request) pour chaque certificat que vous souhaitez remplacer. Vous pouvez générer les CSR avec l'utilitaire Certificate Manager. Placez le certificat et la clé privée dans un emplacement accessible par Platform Services Controller.

Procédure

- 1 Dans un navigateur Web, connectez-vous à Platform Services Controller en spécifiant l'URL suivante :

`https://psc_hostname_or_IP/psc`

Dans un déploiement intégré, le nom d'hôte ou l'adresse IP de Platform Services Controller est identique au nom d'hôte ou à l'adresse IP de vCenter Server.

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

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

- 3 Sous Certificats, sélectionnez **Gestion des certificats** et spécifiez l'adresse et le nom d'hôte de Platform Services Controller, ainsi que le nom d'utilisateur et le mot de passe de l'administrateur du domaine local (administrator@vsphere.local par défaut), puis cliquez sur **Soumettre**.

- 4 Pour remplacer un certificat de la machine, procédez comme suit :

- a Sélectionnez l'onglet **Certificats de la machine** et cliquez sur le certificat que vous souhaitez remplacer.
- b Cliquez sur **Remplacer**, puis sur **Parcourir** pour remplacer la chaîne de certificats, puis sur **Parcourir** pour remplacer la clé privée.

- 5 Pour remplacer les certificats d'utilisateur de la solution, procédez comme suit :

- a Sélectionnez l'onglet **Certificats d'utilisateurs de solutions**, puis cliquez sur le premier des quatre certificats d'un composant, par exemple, **machine**.
- b Cliquez sur **Remplacer**, puis sur **Parcourir** pour remplacer la chaîne de certificats, puis sur **Parcourir** pour remplacer la clé privée.
- c Recommencez le processus pour les trois autres certificats du même composant.

Étape suivante

Redémarrez les services sur Platform Services Controller. Vous pouvez redémarrer Platform Services Controller ou exécuter les commandes suivantes depuis la ligne de commande :

Windows

Sous Windows, la commande service-contrôle se trouve à l'emplacement `VCENTER_INSTALL_PATH\bin`.

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

Gestion de certificats avec l'utilitaire vSphere Certificate Manager

L'utilitaire vSphere Certificate Manager vous permet de réaliser la plupart des tâches de gestion des certificats de manière interactive, à partir de la ligne de commande. vSphere Certificate Manager vous demande la tâche à réaliser, l'emplacement des certificats, ainsi que d'autres informations si nécessaire, puis active et arrête les services et remplace les certificats.

Si vous utilisez vSphere Certificate Manager, vous n'avez pas à placer les certificats dans VECS (VMware Endpoint Certificate Store), ni à démarrer et à arrêter les services.

Avant d'exécuter vSphere Certificate Manager, veuillez 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.

Vous pouvez exécuter l'outil sur la ligne de commande comme suit :

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

Procédure

1 Restaurer la dernière opération effectuée via la republication des anciens certificats

Lorsque vous effectuez une opération de gestion de certificats en utilisant vSphere Certificate Manager, l'état actuel du certificat est stocké dans le magasin BACKUP_STORE de VECS avant le remplacement des certificats. Vous pouvez restaurer la dernière opération effectuée et revenir à l'état antérieur.

2 Réinitialiser tous les certificats

Utilisez l'option `Réinitialiser tous les certificats` si vous voulez remplacer tous les certificats vCenter existants par des certificats signés par VMCA.

3 Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats

Vous pouvez régénérer le certificat racine VMCA et remplacer le certificat SSL de la machine locale, ainsi que les certificats d'utilisateur de la solution locale par des certificats signés par VMCA. Dans les déploiements à nœuds multiples, exécutez vSphere Certificate Manager avec cette option sur Platform Services Controller, réexécutez ensuite l'utilitaire sur tous les autres nœuds et sélectionnez `Remplacer les certificats SSL de machine par des certificats VMCA` et `Remplacer les certificats d'utilisateurs de solution par des certificats VMCA`.

4 Faire de VMCA une autorité de certification intermédiaire (Certificate Manager)

Vous pouvez faire de VMCA une autorité de certification intermédiaire en suivant les invites de l'utilitaire Certificate Manager. À la fin du processus, VMCA signe tous les nouveaux certificats avec la chaîne complète. Si vous le souhaitez, vous pouvez utiliser Certificate Manager pour remplacer tous les certificats existants par de nouveaux certificats signés par VMCA.

5 Remplacer tous les certificats par des certificats personnalisés (Certificate Manager)

Vous pouvez employer l'utilitaire vSphere Certificate Manager pour remplacer tous les certificats par des certificats personnalisés. Avant de démarrer le processus, vous devez envoyer des demandes de signature de certificat (CSR) à votre autorité de certification. Vous pouvez utiliser Certificate Manager pour générer les demandes de signature de certificat.

Restaurer la dernière opération effectuée via la republication des anciens certificats

Lorsque vous effectuez une opération de gestion de certificats en utilisant vSphere Certificate Manager, l'état actuel du certificat est stocké dans le magasin BACKUP_STORE de VECS avant le remplacement des certificats. Vous pouvez restaurer la dernière opération effectuée et revenir à l'état antérieur.

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.

Réinitialiser tous les certificats

Utilisez l'option `Réinitialiser tous les certificats` si vous voulez remplacer tous les certificats vCenter existants par des certificats signés par VMCA.

Si vous utilisez cette option, tous les certificats personnalisés qui se trouvent actuellement dans VECS sont remplacés.

- Sur un nœud Platform Services Controller, vSphere Certificate Manager peut régénérer le certificat racine et remplacer le certificat SSL de machine et le certificat d'utilisateur de solution de machine.
- Sur un nœud de gestion, vSphere Certificate Manager peut remplacer le certificat SSL de machine et tous les certificats d'utilisateurs de solutions de machine.
- Dans un déploiement intégré, vSphere Certificate Manager peut remplacer tous les certificats.

Les certificats remplacés dépendent des options que vous sélectionnez.

Régénérer un nouveau certificat racine VMCA et remplacer tous les certificats

Vous pouvez régénérer le certificat racine VMCA et remplacer le certificat SSL de la machine locale, ainsi que les certificats d'utilisateur de la solution locale par des certificats signés par VMCA. Dans les déploiements à nœuds multiples, exécutez vSphere Certificate Manager avec cette option sur Platform Services Controller, réexécutez ensuite l'utilitaire sur tous les autres nœuds et sélectionnez `Remplacer les certificats SSL de machine par des certificats VMCA` et `Remplacer les certificats d'utilisateurs de solution par des certificats VMCA`.

Lorsque vous exécutez cette commande, vSphere Certificate Manager vous demande le mot de passe ainsi que les informations relatives au certificat et conserve toutes les informations, à l'exception du mot de passe, dans le fichier `certtool.cfg`. Ensuite, l'arrêt des services, le remplacement de tous les certificats et le redémarrage des processus sont automatiques. Les informations suivantes vous sont demandées :

- 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
- L'adresse IP du Platform Services Controller si vous exécutez la commande sur un nœud de gestion

Conditions préalables

Vous devez connaître le 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. L'adresse IP est facultative.

Étape suivante

Après avoir remplacé le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les nœuds vCenter Server avec une instance de Platform Services Controller externe.

Faire de VMCA une autorité de certification intermédiaire (Certificate Manager)

Vous pouvez faire de VMCA une autorité de certification intermédiaire en suivant les invites de l'utilitaire Certificate Manager. À la fin du processus, VMCA signe tous les nouveaux certificats avec la chaîne complète. Si vous le souhaitez, vous pouvez utiliser Certificate Manager pour remplacer tous les certificats existants par de nouveaux certificats signés par VMCA.

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

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat. Soumettez ces demandes de signature de certificat à l'autorité de certification de votre entreprise ou à une autorité de certification externe pour une signature. Vous pouvez utiliser les certificats signés avec les différents processus de remplacement de certificat pris en charge.

- Vous pouvez utiliser vSphere Certificate Manager pour générer la demande de signature de certificat.

- Si vous préférez créer la demande de signature de certificat manuellement, le certificat envoyé pour signature doit satisfaire les conditions suivantes :
 - Taille de clé : 2 048 bits ou plus
 - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
 - x509 version 3
 - Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises.
 - La signature CRL doit être activée.
 - L'utilisation avancée de la clé ne doit impliquer ni authentification client ni authentification 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 2112009 de la base de connaissances de VMware, [Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0](#), pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

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 Démarrez vSphere Certificate Manager et sélectionnez l'option 2.
Initialement, vous utilisez cette option pour générer la demande de signature de certificat, pas pour remplacer des certificats.
- 2 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.

- 3 Sélectionnez l'option 1 pour générer la demande de signature de certificat et répondez aux invites.

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

- 4 Envoyez le certificat pour signature à l'autorité de certification d'entreprise ou à l'autorité de certification externe, puis nommez le fichier `root_signing_cert.cer`.
- 5 Dans un éditeur de texte, combinez les certificats de la façon suivante.

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

- 6 Enregistrez le fichier en tant que `root_signing_chain.cer`.

Étape suivante

Remplacez le certificat racine existant par le certificat racine chaîné. Reportez-vous à [Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats](#).

Remplacer le certificat racine VMCA par un certificat de signature personnalisé et remplacer tous les certificats

Vous pouvez remplacer le certificat racine VMCA par un certificat signé par une autorité de certification qui inclut VMCA comme certificat intermédiaire dans la chaîne de certificats. Par la suite, tous les certificats générés par VMCA incluent l'ensemble de la chaîne.

Exécutez vSphere Certificate Manager sur une installation intégrée ou sur un Platform Services Controller externe pour remplacer le certificat racine VMCA par un certificat de signature personnalisé.

vSphere Certificate Manager vous invite à fournir les informations suivantes :

Conditions préalables

- Générer la demande de signature de certificat.
 - Vous pouvez utiliser vSphere Certificate Manager pour générer la demande de signature de certificat. Reportez-vous à [Générer une demande de signature de certificat avec vSphere 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 : 2 048 bits ou plus
 - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
 - x509 version 3
 - Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises.
 - La signature CRL doit être activée.
 - L'utilisation avancée de la clé ne doit impliquer ni authentification client ni authentification 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 2112009 de la base de connaissances de VMware, [Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0](#), pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

- Après avoir reçu le certificat de votre autorité de certification d'entreprise ou de tierce partie, combinez-le avec le certificat racine VMCA initial pour générer une chaîne complète avec le certificat racine VMCA au bas. Reportez-vous à [Générer une demande de signature de certificat avec vSphere Certificate Manager et préparer un certificat racine \(autorité de certification intermédiaire\)](#).
- Rassemblez les informations qui vous seront 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 Démarrez vSphere Certificat Manager sur une installation intégrée ou un Platform Services Controller externe et sélectionnez l'option 2.

- 2 Sélectionnez l'option 2 pour démarrer le remplacement des certificats et répondre 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 `certtool.cfg`.

- 3 Si vous remplacez le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les vCenter Server.
- 4 Dans les déploiements à nœuds multiples, régénérez tous les certificats de chaque instance vCenter Server en utilisant les options 3 (Remplacer les certificats SSL de la machine par des certificats signés par VMCA) et 6 (Remplacer les certificats d'utilisateurs de solution par des certificats signés par VMCA).

Lorsque vous remplacez les certificats, VMCA signe avec la chaîne complète.

Étape suivante

Selon votre environnement, vous devrez éventuellement remplacer explicitement d'autres certificats.

- Si une stratégie d'entreprise vous impose de remplacer tous les certificats, remplacez le certificat racine vmdir. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#)
- Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à [Remplacer le certificat VMware Directory Service dans des environnement en mode mixte](#)

Remplacer le certificat SSL machine par un certificat VMCA (autorité de certification intermédiaire)

Dans un déploiement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous devez remplacer explicitement le certificat SSL machine. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats SSL machine qui sont altérés ou sur le point d'expirer.

Lorsque vous remplacez le certificat SSL machine existant par un nouveau certificat signé par VMCA, vSphere Certificate Manager vous invite à fournir des informations et à entrer toutes les valeurs, à l'exception du mot passe et de l'adresse IP de Platform Services Controller, dans le fichier `certtool.cfg`.

- Mot de passe pour administrator@vsphere.local.
- Code pays à deux lettres
- Nom de la société

- Nom de l'organisation
- Unité d'organisation
- État
- Ville
- adresse IP (facultatif)
- E-mail
- Nom de l'hôte, à savoir le nom de domaine complet de la machine dont vous souhaitez remplacer le certificat. Si le nom de l'hôte ne correspond pas au nom de domaine complet, le remplacement du certificat ne se fait pas correctement et votre environnement risque de devenir instable.
- Adresse IP du Platform Services Controller si vous exécutez la commande sur un nœud de gestion

Conditions préalables

- Redémarrez explicitement tous les nœuds vCenter Server si vous avez remplacé le certificat racine VMCA dans un déploiement à plusieurs nœuds.
- Vous devez disposer des informations suivantes pour exécuter Certificate Manager avec cette option.
 - Mot de passe pour administrator@vsphere.local.
 - Nom de domaine complet de la machine pour laquelle vous souhaitez générer un nouveau certificat signé par VMCA. Toutes les autres propriétés sont configurées par défaut sur les valeurs prédéfinies mais peuvent être modifiées.
 - Le nom d'hôte ou l'adresse IP de Platform Services Controller si vous utilisez un système vCenter Server disposant d'un Platform Services Controller externe.

Procédure

- 1 Démarrez vSphere Certificate Manager et sélectionnez l'option 3.
- 2 Répondez aux invites.

Certificate Manager enregistre les informations dans le fichier `certtool.cfg`.

Résultats

vSphere Certificate Manager remplace le certificat machine SSL.

Remplacer les certificats d'utilisateurs de solutions par des certificats VMCA (autorité de certification intermédiaire)

Dans un déploiement à plusieurs nœuds qui utilise VMCA comme autorité de certification intermédiaire, vous devez remplacer explicitement les certificats d'utilisateurs de solutions. Vous devez d'abord remplacer le certificat racine VMCA sur le nœud Platform Services Controller, puis

vous pouvez remplacer les certificats sur les nœuds vCenter Server pour faire signer les certificats par toute la chaîne. Vous pouvez également utiliser cette option pour remplacer les certificats d'utilisateurs de solutions qui sont altérés ou sur le point d'expirer.

Conditions préalables

- Redémarrez explicitement tous les nœuds vCenter Server si vous avez remplacé le certificat racine VMCA dans un déploiement à plusieurs nœuds.
- Vous devez disposer des informations suivantes pour exécuter Certificate Manager avec cette option.
 - Mot de passe pour administrator@vsphere.local.
 - Le nom d'hôte ou l'adresse IP de Platform Services Controller si vous utilisez un système vCenter Server disposant d'un Platform Services Controller externe.

Procédure

- 1 Démarrez vSphere Certificate Manager et sélectionnez l'option 6.
- 2 Répondez aux invites.

Résultats

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

Remplacer tous les certificats par des certificats personnalisés (Certificate Manager)

Vous pouvez employer l'utilitaire vSphere Certificate Manager pour remplacer tous les certificats par des certificats personnalisés. Avant de démarrer le processus, vous devez envoyer des demandes de signature de certificat (CSR) à votre autorité de certification. Vous pouvez utiliser Certificate Manager pour générer les demandes de signature de certificat.

Une option consiste à uniquement remplacer le certificat SSL de la machine, puis d'utiliser les certificats d'utilisateurs de solutions fournies 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 êtes responsable du provisionnement de chaque nœud que vous ajoutez à votre environnement avec les certificats personnalisés. VMCA provisionne toujours des certificats signés par VMCA, et il vous incombe de remplacer ces certificats. Vous pouvez employer l'utilitaire vSphere Certificate Manager ou utiliser des interfaces de ligne de commande pour procéder au remplacement manuel des certificats. Les certificats sont stockés dans VECS.

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

Vous pouvez utiliser vSphere Certificate Manager pour générer des demandes de signature de certificat (CSR, Certificate Signing Request) que vous pouvez ensuite utiliser avec votre autorité de

certification d'entreprise ou envoyer à une autorité de certification externe. Vous pouvez utiliser les certificats avec les différents processus de remplacement de certificat pris en charge.

Vous pouvez exécuter l'outil Certificate Manager sur la ligne de commande comme suit :

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

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.
- Si vous générez une demande de signature de certificat dans un environnement avec une instance de Platform Services Controller externe, vous êtes invité à entrer le nom d'hôte ou l'adresse IP de Platform Services Controller.
- Pour générer une demande de signature du certificat SSL d'une machine, vous êtes invité à entrer les propriétés du certificat, qui sont stockées dans le fichier `certtool.cfg`. Pour la plupart des champs, vous pouvez accepter les valeurs par défaut ou entrer des valeurs spécifiques au site. Le FQDN de la machine est requis.

Procédure

- 1 Sur chaque machine de votre environnement, démarrez vSphere Certificate Manager et sélectionnez l'option 1.
- 2 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.
- 3 Sélectionnez l'option 1 pour générer la demande de signature de certificat, répondez aux invites et quittez Certificate Manager.

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

- 4 Si vous souhaitez remplacer tous les certificats d'utilisateurs de solutions, redémarrez Certificate Manager.
- 5 Sélectionnez l'option 5.
- 6 Fournissez le mot de passe et l'adresse IP ou le nom d'hôte de Platform Services Controller, si vous y êtes invité.

- 7 Sélectionnez l'option 1 pour générer les demandes de signature de certificat, répondez aux invites et quittez Certificate Manager.

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

Sur chaque nœud de Platform Services Controller, Certificate Manager génère un certificat et une paire de clés. Sur chaque nœud vCenter Server, Certificate Manager génère quatre certificats et paires de clés.

Étape suivante

Effectuez le remplacement de certificats.

Remplacer le certificat SSL de machine par un certificat personnalisé

Le certificat SSL de machine est utilisé par le service de proxy inverse sur chaque nœud de gestion, Platform Services Controller et chaque déploiement intégré. Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Vous pouvez remplacer le certificat sur chaque nœud par un certificat personnalisé.

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 vSphere 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 aux exigences suivantes :
 - Taille de clé : 2 048 bits ou plus (codée au format PEM)
 - Format CRT
 - x509 version 3
 - SubjectAltName doit contenir DNS Name=<machine_FQDN>
 - Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Reportez-vous également à l'article [2112014 de la base de connaissances, Obtention de certificats vSphere depuis une autorité de certification Microsoft](#).

Procédure

- 1 Démarrez vSphere Certificate Manager et sélectionnez l'option 1.

2 Sélectionnez l'option 2 pour démarrer le remplacement des certificats et répondre aux invites.

vSphere Certificate Manager vous invite à fournir les informations suivantes :

- Mot de passe pour administrator@vsphere.local.
- Certificat personnalisé SSL valide de la machine (fichier .crt).
- Clé personnalisée SSL valide de la machine (fichier .key).
- Certificat de signature valide pour le certificat personnalisé SSL de la machine (fichier .crt).
- Si vous exécutez la commande sur un nœud de gestion dans un déploiement à plusieurs nœuds, adresse IP de Platform Services Controller.

Étape suivante

Selon votre environnement, vous devrez éventuellement remplacer explicitement d'autres certificats.

- Si une stratégie d'entreprise vous impose de remplacer tous les certificats, remplacez le certificat racine vmdir. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#)
- Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à [Remplacer le certificat VMware Directory Service dans des environnement en mode mixte](#)

Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Bon nombre d'entreprises demandent uniquement à ce que vous remplaciez les certificats de services accessibles de façon externe. Toutefois, Certificate Manager prend uniquement en charge le remplacement des certificats de l'utilisateur de solution. Les utilisateurs de solutions sont des collections de services, par exemple, tous les services associés à vSphere Web Client dans les déploiements multi-nœuds remplacent le certificat de l'utilisateur de solution de la machine sur Platform Services Controller et l'ensemble complet d'utilisateurs de solutions sur chaque nœud de gestion.

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 doit être 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 vSphere 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 : 2 048 bits ou plus (codée au format PEM)
 - Format CRT
 - x509 version 3
 - SubjectAltName doit contenir DNS Name=<machine_FQDN>
 - Chaque certificat d'utilisateur de la solution doit avoir un paramètre `Subject` différent. Vous pouvez par exemple saisir le nom de l'utilisateur de la solution (tel que `vpzd`) ou un autre identifiant unique.
 - Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Reportez-vous également à l'article [2112014 de la base de connaissances, Obtention de certificats vSphere depuis une autorité de certification Microsoft](#).

Procédure

- 1 Démarrez vSphere Certificate Manager et sélectionnez l'option 5.
- 2 Sélectionnez l'option 2 pour démarrer le remplacement des certificats et répondre aux invites. vSphere Certificate Manager vous invite à fournir les informations suivantes :
 - Mot de passe pour `administrator@vsphere.local`.
 - Certificat et clé de l'utilisateur de solution de machine
 - Si vous exécutez vSphere Certificate Manager sur un nœud Platform Services Controller, vous êtes invité à saisir le certificat et la clé (`vpzd.crt` et `vpzd.key`) pour l'utilisateur de solution de machine.
 - Si vous exécutez vSphere Certificate Manager sur un nœud de gestion ou sur un déploiement intégré, vous êtes invité à indiquer l'ensemble complet de certificats et de clés (`vpzd.crt` et `vpzd.key`) pour tous les utilisateurs de solution.

Étape suivante

Si vous procédez à une mise à niveau à partir d'un environnement vSphere 5.x, vous devrez éventuellement remplacer le certificat vCenter Single Sign-On dans vmdir. Reportez-vous à [Remplacer le certificat VMware Directory Service dans des environnement en mode mixte](#).

Remplacement manuel de certificats

Dans des situations particulières, par exemple si vous voulez remplacer un seul type de certificat d'utilisateur de solution, vous ne pouvez pas utiliser l'utilitaire vSphere Certificate Manager. Dans ce cas, vous pouvez utiliser les interfaces de ligne de commande incluses dans votre installation pour le remplacement de certificat.

Règles générales de démarrage et d'arrêt des services

Pour certaines parties du remplacement manuel de certificat, vous devez arrêter tous les services, puis démarrer uniquement les services qui gèrent l'infrastructure de certificats. Si vous n'arrêtez les services qu'en cas de besoin, vous pouvez réduire les interruptions.

Suivez ces règles générales.

- N'arrêtez pas les services pour générer de nouvelles paires de clé publique/privée ou de nouveaux certificats.
- Si vous êtes le seul administrateur, il n'est pas nécessaire d'arrêter les services lorsque vous ajoutez un nouveau certificat racine. L'ancien certificat racine demeure disponible et tous les services peuvent toujours s'authentifier avec ce certificat. Arrêtez, puis redémarrez immédiatement tous les services après avoir ajouté le certificat racine pour éviter les problèmes avec vos hôtes.
- Si votre environnement inclut plusieurs administrateurs, arrêtez les services avant d'ajouter un nouveau certificat racine et redémarrez-le après l'ajout d'un nouveau certificat.
- Arrêtez les services juste avant d'effectuer les tâches suivantes :
 - Supprimer un certificat d'utilisateur de solution de machine ou tout certificat d'utilisateur de solution dans VECS.
 - Remplacer un certificat d'utilisateur de solution dans vmdir (service d'annuaire VMware).

Remplacer les certificats existants signés par l'autorité de certification VMware (VMCA) par de nouveaux certificats

Si le certificat racine VMCA expire dans un avenir proche ou si vous voulez le remplacer pour d'autres raisons, vous pouvez générer un nouveau certificat racine et l'ajouter au service d'annuaire VMware. Vous pouvez alors générer de nouveaux certificats SSL de machine et certificats d'utilisateurs de solutions au moyen du nouveau certificat racine.

Faites appel à l'utilitaire vSphere Certificate Manager pour remplacer les certificats dans la plupart des cas.

Si vous avez besoin d'un contrôle précis, ce scénario fournit des instructions pas à pas permettant de remplacer l'ensemble complet de certificats au moyen de commandes d'interface de ligne de commande. Vous pouvez remplacer uniquement des certificats individuels au moyen de la procédure indiquée dans la tâche correspondante.

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 [Ajouter des membres à un groupe vCenter Single Sign-On](#).

Procédure

1 Générer un nouveau certificat racine signé par VMCA

Vous générez de nouveaux certificats signés par l'autorité de certification VMware (VMCA) avec l'interface de ligne de commande `certool` et vous les publiez dans `vmdir`.

2 Remplacer les certificats SSL de la machine par des certificats signés par VMCA

Une fois que vous avez généré un nouveau certificat racine signé par VMCA, vous pouvez remplacer tous les certificats SSL de machine de votre environnement.

3 Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA

Après avoir remplacé les certificats SSL de la machine, vous pouvez remplacer tous les certificats des utilisateurs de solutions. Les certificats d'utilisateurs de solutions doivent être valides (ils ne sont pas arrivés à expiration), mais l'infrastructure de certificats n'utilise aucune des autres informations d'un certificat.

4 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Générer un nouveau certificat racine signé par VMCA

Vous générez de nouveaux certificats signés par l'autorité de certification VMware (VMCA) avec l'interface de ligne de commande `certool` et vous les publiez dans `vmdir`.

Dans un déploiement à plusieurs nœuds, vous exécutez des commandes de génération de certificats racines sur Platform Services Controller.

Procédure

1 Générez un nouveau certificat auto-signé et une clé privée.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>
```


- 2 Remplacez le certificat racine existant par le nouveau certificat.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

La commande génère le certificat et l'ajoute à vmdir, puis à VECS.

- 3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 (Facultatif) Publiez le nouveau certificat racine dans vmdir.

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

Lorsque vous exécutez cette commande, toutes les instances de vmdir sont mises à jour immédiatement. Sinon, la propagation à toutes les instances 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 l'ensemble des étapes nécessaires à la vérification des informations de l'autorité de certification racine et à la régénération du certificat racine.

- 1 (Facultatif) Affichez le certificat racine VMCA pour vous assurer qu'il se trouve dans le magasin de certificats.

- Sur un nœud Platform Services Controller ou une installation intégrée :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- Sur un nœud de gestion (installation externe) :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-  
ip-or-fqdn>
```

Le résultat est semblable à ce qui suit :

```
output:  
Certificate:  
  Data:  
    Version: 3 (0x2)  
    Serial Number:  
      cf:2d:ff:49:88:50:e5:af  
    ...
```

- 2 (Facultatif) Affichez le magasin VECS TRUSTED_ROOTS et comparez le numéro de série du certificat qui s'y trouve au résultat de l'étape 1.

Cette commande fonctionne sur Platform Services Controller et sur les nœuds de gestion, car VECS interroge vmdir.

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"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. Le certificat est ajouté au magasin TRUSTED_ROOTS dans VECS et dans vmdir (service d'annuaire VMware).

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program  
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Sous Windows, `--config` est facultatif, car la commande utilise le fichier `certool.cfg` par défaut.

Remplacer les certificats SSL de la machine par des certificats signés par VMCA

Une fois que vous avez généré un nouveau certificat racine signé par VMCA, vous pouvez remplacer tous les certificats SSL de machine de votre environnement.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un nœud vCenter Server avec une instance de Platform Services Controller externe.

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 `certtool.cfg` pour toutes les machines ayant besoin d'un nouveau certificat.

Vous pouvez rechercher `certtool.cfg` dans l'un des emplacements suivants :

SE	Chemin
Windows	C:\Program Files\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 Modifiez le fichier de configuration personnalisée de chaque machine pour inclure le nom de domaine complet de la machine.

Exécutez `NSLookup` sur l'adresse IP de la machine pour voir le nom figurant dans la liste DNS et utilisez ce nom pour le champ `Hostname` du fichier.

- 3 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque fichier, en transmettant le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

- 4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 5 Ajoutez le nouveau certificat à VECS.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL. Vous devez d'abord supprimer l'entrée existante, puis ajouter la nouvelle entrée.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- 6 Redémarrez tous les services.

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

Exemple : Remplacement des certificats SSL de la machine par des certificats signés par VMCA

- 1 Créez un fichier de configuration pour le certificat SSL et enregistrez-le sous le nom `ssl-config.cfg` dans le répertoire actuel.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

- 2 Générez une paire de clés pour le certificat SSL de machine. Exécutez cette commande sur chaque nœud de gestion et nœud Platform Services Controller ; elle ne requiert pas d'option `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Les fichiers `ssl-key.priv` et `ssl-key.pub` sont créés dans le répertoire actuel.

- 3 Générez le nouveau certificat SSL de machine. Ce certificat est signé par VMCA. Si vous remplacez le certificat racine VMCA par un certificat personnalisé, VMCA signe tous les certificats avec la chaîne complète.

- Sur un nœud Platform Services Controller ou une installation intégrée :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Sur vCenter Server (installation externe) :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

- 4 (Facultatif) Répertoriez le contenu de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Résultat sur Platform Services Controller :

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Résultat sur vCenter Server :

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

- 5 Remplacez le certificat SSL de machine dans VECS par le nouveau certificat SSL de machine. Les valeurs `--store` et `--alias` doivent correspondre exactement aux noms par défaut.

- Sur Platform Services Controller, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Sur chaque nœud de gestion ou déploiement intégré, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT. Vous devez mettre à jour le certificat de chaque machine séparément. En effet, chaque machine possède un nom de domaine complet qui lui est propre.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Étape suivante

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

Après avoir remplacé le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les nœuds vCenter Server avec une instance de Platform Services Controller externe.

Remplacer les certificats d'utilisateurs de solution par de nouveaux certificats signés par VMCA

Après avoir remplacé les certificats SSL de la machine, vous pouvez remplacer tous les certificats des utilisateurs de solutions. Les certificats d'utilisateurs de solutions doivent être valides (ils ne sont pas arrivés à expiration), mais l'infrastructure de certificats n'utilise aucune des autres informations d'un certificat.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

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 `certtool.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 :

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmadd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds.

Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

- 4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
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 `vpzd`.

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.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/clé privée pour chaque utilisateur de solution. Cela inclut une paire pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.

- a Générez une paire de clés pour l'utilisateur de solution de machine d'un déploiement intégré ou pour l'utilisateur de solution de machine de Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (Facultatif) Pour les déploiements comportant un Platform Services Controller externe, générez une paire de clés pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

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

Note Le paramètre `--Name` doit être unique. Il doit comprendre le nom du magasin de l'utilisateur de solution ; par exemple, `vpxd` ou `vpxd-extension` permet de voir facilement la correspondance entre un certificat et un utilisateur de solution.

- a Exécutez la commande suivante sur le nœud Platform Services Controller pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b Générez un certificat pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

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

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

- a Sur le nœud Platform Services Controller, exécutez la commande suivante pour remplacer le certificat d'utilisateur de solution de machine :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud de gestion :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- 4 Mettez à jour le service d'annuaire VMware (vmdir) avec les nouveaux certificats d'utilisateurs de solutions. Vous êtes invité à entrer un mot de passe d'administrateur vCenter Single Sign-On.

- a Exécutez `dir-cli service list` pour obtenir le suffixe d'ID de service unique pour chaque utilisateur de solution. Vous pouvez exécuter cette commande sur un système Platform Services Controller ou vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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 Platform Services Controller. Par exemple, si `machine-29a45d00-60a7-11e4-96ff-00505689639a` correspond à l'utilisateur de solution de machine sur Platform Services Controller, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Étape suivante

Redémarrez tous les services sur chaque nœud Platform Services Controller et chaque nœud de gestion.

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Note La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

- 1 Sur le nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté, remplacez le certificat et la clé SSL de vmdird.

Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

- 2 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.
 - a Effectuez une sauvegarde de tous les fichiers de
C:\ProgramData\VMware\CIS\cfg\vmdird.
 - b Faites une copie du fichier vmdircert.pem sur le nœud 6.x, et renommez-le
<sso_node2.domain.com>.pem, où <sso_node2.domain.com> est le nom de domaine complet du nœud .x.
 - c Copiez le certificat renommé dans C:\ProgramData\VMware\CIS\cfg\vmdird pour
remplacer le certificat de réplication existant.

- 3 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

Vous pouvez redémarrer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Utiliser VMCA en tant qu'autorité de certificat intermédiaire

Vous pouvez remplacer le certificat racine VMCA par un certificat signé par une autorité de certification tierce qui inclut VMCA dans la chaîne de certificats. Par la suite, tous les certificats générés par VMCA incluent l'ensemble de la chaîne. Vous pouvez remplacer des certificats existants par des certificats qui viennent d'être générés. Cette approche associe la sécurité d'un certificat signé par une autorité de certification tierce à l'aspect pratique d'une gestion automatisée des certificats.

Procédure

- 1 [Remplacer le certificat racine \(autorité de certification intermédiaire\)](#)

La première étape du remplacement des certificats VMCA par des certificats personnalisés consiste à générer un CSR et à ajouter le certificat qui est renvoyé au VMCA en tant que certificat racine.

- 2 [Remplacer les certificats SSL de la machine \(autorité de certification intermédiaire\)](#)

Après avoir reçu le certificat signé de l'autorité de certification et en avoir fait le certificat racine VMCA, vous pouvez remplacer tous les certificats SSL de machine.

- 3 [Remplacer les certificats d'utilisateurs de solution \(autorité de certification intermédiaire\)](#)

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution.

4 Remplacer le certificat de service d'annuaire VMware

Si vous décidez d'utiliser un nouveau certificat racine VMCA et que vous annulez la publication du certificat racine VMCA utilisé lors du provisionnement de votre environnement, vous devez remplacer les certificats SSL de machine, les certificats d'utilisateurs de la solution et ceux de certains services internes.

5 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Remplacer le certificat racine (autorité de certification intermédiaire)

La première étape du remplacement des certificats VMCA par des certificats personnalisés consiste à générer un CSR et à ajouter le certificat qui est renvoyé au VMCA en tant que certificat racine.

Le certificat que vous envoyez pour être signé doit répondre aux exigences suivantes :

- Taille de clé : 2 048 bits ou plus
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
- x509 version 3
- Si vous utilisez des certificats personnalisés, l'extension d'autorité de certification doit être définie sur vrai, pour les certificats racine, et la signature de certification doit figurer dans la liste de conditions requises.
- La signature CRL doit être activée.
- L'utilisation avancée de la clé ne doit impliquer ni authentification client ni authentification 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 2112009 de la base de connaissances de VMware, [Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0](#), pour consulter un exemple d'utilisation de l'autorité de certification Microsoft.

VMCA valide les attributs suivants du certificat lorsque vous remplacez le certificat racine :

- Taille de clé de 2 048 bits ou plus

- Utilisation de la clé : Signature de certification
- Contrainte de base : Autorité de certification du type de sujet

Procédure

- 1 Générez une demande de signature de certificat et envoyez-la à votre autorité de certification. Suivez les instructions de votre autorité de certification.
- 2 Préparez un fichier de certificat qui inclut le certificat VMCA signé ainsi que la chaîne complète de l'autorité de certification de votre autorité de certification tierce ou de votre autorité de certification d'entreprise, et enregistrez le fichier, par exemple sous le nom `rootca1.crt`.

Vous pouvez le faire en copiant tous les certificats de l'autorité de certification au format PEM dans un fichier unique. Vous devez commencer par le certificat racine VMCA et terminer par le certificat racine CA PEM. Par exemple :

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
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 (service d'annuaire VMware), publiez le nouveau certificat racine dans vmdir, en fournissant le chemin complet de chaque fichier.

Par exemple :

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

La réplication entre les nœuds vmdir se produit toutes les 30 secondes. Il n'est pas nécessaire d'ajouter le certificat racine à VECS de façon explicite, car VECS interroge vmdir concernant les fichiers de certificat racine toutes les 5 minutes.

- 6 (Facultatif) Le cas échéant, vous pouvez forcer une opération d'actualisation de VECS.

```
vecs-cli force-refresh
```

- 7 Redémarrez tous les services.

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

Exemple : Remplacement du certificat racine

Remplacez le certificat racine VMCA par le certificat racine VMCA personnalisé en utilisant la commande certtool avec l'option `--rootca`.

```
C:\>"C:\Program Files\VMware\VMware Server\vmcad\certtool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\root.key
```

Lorsque vous exécutez cette commande, elle :

- Ajoute le nouveau certificat racine personnalisé à l'emplacement des certificats dans le système de fichiers.
- Ajoute le certificat racine personnalisé au magasin TRUSTED_ROOTS dans VECS.
- Ajoute le certificat racine personnalisé à vmdir.

Étape suivante

Vous pouvez supprimer le certificat racine VMCA initial du magasin de certificats si la stratégie de l'entreprise l'exige. Si vous le faites, vous devez actualiser ces certificats internes :

- Remplacez le certificat de signature vCenter Single Sign-On. Reportez-vous à [Actualiser le certificat STS](#).
- Remplacez le certificat de service d'annuaire VMware. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

Remplacer les certificats SSL de la machine (autorité de certification intermédiaire)

Après avoir reçu le certificat signé de l'autorité de certification et en avoir fait le certificat racine VMCA, vous pouvez remplacer tous les certificats SSL de machine.

Cette procédure est en grande partie identique à celle mise en œuvre pour le remplacement par un certificat qui utilise VMCA comme autorité de certification. Néanmoins, dans ce cas, VMCA signe tous les certificats avec la chaîne complète.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un nœud vCenter Server avec une instance de Platform Services Controller externe.

Conditions préalables

Pour chaque certificat SSL de machine, le `SubjectAltName` doit contenir `DNS Name=<Machine FQDN>`.

Procédure

- 1 Faites une copie de `certtool.cfg` pour toutes les machines ayant besoin d'un nouveau certificat.

Vous pouvez rechercher `certtool.cfg` dans l'un des emplacements suivants :

Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

- 2 Modifiez le fichier de configuration personnalisée de chaque machine pour inclure le nom de domaine complet de la machine.

Exécutez `NSlookup` sur l'adresse IP de la machine pour voir le nom figurant dans la liste DNS et utilisez ce nom pour le champ `Hostname` du fichier.

- 3 Générez une paire de fichiers de clé publique/privée et un certificat pour chaque machine, en transmettant le fichier de configuration que vous venez de personnaliser.

Par exemple :

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

- 4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

- 5 Ajoutez le nouveau certificat à VECS.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL. Vous devez d'abord supprimer l'entrée existante, puis ajouter la nouvelle entrée.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- 6 Redémarrez tous les services.

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

Exemple : Remplacement des certificats SSL de machine (VMCA est l'autorité de certification intermédiaire)

- 1 Créez un fichier de configuration pour le certificat SSL et enregistrez-le sous le nom `ssl-config.cfg` dans le répertoire actuel.

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
```

```
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- 2 Générez une paire de clés pour le certificat SSL de machine. Exécutez cette commande sur chaque nœud de gestion et nœud Platform Services Controller ; elle ne requiert pas d'option `--server`.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

Les fichiers `ssl-key.priv` et `ssl-key.pub` sont créés dans le répertoire actuel.

- 3 Générez le nouveau certificat SSL de machine. Ce certificat est signé par VMCA. Si vous remplacez le certificat racine VMCA par un certificat personnalisé, VMCA signe tous les certificats avec la chaîne complète.

- Sur un nœud Platform Services Controller ou une installation intégrée :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- Sur vCenter Server (installation externe) :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

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

- 4 (Facultatif) Répertoriez le contenu de VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Résultat sur Platform Services Controller :

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- Résultat sur vCenter Server :

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

- 5 Remplacez le certificat SSL de machine dans VECS par le nouveau certificat SSL de machine. Les valeurs `--store` et `--alias` doivent correspondre exactement aux noms par défaut.

- Sur Platform Services Controller, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- Sur chaque nœud de gestion ou déploiement intégré, exécutez la commande suivante pour mettre à jour le certificat SSL de machine dans le magasin MACHINE_SSL_CERT. Vous devez mettre à jour le certificat de chaque machine séparément. En effet, chaque machine possède un nom de domaine complet qui lui est propre.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

Étape suivante

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

Après avoir remplacé le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les nœuds vCenter Server avec une instance de Platform Services Controller externe.

Remplacer les certificats d'utilisateurs de solution (autorité de certification intermédiaire)

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

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 `vpzd`) 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=vpzd.priv --pubkey=vpzd.pub
certool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmafd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds.

Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

- 4 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
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/clé privée pour chaque utilisateur de solution. Cela inclut une paire pour l'utilisateur de solution de machine sur chaque Platform Services Controller et chaque nœud de gestion, et une paire pour chaque utilisateur de solution supplémentaire (vpxd, vpxd-extension, vsphere-webclient) sur chaque nœud de gestion.
 - a Générez une paire de clés pour l'utilisateur de solution de machine d'un déploiement intégré ou pour l'utilisateur de solution de machine de Platform Services Controller.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (Facultatif) Pour les déploiements comportant un Platform Services Controller externe, générez une paire de clés pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

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

Note Le paramètre `--Name` doit être unique. Il doit comprendre le nom du magasin de l'utilisateur de solution ; par exemple, vpxd ou vpxd-extension permet de voir facilement la correspondance entre un certificat et un utilisateur de solution.

- a Exécutez la commande suivante sur le nœud Platform Services Controller pour générer un certificat d'utilisateur de solution pour l'utilisateur de solution de machine sur ce nœud.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b Générez un certificat pour l'utilisateur de solution de machine sur chaque nœud de gestion.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```


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

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certtool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

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

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certtool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

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

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

- a Sur le nœud Platform Services Controller, exécutez la commande suivante pour remplacer le certificat d'utilisateur de solution de machine :

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud de gestion :

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

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

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

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

```
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VCServer\vmadfs\vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vmphere-webclient.crt --key
vsphere-webclient-key.priv
```

- 4 Mettez à jour le service d'annuaire VMware (vmdir) avec les nouveaux certificats d'utilisateurs de solutions. Vous êtes invité à entrer un mot de passe d'administrateur vCenter Single Sign-On.

- a Exécutez `dir-cli service list` pour obtenir le suffixe d'ID de service unique pour chaque utilisateur de solution. Vous pouvez exécuter cette commande sur un système Platform Services Controller ou vCenter Server.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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 Platform Services Controller. Par exemple, si `machine-29a45d00-60a7-11e4-96ff-00505689639a` correspond à l'utilisateur de solution de machine sur Platform Services Controller, exécutez la commande suivante :

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

Remplacer le certificat de service d'annuaire VMware

Si vous décidez d'utiliser un nouveau certificat racine VMCA et que vous annulez la publication du certificat racine VMCA utilisé lors du provisionnement de votre environnement, vous devez remplacer les certificats SSL de machine, les certificats d'utilisateurs de la solution et ceux de certains services internes.

Si vous annulez la publication du certificat racine VMCA, vous devez remplacer le certificat de signature SSL utilisé par vCenter Single Sign-On. Reportez-vous à [Actualiser le certificat STS](#). Vous devez également remplacer le certificat VMware Directory Service (vmdir).

Conditions préalables

Demander un certificat pour vmdir pour votre autorité de certification tierce ou d'entreprise.

Procédure

- 1 Arrêtez vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 Copiez le certificat et la clé que vous venez de générer à l'emplacement de vmdir.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Redémarrez vmdir à partir de vSphere Web Client ou à l'aide de la commande `service-control`.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Note La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

- 1 Sur le nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté, remplacez le certificat et la clé SSL de vmdird.

Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

- 2 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.
 - a Effectuez une sauvegarde de tous les fichiers de `C:\ProgramData\VMware\CIS\cfg\vmdird`.
 - b Faites une copie du fichier `vmdircert.pem` sur le nœud 6.x, et renommez-le `<sso_node2.domain.com>.pem`, où `<sso_node2.domain.com>` est le nom de domaine complet du nœud .x.
 - c Copiez le certificat renommé dans `C:\ProgramData\VMware\CIS\cfg\vmdird` pour remplacer le certificat de réplication existant.

- 3 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

Vous pouvez redémarrer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Utiliser des certificats tiers avec vSphere

Si votre entreprise le prévoit, vous pouvez remplacer tous les certificats utilisés dans vSphere par des certificats tiers signés par une autorité de certification. Dans ce cas, VMCA ne fait pas partie de votre chaîne de certificats mais tous les certificats vCenter doivent être stockés 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 la solution sont utilisés uniquement à des fins d'authentification de vCenter Single Sign-On, sur place.

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

Procédure

- 1 [Demander des certificats et importer un certificat racine personnalisé](#)

Si la stratégie de l'entreprise n'autorise pas d'autorité de certification intermédiaire, VMCA ne peut pas générer les certificats pour vous. Utilisez des certificats personnalisés d'une autorité de certification d'entreprise ou tierce.

- 2 [Remplacer les certificats SSL de machine par des certificats personnalisés](#)

Après avoir reçu les certificats personnalisés, vous pouvez remplacer chaque certificat de machine.

3 Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution signés par VMCA par des certificats tiers ou de l'entreprise.

4 Remplacer le certificat de service d'annuaire VMware

Si vous décidez d'utiliser un nouveau certificat racine VMCA et que vous annulez la publication du certificat racine VMCA utilisé lors du provisionnement de votre environnement, vous devez remplacer les certificats SSL de machine, les certificats d'utilisateurs de la solution et ceux de certains services internes.

5 Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Demander des certificats et importer un certificat racine personnalisé

Si la stratégie de l'entreprise n'autorise pas d'autorité de certification intermédiaire, VMCA ne peut pas générer les certificats pour vous. Utilisez des certificats personnalisés d'une autorité de certification d'entreprise ou tierce.

Conditions préalables

Le certificat doit répondre aux exigences suivantes :

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
- x509 version 3
- Pour les certificats racines, l'extension d'autorité de certification doit être définie sur vrai et la signature de certification doit figurer dans la liste de conditions requises.
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Format CRT
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
- Heure de début antérieure d'un jour à l'heure actuelle
- CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.

Procédure

- 1 Envoyez des demandes de signature de certificat pour les certificats suivants à votre entreprise ou à un fournisseur tiers de certificats.
 - Un certificat SSL de machine pour chaque machine. Pour le certificat SSL de machine, le champ SubjectAltName doit contenir le nom de domaine complet (NOM DNS = *FQDN_machine*)
 - Éventuellement, quatre certificats d'utilisateurs de solutions pour chaque système intégré ou nœud de gestion. Les certificats d'utilisateurs de solutions ne doivent pas inclure d'adresse IP, de nom d'hôte ou d'adresse e-mail. Chaque certificat doit avoir un sujet de certificat différent.

En général, le résultat est un fichier PEM pour la chaîne d'approbation, plus les certificats SSL signés pour chaque Platform Services Controller ou nœud de gestion.

- 2 Répertoriez les magasins TRUSTED_ROOTS et SSL de machine.

```
vecs-cli store list
```

- a Assurez-vous que le certificat racine actuel et tous les certificats SSL de machine sont signés par VMCA.
 - b Prenez note des champs du numéro de série, de l'émetteur et du CN du sujet.
 - c (Facultatif) À l'aide d'un navigateur Web, ouvrez une connexion HTTPS à un nœud sur lequel le certificat sera remplacé, vérifiez les informations relatives au certificat et assurez-vous qu'elles correspondent à celles du certificat SSL de machine.
- 3 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 4 Publiez le certificat racine personnalisé qui correspond au certificat de signature de l'autorité de certification tierce.

```
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 l'entreprise l'exige. Si vous le faites, vous devez actualiser ces certificats internes :

- Remplacez le certificat de signature vCenter Single Sign-On. Reportez-vous à [Actualiser le certificat STS](#).
- Remplacez le certificat de service d'annuaire VMware. Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

Remplacer les certificats SSL de machine par des certificats personnalisés

Après avoir reçu les certificats personnalisés, vous pouvez remplacer chaque certificat de machine.

Chaque machine doit avoir un certificat SSL de machine pour la communication sécurisée avec d'autres services. Dans un déploiement à nœuds multiples, vous devez exécuter les commandes de génération de certificat SSL de la machine sur chaque nœud. Utilisez le paramètre `--server` pour désigner Platform Services Controller à partir d'un nœud vCenter Server avec une instance de Platform Services Controller externe.

Vous devez disposer des informations suivantes avant de pouvoir commencer à remplacer les certificats :

- Mot de passe pour administrator@vsphere.local.
- Certificat personnalisé SSL valide de la machine (fichier `.crt`).
- Clé personnalisée SSL valide de la machine (fichier `.key`).
- Certificat personnalisé valide pour Root (fichier `.crt`).
- Si vous exécutez la commande sur un nœud vCenter Server avec une instance de Platform Services Controller externe dans un déploiement à plusieurs nœuds, l'adresse IP de Platform Services Controller.

Conditions préalables

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

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format CRT
- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Procédure

- 1 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

Les noms de service diffèrent sur Windows et pour le vCenter Server Appliance.

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafd
service-control --start vmdird
service-control --start vmcad
```

- 2 Connectez-vous à chaque nœud et ajoutez à VECS les nouveaux certificats de machine que vous avez reçus de l'autorité de certification.

Le nouveau certificat doit figurer dans le magasin de certificats local de toutes les machines pour que celles-ci puissent communiquer sur SSL.

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 Redémarrez tous les services.

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

Exemple : Remplacer les certificats SSL de machine par des certificats personnalisés

Vous pouvez remplacer le certificat SSL de machine sur chaque nœud en suivant la même procédure.

- 1 Tout d'abord, supprimez le certificat existant dans VECS.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

- 2 Ensuite, ajoutez le certificat de remplacement.

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

Étape suivante

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

Après avoir remplacé le certificat racine dans un déploiement à nœuds multiples, vous devez redémarrer les services sur tous les nœuds vCenter Server avec une instance de Platform Services Controller externe.

Remplacer les certificats d'utilisateurs de solution par des certificats personnalisés

Une fois que vous avez remplacé les certificats SSL de la machine, vous pouvez remplacer les certificats d'utilisateurs de solution signés par VMCA par des certificats tiers ou de l'entreprise.

Les utilisateurs de solutions utilisent des certificats pour s'authentifier sur vCenter Single Sign-On. Si le certificat est valide, vCenter Single Sign-On affecte un jeton SAML à l'utilisateur de la solution et ce dernier l'utilise pour s'authentifier vis-à-vis des autres composants vCenter.

Déterminez si le remplacement des certificats des utilisateurs de solution est nécessaire dans votre environnement. Du fait que les utilisateurs de solution sont placés derrière un serveur proxy et que le certificat SSL de machine est utilisé pour sécuriser le trafic SSL, les certificats des utilisateurs de solution posent moins de problèmes de sécurité.

Remplacez le certificat d'utilisateur de solution de machine sur chaque nœud Platform Services Controller. Remplacez les autres certificats d'utilisateurs de solutions uniquement sur chaque nœud de gestion. Utilisez le paramètre `--server` pour pointer vers Platform Services Controller lorsque vous exécutez des commandes sur un nœud de gestion avec un Platform Services Controller externe.

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

- Taille de clé : 2 048 bits ou plus (codée au format PEM)
- Format CRT
- x509 version 3
- SubjectAltName doit contenir DNS Name=<machine_FQDN>
- Chaque certificat d'utilisateur de la solution doit avoir un paramètre `Subject` différent. Vous pouvez par exemple saisir le nom de l'utilisateur de la solution (tel que `vpxd`) ou un autre identifiant unique.
- Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé

Procédure

- 1 Arrêtez tous les services et démarrez ceux qui gèrent la création, la propagation et le stockage des certificats.

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

- 2 Recherchez le nom de chaque utilisateur de la solution.

```
dir-cli service list
```

Vous pouvez utiliser l'ID unique renvoyé lorsque vous remplacez les certificats. L'entrée et la sortie peuvent se présenter comme suit.

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
```

```
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

Lorsque vous répertoriez les certificats d'utilisateurs de solution dans un déploiement à nœuds multiples, la liste `dir-cli` contient tous les utilisateurs de solution de tous les nœuds.

Exécutez `vmafd-cli get-machine-id --server-name localhost` pour rechercher l'ID de machine locale de chaque hôte. Chaque nom d'utilisateur de solution comprend l'ID de machine.

- 3 Pour chaque utilisateur de solution, remplacez le certificat existant dans VECS puis dans vmdir.

Vous devez ajouter les certificats dans cet ordre.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

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.

- 4 Redémarrez tous les services.

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

Remplacer le certificat de service d'annuaire VMware

Si vous décidez d'utiliser un nouveau certificat racine VMCA et que vous annulez la publication du certificat racine VMCA utilisé lors du provisionnement de votre environnement, vous devez remplacer les certificats SSL de machine, les certificats d'utilisateurs de la solution et ceux de certains services internes.

Si vous annulez la publication du certificat racine VMCA, vous devez remplacer le certificat de signature SSL utilisé par vCenter Single Sign-On. Reportez-vous à [Actualiser le certificat STS](#). Vous devez également remplacer le certificat VMware Directory Service (vmdir).

Conditions préalables

Demander un certificat pour vmdir pour votre autorité de certification tierce ou d'entreprise.

Procédure

- 1 Arrêtez vmdir.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 Copiez le certificat et la clé que vous venez de générer à l'emplacement de vmdir.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 Redémarrez vmdir à partir de vSphere Web Client ou à l'aide de la commande `service-control`.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

Remplacer le certificat VMware Directory Service dans des environnement en mode mixte

Pendant la mise à niveau, votre environnement peut comprendre temporairement à la fois vCenter Single Sign-On version 5.5 et vCenter Single Sign-On version 6. Vous devez alors prendre des mesures supplémentaires pour remplacer le certificat SSL de VMware Directory Service si vous remplacez le certificat SSL du nœud sur lequel le service vCenter Single Sign-On est exécuté.

Le certificat SSL de VMware Directory Service est utilisé par vmdir pour l'établissement de liaisons entre les nœuds du Platform Services Controller qui effectuent la réplication de vCenter Single Sign-On.

Cette procédure n'est pas requise dans un environnement en mode mixte qui inclut des nœuds vSphere 6.0 et vSphere 6.5. Cette procédure est indispensable uniquement si :

- Votre environnement comprend à la fois les services de vCenter Single Sign-On 5.5 et de vCenter Single Sign-On 6.x.
- Les services de vCenter Single Sign-On sont configurés pour répliquer les données de vmdir.
- Vous envisagez de remplacer les certificats signés par VMCA par défaut par les certificats personnalisés du nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté.

Note La mise à niveau de l'intégralité de l'environnement avant de redémarrer les services est considérée comme étant une meilleure pratique. En règle générale, il n'est pas recommandé de remplacer le certificat de VMware Directory Service.

Procédure

- 1 Sur le nœud sur lequel le service de vCenter Single Sign-On 6.x est exécuté, remplacez le certificat et la clé SSL de vmdird.

Reportez-vous à [Remplacer le certificat de service d'annuaire VMware](#).

- 2 Sur le nœud sur lequel le service de vCenter Single Sign-On 5.5 est exécuté, configurez l'environnement de sorte que le service de vCenter Single Sign-On 6.x soit reconnu.
 - a Effectuez une sauvegarde de tous les fichiers de
C:\ProgramData\VMware\CIS\cfg\vmdird.
 - b Faites une copie du fichier vmdircert.pem sur le nœud 6.x, et renommez-le
<sso_node2.domain.com>.pem, où <sso_node2.domain.com> est le nom de domaine complet du nœud .x.
 - c Copiez le certificat renommé dans C:\ProgramData\VMware\CIS\cfg\vmdird pour
remplacer le certificat de réplication existant.

- 3 Redémarrez VMware Directory Service sur toutes les machines sur lesquelles vous avez remplacé les certificats.

Vous pouvez redémarrer le service à partir de vSphere Web Client ou utiliser la commande `service-control`.

Gestion des certificats et des services avec les commandes de l'interface de ligne de commande

Un groupe d'interfaces de ligne de commande vous permet de gérer VMCA (VMware Certificate Authority), VECS (VMware Endpoint Certificate Store) et le VMware Directory Service (vmdir). L'utilitaire vSphere Certificate Manager gère également de nombreuses tâches associées, mais les interfaces de ligne de commande sont indispensables pour la gestion manuelle des certificats.

Tableau 3-5. Outils d'interface de ligne de commande affectés à la gestion des certificats et des services associés

CLI	Description	Reportez-vous à
<code>certool</code>	Génère et gère les certificats et les clés. Fait partie de VMCA.	Référence des commandes d'initialisation de certool
<code>vecs-cli</code>	Gère les contenus des instances de VMware Certificate Store. Fait partie de VMAFD.	Référence des commandes vecs-cli
<code>dir-cli</code>	Crée et met à jour les certificats dans le VMware Directory Service. Fait partie de VMAFD.	Référence des commandes dir-cli
<code>service-control</code>	Démarrez ou arrêtez des services, par exemple faisant partie d'un workflow de remplacement de certificat.	

Emplacements des outils de gestion des certificats

Par défaut, les emplacements des outils, au sein de chaque nœud, sont les suivants.

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
```

Sous Linux, la commande `service-control` ne requiert pas de spécifier le chemin.

Si vous exécutez les commandes à partir d'un nœud de gestion disposant d'un Platform Services Controller externe, vous pouvez spécifier le Platform Services Controller avec le paramètre `--server`.

Privilèges requis pour les opérations de gestion de certificats

Pour la plupart des opérations de gestion de certificat vCenter, vous devez être membre du groupe CAAadmins du domaine vsphere.local. L'utilisateur administrator@vsphere.local est membre du groupe CAAadmins. Certaines opérations sont autorisées pour tous les utilisateurs.

Si vous exécutez l'utilitaire vCenter Certificate Manager, vous êtes invité à saisir le mot de passe d'administrator@vsphere.local. Si vous remplacez les certificats manuellement, différentes options, pour les différentes interfaces de ligne de commande de gestion de certificat, requièrent différents privilèges.

dir-cli

Vous devez être membre du groupe CAAdmins du domaine vsphere.local. Vous êtes invité à saisir un nom d'utilisateur et un mot de passe chaque fois que vous exécutez une commande `dir-cli`.

vecs-cli

Au départ, seul le propriétaire du magasin a accès à ce dernier. Le propriétaire du magasin est l'utilisateur Administrateur sur les systèmes Windows et l'utilisateur racine sur les système Linux. Le propriétaire du magasin peut offrir un accès aux autres utilisateurs.

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 CAAdmins. L'utilisateur administrator@vsphere.local est membre du groupe CAAdmins. Tous les utilisateurs peuvent exécuter les commandes suivantes :

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

Pour la gestion des certificats des hôtes ESXi, vous devez avoir le privilège **Certificates. Gérer les certificats**. Vous pouvez définir ce privilège à partir de vSphere Web Client.

Modification de la configuration de certool

Lorsque vous exécutez `certool --gencert` et certaines autres commandes d'initialisation ou de gestion de certificats, l'interface de ligne de commande lit toutes les valeurs d'un fichier de configuration. Vous pouvez modifier le fichier existant, remplacer le fichier de configuration par défaut (`certool.cfg`) au moyen de l'option `--config=<nom de fichier>` ou remplacer différentes valeurs sur la ligne de commande.

Le fichier de configuration 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 de la configuration comme suit :

- Créez une sauvegarde du fichier de configuration, puis modifiez celui-ci. Si vous utilisez le fichier de configuration par défaut, il est inutile de le spécifier. Autrement, par exemple si vous avez modifié le nom du fichier de configuration, utilisez l'option de ligne de commande `--config`.
- Remplacez la valeur du fichier de configuration sur la ligne de commande. Par exemple, pour remplacer Locality, exécutez la commande suivante :

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```

Spécifiez `--Name` pour remplacer le champ CN du nom de sujet du certificat.

- Pour les certificats d'utilisateurs de solutions, le nom est `<nom_utilisateur_solution>@<domaine>` par convention, mais vous pouvez le modifier si une autre convention est utilisée dans votre environnement.
- Pour les certificats SSL de machine, le nom de domaine complet de la machine est utilisé, car le client SSL vérifie le champ CN du nom du sujet du certificat lors de la vérification du nom d'hôte de la machine. Étant donné qu'une machine peut avoir plusieurs alias, les certificats peuvent comporter l'extension de champ Nom de remplacement du sujet qui vous permet de spécifier d'autres noms (noms DNS, adresses IP, etc.). Toutefois, 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`.

Le paramètre `--Hostname` sert à spécifier le nom DNS du Nom de remplacement du sujet du certificat.

Référence des commandes d'initialisation de certool

Les commandes d'initialisation `certool` vous permettent de générer des demandes de signature de certificat, d'afficher et de générer des certificats et des clés qui sont signés par VMCA, d'importer des certificats racines et d'effectuer d'autres opérations de gestion des certificats.

Dans de nombreux cas, vous soumettez un fichier de configuration à une commande certool. Reportez-vous à [Modification de la configuration de certool](#). Vous trouverez des exemples d'utilisation à la section [Remplacer les certificats existants signés par l'autorité de certification VMware \(VMCA\) par de nouveaux certificats](#).

certool --initcsr

Générez une demande de signature de certificat. La commande génère un fichier PKCS10 et une clé privée.

Option	Description
--initcsr	Requis pour générer les demandes de signature de certificat.
--privkey <fichier_clé>	Nom du fichier de clé privée.
--pubkey <fichier_clé>	Nom du fichier de clé publique.
--csrfile <fichier_csr>	Nom du fichier de demandes de signature de certificat à envoyer au fournisseur d'autorité de certification.
--config <fichier_config>	Nom facultatif du fichier de configuration. Défini sur certool.cfg par défaut.

Exemple :

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

Crée un certificat auto-signé et provisionne le serveur VMCA avec une autorité de certification racine auto-signée. Cette option offre une méthode très simple pour provisionner le serveur VMCA. Si vous préférez, vous pouvez provisionner le serveur VMCA à l'aide d'un certificat racine tiers. Ainsi, VMCA est une autorité de certification intermédiaire. Reportez-vous à [Utiliser VMCA en tant qu'autorité de certificat intermédiaire](#).

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 <nombre_de_minutes>	Permet de définir le champ Non valide avant du certificat racine sur un nombre de minutes avant l'heure actuelle. Cette option peut s'avérer utile pour contrer les problèmes potentiels liés aux fuseaux horaires. La valeur maximale est de trois jours.

Option	Description
<code>--config <fichier_config></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> par défaut.
<code>--server <serveur></code>	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 signer, mais d'autres certificats racines restent disponibles. 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
<code>--rootca</code>	Requis pour importer une autorité de certification racine.
<code>--cert <certfile></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> par défaut.
<code>--privkey <fichier_clé></code>	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
<code>--server <serveur></code>	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
<code>--server <serveur></code>	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
<code>--port <num_port></code>	Numéro de port facultatif. La valeur par défaut est le numéro 389.

Exemple :

```
certool --getdc
```

certool --waitVMDIR

Patienter jusqu'à ce que le service d'annuaire VMware 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
<code>--wait</code>	Nombre facultatif de minutes à attendre. La valeur par défaut est 3.
<code>--server <serveur></code>	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
<code>--port <num_port></code>	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
<code>--wait</code>	Nombre facultatif de minutes à attendre. La valeur par défaut est 3.
<code>--server <serveur></code>	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.
<code>--port <num_port></code>	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
<code>--server <serveur></code>	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. Vous pouvez provisionner des machines ou des utilisateurs de solution à l'aide du certificat.

Option	Description
<code>--genkey</code>	Requis pour générer une clé publique et une clé privée.
<code>--privkey <fichier_clé></code>	Nom du fichier de clé privée.
<code>--pubkey <fichier_clé></code>	Nom du fichier de clé publique.
<code>--server <serveur></code>	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.

Option	Description
<code>--gencert</code>	Requis pour générer un certificat.
<code>--cert <certfile></code>	Nom du fichier de certificat. Ce fichier doit être codé au format PEM.
<code>--privkey <fichier_clé></code>	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
<code>--config <fichier_config></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> par défaut.
<code>--server <serveur></code>	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

Imprime le certificat d'autorité de certification racine actuel dans un format lisible par l'œil humain. Si vous exécutez cette commande à partir d'un nœud de gestion, utilisez le nom de machine du nœud Platform Services Controller pour récupérer l'autorité de certification racine. Cette sortie ne peut pas être utilisée en tant que certificat, elle est modifiée pour devenir lisible par l'œil humain.

Option	Description
<code>--getrootca</code>	Requis pour imprimer le certificat racine.
<code>--server <serveur></code>	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
<code>--viewcert</code>	Requis pour afficher un certificat.
<code>--cert <certfile></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> 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
<code>--enumcert</code>	Requis pour répertorier tous les certificats.
<code>--filter [all active]</code>	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 a été révoqué, Certificate: ACTIVE dans le cas contraire.

Option	Description
<code>--status</code>	Requis pour vérifier l'état d'un certificat.
<code>--cert <certfile></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> par défaut.
<code>--server <serveur></code>	Nom facultatif du serveur VMCA. Par défaut, la commande utilise localhost.

Exemple :

```
certool --status --cert=<filename>
```

certool --genselfcert

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
<code>--genselfcert</code>	Requis pour générer un certificat auto-signé.
<code>--outcert <fichier_cert></code>	Nom du fichier de certificat. Ce fichier doit être codé au format PEM.
<code>--outprivkey <fichier_clé></code>	Nom du fichier de clé privée. Ce fichier doit être codé au format PEM.
<code>--config <fichier_config></code>	Nom facultatif du fichier de configuration. Défini sur <code>certool.cfg</code> 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 VECS (VMware Certificate Store). Utilisez ces commandes en conjonction avec `dir-cli` et `certool` pour gérer votre infrastructure de certificats.

vecs-cli store create

Crée un magasin de certificats.

Option	Description
<code>--name <name></code>	Nom du magasin de certificats.

Exemple :

```
vecs-cli store create --name <store>
```

vecs-cli store delete

Supprime un magasin de certificats. Vous ne pouvez pas supprimer les magasins de certificats prédéfinis par le système.

Option	Description
--name <name>	Nom du magasin de certificats à supprimer.

Exemple :

```
vecs-cli store delete --name <store>
```

vecs-cli store list

Affichez la liste des magasins de certificats.

VECS inclut les magasins suivants.

Tableau 3-6. Magasins dans VECS

Magasin	Description
Magasin de certificats SSL de la machine (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ Utilisé par le service de proxy inverse sur chaque nœud vSphere. ■ Utilisé par le service d'annuaire VMware (vmdir) sur les déploiements intégrés et sur chaque nœud Platform Services Controller. <p>Tous les services de vSphere 6.0 communiquent par l'intermédiaire d'un proxy inversé qui utilise le certificat SSL de machine. Pour la compatibilité descendante, les services 5.x utilisent toujours des ports spécifiques. En conséquence, certains services tels que vpxd ont toujours leur port ouvert.</p>
Magasin de certificats racine approuvés (TRUSTED_ROOTS)	Contient tous les certificats racines approuvés.

Tableau 3-6. Magasins dans VECS (suite)

Magasin	Description
Magasins d'utilisateurs de solution	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).
■ virtuelle	Les certificats d'utilisateurs de solutions sont utilisés pour l'authentification avec vCenter Single Sign-On. vCenter Single Sign-On vérifie que le certificat est valide, mais ne vérifie pas d'autres attributs de certificat. Dans un déploiement intégré, tous les certificats d'utilisateur de la solution se trouvent sur le même système.
■ vpxd	Les magasins de certificats d'utilisateurs de solutions sont inclus dans VECS sur chaque nœud de gestion et chaque déploiement intégré :
■ vpxd-extensions	■ <code>machine</code> : Utilisé par le gestionnaire de composants, le serveur de licences et le service de journalisation.
■ vsphere-webclient	<p>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.</p> <p>■ <code>vpxd</code> : Magasin du démon de service vCenter (vpxd) sur les nœuds de gestion et les déploiements intégrés. vpxd utilise le certificat d'utilisateur de solution de ce magasin pour s'authentifier auprès de vCenter Single Sign-On.</p> <p>■ <code>vpxd-extensions</code> : Magasin d'extensions vCenter. Inclut le service Auto Deploy, Inventory Service et d'autres services ne faisant pas partie d'autres utilisateurs de solution.</p> <p>■ <code>vsphere-webclient</code> : Magasin vSphere Web Client. Inclut également certains services supplémentaires tels que le service de graphiques de performance.</p> <p>Le magasin de machines est également inclus sur chaque nœud Platform Services Controller.</p>

Tableau 3-6. Magasins dans VECS (suite)

Magasin	Description
Magasin de sauvegardes de vSphere Certificate Manager Utility (BACKUP_STORE)	Utilisé par VMCA (VMware Certificate Manager) pour prendre en charge la restauration de certificat. Seul l'état le plus récent est stocké en tant que sauvegarde ; vous ne pouvez pas revenir en arrière de plus d'une étape.
Autres magasins	<p>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 la base de connaissances VMware vous y invite.</p> <p>Note Les CRLS ne sont pas pris en charge dans vSphere 6.0. Néanmoins, 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.</p>

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 contrôle l'intégralité de son magasin, y compris l'octroi et la révocation des autorisations. L'administrateur possède tous les privilèges sur tous les magasins, y compris l'octroi et la révocation des autorisations.

Vous pouvez utiliser `vecs-cli get-permissions --name <store-name>` pour récupérer les paramètres actuels du magasin.

Option	Description
<code>--name <name></code>	Nom du magasin de certificats.
<code>--user <username></code>	Nom unique de l'utilisateur auquel les autorisations sont accordées.
<code>--grant [read write]</code>	Autorisation à accorder : lecture (read) ou écriture (write).
<code>--revoke [read write]</code>	Autorisation à révoquer : lecture (read) ou écriture (write). Commande non prise en charge actuellement.

vecs-cli entry create

Créez une entrée dans VECS. Utilisez cette commande pour ajouter une clé privée ou un certificat à un magasin.

Option	Description
<code>--store <NameOfStore></code>	Nom du magasin de certificats.
<code>--alias <Alias></code>	Alias facultatif du certificat. Cette option est ignorée pour le magasin racine approuvé.
<code>--cert <certificate_file_path></code>	Chemin complet du fichier de certificat.
<code>--key <key-file-path></code>	Chemin complet de la clé correspondant au certificat. Facultatif.

vecs-cli entry list

Affichez la liste des entrées présentes dans un magasin spécifié.

Option	Description
<code>--store <NameOfStore></code>	Nom du magasin de certificats.
<code>--text</code>	Affiche une version du certificat lisible par l'œil humain.

vecs-cli entry getcert

Récupérez 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
<code>--store <NameOfStore></code>	Nom du magasin de certificats.
<code>--alias <Alias></code>	Alias du certificat.
<code>--output <output_file_path></code>	Fichier dans lequel écrire le certificat.
<code>--text</code>	Affiche une version du certificat lisible par l'œil humain.

vecs-cli entry getkey

Récupérez une clé stockée dans 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
<code>--store <NameOfStore></code>	Nom du magasin de certificats.
<code>--alias <Alias></code>	Alias de la clé.
<code>--output <output_file_path></code>	Fichier de sortie dans lequel écrire la clé.
<code>--text</code>	Affiche une version de la clé lisible par l'œil humain.

vecs-cli entry delete

Supprimez 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
<code>--store <NameOfStore></code>	Nom du magasin de certificats.
<code>--alias <Alias></code>	Alias de l'entrée à supprimer.

vecs-cli force-refresh

Force l'actualisation de `vecs-cli`. Lorsque cela se produit, la commande `vecs-cli` est mise à jour de manière à utiliser les informations les plus récentes dans vmdir.. 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.

Référence des commandes dir-cli

L'utilitaire `dir-cli` vous permet de créer et de mettre à jour des utilisateurs de solutions, créer d'autres comptes d'utilisateurs et gérer les certificats et les mots de passe dans vmdir. Utilisez cet utilitaire avec `vecs-cli` et `certool` pour gérer votre infrastructure de certificats.

dir-cli service create

Crée un utilisateur de solution. Principalement utilisé par les solutions tierces.

Option	Description
<code>--name <name></code>	Nom de l'utilisateur de solution à créer
<code>--cert <cert file></code>	Chemin d'accès au fichier de certificat. Il peut s'agir d'un certificat signé par VMCA ou d'un certificat tiers.
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--name</code>	Nom de l'utilisateur de solution à supprimer.
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli service update

Met à jour le certificat pour un utilisateur de solution spécifié, c'est-à-dire une collection de services. Après l'exécution de cette commande, VECS applique la modification 5 minutes plus tard ou vous pouvez utiliser `vecs-cli force-refresh` pour forcer une actualisation.

Option	Description
<code>--name <name></code>	Nom de l'utilisateur de solution à mettre à jour.
<code>--cert <cert_file></code>	Nom du certificat à attribuer au service.
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--account <name></code>	Nom de l'utilisateur vCenter Single Sign-On à créer.
<code>--user-password <password></code>	Mot de passe initial de l'utilisateur.
<code>--first-name <name></code>	Prénom de l'utilisateur.
<code>--last-name <name></code>	Nom de l'utilisateur.
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--account <name></code>	Nom de l'utilisateur vCenter Single Sign-On à supprimer.
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAadmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli group modify

Ajoute un utilisateur ou un groupe à un groupe déjà existant.

Option	Description
<code>--name <name></code>	Nom du groupe dans vmdir.
<code>--add <user_or_group_name></code>	Nom de l'utilisateur ou du groupe à ajouter.

Option	Description
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--name <name></code>	Nom facultatif du groupe dans vmdir. Cette option permet de vérifier l'existence d'un groupe.
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	Mot de passe de l'utilisateur administrateur. Si vous ne spécifiez pas le mot de passe, un message vous invite à l'entrer.

dir-cli trustedcert publish

Publie un certificat racine approuvé dans vmdir.

Option	Description
<code>--cert <file></code>	Chemin d'accès au fichier de certificat.
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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 unpublsh

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
<code>--cert-file <file></code>	Chemin d'accès au fichier de certificat dont vous souhaitez annuler la publication
<code>--crl <file></code>	Chemin d'accès au fichier CRL associé à ce certificat. Actuellement inutilisé.
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--id <cert_ID></code>	ID du certificat à récupérer. L'ID s'affiche dans la commande <code>dir-cli trustedcert list</code> .
<code>--outcert <path></code>	Chemin d'écriture du fichier de certificat.
<code>--outcrl <path></code>	Chemin d'écriture du fichier de CRL. Actuellement inutilisé.
<code>--login <admin_user_id></code>	Par défaut, <code>administrator@vsphere.local</code> . Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--account</code>	Nom du compte auquel attribuer un nouveau mot de passe.
<code>--new</code>	Nouveau mot de passe de l'utilisateur spécifié.
<code>--login <admin_user_id></code>	Par défaut, administrator@vsphere.local. Cet administrateur peut ajouter d'autres utilisateurs au groupe CAAAdmins vCenter Single Sign-On pour leur accorder des privilèges d'administrateur.
<code>--password <motdepasse_admin></code>	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
<code>--account</code>	Nom du compte.
<code>--current</code>	Mot de passe actuel de l'utilisateur qui possède le compte.
<code>--new</code>	Nouveau mot de passe de l'utilisateur qui possède le compte.

Afficher les certificats vCenter dans vSphere Web Client

Vous pouvez afficher les certificats connus de l'autorité de certification vCenter (VMCA) pour savoir si les certificats actifs sont sur le point d'expirer, vérifier les certificats expirés et consulter l'état du certificat racine. Vous devez effectuer toutes les tâches de gestion des certificats au moyen des interfaces de ligne de commande de gestion des certificats.

Vous pouvez afficher les certificats associés à l'instance de VMCA incluse dans votre déploiement intégré ou fournie avec Platform Services Controller. Les informations relatives aux certificats sont répliquées dans les instances du service d'annuaire VMware (vmdir).

Lorsque vous tentez d'afficher les certificats dans vSphere Web Client, vous êtes invité à entrer un nom d'utilisateur et un mot de passe. Spécifiez le nom et le mot de passe d'un utilisateur disposant de privilèges pour l'autorité de certification VMware, c'est-à-dire un utilisateur du groupe CAAdmins vCenter Single Sign-On.

Procédure

- 1 Connectez-vous à vCenter Server en tant que `administrator@vsphere.local` ou un autre utilisateur du groupe CAAdmins vCenter Single Sign-On.
- 2 Sélectionnez **Administration**, cliquez sur **Déploiement**, puis cliquez sur **Configuration système**.
- 3 Cliquez sur **Nœuds**, puis sélectionnez le nœud pour lequel vous souhaitez afficher ou gérer des certificats.
- 4 Cliquez sur l'onglet **Gérer**, puis cliquez sur **Autorité de certification**.
- 5 Cliquez sur le type de certificat pour lequel vous voulez afficher des informations relatives au certificat.

Option	Description
Certificats actifs	Affiche les certificats actifs, y compris les informations de validation les concernant. L'icône verte de date de fin de validité change lorsque la date d'expiration du certificat approche.
Certificats révoqués	Affiche la liste des certificats révoqués. Non pris en charge dans cette version.
Certificats expirés	Répertorie les certificats arrivés à expiration.
Certificats racine	Affiche les certificats racines disponibles pour cette instance de l'autorité de certification vCenter.

- 6 Sélectionnez un certificat et cliquez sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat.

Les détails comprennent le nom du sujet, l'émetteur, la validité et l'algorithme.

Définir le seuil pour les avertissements d'expiration du certificat vCenter

Depuis vSphere 6.0, vCenter Server gère tous les certificats du magasin VECS (VMware Endpoint Certificate Store) et émet une alarme lorsque le délai d'expiration d'un certificat est inférieur ou égal à 30 jours. Vous pouvez modifier le délai d'avertissement à l'aide de l'option avancée `vpxd.cert.threshold`.

Procédure

- 1 Connectez-vous à vSphere Web Client.
- 2 Sélectionnez l'objet vCenter Server, puis sélectionnez l'onglet **Gérer** et le sous-onglet **Paramètres**.
- 3 Cliquez sur **Paramètres avancés**, sélectionnez **Modifier** et sélectionnez le filtre par seuil.
- 4 Modifiez le paramètre `vpxd.cert.threshold` en saisissant la valeur souhaitée et cliquez sur **OK**.

Tâches de gestion des utilisateurs et des autorisations de vSphere

4

vCenter Single Sign-On prend en charge l'authentification, ce qui signifie qu'il détermine si un utilisateur peut accéder à l'intégralité des composants vSphere ou pas. En outre, chaque utilisateur doit être autorisé à consulter ou à manipuler les objets vSphere.

vSphere prend en charge différents mécanismes d'autorisation abordés dans [Présentation des autorisations dans vSphere](#). Cette section aborde essentiellement le modèle d'autorisation vCenter Server et le mode d'exécution des tâches de gestion des utilisateurs.

vCenter Server permet un contrôle plus complet des permissions en général grâce aux autorisations et aux rôles. Lorsque vous attribuez une autorisation à un objet de la hiérarchie d'objets de vCenter Server, vous spécifiez les privilèges dont l'utilisateur ou le groupe dispose sur cet objet. Pour spécifier les privilèges, vous utilisez des rôles, qui sont des ensembles de privilèges.

Initialement, seul l'utilisateur `administrator@vsphere.local` est autorisé à se connecter au système vCenter Server. Cet utilisateur peut alors procéder comme suit :

- 1 Ajouter une source d'identité dans laquelle les utilisateurs et les groupes supplémentaires sont définis sur vCenter Single Sign-On. Reportez-vous à la section [Ajouter une source d'identité de vCenter Single Sign-On](#).
- 2 Accorder des privilèges à un utilisateur ou à un groupe en sélectionnant un objet tel qu'une machine virtuelle ou un système vCenter Server et en attribuant un rôle de cet objet à l'utilisateur ou au groupe.



Rôles, privilèges et autorisations

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/)

Ce chapitre contient les rubriques suivantes :

- [Présentation des autorisations dans vSphere](#)
- [Présentation du modèle d'autorisation vCenter Server](#)
- [Héritage hiérarchique des autorisations](#)
- [Paramètres d'autorisation multiples](#)
- [Gestion des autorisations des composants vCenter](#)
- [Autorisations globales](#)

- [Utilisation des rôles pour assigner des privilèges](#)
- [Meilleures pratiques pour les rôles et les autorisations](#)
- [Privilèges requis pour les tâches courantes](#)

Présentation des autorisations dans vSphere

La principale manière d'autoriser un utilisateur ou un groupe dans vSphere consiste à avoir recours aux autorisations vCenter Server. Selon la tâche que vous souhaitez effectuer, vous aurez éventuellement besoin d'une autre autorisation.

vSphere 6.0 et versions ultérieures permet à des utilisateurs privilégiés d'accorder à d'autres utilisateurs des autorisations d'exécution de tâches des manières suivantes. Ces approches sont pour la plupart mutuellement exclusives ; cependant, vous pouvez attribuer des autorisations globales pour accorder à certains utilisateurs des droits sur l'intégralité de la solution, et des autorisations vCenter Server locales pour accorder à d'autres utilisateurs des droits sur des systèmes vCenter Server individuels.

Autorisations vCenter Server

Le modèle d'autorisation des systèmes vCenter Server repose sur l'attribution d'autorisations sur des objets dans la hiérarchie d'objets de cette instance de vCenter Server. Chaque autorisation accorde à un utilisateur ou à un groupe un ensemble de privilèges, c'est-à-dire un rôle sur l'objet sélectionné. Par exemple, vous pouvez sélectionner un hôte ESXi et attribuer un rôle à un groupe d'utilisateurs pour attribuer à ces utilisateurs les privilèges correspondants sur cet hôte.

Autorisations globales

Les autorisations globales sont appliquées à un objet racine global qui peut couvrir plusieurs solutions à la fois. Par exemple, si vCenter Server et vCenter Orchestrator sont installés, vous pouvez accorder des autorisations sur tous les objets dans les deux hiérarchies d'objets à l'aide d'autorisations globales.

Les autorisations globales sont répliquées dans le domaine vsphere.local. Les autorisations globales ne fournissent pas d'autorisations pour les services gérés via des groupes vsphere.local. Reportez-vous à [Autorisations globales](#).

Appartenance à un groupe dans les groupes vsphere.local

L'utilisateur administrator@vsphere.local peut effectuer des tâches associées à des services inclus dans Platform Services Controller. En outre, les membres d'un groupe vsphere.local peuvent effectuer la tâche correspondante. Par exemple, vous pouvez effectuer la gestion des licences si vous êtes membre du groupe LicenseService.Administrators. Reportez-vous à [Groupes du domaine vsphere.local](#).

Autorisations d'hôte ESXi local

Si vous gérez un système ESXi autonome qui n'est pas géré par un système vCenter Server, vous pouvez attribuer l'un des rôles prédéfinis aux utilisateurs. Consultez la documentation de *Administration de vSphere avec vSphere Client*.

Présentation du modèle d'autorisation vCenter Server

Le modèle d'autorisation des systèmes vCenter Server repose sur l'attribution d'autorisations à des objets dans la hiérarchie d'objets vSphere. Chaque autorisation accorde un ensemble de privilèges à un utilisateur ou à un groupe, c'est-à-dire un rôle pour l'objet sélectionné.

Vous devez comprendre les concepts suivants :

Autorisations

Chaque objet de la hiérarchie des objets vCenter Server a des autorisations associées. Chaque autorisation spécifie pour un groupe ou un utilisateur les privilèges dont dispose ce groupe ou cet utilisateur sur l'objet.

Utilisateurs et groupes

Sur les systèmes vCenter Server, vous ne pouvez attribuer des privilèges qu'aux utilisateurs ou aux groupes d'utilisateurs authentifiés. Les utilisateurs sont authentifiés via vCenter Single Sign-On. Les utilisateurs et les groupes doivent être définis dans la source d'identité utilisée par vCenter Single Sign-On pour l'authentification. Définissez les utilisateurs et les groupes à l'aide des outils de votre source d'identité, par exemple Active Directory.

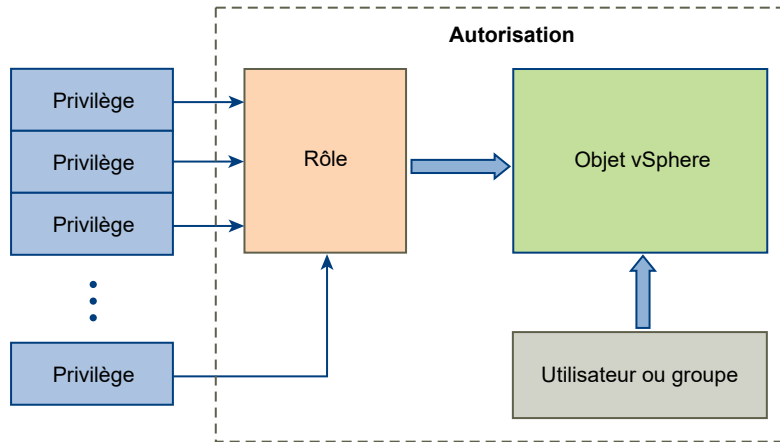
Rôles

Les rôles vous permettent d'attribuer des autorisations sur un objet en fonction d'un ensemble de tâches par défaut exécutées par les utilisateurs. Les rôles par défaut, par exemple Administrateur, sont prédéfinis sur vCenter Server et ne peuvent pas être modifiés. D'autres rôles, par exemple Administrateur de pool de ressources, sont des exemples de rôles prédéfinis. Vous pouvez créer des rôles personnalisés totalement nouveaux, ou cloner et modifier des exemples de rôles.

Privilèges

Les privilèges sont des contrôles d'accès précis. Vous pouvez regrouper ces privilèges dans des rôles, que vous pouvez ensuite mapper à des utilisateurs ou à des groupes.

Figure 4-1. Autorisations de vSphere



Pour attribuer des autorisations à un objet, suivez les étapes suivantes :

- 1 Dans la hiérarchie d'objets vCenter, sélectionnez l'objet auquel vous souhaitez appliquer l'autorisation.
- 2 Sélectionnez le groupe ou l'utilisateur qui doit avoir des privilèges sur l'objet.
- 3 Sélectionnez le rôle, c'est-à-dire l'ensemble de privilèges, que le groupe ou l'utilisateur doit avoir sur l'objet. Par défaut, les autorisations se propagent, c'est-à-dire que le groupe ou l'utilisateur a le rôle sélectionné sur l'objet sélectionné et ses objets enfants.

Le modèle d'autorisations permet d'accélérer la réalisation des tâches en offrant des rôles prédéfinis. Vous pouvez également combiner des privilèges pour créer des rôles personnalisés. Voir [Chapitre 11 Privilèges définis](#) pour obtenir une référence à l'ensemble des privilèges et aux objets auxquels vous pouvez appliquer les privilèges. Voir [Privilèges requis pour les tâches courantes](#) pour consulter des exemples d'ensembles de privilèges dont vous avez besoin pour effectuer ces tâches.

Dans de nombreux cas, les autorisations doivent être définies à la fois sur un objet source et un objet de destination. Par exemple, si vous déplacez une machine virtuelle, vous devez disposer de certains privilèges sur cette machine virtuelle ainsi que sur le centre de données de destination.

Le modèle d'autorisations des hôtes ESXi autonomes est plus simple. Reportez-vous à [Affectation d'autorisations pour ESXi](#)

Validation des utilisateurs de vCenter Server

Les systèmes vCenter Server qui utilisent régulièrement un service d'annuaire valident les utilisateurs et les groupes selon le domaine de l'annuaire utilisateur. La validation est effectuée à intervalles réguliers, comme spécifié dans les paramètres de vCenter Server. Par exemple, si un rôle sur plusieurs objets est attribué à l'utilisateur Smith et que le nom d'utilisateur est remplacé par Smith2 dans le domaine, l'hôte conclut que Smith n'existe plus et supprime des objets vSphere les autorisations associées à cet utilisateur lors de la validation suivante.

De même, si l'utilisateur Smith est supprimé du domaine, toutes les autorisations associées à cet utilisateur sont supprimées lors de la validation suivante. Si un nouvel utilisateur Smith est ajouté au domaine avant la validation suivante, les autorisations des objets de l'ancien utilisateur Smith sont remplacées par celles du nouvel utilisateur Smith.

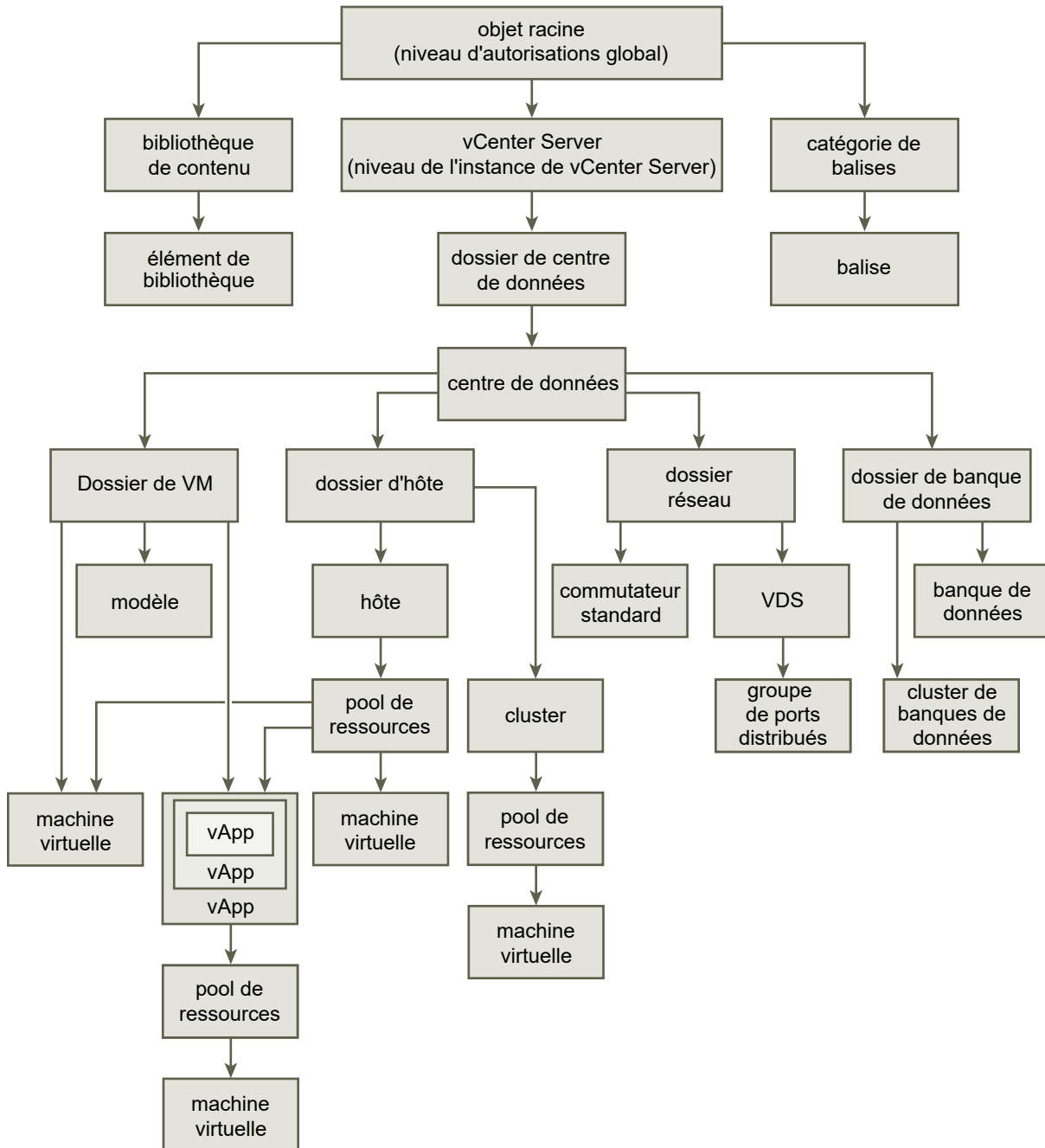
Héritage hiérarchique des autorisations

Quand vous assignez une autorisation à un objet, vous pouvez choisir si l'autorisation propage la hiérarchie d'objet. Vous définissez la propagation pour chaque autorisation. La propagation n'est pas universellement appliquée. Les autorisations définies pour un objet enfant ignorent toujours les autorisations qui sont propagées à partir des objets parent.

La figure illustre la hiérarchie d'inventaire et les chemins par lesquels les autorisations peuvent être propagées.

Note Les autorisations globales prennent en charge l'attribution de privilèges dans plusieurs solutions à partir d'un objet racine global. Reportez-vous à [Autorisations globales](#).

Figure 4-2. Hiérarchie d'inventaire de vSphere



La plupart des objets d'inventaire héritent des autorisations d'un objet parent unique dans la hiérarchie. Par exemple, un centre de données hérite des autorisations de son dossier parent du centre de données ou du centre de données de parent. Les machines virtuelles héritent des autorisations du dossier parent de machine virtuelle et simultanément l'hôte, le cluster ou le pool de ressources parent.

Par exemple, pour définir des autorisations pour un Distributed Switch et ses groupes de ports distribués associés, définissez les autorisations sur un objet parent, tel qu'un dossier ou un centre de données. Vous devez également sélectionner l'option pour propager ces autorisations aux objets enfant.

Les autorisations prennent plusieurs formes dans la hiérarchie :

Entités gérées

Les utilisateurs privilégiés peuvent définir des autorisations sur des entités gérées.

- Clusters
- Centres de données
- Banques de données
- Clusters de banques de données
- Dossiers
- Hôtes
- Réseaux (excepté vSphere Distributed Switches)
- Groupes de ports distribués
- Pools de ressources
- Modèles
- Machines virtuelles
- vSphere vApps

Entités globales

Vous ne pouvez pas modifier les autorisations sur des entités qui dérivent les autorisations du système vCenter Server racine.

- Champs personnalisés
- Licences
- Rôles
- Intervalles de statistiques
- Sessions

Paramètres d'autorisation multiples

Les objets peuvent avoir des autorisations multiples, mais seulement une autorisation pour chaque utilisateur ou groupes. Par exemple, une autorisation peut spécifier que le groupe A dispose des privilèges d'administrateur sur un objet. Une autre autorisation peut spécifier que le groupe B peut avoir des privilèges d'administrateur de machines virtuelles sur le même objet.

Si un objet hérite des autorisations de deux objets parents, les autorisations d'un objet sont ajoutées à celles de l'autre objet. Par exemple, si une machine virtuelle se trouve dans un dossier de machine virtuelle et appartient également à un pool de ressources, cette machine virtuelle hérite de tous les paramètres d'autorisation du dossier de la machine virtuelle et de ceux du pool de ressources.

Les autorisations appliquées sur un objet enfant ignorent toujours les autorisations qui sont appliquées sur un objet parent. Reportez-vous à [Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent](#).

Si des autorisations multiples de groupes sont définies sur le même objet et qu'un utilisateur appartient à au moins deux de ces groupes, deux situations sont possibles :

- Si aucune autorisation n'est définie pour l'utilisateur sur cet objet, l'ensemble de privilèges assignés aux groupes pour cet objet est assigné à l'utilisateur.
- Si une autorisation est définie pour l'utilisateur sur cet objet, l'autorisation de l'utilisateur a la priorité sur toutes les autorisations de groupes.

Exemple 1 : Héritage d'autorisations multiples

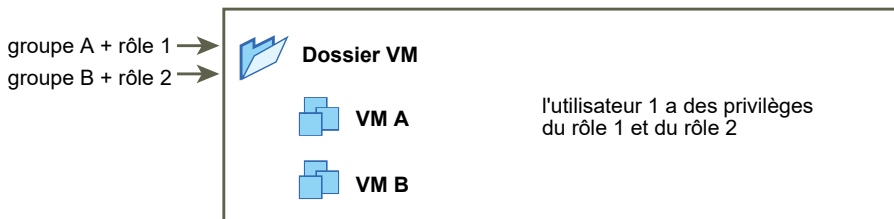
Cet exemple illustre comment un objet peut hériter d'autorisations multiples de groupes auxquels ont été accordés l'autorisation sur un objet parent.

Dans cet exemple, deux autorisations sont assignées sur le même objet pour deux groupes différents.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- Le rôle 2 peut prendre des snapshots de machines virtuelles.
- On accorde au groupes A le rôle 1 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- On accorde au groupes B le rôle 2 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- Aucun privilège spécifique n'est attribué à l'utilisateur 1.

L'utilisateur 1, qui appartient aux groupes A et B, se connecte. L'utilisateur 1 peut mettre sous tension et prendre des snapshots de VM A et de VM B.

Figure 4-3. Exemple 1 : Héritage d'autorisations multiples



Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent

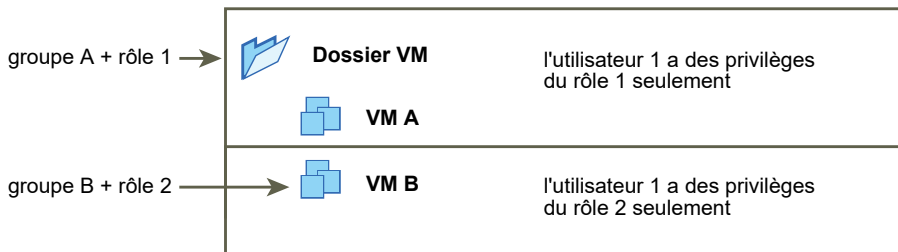
Cet exemple illustre comment les autorisations qui sont assignées sur un objet enfant peuvent ignorer les autorisations qui sont assignées sur un objet parent. Vous pouvez utiliser ce comportement de non prise en compte pour limiter l'accès client à des zones spécifiques de l'inventaire.

Dans cet exemple, des autorisations sont définies sur deux objets différents pour deux groupes différents.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- Le rôle 2 peut prendre des snapshots de machines virtuelles.
- On accorde au groupes A le rôle 1 sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- On accorde le groupes B le rôle 2 sur VM B.

L'utilisateur 1, qui appartient aux groupes A et B, se connecte. Puisque le rôle 2 est assigné à un point inférieur dans la hiérarchie que le rôle 1, il ignore le rôle 1 sur VM B. L'utilisateur 1 peut mettre sous tension VM A, mais ne peut pas prendre des snapshots. L'utilisateur 1 peut prendre des snapshots de VM B, mais ne peut pas les mettre sous tension.

Figure 4-4. Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent



Exemple 3 : Rôle d'utilisateur supprimant un rôle de groupe

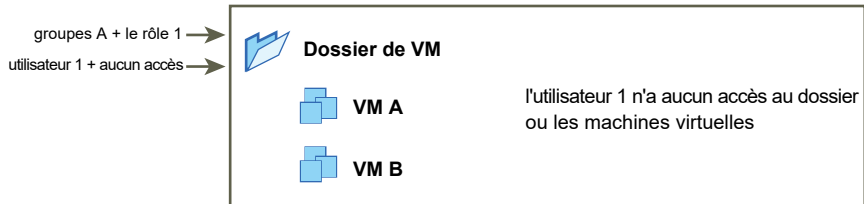
Cet exemple illustre comment le rôle attribué directement à un utilisateur individuel remplace les privilèges associés à un rôle attribué à un groupe.

Dans cet exemple, les autorisations sont définies sur le même objet. Une autorisation associe un groupe à un rôle et l'autre l'autorisation associe un utilisateur individuel à un rôle. L'utilisateur est un membre du groupe.

- Le rôle 1 peut mettre des machines virtuelles sous tension.
- On accorde au groupes A le rôle 1 sur le dossier de VM.
- On accorde à l'utilisateur 1 un rôle Aucun accès sur le dossier de VM.

L'utilisateur 1, qui appartient au groupes A, se connecte. Le rôle Aucun accès accordé à l'utilisateur 1 sur le dossier de VM remplace le rôle attribué au groupe. L'utilisateur 1 n'a aucun accès au dossier ou aux VM A et B. de VM.

Figure 4-5. Exemple 3 : Autorisations d'utilisateurs ignorant des autorisations de groupes



Gestion des autorisations des composants vCenter

Une autorisation est définie sur une hiérarchie d'objets vCenter. Chaque autorisation associe l'objet à un groupe ou un utilisateur et aux rôles d'accès correspondants. Par exemple, vous pouvez sélectionner un objet de machine virtuelle, ajouter une autorisation qui accorde le rôle en lecture seule au Groupe 1 et ajouter une deuxième autorisation qui accorde le rôle d'administrateur à l'utilisateur 2.

En attribuant un rôle différent à un groupe d'utilisateurs sur différents objets, vous contrôlez les tâches que les utilisateurs peuvent effectuer dans votre environnement vSphere. Par exemple, pour autoriser un groupe à configurer la mémoire de l'hôte, sélectionnez l'hôte et ajoutez une autorisation qui accorde à ce groupe un rôle incluant le privilège **Hôte.Configuration.Configuration mémoire**.

Pour gérer les autorisations de vSphere Web Client, vous devez comprendre les concepts suivants :

Autorisations

Chaque objet de la hiérarchie des objets vCenter Server a des autorisations associées. Chaque autorisation spécifie pour un groupe ou un utilisateur les privilèges dont dispose ce groupe ou cet utilisateur sur l'objet.

Utilisateurs et groupes

Sur les systèmes vCenter Server, vous ne pouvez attribuer des privilèges qu'aux utilisateurs ou aux groupes d'utilisateurs authentifiés. Les utilisateurs sont authentifiés via vCenter Single Sign-On. Les utilisateurs et les groupes doivent être définis dans la source d'identité utilisée par vCenter Single Sign-On pour l'authentification. Définissez les utilisateurs et les groupes à l'aide des outils de votre source d'identité, par exemple Active Directory.

Rôles

Les rôles vous permettent d'attribuer des autorisations sur un objet en fonction d'un ensemble de tâches par défaut exécutées par les utilisateurs. Les rôles par défaut, par exemple Administrateur, sont prédéfinis sur vCenter Server et ne peuvent pas être modifiés. D'autres rôles, par exemple Administrateur de pool de ressources, sont des exemples de rôles prédéfinis. Vous pouvez créer des rôles personnalisés totalement nouveaux, ou cloner et modifier des exemples de rôles.

Privilèges

Les privilèges sont des contrôles d'accès précis. Vous pouvez regrouper ces privilèges dans des rôles, que vous pouvez ensuite mapper à des utilisateurs ou à des groupes.

Vous pouvez attribuer des autorisations à des objets sur différents niveaux de la hiérarchie. Vous pouvez, par exemple, attribuer des autorisations à un objet d'hôte ou de dossier qui inclut tous les objets d'hôte. Reportez-vous à [Héritage hiérarchique des autorisations](#). Vous pouvez également attribuer des autorisations à un objet racine global pour appliquer les autorisations à l'ensemble des objets dans toutes les solutions. Reportez-vous à [Autorisations globales](#).

Ajouter une autorisation à un objet d'inventaire

Après avoir créé des utilisateurs et des groupes et avoir défini des rôles, vous devez affecter les utilisateurs et les groupes et leurs rôles aux objets appropriés d'inventaire. Vous pouvez attribuer les mêmes autorisations à plusieurs objets en même temps en déplaçant les objets vers un dossier et en définissant les autorisations du dossier.

Lorsque vous attribuez des autorisations dans vSphere Web Client, les noms des utilisateurs et des groupes doivent correspondre exactement à ceux d'Active Directory, y compris la casse. Si vous avez effectué une mise à niveau à partir de versions antérieures de vSphere, vérifiez le respect de la casse si vous rencontrez des problèmes avec les groupes.

Conditions préalables

Sur l'objet dont vous souhaitez modifier les autorisations, vous devez avoir un rôle qui inclut le privilège **Autorisations.Modifier autorisation**.

Procédure

- 1 Accédez à l'objet auquel vous souhaitez attribuer des autorisations dans le navigateur d'objets de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Autorisations**.
- 3 Cliquez sur l'icône Ajouter, puis cliquez sur **Ajouter**.
- 4 Identifiez l'utilisateur ou le groupe qui disposera des privilèges définis par le rôle sélectionné.
 - a Dans le menu déroulant **Domaine**, sélectionnez le domaine où se trouve l'utilisateur ou le groupes.
 - b Entrez un nom dans la fenêtre de recherche ou sélectionnez un nom dans la liste.

Le système recherche des noms d'utilisateur, des noms de groupe et des descriptions.

- c Sélectionnez l'utilisateur ou le groupe, puis cliquez sur **Ajouter**.

Le nom est ajouté soit à la liste **Utilisateurs** soit à la liste **groupes**.

- d (Facultatif) Cliquez sur **Vérifier les noms** pour vérifier que l'utilisateur ou le groupe existe dans la source d'identité.
- e Cliquez sur **OK**.

- 5 Sélectionner un rôle du menu déroulant **Rôle assigné**.

Les rôles qui sont attribués à l'objet apparaissent dans le menu. Les privilèges contenus dans le rôle sont mentionnés dans la section au-dessous de l'intitulé du rôle.

- 6 (Facultatif) Pour limiter la propagation, décochez la case **Propager vers les objets enfants**.

Le rôle est appliqué seulement à l'objet sélectionné et ne se propage pas aux objets enfant.

- 7 Cliquez sur **OK** pour ajouter l'autorisation.

Changer des autorisations

Après avoir défini un utilisateur ou un groupe et une paire de rôle pour un objet d'inventaire, vous pouvez changer le rôle apparié avec l'utilisateur ou le groupes ou changer le paramètre de la case à cocher **Propager**. Vous pouvez également supprimer le paramètre d'autorisation.

Procédure

- 1 Accédez à l'objet dans le navigateur d'objets de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Autorisations**.
- 3 Cliquer sur l'élément de ligne pour sélectionner l'utilisateur ou le groupes et la paire de rôle.
- 4 Cliquez sur **Modifier rôle de l'autorisation**.
- 5 Sélectionnez un rôle pour l'utilisateur ou le groupe dans le menu déroulant **Rôle assigné**.
- 6 Pour propager les privilèges aux enfants de l'objet d'inventaire assigné, cliquer sur la case à cocher **Propager** et cliquer sur **OK**.

Supprimer les autorisations

Vous pouvez supprimer les autorisations sur un objet de la hiérarchie d'objets, pour un utilisateur spécifique ou pour un groupe. Dans ce cas, l'utilisateur ne dispose plus des privilèges associés au rôle défini sur l'objet.

Procédure

- 1 Accédez à l'objet dans le navigateur d'objets de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** et sélectionnez **Autorisations**.
- 3 Cliquer sur l'élément de ligne approprié pour sélectionner l'utilisateur ou le groupes et la paire de rôle.
- 4 Cliquez sur **Supprimer autorisations**.

Résultats

vCenter Server supprime le paramètre d'autorisation.

Changer les paramètres de validation d'autorisation

vCenter Server valide périodiquement ses listes d'utilisateurs et de groupes selon les utilisateurs et les groupes figurant dans l'annuaire d'utilisateurs. Il supprime alors les utilisateurs ou les groupes qui n'existent plus dans le domaine. Vous pouvez désactiver la validation ou modifier l'intervalle entre les validations. Si vos domaines comportent des milliers de groupes ou d'utilisateurs, ou si les recherches prennent trop de temps, envisagez d'ajuster les paramètres de recherche.

Pour les versions de vCenter Server antérieures à vCenter Server 5.0, ces paramètres s'appliquent à un Active Directory associé à vCenter Server. Pour vCenter Server 5.0 et versions ultérieures, ces paramètres s'appliquent aux sources d'identité de vCenter Single Sign-On.

Note Cette procédure s'applique uniquement aux listes d'utilisateurs de vCenter Server. Les listes d'utilisateurs d'ESXi ne peuvent pas être recherchées de la même manière.

Procédure

- 1 Accédez au système vCenter Server dans le navigateur d'objets de vSphere Web Client.
- 2 Sélectionnez l'onglet **Gérer** et cliquez sur **Paramètres**.
- 3 Cliquez sur **Général** puis sur **Modifier**.
- 4 Sélectionnez **Annuaire utilisateur**.
- 5 Modifiez les valeurs si nécessaire.

Option	Description
Délai d'expiration de l'annuaire d'utilisateurs	Délai d'expiration en secondes pour la connexion au serveur Active Directory. Cette valeur spécifie le délai maximal pendant lequel vCenter Server autorise l'exécution de la recherche sur le domaine sélectionné. La recherche dans de grands domaines peut prendre du temps.
Limite de requête	Cochez cette case pour définir le nombre maximal d'utilisateurs et de groupes qui s'affichent dans vCenter Server.
Taille limite de requête	Spécifie le nombre maximal d'utilisateurs et de groupes qui s'affichent dans vCenter Server depuis le domaine sélectionné dans la boîte de dialogue Choisir les utilisateurs ou les groupes . Si vous entrez 0 (zéro), tous les utilisateurs et groupes apparaissent.
Validation	Décochez cette case pour désactiver la validation
Période de validation	Spécifie combien de fois vCenter Server valide les autorisations, en minutes.

- 6 Cliquez sur **OK**.

Autorisations globales

Les autorisations globales sont appliquées à un objet racine global qui peut couvrir plusieurs solutions à la fois (vCenter Server et vCenter Orchestrator, par exemple). Utilisez les autorisations globales pour accorder à un utilisateur ou à un groupe des privilèges pour tous les objets dans l'ensemble des hiérarchies d'objets.

Un objet racine se trouve dans la hiérarchie d'objets de chaque solution. L'objet racine global agit comme un objet parent sur chaque objet de la solution. Vous pouvez attribuer des autorisations globales à des utilisateurs ou des groupes et choisir le rôle de chaque utilisateur ou de chaque groupe. Le rôle détermine l'ensemble de privilèges. Vous pouvez attribuer un rôle prédéfini ou créer des rôles personnalisés. Reportez-vous à [Utilisation des rôles pour assigner des privilèges](#). Il est important de faire la distinction entre les autorisations vCenter Server et les autorisations globales.

Autorisations vCenter Server

Dans la plupart des cas, vous appliquez une autorisation à un objet d'inventaire vCenter Server tel qu'un hôte ESXi ou une machine virtuelle. À ce moment-là, vous spécifiez qu'un utilisateur ou un groupe dispose d'un ensemble de privilèges (appelé « rôle ») sur l'objet.

Autorisations globales

Les autorisations globales accordent à un utilisateur ou à un groupe des privilèges permettant d'afficher ou de gérer tous les objets dans chaque hiérarchie d'inventaire de votre déploiement.

Si vous affectez une autorisation globale sans sélectionner Propager, les utilisateurs ou les groupes associés à cette autorisation n'ont pas accès aux objets de la hiérarchie. Ils n'ont accès qu'à certaines fonctions globales telles que la création de rôles.

Important Les autorisations globales doivent être utilisées avec précaution. Vérifiez que vous voulez vraiment attribuer des autorisations à tous les objets dans l'ensemble des hiérarchies d'inventaire.

Ajouter une autorisation globale

Vous pouvez utiliser les autorisations globales pour accorder à un utilisateur ou à un groupe des privilèges pour tous les objets dans l'ensemble des hiérarchies d'inventaire de votre déploiement.

Les autorisations globales doivent être utilisées avec précaution. Vérifiez que vous voulez vraiment attribuer des autorisations à tous les objets dans l'ensemble des hiérarchies d'inventaire.

Conditions préalables

Pour effectuer cette tâche, vous devez disposer des privilèges **.Autorisations.Modifier autorisation** sur l'objet racine de l'ensemble des hiérarchies d'inventaire.

Procédure

- 1 Cliquez sur **Administration** et sélectionnez **Autorisations globales** dans la zone Contrôle d'accès.
- 2 Cliquez sur **Gérer**, puis sur l'icône Ajouter autorisation.
- 3 Identifiez l'utilisateur ou le groupe qui disposera des privilèges définis par le rôle sélectionné.
 - a Dans le menu déroulant **Domaine**, sélectionnez le domaine où se trouve l'utilisateur ou le groupes.
 - b Entrez un nom dans la fenêtre de recherche ou sélectionnez un nom dans la liste.
Le système recherche des noms d'utilisateur, des noms de groupe et des descriptions.
 - c Sélectionnez l'utilisateur ou le groupe, puis cliquez sur **Ajouter**.
Le nom est ajouté soit à la liste **Utilisateurs** soit à la liste **groupes**.
 - d (Facultatif) Cliquez sur **Vérifier les noms** pour vérifier que l'utilisateur ou le groupe existe dans la source d'identité.
 - e Cliquez sur **OK**.
- 4 Sélectionner un rôle du menu déroulant **Rôle assigné**.
Les rôles qui sont attribués à l'objet apparaissent dans le menu. Les privilèges contenus dans le rôle sont mentionnés dans la section au-dessous de l'intitulé du rôle.
- 5 Cochez la case Propager vers les enfants dans la plupart des cas.
Si vous affectez une autorisation globale sans sélectionner Propager, les utilisateurs ou les groupes associés à cette autorisation n'ont pas accès aux objets de la hiérarchie. Ils n'ont accès qu'à certaines fonctions globales telles que la création de rôles.
- 6 Cliquez sur **OK**.

Autorisations sur les objets de balise

Dans la hiérarchie d'objets de vCenter Server, les objets de balise ne sont pas des enfants de vCenter Server mais sont créés au niveau racine de vCenter Server. Dans les environnements avec plusieurs instances de vCenter Server, les objets de balise sont partagés entre les instances de vCenter Server. Dans la hiérarchie d'objets de vCenter Server, les autorisations pour les objets de balise fonctionnent différemment des autorisations pour les autres objets.

Seules les autorisations globales ou attribuées à l'objet de balise s'appliquent

Si vous accordez des autorisations à un utilisateur sur un objet d'inventaire de vCenter Server, comme un hôte ou une machine virtuelle ESXi, l'utilisateur ne peut pas effectuer d'opérations de balisage sur cet objet.

Par exemple, si vous accordez le privilège **Attribuer une balise vSphere** à l'utilisateur Dana sur le TPA de l'hôte, cette autorisation ne modifie pas le droit accordé ou non à Dana de lui attribuer des balises. Dana doit disposer du privilège **Attribuer une balise vSphere** au niveau racine - c'est-à-dire une autorisation globale - ou du privilège pour l'objet de balise.

Tableau 4-1. Conséquences des autorisations globales et des autorisations sur les objets sur ce que peuvent faire les utilisateurs

Autorisation globale	Autorisation au niveau des balises	vCenter Server Autorisation au niveau des objets	Autorisation valable
Aucun privilège de balisage accordé	Dana dispose des privilèges Attribuer une balise vSphere ou en annuler l'attribution pour la balise.	Dana dispose des privilèges Supprimer une balise vSphere sur le TPA de l'hôte ESXi	Dana dispose des privilèges Attribuer une balise vSphere ou en annuler l'attribution pour la balise.
Dana dispose des privilèges Attribuer une balise vSphere ou en annuler l'attribution .	Aucun privilège n'est attribué pour la balise.	Dana dispose des privilèges Supprimer une balise vSphere sur le TPA de l'hôte ESXi	Dana dispose des privilèges globaux Attribuer une balise vSphere ou en annuler l'attribution . Ceci inclut des privilèges au niveau des balises.
Aucun privilège de balisage accordé	Aucun privilège n'est attribué pour la balise.	Dana dispose des privilèges Attribuer une balise vSphere ou en annuler l'attribution sur le TPA de l'hôte ESXi	Dana ne dispose des privilèges de balisage sur aucun objet, y compris le TPA de l'hôte.

Les autorisations globales étendent les autorisations sur les objets de balise

Les autorisations globales, c'est-à-dire des autorisations qui sont attribuées sur l'objet racine, complètent les autorisations sur les objets de balise lorsque celles-ci sont trop restrictives. Les autorisations vCenter Server n'affectent pas les objets de balise.

Par exemple, supposons que vous attribuez le privilège **Supprimer une balise vSphere** à l'utilisateur Robin au niveau racine, en utilisant les autorisations globales. Pour la production de balises, vous n'attribuez pas le privilège **Supprimer une balise vSphere** à Robin. Dans ce cas, Robin dispose du privilège, même pour la production de balises car il a l'autorisation globale. Si vous ne modifiez pas l'autorisation globale, vous ne pouvez pas restreindre les privilèges.

Tableau 4-2. Les autorisations globales complètent les autorisations au niveau des balises

Autorisation globale	Autorisation au niveau des balises	Autorisation valable
Robin dispose des privilèges Supprimer une balise vSphere	Robin ne dispose pas des privilèges Supprimer une balise vSphere pour la balise.	Robin dispose des privilèges Supprimer une balise vSphere .
Aucun privilège de balisage accordé	Les privilèges Supprimer une balise vSphere ne sont pas attribués à Robin pour la balise.	Robin ne dispose pas des privilèges Supprimer une balise vSphere

Les autorisations au niveau des balises peuvent étendre les autorisations globales

Vous pouvez utiliser des autorisations au niveau des balises pour étendre les autorisations globales. Cela signifie que les utilisateurs peuvent avoir l'autorisation globale et l'autorisation au niveau des balises sur une balise.

Tableau 4-3. Les autorisations globales étendent les autorisations au niveau des balises

Autorisation globale	Autorisation au niveau des balises	Autorisation valable
Lee dispose du privilège Attribuer une balise vSphere ou en annuler l'attribution.	Lee dispose du privilège Supprimer une balise vSphere.	Lee dispose des privilèges Attribuer une balise vSphere et Supprimer une balise vSphere pour la balise.
Aucun privilège de balisage n'est accordé.	Le privilège Supprimer une balise vSphere est attribué à Lee pour la balise.	Lee dispose du privilège Supprimer une balise vSphere pour la balise.

Utilisation des rôles pour assigner des privilèges

Un rôle est un ensemble prédéfini de privilèges. Les privilèges définissent les droits permettant d'effectuer des actions et de lire des propriétés. Par exemple, le rôle Administrateur de machine virtuelle est constitué de propriétés de lecture et d'un ensemble de droits permettant de réaliser des actions spécifiques. Avec ce rôle, l'utilisateur peut lire et modifier les attributs des machines virtuelles.

Lorsque vous attribuez des autorisations, vous coupez un utilisateur ou un groupe avec un rôle et associez ce couplage à un objet d'inventaire. Un utilisateur ou groupe peut avoir différents rôles pour différents objets de l'inventaire.

Par exemple, si l'inventaire comprend deux pools de ressources, le pool A et le pool B, vous pouvez attribuer à un utilisateur particulier le rôle Utilisateur de machine virtuelle sur le pool A et le rôle Lecture seule sur le pool B. Ainsi, il peut démarrer les machines virtuelles du pool A, mais uniquement afficher les machines virtuelles du pool B.

vCenter Server fournit les rôles système et les exemples de rôles par défaut :

Rôles système

Les rôles système sont permanents. Vous ne pouvez pas éditer les privilèges liés à ces rôles.

Exemples de rôles

VMware fournit des exemples de rôles pour certaines combinaisons réalisées fréquemment. Vous pouvez cloner, modifier ou supprimer ces rôles.

Note Pour éviter de perdre les paramètres prédéfinis dans un exemple de rôle, clonez d'abord le rôle, puis modifiez le clone. Vous ne pouvez pas rétablir les paramètres par défaut de l'exemple.

Les utilisateurs ne peuvent planifier des tâches que si leurs rôles leur donnent des privilèges suffisants pour réaliser ces tâches au moment de leur création.

Note Les modifications apportées aux rôles et aux privilèges prennent effet immédiatement, même si les utilisateurs impliqués sont connectés. Les recherches font toutefois exception : pour celles-ci, les modifications entrent en vigueur une fois que l'utilisateur s'est déconnecté, puis reconnecté.

Rôles personnalisés dans vCenter Server et ESXi

Vous pouvez créer des rôles personnalisés pour vCenter Server et tous les objets qu'il gère, ou pour des hôtes individuels.

Rôles personnalisés de vCenter Server (recommandé)

Créez des rôles personnalisés à l'aide des fonctionnalités de modification de rôles de vSphere Web Client afin de créer des ensembles de privilèges répondant spécifiquement à vos besoins.

Rôles personnalisés d'ESXi

Vous pouvez créer des rôles personnalisés pour des hôtes individuels en utilisant une ligne de commande ou vSphere Client. Reportez-vous à la documentation *Administration de vSphere avec vSphere Client*. Les rôles d'hôtes personnalisés ne sont pas accessibles à partir de vCenter Server.

Si vous gérez des hôtes ESXi au moyen de vCenter Server, la conservation des rôles personnalisés dans l'hôte et dans vCenter Server peut engendrer de la confusion et des utilisations abusives. Dans la plupart des cas, la définition de rôles de vCenter Server est recommandée.

Lorsque vous gérez un hôte à l'aide de vCenter Server, les autorisations associées à cet hôte sont créées via vCenter Server et stockées dans vCenter Server. Si vous vous connectez directement à un hôte, seuls les rôles créés directement sur l'hôte sont disponibles.

Note Si vous ajoutez un rôle personnalisé sans lui attribuer de privilège, celui-ci est créé comme un rôle Lecture seule avec trois privilèges définis par le système : **System.Anonymous**, **System.View** et **System.Read**.



Création de rôles dans vSphere Web Client

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/)

Rôles système de vCenter Server

Un rôle est un ensemble prédéfini de privilèges. Lorsque vous ajoutez des autorisations à un objet, vous associez un utilisateur ou un groupe à un rôle. vCenter Server comprend plusieurs rôles système que vous ne pouvez pas modifier.

Rôles système de vCenter Server

vCenter Server ne fournit que très peu de rôles par défaut. Vous ne pouvez pas changer les privilèges associés aux rôles par défaut. Les rôles par défaut sont organisés de façon hiérarchique ; chaque rôle hérite des privilèges du rôle précédent. Par exemple, le rôle Administrateur hérite des privilèges du rôle Lecture seule. Les rôles que vous créez vous-même n'héritent des privilèges d'aucun rôle système.

Rôle d'administrateur

Les utilisateurs assignés au rôle Administrateur pour un objet sont autorisés à afficher et à exécuter toutes les actions sur cet objet. Ce rôle comprend également tous les privilèges inhérents au rôle en lecture seule. Si vous disposez du rôle d'administrateur sur un objet, vous pouvez attribuer des privilèges à des utilisateurs individuels ou des groupes. Si vous disposez du rôle d'administrateur dans vCenter Server, vous pouvez attribuer des privilèges à des utilisateurs et des groupes dans la source d'identité vCenter Single Sign-On par défaut. Les services d'identité pris en charge incluent Windows Active Directory et OpenLDAP 2.4.

Par défaut, l'utilisateur administrator@vsphere.local a le rôle d'administrateur sur vCenter Single Sign-On et vCenter Server après l'installation. Cet utilisateur peut ensuite associer d'autres utilisateurs disposant du rôle d'administrateur dans vCenter Server.

rôle Aucun accès

Les utilisateurs assignés au rôle aucun accès pour un objet ne peuvent en aucun cas afficher ou modifier l'objet. Les nouveaux utilisateurs et groupes sont assignés à ce rôle par défaut. Vous pouvez modifier le rôle par objet.

Les utilisateurs administrator@vsphere.local, racine et vpxuser sont les seuls utilisateurs auxquels n'est pas attribué le rôle Aucun accès par défaut. Ils sont en revanche assignés au rôle Administrateur. Vous pouvez entièrement supprimer toute autorisation de l'utilisateur racine ou lui accorder le rôle Aucun accès du moment que vous commencez par créer une autorisation de remplacement au niveau de la racine avec le rôle d'administrateur et que vous associez ce rôle à un autre utilisateur.

rôle Lecture seule

Les utilisateurs assignés au rôle Lecture seule pour un objet sont autorisés à afficher l'état et les détails de l'objet. Grâce à ce rôle, un utilisateur peut afficher les caractéristiques d'une machine virtuelle, d'un hôte et d'un pool de ressources. L'utilisateur ne peut pas voir la console à distance pour un hôte. Toutes les actions via les menus et barres d'outils ne sont pas autorisées.

Créer un rôle personnalisé

Vous pouvez créer des rôles personnalisés vCenter Server correspondant aux besoins de contrôle d'accès de votre environnement.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

- 1 Connectez-vous à vCenter Server avec vSphere Web Client.
- 2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.
- 3 Cliquez sur le bouton **Créer une action de rôle (+)**.
- 4 Introduire un nom pour le nouveau rôle.
- 5 Sélectionner les privilèges pour le rôle et cliquer sur **OK**.

Cloner un rôle

Vous pouvez effectuer une copie d'un rôle existant, le renommer et le modifier. Quand vous faites une copie, le nouveau rôle n'est pas appliqué à n'importe quel utilisateur ou groupe et objet. Vous devez attribuer le rôle aux utilisateurs ou groupes et objets.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

- 1 Connectez-vous à vCenter Server avec vSphere Web Client.
- 2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.
- 3 Sélectionnez un rôle et cliquez sur l'icône **Cloner une action de rôle**.
- 4 Saisissez un nom pour le rôle cloné.
- 5 Sélectionnez ou désélectionnez des privilèges pour le rôle, puis cliquez sur **OK**.

Éditer un rôle

Quand vous éditez un rôle, vous pouvez changer les privilèges sélectionnés pour ce rôle. Une fois terminés, ces privilèges sont appliqués à n'importe quel utilisateur ou groupe auquel le rôle modifié a été attribué.

Si vous créez ou modifiez un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server, le service d'annuaire VMware (vmdir) propage les modifications que vous apportez à tous les autres systèmes vCenter Server du groupe. Cependant, les attributions de rôles à des utilisateurs et objets spécifiques ne sont pas partagées entre les systèmes vCenter Server.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'utilisateur avec des privilèges d'administrateur.

Procédure

- 1 Connectez-vous à vCenter Server avec vSphere Web Client.
- 2 Sélectionnez Accueil, cliquez sur **Administration**, puis cliquez sur **Rôles**.
- 3 Sélectionnez un rôle, puis cliquez sur le bouton **Modifier une action de rôle**.
- 4 Sélectionnez ou désélectionnez des privilèges pour le rôle, puis cliquez sur **OK**.

Meilleures pratiques pour les rôles et les autorisations

Utilisez les meilleures pratiques pour les rôles et les autorisations afin de maximiser la sécurité et la gérabilité de votre environnement vCenter Server.

VMware recommande les meilleures pratiques suivantes lorsque vous configurez les rôles et les autorisations dans votre environnement vCenter Server :

- Lorsque cela est possible, attribuez un rôle à un groupe plutôt qu'à des utilisateurs individuels pour accorder des privilèges à ce groupe.
- Accordez des autorisations uniquement sur les objets lorsque cela est nécessaire et attribuez des privilèges uniquement aux utilisateurs ou aux groupes qui doivent en disposer. Utiliser un nombre minimal d'autorisations facilite la compréhension et la gestion de votre structure d'autorisations.
- Si vous assignez un rôle restrictif à un groupe, vérifiez que le groupes ne contient pas l'utilisateur d'administrateur ou d'autres utilisateurs avec des privilèges administratifs. Sinon, vous pourriez involontairement limiter les privilèges des administrateurs dans les parties de la hiérarchie d'inventaire où vous avez assigné à ce groupes le rôle restrictif.
- Utilisez des dossiers pour grouper des objets. Par exemple, si vous souhaitez accorder une autorisation de modification sur un ensemble d'hôtes et afficher une autorisation sur un autre ensemble d'hôtes, placez chaque ensemble d'hôtes dans un dossier.

- Soyez prudent lorsque vous ajoutez une autorisation aux objets vCenter Server racine. Les utilisateurs disposant de privilèges au niveau racine ont accès à des données globales sur vCenter Server, telles que les rôles, les attributs personnalisés et les paramètres vCenter Server.
- Dans la plupart des cas, activez la propagation lorsque vous attribuez des autorisations à un objet. Ceci garantit que quand de nouveaux objets sont insérés dans la hiérarchie d'inventaire, ils héritent des autorisations et sont accessibles aux utilisateurs.
- Utilisez le rôle Aucun Accès pour masquer des zones spécifiques de la hiérarchie si vous souhaitez empêcher l'accès de certains utilisateurs ou groupes aux objets qui se trouvent dans cette partie de la hiérarchie d'objets.
- Les modifications apportées aux licences sont appliquées à tous les systèmes vCenter Server qui sont liés au même Platform Services Controller ou aux Platform Services Controller se trouvant dans le même domaine vCenter Single Sign-On, même si l'utilisateur ne dispose pas de privilèges sur tous les systèmes vCenter Server.

Privilèges requis pour les tâches courantes

Beaucoup de tâches exigent des autorisations sur plus d'un objet dans l'inventaire. Vous pouvez passer en revue les privilèges requis pour exécuter les tâches et, le cas échéant, les rôles modèles appropriés.

Le tableau suivant répertorie les tâches courantes qui exigent plusieurs privilèges. Vous pouvez ajouter des autorisations à des objets d'inventaire en associant un utilisateur à l'un des rôles prédéfinis. Vous pouvez également créer des rôles personnalisés avec l'ensemble des privilèges que vous prévoyez d'utiliser plusieurs fois.

Si la tâche que vous souhaitez exécuter ne se trouve pas dans ce tableau, les règles suivantes peuvent vous aider à déterminer l'emplacement dans lequel vous devez attribuer des autorisations pour autoriser certaines opérations :

- N'importe quelle opération qui consomme l'espace de stockage, telle que la création d'un disque virtuel ou la prise d'un snapshot, exige le privilège **Banque de données.Allouer l'espace** sur la banque de données cible, ainsi que le privilège d'exécuter l'opération elle-même.
- Le déplacement d'un objet dans la hiérarchie d'inventaire exige les privilèges appropriés sur l'objet lui-même, l'objet parent source (tel qu'un dossier ou un cluster) et l'objet parent de destination.
- Chaque hôte et chaque cluster ont leur propre pool de ressources implicite qui contient toutes les ressources de cet hôte ou de ce cluster. Le déploiement d'une machine virtuelle directement sur un hôte ou un cluster exige le privilège **Ressource.Attribuer une machine virtuelle au pool de ressources**.

Tableau 4-4. Privilèges requis pour les tâches courantes

Tâche	Privilèges requis	Rôle applicable
Créer une machine virtuelle	Dans le dossier ou le centre de données de destination : <ul style="list-style-type: none"> ■ Machine virtuelle.Inventaire .Créer nouveau ■ Machine virtuelle.Configuration.Ajouter un nouveau disque (en cas de création d'un nouveau disque virtuel) ■ Machine virtuelle.Configuration.Ajouter un disque existant (en cas d'utilisation d'un disque virtuel existant) ■ Machine virtuelle.Configuration.Périphérique brut (en cas d'utilisation d'un périphérique de relais RDM ou SCSI) 	Administrateur
	Sur l'hôte, cluster ou pool de ressources de destination : Ressource.Attribuer une machine virtuelle au pool de ressources	Administrateur de pool de ressources ou Administrateur
	Sur la banque de données ou le dossier de destination contenant une banque de données : Banque de données.Allouer de l'espace	Utilisateur de banque de données ou Administrateur
	Sur le réseau auquel la machine virtuelle sera assignée : Réseau.Assign un réseau	Utilisateur réseau ou Administrateur
Déployer une machine virtuelle à partir d'un modèle	Dans le dossier ou le centre de données de destination : <ul style="list-style-type: none"> ■ Machine virtuelle .Inventaire .Créer à partir d'un modèle/d'une machine virtuelle existante ■ Machine virtuelle.Configuration.Ajouter un nouveau disque 	Administrateur
	Sur un modèle ou un dossier des modèles : Machine virtuelle.Provisionnement.Déployer un modèle	Administrateur
	Sur l'hôte, le cluster ou le pool de ressources de destination : Ressource.Attribuer une machine virtuelle au pool de ressources	Administrateur
	Sur la banque de données de destination ou le dossier des banques de données : Banque de données.Allouer de l'espace	Utilisateur de banque de données ou Administrateur
	Sur le réseau auquel la machine virtuelle sera assignée : Réseau.Assign un réseau	Utilisateur réseau ou Administrateur
Faire un snapshot de machine virtuelle	Sur la machine virtuelle ou un dossier des machines virtuelles : Machine virtuelle.Gestion des snapshots.Créer un snapshot	Utilisateur avancé de machines virtuelles ou Administrateur
Déplacer une machine virtuelle dans un pool de ressources	Sur la machine virtuelle ou le dossier des machines virtuelles : <ul style="list-style-type: none"> ■ Ressource.Attribuer une machine virtuelle au pool de ressources ■ Machine virtuelle.Inventaire .Déplacer 	Administrateur
	Sur le pool de ressources de destination : Ressource.Attribuer une machine virtuelle au pool de ressources	Administrateur

Tableau 4-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
Installer un système d'exploitation invité sur une machine virtuelle	<p>Sur la machine virtuelle ou le dossier des machines virtuelles :</p> <ul style="list-style-type: none"> ■ Machine virtuelle.Interaction.Répondre à une question ■ Machine virtuelle.Interaction.Interaction avec une console ■ Machine virtuelle.Interaction.Connexion de périphérique ■ Machine virtuelle.Interaction.Mettre hors tension ■ Machine virtuelle.Interaction.Mettre sous tension ■ Machine virtuelle.Interaction.Réinitialiser ■ Machine virtuelle.Interaction.Configurer un support CD (en cas d'installation à partir d'un CD) ■ Machine virtuelle.Interaction.Configurer un support de disquette (en cas d'installation à partir d'une disquette) ■ Machine virtuelle.Interaction.Installer VMware Tools 	Utilisateur avancé de machines virtuelles ou Administrateur
	<p>Sur une banque de données contenant l'image ISO de support d'installation :</p> <p>Banque de données.Parcourir une banque de données (en cas d'installation à partir d'une image ISO sur une banque de données)</p> <p>Sur la banque de données sur laquelle vous chargez l'image ISO de support d'installation :</p> <ul style="list-style-type: none"> ■ Banque de données.Parcourir une banque de données ■ Banque de données.Opérations de fichier de niveau inférieur 	Utilisateur avancé de machines virtuelles ou Administrateur
Migrer une machine virtuelle avec vMotion	<p>Sur la machine virtuelle ou le dossier des machines virtuelles :</p> <ul style="list-style-type: none"> ■ Ressource.Migrer une machine virtuelle sous tension ■ Ressource.Attribuer une machine virtuelle au pool de ressources (si la destination est un pool de ressources différent de la source) 	Administrateur de pool de ressources ou Administrateur
	<p>Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) :</p> <p>Ressource.Attribuer une machine virtuelle au pool de ressources</p>	Administrateur de pool de ressources ou Administrateur
Migrer à froid (relocaliser) une machine virtuelle	<p>Sur la machine virtuelle ou le dossier des machines virtuelles :</p> <ul style="list-style-type: none"> ■ Ressource.Migrer une machine virtuelle hors tension ■ Ressource.Attribuer une machine virtuelle au pool de ressources (si la destination est un pool de ressources différent de la source) 	Administrateur de pool de ressources ou Administrateur
	<p>Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) :</p> <p>Ressource.Attribuer une machine virtuelle au pool de ressources</p>	Administrateur de pool de ressources ou Administrateur
	<p>Sur la banque de données de destination (si différent de la source) :</p> <p>Banque de données.Allouer de l'espace</p>	Utilisateur de banque de données ou Administrateur
Migration d'une machine virtuelle avec Storage vMotion	<p>Sur la machine virtuelle ou le dossier des machines virtuelles :</p> <p>Ressource.Migrer une machine virtuelle sous tension</p>	Administrateur de pool de ressources ou Administrateur

Tableau 4-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
	Sur la banque de données de destination : Banque de données.Allouer de l'espace	Utilisateur de banque de données ou Administrateur
Déplacer un hôte dans un cluster	Sur l'hôte : Hôte.Inventaire.Ajouter un hôte au cluster	Administrateur
	Sur le cluster de destination : Hôte.Inventaire.Ajouter un hôte au cluster	Administrateur

Sécurisation des hôtes ESXi

5

L'architecture de l'hyperviseur ESXi intègre de nombreuses fonctionnalités de sécurité, telles que l'isolation du CPU, l'isolation de la mémoire et l'isolation des périphériques. Vous pouvez configurer des fonctionnalités supplémentaires, comme le mode de verrouillage, le remplacement de certificats et l'authentification par carte à puce, pour renforcer la sécurité.

Un hôte ESXi est également protégé par un pare-feu. Vous pouvez ouvrir les ports au trafic entrant et sortant selon vos besoins, mais limitez l'accès aux services et aux ports. L'utilisation du mode verrouillage ESXi et la limitation de l'accès à ESXi Shell peuvent également contribuer à sécuriser davantage l'environnement. À partir de vSphere 6.0, les hôtes ESXi participent à l'infrastructure de certificats. Les hôtes sont provisionnés à l'aide de certificats signés par l'autorité de certification VMware (VMCA) par défaut.

Pour plus d'informations sur la sécurité d'ESXi, reportez-vous au livre blanc VMware ESXi.

Ce chapitre contient les rubriques suivantes :

- [Utiliser des scripts pour gérer des paramètres de configuration d'hôte](#)
- [Configurer des hôtes ESXi avec des profils d'hôte](#)
- [Recommandations générales de sécurité pour ESXi](#)
- [Gestion de certificats pour les hôtes ESXi](#)
- [Personnalisation des hôtes avec le profil de sécurité](#)
- [Affectation d'autorisations pour ESXi](#)
- [Utilisation d'Active Directory pour gérer des utilisateurs ESXi](#)
- [Utiliser vSphere Authentication Proxy](#)
- [Meilleures pratiques de sécurité de ESXi](#)
- [Configuration de l'authentification par carte à puce pour ESXi](#)
- [Clés SSH ESXi](#)
- [Utilisation du ESXi Shell](#)
- [Modifier les paramètres proxy Web ESXi](#)
- [Considérations relatives à la sécurité dans vSphere Auto Deploy](#)
- [Gestion des fichiers journaux ESXi](#)

Utiliser des scripts pour gérer des paramètres de configuration d'hôte

Dans les environnements comportant de nombreux hôtes, la gestion des hôtes avec des scripts est plus rapide et moins susceptible de provoquer des erreurs que la gestion des hôtes depuis vSphere Web Client.

vSphere inclut plusieurs langages de script pour la gestion des hôtes. Reportez-vous à la *Documentation sur la ligne de commande de vSphere* et à la *Documentation sur vSphere API/SDK* pour obtenir des informations de référence et des astuces de programmation, et pour accéder à des communautés VMware afin d'obtenir des conseils supplémentaires sur la gestion par scripts. La documentation de l'administrateur de vSphere est principalement axée sur l'utilisation de vSphere Web Client pour la gestion.

vSphere PowerCLI

VMware vSphere PowerCLI est une interface Windows PowerShell avec vSphere API. Elle inclut des applets de commande PowerShell pour l'administration des composants vSphere.

vSphere PowerCLI inclut plus de 200 applets de commande, un ensemble d'exemples de scripts et une bibliothèque de fonctions pour la gestion et l'automatisation. Reportez-vous à la *Documentation de vSphere PowerCLI*.

vSphere Command-Line Interface (vCLI)

vCLI inclut un ensemble de commandes pour la gestion des hôtes ESXi et des machines virtuelles. Le programme d'installation, qui installe également le vSphere SDK for Perl, s'exécute sur les systèmes Windows ou Linux, et installe des commandes ESXCLI, des commandes vicfg- et un ensemble d'autres commandes vCLI. Reportez-vous à la *Documentation de vSphere Command-Line Interface*.

À partir de vSphere 6.0, vous pouvez également utiliser l'une des interfaces de script au vCloud Suite SDK, comme vCloud Suite SDK for Python.

Procédure

- 1 Créez un rôle personnalisé ayant des privilèges limités.

Par exemple, considérez la création d'un rôle disposant d'un ensemble de privilèges pour la gestion d'hôtes mais sans privilège pour la gestion de machines virtuelles, du stockage ou de la mise en réseau. Si le script que vous souhaitez utiliser extrait uniquement des informations, vous pouvez créer un rôle disposant de privilèges de lecture seule pour l'hôte.

- 2 Dans vSphere Web Client, créez un compte de service et attribuez-lui le rôle personnalisé.

Vous pouvez créer plusieurs rôles personnalisés avec différents niveaux d'accès si vous souhaitez que l'accès à certains hôtes soit assez limité.

- 3 Écrivez des scripts pour effectuer la vérification ou la modification de paramètres, puis exécutez-les.

Par exemple, vous pouvez vérifier ou définir le délai d'expiration interactif du shell d'un hôte de la façon suivante :

Langue	Commandes
vCLI (ESXCLI)	<pre>esxcli <conn_options> system settings advanced get / UserVars/ESXiShellTimeOut</pre> <pre>esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list grep /UserVars/ ESXiShellTimeOut</pre>
PowerCLI	<pre>#List UserVars.ESXiShellInteractiveTimeOut for each host Get-VMHost Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={\$_ Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut Select -ExpandProperty Value}}</pre> <pre># Set UserVars.ESXiShellTimeOut to 900 on all hosts Get-VMHost Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeOut Set- AdvancedSetting -Value 900 }</pre>

- 4 Dans les environnements de grande envergure, créez des rôles avec des privilèges d'accès différents et des hôtes du groupe dans des dossiers en fonction des tâches que vous souhaitez effectuer. Vous pouvez ensuite exécuter des scripts sur les différents dossier depuis les différents comptes de service.
- 5 Vérifiez que les modifications ont été appliquées après l'exécution de la commande.

Configurer des hôtes ESXi avec des profils d'hôte

Les profils d'hôte vous permettent de définir des configurations standard pour vos hôtes ESXi et d'automatiser la conformité avec ces paramètres de configuration. Les profils d'hôte permettent de contrôler de nombreux aspects de la configuration de l'hôte, notamment la mémoire, le stockage, la mise en réseau, etc.

Il est possible de configurer les profils d'hôte d'un hôte de référence à partir de vSphere Web Client et d'appliquer un profil d'hôte à tous les hôtes partageant les caractéristiques de l'hôte de référence. Vous pouvez également utiliser les profils d'hôte pour surveiller les hôtes à la recherche de modifications de la configuration des hôtes. Consultez la documentation de *Profils d'hôte vSphere*.

Vous pouvez associer le profil d'hôte à un cluster afin de l'appliquer à tous ses hôtes.

Procédure

- 1 Configurez l'hôte de référence conformément aux spécifications et créez le profil d'hôte.
- 2 Associez le profil à un hôte ou à un cluster.
- 3 Appliquez le profil d'hôte de l'hôte de référence à tous les autres hôtes ou clusters.

Recommandations générales de sécurité pour ESXi

Pour protéger un hôte ESXi contre les intrusions et autorisations illégales, VMware impose des contraintes au niveau de plusieurs paramètres et activités. Vous pouvez atténuer les contraintes pour répondre à vos besoins de configuration. Si vous le faites, assurez-vous de travailler dans un environnement sécurisé et de prendre suffisamment d'autres mesures de sécurité pour protéger le réseau globalement ainsi que les périphériques connectés à l'hôte.

Fonctionnalités de sécurité intégrées

Les risques encourus par les hôtes sont limités par défaut, de la façon suivante :

- ESXi Shell et SSH sont désactivés par défaut.
- Un nombre limité de ports de pare-feu sont ouverts par défaut. Vous pouvez ouvrir explicitement des ports de pare-feu supplémentaires associés à des services spécifiques.
- ESXi exécute uniquement les services essentiels pour gérer ses fonctions. La distribution est limitée aux fonctionnalités requises pour exécuter ESXi.
- Par défaut, tous les ports non requis pour la gestion des accès à l'hôte sont fermés. Vous devez ouvrir spécialement les ports associés aux services supplémentaires dont vous avez besoin.
- Par défaut, les chiffrements faibles sont désactivés et les communications provenant des clients sont sécurisées par SSL. Les algorithmes exacts utilisés pour la sécurisation du canal dépendant de l'algorithme de négociation SSL. Les certificats par défaut créés sur ESXi utilisent PKCS#1 SHA-256 avec le chiffrement RSA en tant qu'algorithme de signature.
- Le service Web Tomcat, utilisé en interne par ESXi pour soutenir les accès des clients Web, a été modifié : il exécute uniquement les fonctions requises pour les tâches d'administration et de surveillance effectuées par un client Web. Par conséquent, ESXi n'est pas vulnérable aux problèmes de sécurité Tomcat signalés lors d'utilisations massives.
- VMware assure la surveillance de toutes les alertes de sécurité susceptibles d'affecter la sécurité d'ESXi et envoie un correctif de sécurité en cas de besoin.
- Les services non sécurisés (tels que FTP et Telnet) ne sont pas installés, et les ports associés à ces services sont fermés par défaut. Vous trouverez facilement des services plus sécurisés tels que SSH et SFTP. Il est donc conseillé de les privilégier et d'éviter d'utiliser les services non sécurisés. Par exemple, utilisez Telnet avec SSL pour accéder aux ports série virtuels si SSH n'est pas disponible et que vous devez utiliser Telnet.

Si vous devez utiliser des services non sécurisés et que l'hôte bénéficie d'un niveau suffisant de sécurité, vous pouvez ouvrir des ports explicitement pour les prendre en charge.

Mesures de sécurité supplémentaires

Tenez compte des recommandations suivantes lorsque vous évaluez la sécurité de l'hôte et l'administration.

Limiter l'accès

Si vous décidez d'activer l'accès à l'interface DCUI (Direct Console User Interface), ESXi Shell ou SSH impose des stratégies de sécurité d'accès strictes.

L'ESXi Shell possède un accès privilégié à certaines parties de l'hôte. Octroyez un accès de connexion à ESXi Shell uniquement aux utilisateurs approuvés.

Ne pas accéder directement aux hôtes gérés

Utilisez vSphere Web Client pour administrer les hôtes ESXi qui sont gérés par vCenter Server. Évitez d'accéder aux hôtes gérés directement avec vSphere Client, et n'apportez pas de modifications aux hôtes gérés à partir de l'interface utilisateur DCUI (Direct Console User Interface).

Si vous gérez les hôtes à l'aide d'une interface de script ou d'une API, ne ciblez pas directement l'hôte. Ciblez plutôt le système vCenter Server qui gère l'hôte et spécifiez le nom de l'hôte.

Administrer les hôtes ESXi autonomes à l'aide de vSphere Client ou des API ou des interfaces de ligne de commande VMware

Pour administrer vos hôtes ESXi, utilisez vSphere Client ou une API ou une interface de ligne de commande VMware. Accédez à l'hôte via l'interface DCUI ou ESXi Shell en tant qu'utilisateur racine uniquement pour le dépannage. Si vous choisissez d'utiliser ESXi Shell, limitez les comptes avec des droits d'accès et définissez des délais d'expiration.

N'utilisez que des sources VMware pour mettre à niveau les composants ESXi.

L'hôte utilise un grand nombre de produits tiers pour soutenir les interfaces de gestion ou les tâches de gestion à exécuter. VMware ne prend pas en charge la mise à niveau de ces produits s'ils ne proviennent pas d'une source VMware. Si vous utilisez un téléchargement ou un correctif provenant d'une autre source, cela risque de porter préjudice à la sécurité ou aux fonctions de l'interface de gestion. Visitez régulièrement les sites Web de fournisseurs tiers, ainsi que la base de connaissances VMware pour connaître les alertes de sécurité correspondantes.

Note Suivez les instructions de sécurité fournies par VMware, disponible sur le site <http://www.vmware.com/security/>.

Verrouillage des mots de passe et des comptes ESXi

Pour les hôtes ESXi, vous devez utiliser un mot de passe avec des exigences prédéfinies. Vous pouvez modifier la longueur requise et l'exigence de classes de caractères ou autoriser les phrases secrètes à l'aide de l'option avancée `Security.PasswordQualityControl`.

ESXi utilise le module Linux PAM `pam_passwdqc` pour la gestion et le contrôle des mots de passe. Pour plus d'informations, reportez-vous aux pages du manuel concernant `pam_passwdqc`.

Note Les exigences par défaut pour les mots de passe ESXi dépendent de la version. Vous pouvez vérifier et modifier les restrictions de mot de passe par défaut à l'aide de l'option avancée `Security.PasswordQualityControl`.

Mots de passe d'ESXi

ESXi exige un mot de passe pour un accès à partir de l'interface DCUI (Direct Console User Interface), d'ESXi Shell, de SSH ou de vSphere Client. Lorsque vous créez un mot de passe, vous devez inclure par défaut un mélange de quatre classes de caractères : lettres en minuscule, lettres en majuscule, chiffres et caractères spéciaux comme un trait de soulignement ou un tiret.

Note Un caractère en majuscule au début d'un mot de passe ne compte pas dans le nombre de classes de caractères utilisées. Un chiffre à la fin d'un mot de passe ne compte pas dans le nombre de classes de caractères utilisées.

Les mots de passe ne doivent pas contenir un mot du dictionnaire ou une partie d'un mot du dictionnaire.

Exemple de mots de passe d'ESXi

Les candidats de mot de passe suivants illustrent les mots de passe possibles si l'option est définie de la manière suivante.

```
retry=3 min=disabled,disabled,disabled,7,7
```

Avec ce paramètre, les mots de passe avec une ou deux classes de caractères et les phrases secrètes ne sont pas autorisés, car les trois premiers éléments sont désactivés. Les mots de passe composés de trois et quatre classes de caractères exigent sept caractères. Pour plus d'informations, reportez-vous à page du manuel concernant `pam_passwdqc`.

Avec ces paramètres, les mots de passe suivants sont autorisés.

- `xQaTEhb!` : contient huit caractères provenant de trois classes de caractères.
- `xQaT3#A` : contient sept caractères provenant de quatre classes de caractères.

Les candidats de mot de passe suivants ne répondent pas aux exigences.

- `Xqat3hi` : commence par un caractère majuscule, réduisant ainsi le nombre effectif de classes de caractères à deux. Trois classes de caractères au minimum sont exigées.

- xQaTEh2 : se termine par un chiffre, réduisant ainsi le nombre effectif de classes de caractères à deux. Trois classes de caractères au minimum sont exigées.

Phrase secrète ESXi

Vous pouvez également utiliser une phrase secrète à la place d'un mot de passe. Néanmoins, les phrases secrètes sont désactivées par défaut. Vous pouvez modifier cette valeur par défaut ou d'autres paramètres à l'aide de `Security.PasswordQualityControl` l'option avancée depuis vSphere Web Client.

Par exemple, vous pouvez remplacer l'option par la suivante.

```
retry=3 min=disabled,disabled,16,7,7
```

Cet exemple autorise des phrases secrètes d'au moins 16 caractères et d'au moins 3 mots, séparés par des espaces.

Pour les hôtes hérités, la modification du fichier `/etc/pamd/passwd` est toujours autorisée, mais vous ne pourrez plus le modifier dans les futures versions. Utilisez plutôt l'option avancée `Security.PasswordQualityControl`.

Modification des restrictions de mot de passe par défaut

Vous pouvez modifier les restrictions par défaut des mots de passe ou des phrases secrètes en utilisant l'option avancée `Security.PasswordQualityControl` de votre hôte ESXi. Reportez-vous à la documentation *Gestion de vCenter Server et des hôtes* pour obtenir plus d'informations sur la configuration des options avancées d'ESXi.

Vous pouvez modifier la valeur par défaut, par exemple, pour exiger un minimum de 15 caractères et un nombre minimal de quatre mots, comme suit :

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Pour plus d'informations, reportez-vous à la page du manuel concernant `pam_passwdqc`.

Note Les combinaisons possibles des options de `pam_passwdqc` n'ont pas toutes été testées. Effectuez des tests supplémentaires après avoir modifié les paramètres du mot de passe par défaut.

Comportement de verrouillage de compte d'ESXi

À partir de vSphere 6.0, le verrouillage des comptes est pris en charge pour l'accès via SSH et vSphere Web Services SDK. L'interface de console directe (DCUI) et ESXi Shell ne prennent pas en charge le verrouillage de compte. Par défaut, un nombre maximal de dix tentatives de connexion échouées est autorisé avant le verrouillage du compte. Par défaut, le compte est déverrouillé au bout de deux minutes.

Configuration du comportement de connexion

Vous pouvez configurer le comportement de connexion de votre hôte ESXi à l'aide des options avancées suivantes :

- `Security.AccountLockFailures`. Nombre maximal de tentatives de connexion échouées autorisées avant le verrouillage du compte de l'utilisateur. La valeur zéro désactive le verrouillage du compte.
- `Security.AccountUnlockTime`. Nombre de secondes pendant lequel le compte d'un utilisateur est verrouillé.

Reportez-vous à la documentation *Gestion de vCenter Server et des hôtes* pour obtenir plus d'informations sur la configuration des options avancées d'ESXi.

Recommandations de sécurité pour la mise en réseau d'ESXi

L'isolation du trafic réseau est essentielle pour un environnement ESXi sécurisé. Des réseaux différents requièrent un accès et un niveau d'isolation distincts.

Votre hôte ESXi utilise plusieurs réseaux. Utilisez des mesures de sécurité appropriées à chaque réseau et isolez le trafic pour des applications et fonctions spécifiques. Par exemple, assurez-vous que le trafic vSphere vMotion n'est pas acheminé via des réseaux sur lesquels se trouvent les machines virtuelles. L'isolation empêche l'écoute. Il est également recommandé d'utiliser des réseaux séparés pour des raisons de performance.

- Les réseaux de l'infrastructure vSphere sont utilisés pour certaines fonctions comme VMware vSphere vMotion®, VMware vSphere Fault Tolerance et le stockage. Ces réseaux sont considérés comme étant isolés pour leurs fonctions spécifiques et ne sont généralement pas acheminés à l'extérieur d'un ensemble physique unique de racks de serveurs.
- Un réseau de gestion isole le trafic client, le trafic de l'interface de ligne de commande ou de l'API ou le trafic des logiciels tiers du trafic normal. Ce réseau doit être accessible uniquement aux administrateurs système, réseau et sécurité. Utilisez les systèmes JumpBox ou le réseau privé virtuel (VPN) pour sécuriser l'accès au réseau de gestion. Veillez à contrôler strictement l'accès à ce réseau des sources potentielles de programmes malveillants.
- Le trafic des machines virtuelles peut traverser un ou plusieurs réseaux. Vous pouvez renforcer l'isolation des machines virtuelles en utilisant des solutions de pare-feu qui définissent des règles de pare-feu au niveau du contrôleur du réseau virtuel. Ces paramètres sont acheminés avec une machine virtuelle dès lors qu'elle migre d'un hôte à un autre dans votre environnement vSphere.

Désactiver le Managed Object Browser (MOB)

Le MOB fournit une possibilité d'explorer le modèle d'objet VMkernel. Cependant, les pirates peuvent utiliser cette interface pour effectuer des actions ou des modifications de configuration malveillantes, car vous pouvez modifier la configuration de l'hôte à l'aide de Managed Object Browser. Utilisez Managed Object Browser uniquement à des fins de débogage et assurez-vous qu'il est désactivé dans les systèmes de production.

À partir de vSphere 6.0, le MOB est désactivé par défaut. Cependant, pour certaines tâches, par exemple lors de l'extraction de l'ancien certificat d'un système, vous devez utiliser le MOB.

Procédure

- 1 Sélectionnez l'hôte de vSphere Web Client, puis accédez à l'option **Paramètres système avancés**.
- 2 Contrôlez la valeur de **Config.HostAgent.plugins.solo.enableMob** et modifiez-la, le cas échéant.

Il n'est plus recommandé d'utiliser `vim-cmd` dans ESXi Shell.

Désactiver les clés autorisées (SSH)

Les clés autorisées vous permettent d'activer l'accès à un hôte ESXi via SSH sans demander d'authentification d'utilisateur. Pour renforcer la sécurité de l'hôte, ne permettez pas aux utilisateurs d'accéder à un hôte en utilisant des clés autorisées.

Un utilisateur est considéré comme approuvé si sa clé publique est dans le fichier `/etc/ssh/keys-root/authorized_keys` d'un hôte. Les utilisateurs distants approuvés sont autorisés à accéder à l'hôte sans fournir de mot de passe.

Procédure

- ◆ Pour les opérations quotidiennes, désactivez SSH sur les hôtes ESXi.
- ◆ Si SSH est désactivé, même temporairement, contrôlez le contenu du fichier `/etc/ssh/keys-root/authorized_keys`, afin de vous assurer qu'aucun utilisateur n'est autorisé à accéder à l'hôte sans authentification adéquate.
- ◆ Contrôlez le fichier `/etc/ssh/keys-root/authorized_keys`, afin de vérifier qu'il est vide et qu'aucune clé SSH n'a été ajoutée au fichier.
- ◆ Si vous découvrez que le fichier `/etc/ssh/keys-root/authorized_keys` n'est pas vide, supprimez toutes les clés.

Résultats

La désactivation de l'accès à distance à l'aide de clés autorisées peut limiter votre capacité à exécuter des commandes à distance sur un hôte sans fournir d'identifiant de connexion valide. Cela pourrait par exemple vous empêcher d'exécuter un script sans assistance à distance.

Gestion de certificats pour les hôtes ESXi

Dans vSphere 6.0 et versions ultérieures, VMware Certificate Authority (VMCA) provisionne chaque nouvel hôte ESXi avec un certificat signé dont VMCA est l'autorité de certification racine par défaut. Le provisionnement s'effectue lorsque l'hôte est explicitement ajouté à vCenter Server ou dans le cadre d'une installation ou d'une mise à niveau vers ESXi 6.0 ou version ultérieure.

Vous pouvez afficher et gérer les certificats depuis vSphere Web Client et en utilisant l'API `vim.CertificateManager` dans vSphere Web Services SDK. Vous ne pouvez pas afficher ou gérer des certificats ESXi à l'aide des interfaces de ligne de commande de gestion de certificats disponibles pour la gestion des certificats vCenter Server.

Certificats dans vSphere 5.5 et dans vSphere 6.0

Lorsqu'ESXi et vCenter Server communiquent, ils utilisent SSL pour presque tout le trafic de gestion.

Dans vSphere 5.5 et versions antérieures, les points de terminaison SSL sont sécurisés uniquement par une combinaison de nom d'utilisateur, mot de passe et empreinte. Les utilisateurs peuvent remplacer les certificats autosignés correspondants par leur propres certificats. Reportez-vous au Centre de documentation vSphere 5.5.

Dans vSphere 6.0 et versions ultérieures, vCenter Server prend en charge les modes de certificat suivants pour les hôtes ESXi.

Tableau 5-1. Modes de certificat des hôtes ESXi

Mode de certificat	Description
VMware Certificate Authority (par défaut)	<p>Utilisez ce mode si VMCA provisionne tous les hôtes ESXi, comme autorité de certification de niveau supérieur ou comme autorité de certification intermédiaire.</p> <p>Par défaut, VMCA provisionne les hôtes ESXi avec des certificats.</p> <p>Dans ce mode, vous pouvez actualiser et renouveler les certificats dans vSphere Web Client.</p>
Autorité de certification personnalisée	<p>Utilisez ce mode si vous souhaitez uniquement utiliser des certificats qui sont signés par une autorité de certification tierce.</p> <p>Dans ce mode, vous êtes responsable de la gestion des certificats. Vous ne pouvez pas actualiser et renouveler des certificats dans vSphere Web Client.</p> <hr/> <p>Note Sauf si vous définissez le mode de certificat sur Autorité de certification personnalisée, VMCA peut remplacer des certificats personnalisés, notamment lorsque vous sélectionnez Renouveler dans vSphere Web Client.</p>
Mode d'empreinte	<p>vSphere 5.5 utilisait le mode empreinte numérique. Ce mode reste disponible en tant qu'option de repli pour vSphere 6.0. Dans ce mode, vCenter Server s'assure que le certificat est formaté correctement, mais ne vérifie pas sa validité. Même les certificats expirés sont acceptés.</p> <p>N'utilisez ce mode que si vous rencontrez des problèmes que vous ne pouvez pas résoudre avec l'un des deux autres modes. Certains services vCenter 6.0 et versions ultérieures ne fonctionnent pas correctement en mode d'empreinte.</p>

Expiration du certificat

À partir de vSphere 6.0, vous pouvez afficher des informations sur l'expiration des certificats qui sont signés par VMCA ou par une autorité de certification tierce dans vSphere Web Client. Vous pouvez afficher les informations de tous les hôtes qui sont gérés par un système vCenter Server ou les informations d'hôtes individuels. Une alarme jaune se déclenche si le certificat est dans l'état **Expiration prochaine** (inférieure à 8 mois). Une alarme rouge se déclenche si le certificat est dans l'état **Expiration imminente** (inférieure à 2 mois).

Provisionnement d'ESXi et VMCA

Lorsque vous démarrez un hôte ESXi à partir d'un support d'installation, l'hôte dispose initialement d'un certificat automatiquement généré. Lorsque l'hôte est ajouté au système vCenter Server, il est provisionné avec un certificat signé par VMCA comme autorité de certification racine.

Le processus est similaire pour les hôtes qui sont provisionnés avec Auto Deploy. Cependant, comme ces hôtes ne stockent pas d'état, le certificat signé est stocké par le serveur Auto Deploy dans son magasin de certificats local. Le certificat est réutilisé lors des démarrages suivants des hôtes ESXi. Un serveur Auto Deploy fait partie d'un déploiement intégré ou d'un nœud de gestion.

Si VMCA n'est pas disponible lorsqu'un hôte Auto Deploy démarre pour la première fois, l'hôte tente d'abord de se connecter, puis effectue des mises à l'arrêt et redémarrages successifs jusqu'à ce que VMCA devienne disponible et que l'hôte puisse être provisionné avec un certificat signé.

Modifications de nom d'hôte et d'adresse IP

Dans vSphere 6.0 et versions ultérieures, une modification de nom d'hôte ou d'adresse IP peut déterminer si vCenter Server considère valide le certificat d'un hôte. Le mode d'ajout de l'hôte à vCenter Server détermine si une intervention manuelle est nécessaire. Lors d'une intervention manuelle, vous reconnectez l'hôte, ou vous le supprimez de vCenter Server et le rajoutez.

Tableau 5-2. Quand des modifications de nom d'hôte ou d'adresse IP nécessitent-elles une intervention manuelle ?

Hôte ajouté à vCenter Server à l'aide de...	Modifications de nom d'hôte	Modifications d'adresse IP
Nom d'hôte	Problème de connectivité de vCenter Server. Intervention manuelle requise.	Aucune intervention requise.
Adresse IP	Aucune intervention requise.	Problème de connectivité de vCenter Server. Intervention manuelle requise.



Gestion des certificats ESXi

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

Mises à niveau d'hôtes et certificats

Si vous mettez à niveau un hôte ESXi vers ESXi 6.0 ou version ultérieure, le processus de mise à niveau remplace les certificats auto-signés par des certificats signés par VMCA. Le processus conserve les certificats personnalisés même si ces certificats ont expiré ou sont non valides.

Le workflow de mise à niveau recommandé dépend des certificats actuels.

Hôte provisionné avec des certificats d'empreinte

Si votre hôte utilise actuellement des certificats d'empreinte, des certificats VMCA lui sont automatiquement attribués dans le cadre du processus de mise à niveau.

Note Vous ne pouvez pas provisionner des hôtes hérités avec des certificats VMCA. Vous devez procéder à une mise à niveau vers ESXi 6.0 ou une version ultérieure.

Hôte provisionné avec des certificats personnalisés

Si votre hôte est provisionné avec des certificats personnalisés, généralement des certificats signés par une autorité de certification tierce, ces certificats restent en place. Modifiez le mode de certification à Personnalisé pour vous assurer que les certificats ne sont pas remplacés accidentellement.

Note Si votre environnement est en mode VMCA et que vous actualisez les certificats dans vSphere Web Client, tous les certificats existants sont remplacés par des certificats signés par VMCA.

Par la suite, vCenter Server surveille les certificats et affiche des informations, notamment sur l'expiration des certificats, dans vSphere Web Client.

Si vous décidez de ne pas mettre à niveau vos hôtes vers vSphere 6.0 ou version ultérieure, les hôtes conservent les certificats que vous utilisez actuellement même si l'hôte est géré par un système vCenter Server qui utilise des certificats VMCA.

Les hôtes qui sont provisionnés par Auto Deploy obtiennent toujours de nouveaux certificats lors de leur premier démarrage avec le logiciel ESXi 6.0. Lorsque vous mettez à niveau un hôte qui est provisionné par Auto Deploy, le serveur Auto Deploy génère une demande de signature de certificat (CSR) pour l'hôte et la soumet à VMCA. VMCA stocke le certificat signé pour l'hôte. Lorsque le serveur Auto Deploy provisionne l'hôte, il récupère le certificat de VMCA et l'inclut dans le cadre du processus de provisionnement.

Vous pouvez utiliser Auto Deploy avec des certificats personnalisés.

Paramètres par défaut des certificats ESXi

Lorsque vCenter Server émet une demande de signature de certificat (CSR) auprès d'un hôte ESXi, il utilise les paramètres par défaut. La plupart des valeurs par défaut conviennent à de nombreuses situations, mais les informations spécifiques à l'entreprise peuvent être modifiées.

Envisagez de changer les informations sur l'entreprise et l'emplacement. Vous pouvez modifier un grand nombre des paramètres par défaut à l'aide de vSphere Web Client. Reportez-vous à [Modifier les paramètres par défaut de certificat](#).

Tableau 5-3. Paramètres CSR

Paramètre	Valeur par défaut	Option avancée
Taille de la clé	2048	S.O.
Algorithme de clé	RSA	S.O.
Algorithme de signature de certificat	sha256WithRSAEncryption	S.O.
Nom commun	Nom de l'hôte si ce dernier a été ajouté à vCenter Server par nom d'hôte. Adresse IP de l'hôte si ce dernier a été ajouté à vCenter Server par adresse IP.	S.O.
Pays	États-Unis	vpxd.certmgmt.certs.cn.country
Adresse e-mail	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
Localité (ville)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
Nom d'unité d'organisation	VMware Engineering	vpxd.certmgmt.certs.cn.organizationalUnitName
Nom de l'organisation	VMware	vpxd.certmgmt.certs.cn.organizationName
État ou province	Californie	vpxd.certmgmt.certs.cn.state
Nombre de jours de validité du certificat.	1825	vpxd.certmgmt.certs.cn.daysValid
Seuil fixe d'expiration du certificat. vCenter Server génère une alarme rouge lorsque ce seuil est atteint.	30 jours	vpxd.certmgmt.certs.cn.hardThreshold
Intervalle d'interrogation des vérifications de la validité des certificats de vCenter Server.	5 jours	vpxd.certmgmt.certs.cn.pollIntervalDays

Tableau 5-3. Paramètres CSR (suite)

Paramètre	Valeur par défaut	Option avancée
Seuil dynamique d'expiration du certificat. vCenter Server génère un événement lorsque ce seuil est atteint.	240 jours	vpxd.certmgmt.certs.cn.softThreshold
Mode employé par les utilisateurs de vCenter Server pour déterminer si les certificats existants sont remplacés. Modifiez ce mode pour conserver les certificats personnalisés pendant la mise à niveau. Reportez-vous à Mises à niveau d'hôtes et certificats .	La valeur par défaut est vmca. Vous pouvez également spécifier Empreinte ou Personnalisé. Reportez-vous à Changer le mode de certificat .	vpxd.certmgmt.mode

Afficher les informations d'expiration de certificat pour plusieurs hôtes ESXi

Si vous utilisez ESXi 6.0 ou version ultérieure, vous pouvez afficher l'état du certificat de tous les hôtes gérés par votre système vCenter Server. Cet affichage vous permet de déterminer si l'un des certificats est sur le point d'expirer.

Vous pouvez afficher des informations sur l'état d'un certificat pour les hôtes qui utilisent le mode VMCA, ainsi que pour ceux qui utilisent le mode personnalisé dans vSphere Web Client. Il n'est pas possible d'afficher des informations sur l'état du certificat pour les hôtes en mode Empreinte.

Procédure

- 1 Accédez à l'hôte dans la hiérarchie de l'inventaire de vSphere Web Client.
Par défaut, l'affichage des hôtes n'inclut pas l'état du certificat.
- 2 Cliquez avec le bouton droit sur le champ Nom et sélectionnez l'option **Afficher/masquer les colonnes**.
- 3 Sélectionnez **Certificat valide pour**, cliquez sur **OK** et faites défiler vers la droite, si nécessaire.
Les informations relatives au certificat s'affichent lorsque le certificat expire.
Si un hôte est ajouté à vCenter Server ou reconnecté après une déconnexion, vCenter Server renouvelle le certificat si son état est Expiré, Expiration, Expiration prochaine ou Expiration imminente. L'état est Expiration si la validité du certificat est inférieure à huit mois, Expiration prochaine si la validité est inférieure à deux mois et Expiration imminente si elle est inférieure à un mois.
- 4 (Facultatif) Désélectionnez les autres colonnes pour faciliter l'observation de ce qui vous intéresse.

Étape suivante

Renouvelez les certificats qui sont sur le point d'expirer. Reportez-vous à [Renouveler ou actualiser des certificats ESXi](#).

Afficher les détails de certificat pour un hôte ESXi spécifique

Pour les hôtes ESXi 6.0 et versions ultérieures qui sont en mode VMCA ou en mode personnalisé, vous pouvez afficher les détails du certificat dans vSphere Web Client. Les informations sur le certificat peuvent être utiles lors d'un débogage.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sélectionnez **Système**, puis cliquez sur **Certificat**.

Vous pouvez afficher les informations suivantes. Ces informations sont disponibles uniquement dans la vue d'hôte unique.

Champ	Description
Objet	Objet utilisé lors de la génération du certificat.
Émetteur	Émetteur du certificat.
Date de début de validité	Date à laquelle le certificat a été généré.
Date de fin de validité	Date à laquelle le certificat expire.
État	État du certificat, à savoir l'un des états suivants. <div> <div>Bon</div> <div>Fonctionnement normal.</div> <div>Expiration</div> <div>Le certificat va bientôt expirer.</div> <div>Expiration imminente</div> <div>La date d'expiration du certificat se situe dans huit mois ou moins (par défaut).</div> <div>Expiration imminente</div> <div>Le certificat se situe à 2 mois ou moins de sa date d'expiration (par défaut).</div> <div>Expiré</div> <div>Le certificat n'est pas valide, car il a expiré.</div> </div>

Renouveler ou actualiser des certificats ESXi

Si l'autorité de certification VMware (VMCA) attribue des certificats à vos hôtes ESXi (6.0 et version ultérieure), vous pouvez renouveler ces certificats à partir de vSphere Web Client. Vous pouvez également actualiser tous les certificats du magasin TRUSTED_ROOTS associés à vCenter Server.

Vous pouvez renouveler vos certificats lorsqu'ils sont sur le point d'expirer ou si vous souhaitez provisionner l'hôte avec un nouveau certificat pour d'autres raisons. Si le certificat a déjà expiré, vous devez déconnecter puis reconnecter l'hôte.

Par défaut, vCenter Server renouvelle les certificats des hôtes dont l'état est Expiré, Expire immédiatement ou Expiration chaque fois que l'hôte est ajouté à l'inventaire ou qu'il est reconnecté.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sélectionnez l'option **Système** et cliquez sur **Certificat**.

Il est possible d'afficher des informations détaillées sur le certificat de l'hôte sélectionné.

- 4 Cliquez sur **Renouveler** ou sur **Actualiser les certificats d'autorité de certification**.

Option	Description
Renouveler	Récupère, auprès de l'autorité de certification VMware (VMCA), un certificat venant d'être signé pour l'hôte.
Actualiser les certificats d'autorité de certification	Pousse tous les certificats du magasin TRUSTED_ROOTS dans le magasin VECS de vCenter Server vers l'hôte.

- 5 Cliquez sur **Oui** pour confirmer.

Modifier les paramètres par défaut de certificat

Lorsqu'un hôte est ajouté à un système vCenter Server, vCenter Server envoie une demande de signature de certificat (CSR) pour l'hôte à VMCA. Vous pouvez modifier certains paramètres par défaut dans la demande CSR en utilisant les paramètres avancés de vCenter Server dans vSphere Web Client.

Modifiez les paramètres par défaut du certificat spécifiques à l'entreprise. Reportez-vous à [Paramètres par défaut des certificats ESXi](#) pour obtenir la liste complète des paramètres par défaut. Certaines valeurs par défaut ne peuvent pas être modifiées.

Procédure

- 1 Dans vSphere Web Client, sélectionnez le système vCenter Server qui gère les hôtes.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

- 3 Cliquez sur **Paramètres avancés**, puis sur **Modifier**.
- 4 Dans la zone Filtre, entrez **certmgmt** pour afficher uniquement les paramètres de gestion des certificats.
- 5 Modifiez la valeur des paramètres existants pour appliquer la stratégie de l'entreprise, puis cliquez sur **OK**.

Lors du prochain ajout d'un hôte à vCenter Server, les nouveaux paramètres seront utilisés dans la demande CSR que vCenter Server enverra à VMCA et dans le certificat attribué à l'hôte.

Étape suivante

Les modifications apportées aux métadonnées des certificats affectent uniquement les nouveaux certificats. Si vous souhaitez modifier les certificats d'hôtes déjà gérés par le système vCenter Server, vous pouvez déconnecter et reconnecter les hôtes.

Présentation des changements de mode de certificat

À partir de vSphere 6.0, les hôtes ESXi sont provisionnés avec des certificats par VMCA par défaut. Vous pouvez plutôt utiliser le mode de certificat personnalisé ou, à des fins de débogage, le mode d'empreinte. Dans la plupart des cas, les changements de mode sont perturbateurs et ne sont pas nécessaires. Si un changement de mode s'impose, évaluez l'impact potentiel avant de commencer.

Dans vSphere 6.0 et versions ultérieures, vCenter Server prend en charge les modes de certificat suivants pour les hôtes ESXi.

Tableau 5-4. Modes de certificat des hôtes ESXi

Mode de certificat	Description
VMware Certificate Authority (par défaut)	Par défaut, VMware Certificate Authority est utilisée comme autorité de certification pour les certificats des hôtes ESXi. VMCA est l'autorité de certification racine par défaut, mais elle peut être définie comme autorité de certification intermédiaire vers une autre autorité de certification. Dans ce mode, les utilisateurs peuvent gérer des certificats dans vSphere Web Client. Ce mode est également utilisé si VMCA est un certificat subordonné.
Autorité de certification personnalisée	Certains clients préfèrent gérer leur propre autorité de certification externe. Dans ce mode, les clients sont responsables de la gestion des certificats et ne peuvent pas les gérer depuis vSphere Web Client.
Mode d'empreinte	vSphere 5.5 utilisait le mode d'empreinte et ce mode reste disponible en tant qu'option de repli pour vSphere 6.0. Toutefois, n'utilisez pas ce mode en cas de problèmes avec l'un ou les deux autres modes que vous ne pouvez pas résoudre. Certains services vCenter 6.0 et versions ultérieures ne fonctionnent pas correctement en mode d'empreinte.

Utilisation de certificats ESXi personnalisés

Si la stratégie de votre entreprise impose l'utilisation d'une autorité de certification racine autre que VMCA, vous pouvez changer le mode de certification de votre environnement après avoir procédé à une planification rigoureuse. Le workflow recommandé est le suivant.

- 1 Obtenez les certificats que vous souhaitez utiliser.
- 2 Placez le ou les hôtes en mode de maintenance et déconnectez-les du système vCenter Server.
- 3 Ajoutez le certificat racine de l'autorité de certification personnalisée à VECS.
- 4 Déployez les certificats de l'autorité de certification personnalisée sur chaque hôte et redémarrez les services sur cet hôte.
- 5 Passez au mode d'autorité de certification personnalisée. Reportez-vous à la section [Changer le mode de certificat](#).
- 6 Connectez le ou les hôtes au système vCenter Server.

Passage du mode d'autorité de certification personnalisée au mode VMCA

Si vous utilisez le mode d'autorité de certification personnalisée et en venez à la conclusion que VMCA fonctionne mieux dans votre environnement, vous pouvez procéder au changement de mode après une planification rigoureuse. Le workflow recommandé est le suivant.

- 1 Retirez tous les hôtes du système vCenter Server.
- 2 Sur le système vCenter Server, retirez de VECS le certificat racine de l'autorité de certification tierce.
- 3 Passez au mode VMCA. Reportez-vous à la section [Changer le mode de certificat](#).
- 4 Ajoutez les hôtes au système vCenter Server.

Note Tout autre workflow pour ce mode peut entraîner un comportement imprévisible.

Conservation des certificats du mode d'empreinte pendant la mise à niveau

Le passage du mode VMCA au mode d'empreinte peut être nécessaire si vous rencontrez des problèmes avec les certificats VMCA. En mode d'empreinte, le système vCenter Server vérifie uniquement la présence et le format d'un certificat, mais pas sa validité. Voir [Changer le mode de certificat](#) pour plus d'informations.

Passage du mode d'empreinte au mode VMCA

Si vous utilisez le mode d'empreinte et que vous souhaitez commencer à utiliser des certificats signés par VMCA, le changement nécessite de la planification. Le workflow recommandé est le suivant.

- 1 Retirez tous les hôtes du système vCenter Server.

- 2 Passez au mode de certification VMCA. Reportez-vous à la section [Changer le mode de certificat](#).
- 3 Ajoutez les hôtes au système vCenter Server.

Note Tout autre workflow pour ce mode peut entraîner un comportement imprévisible.

Passage du mode d'autorité de certification personnalisé au mode d'empreinte

Si vous rencontrez des problèmes avec votre autorité de certification personnalisée, envisagez de passer temporairement au mode d'empreinte. Le changement s'effectue de façon transparente si vous suivez les instructions de la section [Changer le mode de certificat](#). Après le changement de mode, le système vCenter Server vérifie uniquement le format du certificat et ne vérifie plus la validité du certificat proprement dit.

Passage du mode d'empreinte au mode d'autorité de certification personnalisée

Si vous définissez votre environnement sur le mode d'empreinte pendant un dépannage et que vous souhaitez commencer à utiliser le mode d'autorité de certification personnalisée, vous devez d'abord générer les certificats requis. Le workflow recommandé est le suivant.

- 1 Retirez tous les hôtes du système vCenter Server.
- 2 Ajoutez le certificat racine de l'autorité de certification personnalisée au magasin TRUSTED_ROOTS dans VECS sur le système vCenter Server. Reportez-vous à la section [Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server \(Certificats personnalisés\)](#).
- 3 Pour chaque hôte ESXi :
 - a Déployez le certificat et la clé de l'autorité de certification personnalisée.
 - b Redémarrez les services sur l'hôte.
- 4 Passez au mode personnalisé. Reportez-vous à la section [Changer le mode de certificat](#).
- 5 Ajoutez les hôtes au système vCenter Server.

Changer le mode de certificat

Dans la plupart des cas, la meilleure solution consiste à utiliser VMCA pour provisionner les hôtes ESXi dans votre environnement. Si la stratégie de l'entreprise exige que vous utilisiez des certificats personnalisés avec une autorité de certification racine différente, vous pouvez modifier les options avancées de vCenter Server afin d'éviter que les hôtes soient automatiquement provisionnés à l'aide de certificats VMCA lorsque vous actualisez les certificats. Vous êtes alors responsable de la gestion des certificats dans votre environnement.

Vous pouvez utiliser les paramètres avancés de vCenter Server pour passer au mode d'empreinte ou d'autorité de certification personnalisée. N'utilisez le mode d'empreinte que comme option de secours.

Procédure

- 1 Sélectionnez le système vCenter Server qui gère les hôtes et cliquez sur **Paramètres**.

- 2 Cliquez sur **Paramètres avancés**, puis sur **Modifier**.
- 3 Dans le champ Filtre, entrez **certmgmt** pour afficher uniquement les clés de gestion des certificats.
- 4 Définissez `vpxd.certmgmt.mode` sur **personnalisé** si vous souhaitez gérer vos propres certificats ou sur **empreinte** si vous préférez utiliser temporairement le mode d'empreinte, puis cliquez sur **OK**.
- 5 Redémarrez le service vCenter Server.

Remplacement de certificats et de clés SSL pour ESXi

Selon la stratégie de sécurité de votre entreprise, vous devrez peut-être remplacer le certificat SSL défini par défaut pour ESXi par un certificat signé par une autorité de certification tierce sur chaque hôte.

Par défaut, les composants vSphere utilisent le certificat signé par VMCA et la clé créés lors de l'installation. Si vous supprimez accidentellement le certificat signé par VMCA, supprimez l'hôte de son système vCenter Server, puis ajoutez-le de nouveau. Lorsque vous ajoutez l'hôte, vCenter Server demande un nouveau certificat à VMCA et provisionne l'hôte à l'aide de celui-ci.

Si la stratégie de l'entreprise l'impose, remplacez les certificats signés par VMCA par des certificats provenant d'une autorité de certification approuvée (une autorité de certification commerciale ou l'autorité de certification d'une organisation).

Les certificats par défaut se trouvent au même emplacement que les certificats vSphere 5.5. Vous pouvez remplacer de plusieurs manières les certificats par défaut par des certificats approuvés.

Note Vous pouvez également utiliser les objets gérés `vim.CertificateManager` et `vim.host.CertificateManager` dans vSphere Web Services SDK. Reportez-vous à la documentation vSphere Web Services SDK.

Après avoir remplacé le certificat, vous devez mettre à jour le magasin TRUSTED_ROOTS dans VECS sur le système vCenter Server qui gère l'hôte, afin de garantir une relation de confiance entre vCenter Server et l'hôte ESXi.

■ Configuration requise pour les demandes de signature de certificat ESXi

Si vous souhaitez utiliser un certificat signé par une autorité de certification tierce, que ce soit en utilisant VMCA en tant qu'autorité subordonnée ou en recourant à une autorité de certification personnalisée, vous devez envoyer une demande de signature de certificat (Certificate Signing Request, CSR) à l'autorité de certification.

■ Remplacer le certificat et la clé par défaut dans ESXi Shell

Vous pouvez remplacer les certificats ESXi signés par VMCA par défaut dans ESXi Shell.

■ Remplacer un certificat et une clé par défaut à l'aide de la commande `vifs`

Vous pouvez remplacer les certificats ESXi par défaut signés par l'autorité de certification VMware (VMCA) à l'aide de la commande `vifs`.

- [Remplacer un certificat par défaut à l'aide de HTTPS PUT](#)

Vous pouvez utiliser des applications tierces pour télécharger des certificats et une clé. Les applications prenant en charge les opérations HTTPS PUT utilisent l'interface HTTPS incluse avec ESXi.

- [Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server \(Certificats personnalisés\)](#)

Si vous configurez vos hôtes ESXi pour qu'ils utilisent des certificats personnalisés, vous devez mettre à niveau le magasin TRUSTED_ROOTS du système vCenter Server qui gère les hôtes.

Configuration requise pour les demandes de signature de certificat ESXi

Si vous souhaitez utiliser un certificat signé par une autorité de certification tierce, que ce soit en utilisant VMCA en tant qu'autorité subordonnée ou en recourant à une autorité de certification personnalisée, vous devez envoyer une demande de signature de certificat (Certificate Signing Request, CSR) à l'autorité de certification.

Utilisez une demande de signature de certificat présentant les caractéristiques suivantes :

- 2 048 bits
- PKCS1
- Aucun caractère générique
- 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.

Remplacer le certificat et la clé par défaut dans ESXi Shell

Vous pouvez remplacer les certificats ESXi signés par VMCA par défaut dans ESXi Shell.

Conditions préalables

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

- 1 Connectez-vous à ESXi Shell, directement à partir de l'interface utilisateur de la console directe (DCUI) ou à partir d'un client SSH, en tant qu'utilisateur disposant de privilèges d'administrateur.
- 2 Dans l'inventaire `/etc/vmware/ssl`, renommer les certificats existants à l'aide des commandes suivantes :

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

- 3 Copiez les certificats à utiliser dans `/etc/vmware/ssl`.
- 4 Renommer le nouveau certificat et la clé dans `rui.crt` et `rui.key`.
- 5 Redémarrez l'hôte après avoir installé le nouveau certificat.

Vous pouvez également mettre l'hôte en mode de maintenance, installer le nouveau certificat, utiliser l'interface utilisateur de console directe (DCUI) pour redémarrer les agents de gestion, puis configurer l'hôte pour quitter le mode de maintenance.

Étape suivante

Mettez à jour le magasin TRUSTED_ROOTS de vCenter Server. Reportez-vous à [Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server \(Certificats personnalisés\)](#).

Remplacer un certificat et une clé par défaut à l'aide de la commande vifs

Vous pouvez remplacer les certificats ESXi par défaut signés par l'autorité de certification VMware (VMCA) à l'aide de la commande `vifs`.

Conditions préalables

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

- 1 Sauvegardez les certificats existants.
- 2 Générez une demande de certificat en suivant les instructions de l'autorité de certification.

- 3 Lorsque vous avez le certificat, utilisez la commande `vifs` pour télécharger le certificat à l'emplacement approprié sur l'hôte à partir d'une connexion SSH vers l'hôte.

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

- 4 Redémarrez l'hôte.

Étape suivante

Mettez à jour le magasin vCenter Server TRUSTED_ROOTS. Reportez-vous à [Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server \(Certificats personnalisés\)](#).

Remplacer un certificat par défaut à l'aide de HTTPS PUT

Vous pouvez utiliser des applications tierces pour télécharger des certificats et une clé. Les applications prenant en charge les opérations HTTPS PUT utilisent l'interface HTTPS incluse avec ESXi.

Conditions préalables

- Si vous souhaitez utiliser des certificats signés par une autorité de certification tierce, générez la demande de certificat, envoyez-la à l'autorité de certification et stockez les certificats sur chaque hôte ESXi.
- Si nécessaire, activez ESXi Shell ou activez le trafic SSH dans vSphere Web Client. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'activation de l'accès à ESXi Shell.
- Tous les transferts de fichiers et autres communications se produisent lors d'une session HTTPS sécurisée. L'utilisateur servant à authentifier la session doit disposer du privilège **Hôte.Config.AdvancedConfig** sur l'hôte. Consultez la publication *Sécurité vSphere* pour plus d'informations sur l'attribution de privilèges par le biais de rôles.

Procédure

- 1 Sauvegardez les certificats existants.
- 2 Dans votre application de téléchargement, traitez chaque fichier de la manière suivante :
 - a Ouvrez le fichier.
 - b Publiez le fichier à l'un de ces emplacements.

Option	Description
Certificats	<code>https://hostname/host/ssl_cert</code>
Clés	<code>https://hostname/host/ssl_key</code>

Les emplacements `/host/ssl_cert` et `host/ssl_key` sont reliés aux fichiers de certificats dans `/etc/vmware/ssl`.

- 3 Redémarrez l'hôte.

Étape suivante

Mettez à jour le magasin TRUSTED_ROOTS de vCenter Server. Reportez-vous à [Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server \(Certificats personnalisés\)](#).

Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés)

Si vous configurez vos hôtes ESXi pour qu'ils utilisent des certificats personnalisés, vous devez mettre à niveau le magasin TRUSTED_ROOTS du système vCenter Server qui gère les hôtes.

Conditions préalables

Remplacez les certificats de chacun des hôtes par des certificats personnalisés.

Procédure

- 1 Connectez-vous au système vCenter Server qui gère les hôtes ESXi.

Connectez-vous au système Windows sur lequel vous avez installé le logiciel ou au shell vCenter Server Appliance.

- 2 Exécutez `vecs-cli` pour ajouter les nouveaux certificats au magasin TRUSTED_ROOTS, par exemple :

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

Option	Description
Linux	<pre>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt</pre>
Windows	<pre>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt</pre>

Étape suivante

Définissez le mode de certificat sur Personnalisé. Si le mode de certificat est VMCA (c'est-à-dire la valeur par défaut) et que vous effectuez une actualisation des certificats, vos certificats personnalisés sont remplacés par des certificats signés par l'autorité de certification VMware (VMCA). Reportez-vous à [Changer le mode de certificat](#).

Utiliser des certificats personnalisés avec Auto Deploy

Par défaut, le serveur Auto Deploy provisionne chaque hôte avec des certificats signés par VMCA. Vous pouvez configurer le serveur Auto Deploy de manière à provisionner tous les hôtes à l'aide de certificats personnalisés non signés par VMCA. Dans ce scénario, le serveur Auto Deploy devient une autorité de certification subordonnée de l'autorité de certification tierce.

Conditions préalables

- Demandez un certificat de votre autorité de certification qui réponde aux conditions requises.
 - Taille de clé : 2 048 bits ou plus (codée au format PEM)
 - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8
 - x509 version 3
 - Pour les certificats racines, l'extension d'autorité de certification doit être définie sur vrai et la signature de certification doit figurer dans la liste de conditions requises.
 - SubjectAltName doit contenir DNS Name=<machine_FQDN>
 - Format CRT
 - Contient les utilisations de clé suivantes : signature numérique, non-répudiation, chiffrement de la clé
 - Heure de début antérieure d'un jour à l'heure actuelle
 - CN (et SubjectAltName) défini sur le nom de l'hôte (ou l'adresse IP) de l'hôte ESXi dans l'inventaire vCenter Server.
- Nom du certificat et fichiers de clés `rbd-ca.crt` et `rbd-ca.key`.

Procédure

- 1 Sauvegardez les certificats ESXi par défaut.

Les certificats se situent à l'emplacement `/etc/vmware-rbd/ssl/`.

- 2 Dans vSphere Web Client, arrêtez le service Auto Deploy.
 - a Sélectionnez **Administration**, puis cliquez sur **Configuration système** sous **Déploiement**.
 - b Cliquez sur **Services**.
 - c Cliquez avec le bouton droit sur le service que vous souhaitez arrêter et sélectionnez **Arrêter**.
- 3 Sur le système qui exécute le service Auto Deploy, dans `/etc/vmware-rbd/ssl/`, remplacez `rbd-ca.crt` et `rbd-ca.key` par votre certificat personnalisé et votre fichier de clé.
- 4 Sur le système qui exécute le service Auto Deploy, mettez à jour le magasin TRUSTED_ROOTS dans VECS pour utiliser vos nouveaux certificats.

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
    rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
    rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

Windows

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

Linux

```
/usr/lib/vmware-vmadfd/bin/vecs-cli
```

- 5 Créez un fichier `castore.pem` contenant tout ce qui se trouve dans `TRUSTED_ROOTS` et placez-le dans le répertoire `/etc/vmware-rbd/ssl/`.

En mode personnalisé, vous êtes responsable de la gestion de ce fichier.

- 6 Définissez le mode de certificat du système vCenter Server sur **Personnalisé**.

Reportez-vous à [Changer le mode de certificat](#).

- 7 Redémarrez le service vCenter Server et démarrez le service Auto Deploy.

Résultats

La prochaine fois que vous provisionnez un hôte configuré pour utiliser Auto Deploy, le serveur Auto Deploy génèrera un certificat à l'aide du certificat racine que vous venez d'ajouter au magasin `TRUSTED_ROOTS`.

Restaurer les fichiers de certificat et de clé ESXi

Lorsque vous remplacez un certificat sur un hôte ESXi à l'aide de vSphere Web Services SDK, le certificat et la clé antérieurs sont ajoutés à un fichier `.bak`. Vous pouvez restaurer les certificats précédents en déplaçant les informations du fichier `.bak` vers les fichiers de certificat et de clé actuels.

Le certificat et la clé de l'hôte résident dans `/etc/vmware/ssl/rui.crt` et `/etc/vmware/ssl/rui.key`. Lorsque vous remplacez le certificat et la clé d'un hôte à l'aide de l'objet géré `vim.CertificateManager` de vSphere Web Services SDK, le certificat et la clé antérieurs sont ajoutés au fichier `/etc/vmware/ssl/rui.bak`.

Note Si vous remplacez le certificat à l'aide de HTTP PUT, `vifs` ou à partir d'ESXi Shell, les certificats existants ne sont pas ajoutés au fichier `.bak`.

Procédure

- 1 Sur l'hôte ESXi, accédez au fichier `/etc/vmware/ssl/rui.bak`.

Le format du fichier est le suivant :

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 Copiez le texte qui commence par -----BEGIN PRIVATE KEY----- et termine par -----END PRIVATE KEY----- dans le fichier `/etc/vmware/ssl/rui.clé`.

Incluez -----BEGIN PRIVATE KEY----- et -----END PRIVATE KEY-----.

- 3 Copiez le texte entre -----BEGIN CERTIFICATE----- et -----END CERTIFICATE----- dans le fichier `/etc/vmware/ssl/rui.crt`.

Incluez -----BEGIN CERTIFICATE----- et -----END CERTIFICATE-----.

- 4 Redémarrez l'hôte ou envoyez des événements `ssl_reset` à tous les services qui utilisent les clés.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

Personnalisation des hôtes avec le profil de sécurité

Vous pouvez personnaliser la plupart des paramètres de sécurité essentiels de votre hôte via le panneau Profil de sécurité disponible dans vSphere Web Client. Le profil de sécurité est particulièrement utile pour la gestion d'hôte unique. Si vous gérez plusieurs hôtes, pensez à utiliser l'une des lignes de commande (CLI) ou l'un des kits de développement logiciel (SDK) et à automatiser la personnalisation.

Configuration du pare-feu ESXi

ESXi contient un pare-feu activé par défaut.

Lors de l'installation, le pare-feu ESXi est configuré pour bloquer le trafic entrant et sortant, sauf le trafic des services activés dans le profil de sécurité de l'hôte.

Réfléchissez bien avant d'ouvrir des ports sur le pare-feu, car l'accès illimité aux services qui s'exécutent sur un hôte ESXi peut exposer ce dernier aux attaques extérieures et aux accès non autorisés. Pour minimiser les risques, configurez le pare-feu ESXi de manière à autoriser l'accès uniquement depuis les réseaux autorisés.

Note Le pare-feu permet également d'utiliser les commandes ping ICMP (Internet Control Message Protocol) et autorise les communications avec les clients DHCP et DNS (UDP uniquement).

Vous pouvez gérer les ports du pare-feu d'ESXi de la manière suivante :

- Utilisez le profil de sécurité de chacun des hôtes dans vSphere Web Client. Reportez-vous à la section [Gérer les paramètres du pare-feu ESXi](#).

- Utilisez les commandes ESXCLI dans la ligne de commande ou dans les scripts. Reportez-vous à la section [Commandes de pare-feu ESXCLI d'ESXi](#).
- Utilisez un VIB personnalisé si le port que vous cherchez à ouvrir n'est pas inclus dans le profil de sécurité.

Vous créez des VIB personnalisés avec l'outil vibauthor disponible dans VMware Labs. Pour installer le VIB personnalisé, vous devez modifier le niveau d'acceptation de l'hôte ESXi sur CommunitySupported. Reportez-vous à l'article [2007381](#) de la base de connaissances VMware.

Note Si vous contactez le support technique VMware pour examiner un problème relatif à un hôte ESXi avec un VIB CommunitySupported installé, il se peut que le support VMware demande de désinstaller le VIB CommunitySupported dans le cadre de la résolution du problème afin de déterminer si ce VIB est associé au problème étudié.



Concepts du pare-feu d'ESXi

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/)

Le comportement de l'ensemble de règles du client NFS (`nfsClient`) diffère de celui des autres ensembles de règles. Lorsque l'ensemble de règles du client NFS est activé, tous les ports TCP sortants sont ouverts aux hôtes de destination figurant dans la liste des adresses IP autorisées. Consultez [Comportement du pare-feu client NFS](#) pour plus d'informations.

Gérer les paramètres du pare-feu ESXi

Vous pouvez configurer les connexions de pare-feu entrantes et sortantes pour un agent de service ou de gestion dans vSphere Web Client ou sur la ligne de commande.

Note Si différents services ont des règles de port qui se chevauchent, l'activation d'un service peut implicitement activer d'autres services. Vous pouvez spécifier les adresses IP qui sont autorisées à accéder à chacun des services sur l'hôte afin d'éviter ce problème.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Cliquez sur **Profil de sécurité**.

vSphere Web Client affiche la liste des connexions entrantes et sortantes actives avec les ports de pare-feu correspondants.

- 4 Dans la section Pare-feu, cliquez sur **Modifier**.

L'écran affiche des ensembles de règles de pare-feu avec le nom de la règle et les informations associées.

- Sélectionnez les ensembles de règles à activer, ou désélectionnez ceux à désactiver.

Colonne	Description
Ports entrants et port sortants	Les ports que vSphere Web Client ouvre pour le service
Protocole	Protocole utilisé par un service.
Processus	Statut des démons associés au service

- Pour certains services, vous pouvez gérer les détails du service.
 - Utilisez les boutons **Démarrer**, **Arrêter** ou **Redémarrer** pour modifier temporairement l'état d'un service.
 - Modifier la stratégie de démarrage pour que le service démarre avec l'hôte ou avec l'utilisation du port.
- Pour certains services, vous pouvez spécifier explicitement les adresses IP à partir desquelles les connexions sont autorisées.
Reportez-vous à [Ajouter des adresses IP autorisées pour un hôte ESXi](#).
- Cliquez sur **OK**.

Ajouter des adresses IP autorisées pour un hôte ESXi

Par défaut, le pare-feu de chaque service autorise l'accès à toutes les adresses IP. Pour restreindre le trafic, modifiez chaque service pour autoriser uniquement le trafic provenant de votre sous-réseau de gestion. Vous pouvez également annuler la sélection de certains services si votre environnement ne les utilise pas.

Vous pouvez utiliser vSphere Web Client, vCLI ou PowerCLI pour mettre à jour la liste des adresses IP autorisées d'un service. Par défaut, toutes les adresses IP sont autorisées pour un service.



Ajout d'adresses IP autorisées au pare-feu ESXi
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/)

Procédure

- Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- Dans Système, cliquez sur **Profil de sécurité**.
- Dans la section Pare-feu, cliquez sur **Modifier**, puis sélectionnez un service dans la liste.
- Dans la section Adresses IP autorisées, désélectionnez **Autoriser les connexions de toutes les adresses IP**, puis saisissez les adresses IP des réseaux autorisés à se connecter à l'hôte.
Séparez les adresses IP avec des virgules. Vous pouvez utiliser les formats d'adresse suivants :
 - 192.168.0.0/24

- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

6 Cliquez sur **OK**.

Ports de pare-feu entrants et sortants pour les hôtes ESXi

vSphere Web Client vous permet d'ouvrir et de fermer les ports de pare-feu pour chaque service ou encore d'autoriser le trafic provenant d'adresses IP sélectionnées.

Le tableau ci-dessous répertorie les pare-feu pour les services généralement installés. Il est possible de disposer de services et de ports de pare-feu supplémentaires en installant d'autres VIB sur l'hôte.

Tableau 5-5. Connexions de pare-feu entrantes

Service	Port	Commentaire
Serveur CIM	5988 (TCP)	Serveur pour CIM (Common Information Model).
Serveur sécurisé CIM	5989 (TCP)	Serveur sécurisé pour CIM.
SLP CIM	427 (TCP, UDP)	Le client CIM utilise le Service Location Protocol, version 2 (SLPv2) pour rechercher des serveurs CIM.
DHCPv6	546 (TCP, UDP)	Client DHCP pour IPv6.
DVSSync	8301, 8302 (UDP)	Les ports DVSSync permettent de synchroniser les états des ports virtuels distribués entre les hôtes pour lesquels l'enregistrement et la lecture VMware FT sont activés. Seuls les ports des hôtes qui exécutent des machines virtuelles principales ou de sauvegarde doivent être ouverts. Sur les ports qui n'utilisent pas VMware FT, ces ports n'ont pas besoin d'être ouverts.
NFC	902 (TCP)	La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. ESXi utilise par défaut la technologie NFC pour des opérations comme la copie ou le transfert de données entre banques de données.
Service de clustering Virtual SAN	12345, 23451 (UDP)	Service d'annuaire pour l'adhésion au cluster Virtual SAN et la surveillance de ce dernier. Utilise la multidiffusion IP basée sur UDP pour établir les membres du cluster et distribuer les métadonnées Virtual SAN à tous les membres du cluster. Si ce service est désactivé, Virtual SAN ne fonctionne pas.
Client DHCP	68 (UDP)	Client DHCP pour IPv4.
Client DNS	53 (UDP)	Client DNS.

Tableau 5-5. Connexions de pare-feu entrantes (suite)

Service	Port	Commentaire
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Trafic entre les hôtes pour vSphere Fault Tolerance (FT).
Service de routeur logique distribué NSX	6999 (UDP)	Service de routeur distribué virtuel NSX. Le port de pare-feu associé à ce service est ouvert lorsque les VIB NSX sont installés et que le module VDR (Virtual Distributed Router) est créé. Si aucune instance de VDR n'est associée à l'hôte, le port n'a pas besoin d'être ouvert. Ce service s'appelait « Service de routeur logique distribué NSX » dans les versions précédentes du produit.
Transport Virtual SAN	2233 (TCP)	Transport de datagramme fiable pour Virtual SAN. Exploite TCP et est employé pour les E/S de stockage Virtual SAN. Si ce service est désactivé, Virtual SAN ne fonctionne pas.
Serveur SNMP	161 (UDP)	Permet à l'hôte de se connecter à un serveur SNMP.
Serveur SSH	22 (TCP)	Requis pour l'accès SSH.
vMotion	8000 (TCP)	Requis pour la migration de machines virtuelles avec vMotion.
vSphere Web Client	902, 443 (TCP)	Connexions client
vsanvp	8080 (TCP)	Fournisseur de distributeur VSAN VASA. Utilisé pour le service de gestion du stockage (SMS) inclus dans vCenter pour accéder aux informations relatives à la conformité, aux capacités et aux profils de stockage Virtual SAN. Si le service est désactivé, Virtual SAN Storage Profile Based Management (SPBM) ne fonctionne pas.
vSphere Web Access	80 (TCP)	Page de bienvenue, avec liens de téléchargement pour différentes interfaces.
Protocole RFB	5900-5964 (TCP)	Utilisé par les outils de gestion tels que VNC.

Tableau 5-6. Connexions de pare-feu sortantes

Service	Port	Commentaire
SLP CIM	427 (TCP, UDP)	Le client CIM utilise le Service Location Protocol, version 2 (SLPv2) pour rechercher des serveurs CIM.
DHCPv6	547 (TCP, UDP)	Client DHCP pour IPv6.

Tableau 5-6. Connexions de pare-feu sortantes (suite)

Service	Port	Commentaire
DVSSync	8301, 8302 (UDP)	Les ports DVSSync permettent de synchroniser les états des ports virtuels distribués entre les hôtes pour lesquels l'enregistrement et la lecture VMware FT sont activés. Seuls les ports des hôtes qui exécutent des machines virtuelles principales ou de sauvegarde doivent être ouverts. Sur les ports qui n'utilisent pas VMware FT, ces ports n'ont pas besoin d'être ouverts.
HBR	44046, 31031 (TCP)	Utilisé par vSphere Replication et VMware Site Recovery Manager pour le trafic de réplication en cours.
NFC	902 (TCP)	La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. ESXi utilise par défaut la technologie NFC pour des opérations comme la copie ou le transfert de données entre banques de données.
WOL	9 (UDP)	Utilisé par Réveil sur réseau local LAN.
Service de clustering Virtual SAN	12345 23451 (UDP)	Surveillance du cluster, appartenance et service d'annuaire utilisé par Virtual SAN.
Client DHCP	68 (UDP)	Client DHCP.
Client DNS	53 (TCP, UDP)	Client DNS.
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Prend en charge VMware Fault Tolerance.
Client de logiciel iSCSI	3260 (TCP)	Prend en charge l'iSCSI logiciel.
Service de routeur logique distribué NSX	6999 (UDP)	Le port de pare-feu associé à ce service est ouvert lorsque les VIB NSX sont installés et que le module VDR (Virtual Distributed Router) est créé. Si aucune instance de VDR n'est associée à l'hôte, le port n'a pas besoin d'être ouvert.
rabbitmqproxy	5671 (TCP)	Proxy s'exécutant sur l'hôte ESXi, qui permet aux applications exécutées sur des machines virtuelles de communiquer avec les brokers AMQP qui s'exécutent dans le domaine réseau de vCenter. Il n'est pas nécessaire que la machine virtuelle se trouve sur le réseau. En d'autres termes, aucune carte réseau n'est requise. Le proxy se connecte aux brokers dans le domaine de réseau vCenter. Par conséquent, les adresses IP des connexions sortantes doivent inclure au moins les brokers actuellement utilisés ou les futurs brokers. Si un client souhaite monter en charge, il est possible d'ajouter des brokers.

Tableau 5-6. Connexions de pare-feu sortantes (suite)

Service	Port	Commentaire
Transport Virtual SAN	2233 (TCP)	Utilisé pour le trafic RDT (communication monodiffusion de poste à poste) entre nœuds Virtual SAN.
vMotion	8000 (TCP)	Requis pour la migration de machines virtuelles avec vMotion.
Agent VMware vCenter	902 (UDP)	Agent vCenter Server.
vsanvp	8080 (TCP)	Utilisé pour le trafic de fournisseur de distributeur Virtual SAN.

Comportement du pare-feu client NFS

L'ensemble de règles de pare-feu du client NFS ne se comporte pas comme les ensembles de règles de pare-feu ESXi. ESXi configure les paramètres du client NFS lorsque vous montez ou démontez une banque de données NFS. Le comportement dépend de la version de NFS.

Lorsque vous ajoutez, montez ou démontez une banque de données NFS, le comportement obtenu dépend de la version de NFS.

Comportement du pare-feu NFS v3

Lorsque vous ajoutez ou montez une banque de données NFS v3, ESXi vérifie l'état de l'ensemble de règles de pare-feu du client NFS (`nfsClient`).

- Si l'ensemble de règles `nfsClient` est désactivé, ESXi active l'ensemble de règles et désactive la stratégie « Autoriser toutes les adresses IP » en définissant l'indicateur `allowedAll` sur `FALSE`. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.
- Si l'ensemble de règles `nfsClient` est activé, l'état de l'ensemble de règles et la stratégie d'adresse IP autorisée ne sont pas modifiés. L'adresse IP du serveur NFS est ajoutée à la liste des adresses IP sortantes autorisées.

Note Si vous activez manuellement l'ensemble de règles `nfsClient` ou configurez manuellement la stratégie Autoriser toutes les adresses IP, avant ou après avoir ajouté une banque de données NFS v3 dans le système, vos paramètres sont remplacés lorsque la dernière banque de données NFS v3 est démontée. L'ensemble de règles `nfsClient` est désactivé lorsque toutes les banques de données NFS v3 sont démontées.

Lorsque vous supprimez ou démontez une banque de données NFS v3, ESXi réalise l'une des actions suivantes.

- Si aucune des banques de données NFS v3 restantes n'est montée à partir du serveur de la banque de données que vous êtes en train de démonter, ESXi supprime l'adresse IP du serveur dans la liste des adresses IP sortantes.
- S'il ne reste aucune banque de données NFS v3 montée une fois l'opération de démontage terminée, ESXi désactive l'ensemble de règles de pare-feu `nfsClient`.

Comportement du pare-feu NFS v4.1

Lorsque vous montez la première banque de données NFS v4.1, ESXi active l'ensemble de règles `nfs41client` et définit son indicateur `allowedAll` sur `TRUE`. Cette action provoque l'ouverture du port 2049 pour toutes les adresses IP. Le démontage d'une banque de données NFS v4.1 n'a pas d'impact sur l'état du pare-feu. En d'autres termes, le port 2049 s'ouvre la première fois que vous montez une banque de données NFS v4.1 et reste ouvert jusqu'à ce que vous le fermiez explicitement.

Commandes de pare-feu ESXCLI d'ESXi

Si votre environnement inclut plusieurs hôtes ESXi, l'automatisation de la configuration de pare-feu à l'aide de commandes ESXCLI ou de vSphere Web Services SDK est recommandée.

Vous pouvez utiliser les commandes d'ESXi Shell ou de vSphere CLI pour configurer ESXi sur la ligne de commande afin d'automatiser la configuration du pare-feu. Reportez-vous à *Démarrage avec vSphere Command-Line Interfaces* pour une introduction et à *Concepts et exemples d'interfaces de ligne de commande vSphere* pour des exemples d'utilisation d'ESXCLI pour manipuler des pare-feu et des règles de pare-feu.

Tableau 5-7. Commandes du pare-feu

Commande	Description
<code>esxcli network firewall get</code>	Renvoie l'état activé ou désactivé du pare-feu et répertorie les actions par défaut.
<code>esxcli network firewall set --default-action</code>	Définir sur <code>True</code> pour transmettre les paquets par défaut. Définir sur <code>False</code> pour rejeter les paquets par défaut.
<code>esxcli network firewall set --enabled</code>	Activer ou désactiver le pare-feu d'ESXi.
<code>esxcli network firewall load</code>	Charger le module du pare-feu et les fichiers de configuration d'ensemble de règles.
<code>esxcli network firewall refresh</code>	Actualiser la configuration du pare-feu en lisant les fichiers d'ensemble de règles si le module du pare-feu est chargé.
<code>esxcli network firewall unload</code>	Détruire les filtres et décharger le module du pare-feu.
<code>esxcli network firewall ruleset list</code>	Répertorier les informations des ensembles de règles.
<code>esxcli network firewall ruleset set --allowed-all</code>	Définir sur <code>True</code> pour permettre l'accès à toutes les adresses IP. Définir sur <code>False</code> pour utiliser une liste d'adresses IP autorisées.
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<string></code>	Définir sur <code>True</code> pour activer l'ensemble de règles spécifié. Définir sur <code>False</code> pour le désactiver.
<code>esxcli network firewall ruleset allowedip list</code>	Répertorier les adresses IP autorisées de l'ensemble de règles spécifié.
<code>esxcli network firewall ruleset allowedip add</code>	Autoriser l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.

Tableau 5-7. Commandes du pare-feu (suite)

Commande	Description
<code>esxcli network firewall ruleset allowedip remove</code>	Supprimer l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.
<code>esxcli network firewall ruleset rule list</code>	Lister les règles de chaque ensemble de règles du pare-feu.

Personnalisation des services ESXi à partir du profil de sécurité

Un hôte ESXi inclut plusieurs services s'exécutant par défaut. D'autres services, par exemple SSH, sont inclus dans le profil de sécurité de l'hôte. Vous pouvez activer et désactiver ces services en fonction des besoins si la stratégie de l'entreprise l'autorise.

[Utiliser vSphere Web Client pour activer l'accès à ESXi Shell](#) est un exemple de procédure d'activation d'un service.

Note L'activation de services affecte la sécurité de votre hôte. N'activez un service que si cela est strictement nécessaire.

Les services disponibles varient en fonction des VIB installés sur l'hôte ESXi. Vous ne pouvez pas ajouter de services sans installer un VIB. Certains produits VMware (par exemple, vSphere HA) installent des VIB sur des hôtes et rendent disponibles des services et les ports de pare-feu correspondants.

Dans une installation par défaut, vous pouvez modifier l'état des services suivants dans vSphere Web Client.

Tableau 5-8. Services ESXi du profil de sécurité

Service	Par défaut	Description
IU de Direct Console	En cours d'exécution	Le service DCUI (Direct Console User Interface) vous permet d'interagir avec un hôte ESXi à partir de l'hôte de la console locale à l'aide de menus textuels.
ESXi Shell	Arrêté	ESXi Shell est disponible dans l'interface DCUI et inclut un ensemble de commandes intégralement prises en charge et un ensemble de commandes assurant le dépannage et la correction. Vous devez activer l'accès à ESXi Shell dans la console directe de chaque système. Vous pouvez activer l'accès à ESXi Shell ou accéder à ESXi Shell avec SSH.
SSH	Arrêté	Service client SSH de l'hôte qui permet les connexions à distance via SSH (Secure Shell).
Démon d'association basé sur la charge	En cours d'exécution	Association basée sur la charge.
Serveur d'authentification de sécurité locale (Service Active Directory)	Arrêté	Partie du service Active Directory. Lorsque vous configurez ESXi pour Active Directory, ce service démarre.

Tableau 5-8. Services ESXi du profil de sécurité (suite)

Service	Par défaut	Description
Redirecteur d'E/S (Service Active Directory)	Arrêté	Partie du service Active Directory. Lorsque vous configurez ESXi pour Active Directory, ce service démarre.
Serveur de connexion au réseau (Service Active Directory)	Arrêté	Partie du service Active Directory. Lorsque vous configurez ESXi pour Active Directory, ce service démarre.
Processus NTP	Arrêté	Démon NTP (Network Time Protocol).
Serveur CIM	En cours d'exécution	Service pouvant être utilisé par les applications CIM (Common Information Model).
Serveur SNMP	Arrêté	Démon SNMP. Reportez-vous à <i>Surveillance et performances de vSphere</i> pour obtenir des informations sur la configuration de SNMP v1, v2 et v3.
Serveur Syslog	Arrêté	Démon Syslog. Vous pouvez activer syslog à partir des Paramètres système avancés de vSphere Web Client. Reportez-vous à <i>Installation et configuration de vSphere</i> .
Agent vSphere haute disponibilité	Arrêté	Prend en charge la fonctionnalité vSphere High Availability.
Démon vProbe	Arrêté	Démon vProbe.
Agent VMware vCenter	En cours d'exécution	Agent vCenter Server. Autorise un système vCenter Server à se connecter à un hôte ESXi. Spécifiquement, vpxa est le conduit de communication au démon de l'hôte qui communique avec le noyau ESXi.
X.Org Server	Arrêté	X.Org Server. Cette fonctionnalité facultative est utilisée en interne pour les graphiques 3D des machines virtuelles.

Activer ou désactiver un service dans le profil de sécurité

Vous pouvez activer ou désactiver l'un des services répertoriés dans le profil de sécurité depuis vSphere Web Client.

Après l'installation, certains services s'exécutent par défaut, tandis que d'autres sont arrêtés. Dans certains cas, une configuration supplémentaire est nécessaire avant qu'un service devienne disponible dans l'interface utilisateur de vSphere Web Client. Par exemple, le service NTP permet d'obtenir des informations horaires précises, mais ce service fonctionne uniquement lorsque les ports requis sont ouverts dans le pare-feu.

Conditions préalables

Connectez-vous à vCenter Server avec vSphere Web Client.

Procédure

- 1 Accédez à un hôte dans l'inventaire vSphere Web Client, puis sélectionnez-le.

- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sous Système, sélectionnez **Profil de sécurité** et cliquez sur **Modifier**.
- 4 Accédez au service que vous souhaitez modifier.
- 5 Dans le volet Détails du service, sélectionnez **Démarrer**, **Arrêter** ou **Redémarrer** pour une modification ponctuelle de l'état de l'hôte ou faites votre choix dans le menu **Règle démarrage** pour modifier l'état de l'hôte lors des redémarrages.
 - **Démarrer automatiquement si ports ouverts, et arrêter quand tous ports fermés** : paramètre par défaut pour ces services. Si un port est ouvert, le client tente de contacter les ressources réseau du service. Si certains ports sont ouverts, mais que le port d'un service particulier est fermé, la tentative échoue. Lorsque le port sortant applicable est ouvert, le service termine son démarrage.
 - **Démarrer et arrêter avec hôte** : le service démarre peu de temps après le démarrage de l'hôte et se ferme juste avant l'arrêt de l'hôte. Plutôt semblable à l'option **Démarrer automatiquement si ports ouverts, et arrêter quand tous ports fermés**, cette option signifie que le service tente régulièrement d'effectuer sa tâche, telle que contacter le serveur NTP spécifié. Si le port a été fermé, mais est rouvert par la suite, le client commence à effectuer sa tâche peu après.
 - **Démarrer et arrêter manuellement** : L'hôte préserve les paramètres de service déterminés par l'utilisateur, quels que soient les ports ouverts ou non. Lorsqu'un utilisateur démarre le service NTP, ce service reste en exécution tant que l'hôte est alimenté. Si le service est démarré et que l'hôte est mis hors tension, le service est arrêté dans le cadre du processus d'arrêt, mais dès que l'hôte est mis sous tension, le service redémarre et conserve l'état déterminé par l'utilisateur.

Note Ces paramètres s'appliquent uniquement aux paramètres de service qui sont configurés par le biais de vSphere Web Client ou aux applications créées avec vSphere Web Services SDK. Les configurations effectuées par d'autres moyens (par exemple, dans ESXi Shell ou avec les fichiers de configuration, ne sont pas modifiées par ces paramètres).

Mode verrouillage

Pour augmenter le niveau de sécurité des hôtes ESXi, vous pouvez les placer en mode de verrouillage. En mode de verrouillage, les opérations doivent être exécutées via vCenter Server par défaut.

vSphere 6.0 propose différents degrés de verrouillage par le biais de deux modes de verrouillage : normal et strict. La liste d'utilisateurs exceptionnels est une autre nouveauté de vSphere 6.0. Les utilisateurs exceptionnels ne perdent pas leurs privilèges lorsque l'hôte entre en mode de verrouillage. Utilisez la liste d'utilisateurs exceptionnels pour ajouter les comptes de solutions tierces et d'applications externes qui doivent accéder directement à l'hôte lorsque celui-ci est en mode de verrouillage. Reportez-vous à la section [Spécifier les utilisateurs exceptionnels du mode de verrouillage](#).



Mode verrouillage dans vSphere 6

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

Mode de verrouillage normal et mode de verrouillage strict

À partir de vSphere 6.0, vous pouvez sélectionner le mode de verrouillage normal ou le mode de verrouillage strict, ce qui offre différents degrés de verrouillage.

Mode de verrouillage normal

En mode de verrouillage normal, le service DCUI n'est pas interrompu. En cas de perte de connexion avec le système vCenter Server, si l'accès via vSphere Web Client n'est plus disponible, les comptes disposant de privilèges peuvent se connecter à l'interface utilisateur de la console directe de l'hôte ESXi et quitter le mode de verrouillage. Seuls les comptes suivants peuvent accéder à l'interface utilisateur de la console directe :

- Comptes répertoriés dans la liste des utilisateurs exceptionnels pour le mode de verrouillage qui disposent des privilèges d'administration sur l'hôte. La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches très spécifiques. L'ajout d'administrateurs ESXi à cette liste serait contraire à l'objectif du mode de verrouillage.
- Les utilisateurs définis dans l'option avancée DCUI.Access de l'hôte. Cette option sert d'accès de secours à l'interface utilisateur de la console directe en cas de perte de connexion avec vCenter Server. Ces utilisateurs n'ont pas besoin de disposer de privilèges d'administration sur l'hôte.

Mode de verrouillage strict

En mode de verrouillage strict (nouveau dans vSphere 6.0), le service DCUI est interrompu. En cas de perte de la connexion avec vCenter Server, si vSphere Web Client n'est plus disponible, l'hôte ESXi n'est plus disponible non plus, à moins que les services ESXi Shell et SSH soient activés et que des utilisateurs exceptionnels soient définis. Si vous ne pouvez pas rétablir la connexion avec le système vCenter Server, vous devez réinstaller l'hôte.

Mode de verrouillage et services ESXi Shell et SSH

Le mode de verrouillage strict interrompt le service DCUI. Toutefois, les services ESXi Shell et SSH sont indépendants du mode de verrouillage. Pour que le mode de verrouillage constitue une mesure de sécurité efficace, assurez-vous que les services ESXi Shell et SSH sont également désactivés. Ils sont désactivés par défaut.

Lorsqu'un hôte est en mode de verrouillage, les utilisateurs répertoriés dans la liste des utilisateurs exceptionnels peuvent accéder à l'hôte à partir de ESXi Shell et via SSH s'ils disposent du rôle Administrateur sur l'hôte. Cet accès reste possible en mode de verrouillage strict. Pour une sécurité maximale, laissez les services ESXi Shell et SSH désactivés.

Note La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches spécifiques, telles que les sauvegardes d'hôtes, pas aux administrateurs. L'ajout d'utilisateurs administrateurs à la liste des utilisateurs exceptionnels annule le mode de verrouillage.

Activation et désactivation du mode de verrouillage

Les utilisateurs disposant de privilèges peuvent activer le mode de verrouillage de plusieurs manières :

- En ajoutant un hôte à un système vCenter Server à l'aide de l'assistant **Ajouter hôte**.
- En utilisant vSphere Web Client. Reportez-vous à la section [Activation du mode verrouillage à l'aide de vSphere Web Client](#). Vous pouvez activer le mode de verrouillage normal et le mode de verrouillage strict dans vSphere Web Client.
- En utilisant l'interface utilisateur de la console directe (DCUI). Reportez-vous à la section [Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe](#).

Les utilisateurs disposant de privilèges peuvent désactiver le mode de verrouillage dans vSphere Web Client. Dans cette interface, ils peuvent désactiver le mode de verrouillage normal, mais pas le mode de verrouillage strict.

Note Si vous activez ou désactivez le mode de verrouillage en utilisant l'interface utilisateur de la console directe, les autorisations des utilisateurs et des groupes sont ignorées sur l'hôte. Pour conserver ces autorisations, vous pouvez activer et désactiver le mode de verrouillage à l'aide de vSphere Web Client.

Comportement du mode de verrouillage

En mode de verrouillage, certains services sont désactivés et d'autres ne sont accessibles qu'à certains utilisateurs.

Services du mode de verrouillage pour différents utilisateurs

Lorsque l'hôte est en cours d'exécution, les services disponibles varient selon que le mode de verrouillage est activé et en fonction du type de mode de verrouillage.

- En mode de verrouillage strict et normal, les utilisateurs disposant de privilèges peuvent accéder à l'hôte via vCenter Server à l'aide de vSphere Web Client ou de vSphere Web Services SDK.

- Le comportement de l'interface de console directe du mode de verrouillage strict est différent de celui du mode de verrouillage normal.
 - En mode de verrouillage strict, le service d'interface utilisateur de la console directe est désactivé.
 - En mode de verrouillage normal, les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur et les utilisateurs spécifiés dans le paramètre système avancé DCUI.Access peuvent accéder à l'interface de console directe.
- Si ESXi Shell ou SSH est activé et que l'hôte est placé en mode de verrouillage strict ou normal, les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur peuvent utiliser ces services. ESXi Shell ou SSH est désactivé pour tous les autres utilisateurs. À partir de vSphere 6.0, les sessions ESXi ou SSH des utilisateurs qui ne disposent pas de privilèges d'administrateur sont terminées.

Tout accès est connecté à la fois pour le mode de verrouillage strict et normal.

Tableau 5-9. Comportement du mode de verrouillage

Service	Mode normal	Mode de verrouillage normal :	Mode verrouillage strict
API vSphere Web Services	Tous les utilisateurs, en fonction des autorisations	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)
Fournisseurs CIM	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)	vCenter (vpxuser) Utilisateurs exceptionnels, en fonction des autorisations vCloud Director (vslauser, s'il est disponible)
Interface utilisateur de la console directe (DCUI)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte et utilisateurs de l'option avancée DCUI.Access	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Le service de l'interface DCUI est arrêté

Tableau 5-9. Comportement du mode de verrouillage (suite)

Service	Mode normal	Mode de verrouillage normal :	Mode verrouillage strict
ESXi Shell (s'il est activé)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte
SSH (s'il est activé)	Utilisateurs disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte	Utilisateurs définis dans l'option avancée DCUI.Access Utilisateurs exceptionnels disposant des privilèges d'administrateur sur l'hôte

Utilisateurs connectés à ESXi Shell lorsque le mode de verrouillage est activé

Si des utilisateurs sont connectés à ESXi Shell ou accèdent à l'hôte via SSH avant d'activer le mode de verrouillage, les utilisateurs qui se trouvent sur la liste des utilisateurs exceptionnels et qui disposent des privilèges d'administrateur sur l'hôte restent connectés. À partir de vSphere 6.0, la session est terminée pour tous les autres utilisateurs. Ce comportement s'applique à la fois au mode de verrouillage normal et strict.

Activation du mode verrouillage à l'aide de vSphere Web Client

Vous pouvez activer le mode de verrouillage afin d'imposer l'apport des modifications de configuration via vCenter Server. vSphere 6.0 et versions ultérieures prennent en charge le mode de verrouillage normal et strict.

Pour interdire complètement tout accès direct à un hôte, vous pouvez sélectionner le mode de verrouillage strict. Le mode de verrouillage strict empêche d'accéder à un hôte si vCenter Server n'est pas disponible et que SSH et ESXi Shell sont désactivés. Reportez-vous à [Comportement du mode de verrouillage](#).

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans **Système**, sélectionnez **Profil de sécurité**.
- 4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.

- 5 Cliquez sur **Mode verrouillage** et sélectionnez l'une des options du mode de verrouillage.

Option	Description
Normale	Vous pouvez accéder à l'hôte via vCenter Server. Seuls les utilisateurs qui se trouvent dans la liste des utilisateurs exceptionnels et qui disposent des privilèges d'administrateur peuvent se connecter à l'interface utilisateur de la console directe. Si SSH ou ESXi Shell sont activés, il peut être possible d'y accéder.
Strict	Vous ne pouvez accéder à l'hôte que via vCenter Server. Si SSH ou ESXi Shell sont activés, les sessions des comptes de l'option avancée DCUI.Access et des comptes d'utilisateurs exceptionnels disposant de privilèges d'administrateur restent activées. Toutes les autres sessions sont terminées.

- 6 Cliquez sur **OK**.

Désactiver le mode de verrouillage à l'aide de vSphere Web Client

Désactivez le mode de verrouillage pour permettre des modifications de configuration à partir de connexions directes à l'hôte ESXi. Lorsque le mode de verrouillage est activé, la sécurité de l'environnement est accrue.

Dans vSphere 6.0, vous pouvez désactiver le mode de verrouillage comme suit :

Dans vSphere Web Client

Les utilisateurs peuvent désactiver à la fois le mode de verrouillage normal et strict dans vSphere Web Client.

Dans l'interface utilisateur de la console directe

Les utilisateurs qui peuvent accéder à l'interface utilisateur de la console directe sur l'hôte ESXi peuvent désactiver le mode de verrouillage normal. En mode de verrouillage strict, le service d'interface de console directe est arrêté.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans **Système**, sélectionnez **Profil de sécurité**.
- 4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.
- 5 Cliquez sur **Mode verrouillage** et sélectionnez **Aucun** pour désactiver le mode de verrouillage.

Résultats

Le système quitte le mode de verrouillage, vCenter Server affiche une alarme et une entrée est ajoutée au journal d'audit.

Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe

Vous pouvez activer et désactiver le mode de verrouillage normal dans l'interface utilisateur de la console directe (DCUI). Vous ne pouvez activer et désactiver le mode de verrouillage strict que dans vSphere Web Client.

Lorsque l'hôte est en mode de verrouillage normal, les comptes suivants peuvent accéder à l'interface utilisateur de la console directe :

- Les comptes de la liste des utilisateurs exceptionnels qui disposent des privilèges d'administrateur sur l'hôte. La liste des utilisateurs exceptionnels est destinée aux comptes de service tels qu'un agent de sauvegarde.
- Les utilisateurs définis dans l'option avancée DCUI.Access de l'hôte. Cette option peut être utilisée pour activer l'accès en cas de défaillance irrémédiable.

Pour ESXi 6.0 et versions ultérieures, les autorisations des utilisateurs sont conservées lorsque vous activez le mode de verrouillage et restaurées lorsque vous désactivez ce mode dans l'interface de console directe.

Note Si vous mettez à niveau un hôte en mode de verrouillage vers ESXi 6.0 sans quitter le mode de verrouillage, puis que vous quittez ce mode après la mise à niveau, toutes les autorisations définies avant que l'hôte n'entre en mode de verrouillage sont perdues. Le système attribue le rôle d'administrateur à tous les utilisateurs qui se trouvent dans l'option avancée DCUI.Access afin d'assurer l'accès à l'hôte.

Pour conserver les autorisations, désactivez le mode de verrouillage de l'hôte dans vSphere Web Client avant la mise à niveau.

Procédure

- 1 Dans l'interface utilisateur de la console directe de l'hôte, appuyez sur F2 et ouvrez une session.
- 2 Faites défiler jusqu'au paramètre **Configurer le mode verrouillage** et appuyez sur Entrée pour modifier le paramètre actuel.
- 3 Appuyez sur Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

Spécification des comptes disposant de privilèges d'accès en mode de verrouillage

Vous pouvez spécifier les comptes de service qui peuvent accéder à l'hôte ESXi directement en les ajoutant à la liste des utilisateurs exceptionnels. Vous pouvez spécifier un utilisateur qui peut accéder à l'hôte ESXi en cas de défaillance irrémédiable de vCenter Server.

Les actions par défaut que peuvent effectuer les différents comptes lorsque le mode de verrouillage est activé et le mode de modification du comportement par défaut dépendent de la version de l'environnement vSphere.

- Dans les versions de vSphere antérieures à vSphere 5.1, seul l'utilisateur racine peut se connecter à l'interface utilisateur de la console directe sur un hôte ESXi en mode de verrouillage.
- Dans vSphere 5.1 et versions ultérieures, vous pouvez ajouter un utilisateur au paramètre système avancé DCUI.Access pour chaque hôte. Cette option est conçue pour répondre aux défaillances irrémédiables de vCenter Server et le mot de passe de l'utilisateur disposant de cet accès est habituellement verrouillé dans un coffre-fort. Un utilisateur de la liste DCUI.Access n'a pas besoin de disposer de tous les privilèges administratifs sur l'hôte.
- Dans vSphere 6.0 et versions ultérieures, le paramètre système avancé DCUI.Access est toujours pris en charge. En outre, vSphere 6.0 et versions ultérieures prennent en charge une liste des utilisateurs exceptionnels destinée aux comptes de service qui doivent se connecter directement à l'hôte. Les comptes d'administrateur disposant des privilèges d'administrateur, qui se trouvent dans la liste des utilisateurs exceptionnels, peuvent se connecter à ESXi Shell. En outre, ces utilisateurs peuvent se connecter à l'interface DCUI d'un hôte en mode de verrouillage normal et quitter ce même mode.

Spécifiez les utilisateurs exceptionnels dans vSphere Web Client

Note Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant de privilèges définis localement pour l'hôte ESXi. Les utilisateurs qui sont membres d'un groupe Active Directory perdent leurs autorisations lorsque l'hôte est en mode de verrouillage.

Option avancée Ajouter des utilisateurs à DCUI.Access

L'option avancée DCUI.Access a pour objectif principal de vous permettre de quitter le mode de verrouillage en cas de défaillance irrémédiable, lorsque vous ne pouvez pas accéder à l'hôte à partir de vCenter Server. Vous ajoutez des utilisateurs à la liste en modifiant les paramètres avancés de l'hôte à partir de vSphere Web Client.

Note Les utilisateurs de la liste DCUI.Access peuvent modifier les paramètres du mode de verrouillage, quels que soient leurs privilèges. Cela peut avoir un impact sur la sécurité de votre hôte. Pour les comptes de services qui ont besoin d'un accès direct à l'hôte, pensez plutôt à ajouter des utilisateurs à la liste des utilisateurs exceptionnels. Les utilisateurs exceptionnels peuvent uniquement exécuter les tâches pour lesquelles ils ont des privilèges. Reportez-vous à [Spécifier les utilisateurs exceptionnels du mode de verrouillage](#).

Procédure

- 1 Accédez à l'hôte dans le navigateur d'objets de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sélectionnez **Paramètres**.
- 3 Cliquez sur **Paramètres système avancés**, puis sélectionnez le paramètre **DCUI.Access**.

- 4 Cliquez sur **Modifier** et saisissez les noms d'utilisateur, séparés par des virgules.

L'utilisateur racine est inclus par défaut. Pensez à supprimer la racine de la liste DCUI.Access et à spécifier un compte nommé pour un meilleur contrôle.

- 5 Cliquez sur **OK**.

Spécifier les utilisateurs exceptionnels du mode de verrouillage

Dans vSphere 6.0 et versions ultérieures, vous pouvez ajouter des utilisateurs à la liste des utilisateurs exceptionnels dans vSphere Web Client. Ces utilisateurs ne perdent pas leurs autorisations lorsque l'hôte entre en mode de verrouillage. Il est logique d'ajouter des comptes de services tels qu'un agent de sauvegarde à la liste des utilisateurs exceptionnels.

Les utilisateurs exceptionnels ne perdent pas leurs privilèges lorsque l'hôte entre en mode de verrouillage. Habituellement, ces comptes représentent des solutions tierces et des applications externes qui doivent continuer à fonctionner en mode de verrouillage.

Note La liste des utilisateurs exceptionnels est destinée aux comptes de service qui exécutent des tâches très spécifiques, pas aux administrateurs. L'ajout d'utilisateurs administrateurs à la liste des utilisateurs exceptionnels annule le mode de verrouillage.

Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant de privilèges définis localement pour l'hôte ESXi. Ils ne sont ni membres d'un groupe Active Directory ni utilisateurs de vCenter Server. Ces utilisateurs sont autorisés à effectuer des opérations sur l'hôte en fonction de leurs privilèges. Par exemple, cela signifie que l'utilisateur en lecture seule ne peut pas désactiver le mode de verrouillage sur un hôte.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans Système, sélectionnez **Profil de sécurité**.
- 4 Dans le panneau mode verrouillage, cliquez sur **Modifier**.
- 5 Cliquez sur **Utilisateurs exceptionnels** et sur l'icône représentant le signe plus pour ajouter des utilisateurs exceptionnels.

Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB

Pour protéger l'intégrité de l'hôte ESXi, n'autorisez pas les utilisateurs à installer des VIB non signés (communautaires). Un VIB non signé contient un code qui n'est ni certifié ni approuvé ni pris en charge par VMware ou ses partenaires. Les VIB communautaires n'ont pas de signature numérique.

Vous pouvez utiliser des commandes ESXCLI pour définir le niveau de l'acceptation d'un hôte. Le niveau d'acceptation de l'hôte doit être le même ou moins restrictif que celui d'un VIB que vous souhaitez ajouter à l'hôte. Pour protéger la sécurité et l'intégrité de vos hôtes ESXi, ne permettez pas l'installation de VIB non signés (CommunitySupported) sur des hôtes dans des systèmes de production.

Les niveaux d'acceptation suivants sont pris en charge.

VMwareCertified

Le niveau d'acceptation VMwareCertified a les exigences les plus contraignantes. Les VIB avec ce niveau sont soumis à des tests minutieux équivalents aux tests d'assurance qualité réalisés en interne de VMware pour la même technologie. Actuellement, seuls les pilotes IOVP sont publiés à ce niveau. VMware prend en charge les appels d'assistance pour les VIB avec ce niveau d'acceptation.

VMwareAccepted

Les VIB avec ce niveau d'acceptation sont soumis à des tests de vérification minutieux, mais ces tests ne testent pas entièrement chaque fonction du logiciel. Le partenaire exécute les tests et VMware vérifie le résultat. Actuellement, les fournisseurs CIM et les plug-ins PSA font partie des VIB publiés à ce niveau. VMware dirige les appels d'assistance pour les VIB avec ce niveau d'acceptation vers l'organisation d'assistance du partenaire.

PartnerSupported

Les VIB avec le niveau d'acceptation PartnerSupported sont publiés par un partenaire en qui VMware a confiance. Le partenaire effectue tous les tests. VMware ne vérifie pas les résultats. Ce niveau est utilisé pour une technologie nouvelle ou non courante que des partenaires souhaitent activer pour les systèmes VMware. Actuellement, les technologies VIB de pilotes telles que Infiniband, ATAoE et SSD sont à ce niveau avec des pilotes de matériel non standard. VMware dirige les appels d'assistance pour les VIB avec ce niveau d'acceptation vers l'organisation d'assistance du partenaire.

CommunitySupported

Le niveau d'acceptation CommunitySupported est destiné aux VIB créés par des individus ou des entreprises en dehors des programmes de partenariat de VMware. Les VIB à ce niveau d'acceptation ne sont soumis à aucun programme de test approuvé par VMware et ne sont pas pris en charge par l'assistance technique de VMware ou un partenaire de VMware.

Procédure

- 1 Connectez-vous à chaque hôte ESXi et vérifiez que le niveau d'acceptation est défini sur VMwareCertified ou VMwareAccepted en exécutant la commande suivante.

```
esxcli software acceptance get
```

- 2 Si le niveau d'acceptation de l'hôte n'est pas VMwareCertified ou VMwareAccepted, déterminez si l'un des VIBs ne se trouve pas au niveau VMwareCertified ou VMwareAccepted en exécutant les commandes suivantes.

```
esxcli software vib list
esxcli software vib get -n vibname
```

- 3 Supprimez les VIB qui sont au niveau PartnerSupported ou CommunitySupported en exécutant la commande suivante.

```
esxcli software vib remove --vibname vib
```

- 4 Changez le niveau d'acceptation de l'hôte en exécutant la commande suivante.

```
esxcli software acceptance set --level acceptance_level
```

Affectation d'autorisations pour ESXi

Les privilèges sont généralement octroyés aux utilisateurs par attribution d'autorisations aux objets hôtes ESXi gérés par un système vCenter Server. Si vous utilisez un hôte ESXi autonome, vous pouvez attribuer les privilèges directement.

Attribution d'autorisations aux hôtes ESXi gérés par vCenter Server

Si votre hôte ESXi est géré par vCenter Server, effectuez les tâches de gestion à l'aide de vSphere Web Client.

Vous pouvez sélectionner l'objet hôte ESXi dans la hiérarchie d'objets de vCenter Server et attribuer le rôle d'administrateur à un nombre limité d'utilisateurs susceptibles d'effectuer la gestion directe sur l'hôte ESXi. Reportez-vous à [Utilisation des rôles pour assigner des privilèges](#).

Il est recommandé de créer au moins un compte d'utilisateur nommé et de lui attribuer des privilèges d'administration complets sur l'hôte, puis de l'utiliser à la place du compte racine. Définissez un mot de passe avec un niveau de complexité élevé pour le compte racine et limitez l'utilisation de ce compte. (Ne supprimez pas le compte racine.)

Attribution d'autorisations aux hôtes ESXi autonomes

Si votre environnement ne comprend pas de système vCenter Server, les utilisateurs suivants sont prédéfinis.

- utilisateur racine. Reportez-vous à [Privilèges de l'utilisateur racine](#).
- vpxuser. Reportez-vous à [Privilèges vpxuser](#).
- utilisateur dcui. Reportez-vous à [Privilèges de l'utilisateur dcui](#).

Dans l'onglet Gestion de vSphere Client, vous pouvez ajouter des utilisateurs locaux et définir des rôles personnalisés.

Pour toutes les versions d'ESXi, vous pouvez voir la liste des utilisateurs prédéfinis dans le fichier `/etc/passwd`.

Les rôles suivants sont prédéfinis :

Lecture seule

Permet à un utilisateur d'afficher les objets associés à l'hôte ESXi, mais pas de les modifier.

Administrateur

Rôle d'administrateur.

Aucun accès

Aucun accès. Ceci est la configuration par défaut. Si nécessaire, vous pouvez remplacer la valeur par défaut.

Vous pouvez gérer les utilisateurs et groupes locaux et ajouter des rôles personnalisés locaux à un hôte ESXi à l'aide d'un vSphere Client directement connecté à l'hôte ESXi.

À partir de vSphere 6.0, vous pouvez gérer les comptes d'utilisateurs locaux ESXi à l'aide des commandes de gestion de compte ESXCLI. Vous pouvez définir ou supprimer des autorisations sur les comptes Active Directory (utilisateurs et groupes) et sur les comptes locaux ESXi (utilisateurs uniquement) à l'aide des commandes de gestion des autorisations ESXCLI.

Note Si vous définissez un utilisateur pour l'hôte ESXi en le connectant directement à l'hôte et qu'il existe un utilisateur de même nom dans vCenter Server, ces deux utilisateurs sont distincts. Si vous attribuez un rôle à l'un des utilisateurs, il n'est pas attribué à l'autre utilisateur.

Privilèges de l'utilisateur racine

Par défaut, chaque hôte ESXi dispose d'un compte d'utilisateur racine unique ayant le rôle Administrateur. Ce compte d'utilisateur racine peut être utilisé pour l'administration locale et pour connecter l'hôte à vCenter Server.

Ce compte racine commun peut simplifier la pénétration dans un hôte ESXi et complique la mise en correspondance d'actions à un administrateur spécifique.

Définissez un mot de passe très complexe pour le compte racine et limitez l'utilisation de ce compte (par exemple, pour une utilisation lors de l'ajout d'un hôte à vCenter Server). Ne supprimez pas le compte racine. Dans vSphere 5.1 et versions ultérieures, seul l'utilisateur racine (aucun autre utilisateur nommé disposant du rôle Administrateur) est autorisé à ajouter un hôte à vCenter Server.

Il convient de s'assurer que tout compte disposant du rôle Administrateur sur un hôte ESXi est attribué à un utilisateur spécifique ayant un compte nommé. Utilisez les possibilités Active Directory d'ESXi qui vous permettent de gérer les informations d'identification Active Directory le cas échéant.

Important Si vous supprimez les privilèges d'accès de l'utilisateur racine, vous devez d'abord créer une autre autorisation au niveau de la racine ayant un autre utilisateur affecté au rôle d'administrateur.

Privilèges vpxuser

vCenter Server utilise les privilèges vpxuser pour gérer les activités de l'hôte.

vCenter Server possède des privilèges d'administrateur sur l'hôte qu'il gère. Par exemple, vCenter Server peut transférer des machines virtuelles vers/depuis des hôtes et effectuer les changements de configuration requis pour prendre en charge des machines virtuelles.

L'administrateur vCenter Server peut exécuter sur l'hôte la majorité des tâches de l'utilisateur racine, mais aussi programmer des tâches, utiliser des modèles, etc. Cependant, l'administrateur vCenter Server ne peut pas directement créer, supprimer ou modifier des utilisateurs et groupes locaux pour des hôtes. Ces tâches peuvent uniquement être exécutées par un utilisateur disposant des autorisations administrateur directement sur chaque hôte.

Note Vous ne pouvez pas gérer vpxuser via Active Directory.

Attention Ne modifiez vpxuser en aucune façon. Ne modifiez pas son mot de passe. Ne modifiez pas ses autorisations. Dans le cas contraire, vous risquez d'avoir des difficultés à utiliser des hôtes via vCenter Server.

Privilèges de l'utilisateur dcui

L'utilisateur dcui s'exécute sur des hôtes et dispose des droits d'Administrateur. L'objectif principal de cet utilisateur est de configurer des hôtes pour le mode verrouillage à partir de l'interface utilisateur de console directe (DCUI).

Cet utilisateur agit en tant qu'agent pour la console directe et ne peut pas être modifié ou utilisé par des utilisateurs interactifs.

Utilisation d'Active Directory pour gérer des utilisateurs ESXi

Vous pouvez configurer l'hôte ESXi afin qu'il utilise un service d'annuaire tel qu'Active Directory pour gérer les utilisateurs.

La création de comptes utilisateurs locaux sur chaque hôte pose des difficultés de synchronisation du nom et du mot de passe des comptes parmi plusieurs hôtes. Intégrez les hôtes ESXi à un domaine Active Directory pour éliminer la nécessité de créer et de maintenir des comptes utilisateurs locaux. L'utilisation d'Active Directory pour l'authentification des utilisateurs simplifie la configuration de l'hôte ESXi et réduit le risque de problèmes de configuration qui pourraient entraîner des accès non autorisés.

Lorsque vous utilisez Active Directory, les utilisateurs entrent les informations d'identification Active Directory et le nom de domaine du serveur Active Directory lorsqu'ils ajoutent un hôte à un domaine.

Installer ou mettre à niveau vSphere Authentication Proxy

Installez vSphere Authentication Proxy pour permettre aux hôtes ESXi de rejoindre un domaine sans utiliser les informations d'identification Active Directory. vSphere Authentication Proxy renforce la sécurité des hôtes démarrés par PXE et des hôtes provisionnés à l'aide d'Auto Deploy en évitant de stocker les informations d'identification Active Directory dans la configuration de l'hôte.

Si une version antérieure de vSphere Authentication Proxy est installée sur votre système, cette procédure met à niveau vSphere Authentication Proxy vers la version actuelle.

Vous pouvez installer vSphere Authentication Proxy sur la même machine que le système vCenter Server associé ou sur une machine différente disposant d'une connexion réseau à vCenter Server. vSphere Authentication Proxy est pris en charge par vCenter Server version 5.0 et versions ultérieures.

Le service vSphere Authentication Proxy se lie à une adresse IPv4 pour communiquer avec vCenter Server et ne prend pas en charge IPv6. L'instance de vCenter Server peut être installée sur une machine hôte dans un environnement réseau en mode IPv4 uniquement, en mode mixte IPv4/IPv6 ou en mode IPv6 uniquement, mais la machine qui se connecte à vCenter Server via vSphere Web Client doit disposer d'une adresse IPv4 pour que le service vSphere Authentication Proxy fonctionne.

Conditions préalables

- Installez Microsoft .NET Framework 3.5 sur la machine sur laquelle vous voulez installer vSphere Authentication Proxy.
- Vérifiez que vous disposez des privilèges d'administrateur.
- Vérifiez que la machine hôte est dotée d'un processeur et d'un système d'exploitation compatibles.
- Vérifiez que la machine hôte possède une adresse IPv4 valide. Vous pouvez installer vSphere Authentication Proxy sur une machine dans un environnement réseau exclusivement en mode IPv4 ou en mode mixte IPv4/IPv6, mais vous ne pouvez pas installer vSphere Authentication Proxy sur une machine dans un environnement exclusivement en mode IPv6.

- Si vous installez vSphere Authentication Proxy sur une machine hôte Windows Server 2008 R2, téléchargez et installez le correctif logiciel Windows décrit dans Windows KB Article 981506 sur le site Web support.microsoft.com. Si vous n'installez pas ce correctif, l'initialisation de vSphere Authentication Proxy Adapter échoue. Ce problème est accompagné de messages d'erreur consignés dans `camadapter.log` similaires à `Échec de la liaison du site Web CAM avec CTL` et `Échec de l'initialisation de CAMAdapter`.
- Téléchargez le programme d'installation vCenter Server.

Collectez les informations suivantes pour terminer l'installation ou la mise à niveau :

- L'emplacement d'installation de vSphere Authentication Proxy si vous n'utilisez pas l'emplacement par défaut.
- L'adresse et les informations d'identification du vCenter Server auquel vSphere Authentication Proxy doit se connecter : adresse IP ou nom, port HTTP, nom d'utilisateur et mot de passe.
- Le nom d'hôte ou l'adresse IP pour identifier vSphere Authentication Proxy sur le réseau.

Procédure

- 1 Ajoutez au domaine la machine hôte sur laquelle vous aller installer le service proxy d'authentification.
- 2 Utilisez le compte Administrateur de domaine pour vous connecter à la machine hôte.
- 3 Dans l'inventaire du logiciel d'installation, faites un double clic sur le fichier `autorun.exe` pour lancer l'installation.
- 4 Sélectionnez **VMware vSphere Authentication Proxy** et cliquez sur **Installer**.
- 5 Suivez les invites de l'assistant pour terminer l'installation ou la mise à niveau.

Au cours de l'installation, le service d'authentification s'enregistre dans l'instance vCenter Server où Auto Deploy est enregistré.

Résultats

Lorsque vous installez le service vSphere Authentication Proxy, le programme d'installation crée un compte de domaine avec les privilèges appropriés pour exécuter le service proxy d'authentification. Le nom de compte commence par le préfixe `CAM-` et est associé à un mot de passe à 32 caractères généré de façon aléatoire. Le mot de passe n'expire jamais. Ne changez pas les paramètres du généraux.

Configurer un hôte pour utiliser Active Directory

Vous pouvez configurer un hôte pour utiliser un service d'annuaire comme Active Directory afin de gérer les groupes de travail et les utilisateurs.

Lorsque vous ajoutez un hôte ESXi à Active Directory, le groupe DOMAIN **ESX Admins** obtient un accès administratif complet à l'hôte s'il existe. Si vous ne voulez pas rendre disponible l'accès administratif complet, consultez l'article 1025569 de la base de connaissances VMware pour une solution.

Si un hôte est provisionné avec Auto Deploy, les informations d'identification Active Directory ne peuvent pas être stockées sur les hôtes. Vous pouvez utiliser vSphere Authentication Proxy pour joindre l'hôte à un domaine Active Directory. Comme une chaîne d'approbation existe entre vSphere Authentication Proxy et l'hôte, Authentication Proxy peut joindre l'hôte au domaine Active Directory. Reportez-vous à [Utiliser vSphere Authentication Proxy](#).

Note Lorsque vous définissez des paramètres de comptes d'utilisateurs dans Active Directory, vous pouvez limiter les ordinateurs auxquels un utilisateur peut se connecter en fonction du nom de ces ordinateurs. Par défaut, aucune restriction équivalente n'est définie pour un compte utilisateur. Si vous définissez cette limitation, les demandes Bind LDAP pour le compte d'utilisateur échouent avec le message LDAP `binding not successful`, même si la demande provient d'un ordinateur référencé. Vous pouvez éviter ce problème en ajoutant le nom netBIOS du serveur Active Directory à la liste des ordinateurs auxquels le compte utilisateur peut se connecter.

Conditions préalables

- Vérifiez que vous disposez d'un domaine Active Directory. Reportez-vous à la documentation de votre serveur d'annuaire.
- Assurez-vous que le nom d'hôte d'ESXi est complet et inclut le nom de domaine de la forêt Active Directory.

fully qualified domain name = host_name.domain_name

Procédure

- 1 Synchronisez le temps entre ESXi et le système de service d'annuaire en utilisant NTP.
Consultez la base des connaissances [Synchroniser les horloges ESXi avec un serveur de temps réseau](#) ou la base des connaissances VMware pour plus d'informations sur la synchronisation de l'heure ESXi avec un contrôleur de domaine Microsoft.
- 2 Assurez-vous que les serveurs DNS que vous avez configurés pour l'hôte peuvent résoudre les noms d'hôtes des contrôleurs Active Directory.
 - a Accédez à l'hôte dans le navigateur d'objets de vSphere Web Client.
 - b Cliquez sur l'onglet **Gérer**, puis cliquez sur **Mise en réseau**.
 - c Cliquez sur DNS et vérifiez que le nom de l'hôte et les informations sur le serveur DNS de l'hôte sont corrects.

Étape suivante

Utilisez vSphere Web Client pour rejoindre un domaine de service d'annuaire. Pour les hôtes provisionnés avec Auto Deploy, configurez vSphere Authentication Proxy. Reportez-vous à [Utiliser vSphere Authentication Proxy](#).

Ajouter un hôte à un domaine de service d'annuaire

Pour que votre hôte utilise un service d'annuaire, vous devez joindre l'hôte au domaine du service d'annuaire.

Vous pouvez entrer le nom de domaine de l'une des deux façons suivantes :

- **name.tld** (par exemple, **domain.com**): Le compte est créé sous le récipient par défaut.
- **name.tld/container/path** (par exemple, **domain.com/OU1/OU2**) : Le compte est créé sous une unité d'organisation (OU) précise.

Pour utiliser le service vSphere Authentication Proxy, consultez [Utiliser vSphere Authentication Proxy](#).

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sous Système, sélectionnez **Services d'authentification**.
- 4 Cliquez sur **Joindre le domaine**.
- 5 Entrez un domaine.
Utilisez le format **name.tld** ou **name.tld/container/path**.
- 6 Entrez le nom d'utilisateur et le mot de passe d'un utilisateur service d'annuaire autorisé à lier l'hôte au domaine, puis cliquez sur **OK**.
- 7 (Facultatif) Si vous avez l'intention d'utiliser un proxy d'authentification, entrez l'adresse IP du serveur proxy.
- 8 Cliquez sur **OK** pour fermer la boîte de dialogue Configuration des services d'annuaire.

Afficher les paramètres du service d'annuaire

Vous pouvez afficher le type de serveur d'annuaire, le cas échéant, que l'hôte utilise pour authentifier les utilisateurs et les paramètres du serveur d'annuaire.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.

3 Sous Système, sélectionnez **Services d'authentification**.

La page Services d'authentification affiche le service d'annuaire et les paramètres du domaine.

Utiliser vSphere Authentication Proxy

Lorsque vous utilisez vSphere Authentication Proxy, il est inutile de transmettre les données d'identification Active Directory à l'hôte. Les utilisateurs entrent le nom de domaine du serveur Active Directory et l'adresse IP du serveur proxy d'authentification lorsqu'ils ajoutent un hôte à un domaine.

Lorsqu'il est employé conjointement avec Auto Deploy, vSphere Authentication Proxy s'avère particulièrement utile. Vous configurez un hôte de référence pointant vers vSphere Authentication Proxy, ainsi qu'une règle appliquant le profil de l'hôte de référence à tout hôte ESXi provisionné avec Auto Deploy. Même si vous exploitez vSphere Authentication Proxy dans un environnement utilisant des certificats provisionnés par VMCA ou des certificats tiers, le processus se déroule de manière transparente dans la mesure où vous suivez les instructions d'utilisation des certificats personnalisés avec Auto Deploy. Reportez-vous à [Utiliser des certificats personnalisés avec Auto Deploy](#).

Note Vous ne pouvez pas utiliser vSphere Authentication Proxy dans un environnement qui prend uniquement en charge IPv6.

Installer ou mettre à niveau vSphere Authentication Proxy

Installez vSphere Authentication Proxy pour permettre aux hôtes ESXi de rejoindre un domaine sans utiliser les informations d'identification Active Directory. vSphere Authentication Proxy renforce la sécurité des hôtes démarrés par PXE et des hôtes provisionnés à l'aide d'Auto Deploy en évitant de stocker les informations d'identification Active Directory dans la configuration de l'hôte.

Si une version antérieure de vSphere Authentication Proxy est installée sur votre système, cette procédure met à niveau vSphere Authentication Proxy vers la version actuelle.

Vous pouvez installer vSphere Authentication Proxy sur la même machine que le système vCenter Server associé ou sur une machine différente disposant d'une connexion réseau à vCenter Server. vSphere Authentication Proxy est pris en charge par vCenter Server version 5.0 et versions ultérieures.

Le service vSphere Authentication Proxy se lie à une adresse IPv4 pour communiquer avec vCenter Server et ne prend pas en charge IPv6. L'instance de vCenter Server peut être installée sur une machine hôte dans un environnement réseau en mode IPv4 uniquement, en mode mixte IPv4/IPv6 ou en mode IPv6 uniquement, mais la machine qui se connecte à vCenter Server via vSphere Web Client doit disposer d'une adresse IPv4 pour que le service vSphere Authentication Proxy fonctionne.

Conditions préalables

- Installez Microsoft .NET Framework 3.5 sur la machine sur laquelle vous voulez installer vSphere Authentication Proxy.
- Vérifiez que vous disposez des privilèges d'administrateur.
- Vérifiez que la machine hôte est dotée d'un processeur et d'un système d'exploitation compatibles.
- Vérifiez que la machine hôte possède une adresse IPv4 valide. Vous pouvez installer vSphere Authentication Proxy sur une machine dans un environnement réseau exclusivement en mode IPv4 ou en mode mixte IPv4/IPv6, mais vous ne pouvez pas installer vSphere Authentication Proxy sur une machine dans un environnement exclusivement en mode IPv6.
- Si vous installez vSphere Authentication Proxy sur une machine hôte Windows Server 2008 R2, téléchargez et installez le correctif logiciel Windows décrit dans Windows KB Article 981506 sur le site Web support.microsoft.com. Si vous n'installez pas ce correctif, l'initialisation de vSphere Authentication Proxy Adapter échoue. Ce problème est accompagné de messages d'erreur consignés dans `camadapter.log` similaires à `Échec de la liaison du site Web CAM avec CTL` et `Échec de l'initialisation de CAMAdapter`.
- Téléchargez le programme d'installation vCenter Server.

Collectez les informations suivantes pour terminer l'installation ou la mise à niveau :

- L'emplacement d'installation de vSphere Authentication Proxy si vous n'utilisez pas l'emplacement par défaut.
- L'adresse et les informations d'identification du vCenter Server auquel vSphere Authentication Proxy doit se connecter : adresse IP ou nom, port HTTP, nom d'utilisateur et mot de passe.
- Le nom d'hôte ou l'adresse IP pour identifier vSphere Authentication Proxy sur le réseau.

Procédure

- 1 Ajoutez au domaine la machine hôte sur laquelle vous aller installer le service proxy d'authentification.
- 2 Utilisez le compte Administrateur de domaine pour vous connecter à la machine hôte.
- 3 Dans l'inventaire du logiciel d'installation, faites un double clic sur le fichier `autorun.exe` pour lancer l'installation.
- 4 Sélectionnez **VMware vSphere Authentication Proxy** et cliquez sur **Installer**.
- 5 Suivez les invites de l'assistant pour terminer l'installation ou la mise à niveau.

Au cours de l'installation, le service d'authentification s'enregistre dans l'instance vCenter Server où Auto Deploy est enregistré.

Résultats

Lorsque vous installez le service vSphere Authentication Proxy, le programme d'installation crée un compte de domaine avec les privilèges appropriés pour exécuter le service proxy d'authentification. Le nom de compte commence par le préfixe **CAM-** et est associé à un mot de passe à 32 caractères généré de façon aléatoire. Le mot de passe n'expire jamais. Ne changez pas les paramètres du généraux.

Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification

Après avoir installé le service vSphere Authentication Proxy (service CAM), vous devez configurer l'hôte pour utiliser le serveur proxy d'authentification pour authentifier les utilisateurs.

Conditions préalables

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte. Reportez-vous à [Installer ou mettre à niveau vSphere Authentication Proxy](#).

Procédure

- 1 Utilisez IIS manager sur l'hôte pour définir la plage DHCP.

Définir la plage permet aux hôtes utilisant le DHCP dans le réseau de gestion d'utiliser le service de proxy d'authentification.

Option	Action
Pour IIS 6	<ol style="list-style-type: none"> Naviguez jusqu'au Site Web de gestion des comptes d'ordinateur. Cliquez avec le bouton droit sur le répertoire virtuel CAM ISAPI. Sélectionnez Propriétés > Sécurité du répertoire > Modifier l'adresse IP et les restrictions de nom de domaine > Ajouter un groupe d'ordinateurs.
Pour IIS 7	<ol style="list-style-type: none"> Naviguez jusqu'au Site Web de gestion des comptes d'ordinateur. Cliquez sur le répertoire virtuel CAM ISAPI du volet gauche et ouvrez Adresse IPv4 et restrictions de domaine. Sélectionnez Ajouter entrée autorisée > Plage d'adresse IPv4.

- 2 Si un hôte n'est pas provisionné par Auto Deploy, remplacez le certificat SSL par défaut par un certificat auto-signé ou par un certificat signé par une autorité de certification (CA) privée.

Option	Description
Certificat d'autorité de certification VMware (VMCA)	<p>Si vous utilisez les certificats signés par VMCA par défaut, vous devez vous assurer que l'hôte proxy d'authentification approuve le certificat VMCA.</p> <ol style="list-style-type: none"> Ajoutez manuellement le certificat VMCA au magasin de certificats des autorités de certification racine approuvées. Ajoutez le certificat signé par VMCA (<code>root.cer</code>) au magasin local des certificats de confiance sur le système sur lequel le service proxy d'authentification est installé. Vous trouverez le fichier dans <code>C:\ProgramData\VMware\CIS\data\vmca</code>. Redémarrez le service vSphere Authentication Proxy.
Certificat signé par l'autorité de certification tierce	<p>Ajoutez le certificat signé par l'autorité de certification (codé DER) au magasin local des certificats de confiance sur le système sur lequel le service proxy d'authentification est installé et redémarrez le service vSphere Authentication Proxy.</p> <ul style="list-style-type: none"> ■ Pour Windows 2003, copiez le fichier du certificat sur <code>C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust</code>. ■ Pour Windows 2008, copiez le fichier du certificat sur <code>C:\Program Data\VMware\vSphere Authentication Proxy\trust</code>.

Configuration de vSphere Authentication Proxy

Vos hôtes ESXi peuvent utiliser vSphere Authentication Proxy s'ils disposent des informations de certificat associées.

Vous ne devez authentifier le serveur qu'une seule fois.

Note ESXi et le serveur vSphere Authentication Proxy doivent être en mesure de s'authentifier. Assurez-vous que cette fonction d'authentification est toujours activée. Si vous désactivez l'authentification, vous pouvez utiliser la boîte de dialogue Paramètres avancés pour définir l'attribut `UserVars.ActiveDirectoryVerifyCAMCertificate` sur 0.

Exporter le certificat de vSphere Authentication Proxy

Pour authentifier vSphere Authentication Proxy dans ESXi, vous devez fournir à ESXi le certificat du serveur proxy.

Conditions préalables

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte. Reportez-vous à [Installer ou mettre à niveau vSphere Authentication Proxy](#).

Procédure

- 1 Sur le système du serveur proxy d'authentification, utilisez IIS Manager pour exporter le certificat.

Option	Action
Pour IIS 6	<ol style="list-style-type: none"> a Cliquez avec le bouton droit de la souris sur Site Web de gestion des comptes d'ordinateur. b Sélectionnez Propriétés > Sécurité d'annuaire > Afficher le certificat.
Pour IIS 7	<ol style="list-style-type: none"> a Cliquez sur Site Web de gestion des comptes d'ordinateur dans le volet de gauche. b Sélectionnez Liaisons pour ouvrir la boîte de dialogue Liaisons de sites. c Sélectionnez la liaison https. d Sélectionnez Éditer > Afficher le certificat SSL.

- 2 Sélectionnez **Détails > Copier vers un fichier**.
- 3 Sélectionnez les options **Ne pas exporter la clé privée** et **X.509 codé en base 64 (CER)**.

Étape suivante

Importez le certificat vers ESXi.

Importer un certificat de serveur proxy dans ESXi

Pour authentifier le serveur vSphere Authentication Proxy dans ESXi, téléchargez le certificat du serveur proxy à ESXi.

Vous pouvez utiliser l'interface utilisateur de vSphere Web Client pour charger le certificat du serveur vSphere Authentication Proxy sur l'hôte ESXi.

Conditions préalables

Installez le service vSphere Authentication Proxy (service CAM) sur un hôte. Reportez-vous à [Installer ou mettre à niveau vSphere Authentication Proxy](#).

Exportez le certificat du serveur vSphere Authentication Proxy comme décrit dans [Exporter le certificat de vSphere Authentication Proxy](#).

Procédure

- 1 Accédez à l'hôte, cliquez sur l'onglet **Gérer**, cliquez sur **Paramètres**, puis sur **Services d'authentification**.
- 2 Cliquez sur **Importer un certificat**.
- 3 Entrez le chemin complet du certificat du serveur proxy d'authentification sur l'hôte et l'adresse IP du serveur proxy d'authentification.
Utilisez le format `[datastore name] file path` pour entrer le chemin d'accès au serveur proxy.
- 4 Cliquez sur **OK**.

Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine

Lorsque vous joignez un hôte à un domaine de service d'annuaire, vous pouvez utiliser le serveur vSphere Authentication Proxy pour l'authentification au lieu de transmettre les informations d'identification Active Directory fournies par l'utilisateur.

Vous pouvez entrer le nom de domaine de l'une des deux façons suivantes :

- **name.tld** (par exemple, **domain.com**): Le compte est créé sous le récipient par défaut.
- **name.tld/container/path** (par exemple, **domain.com/OU1/OU2**) : Le compte est créé sous une unité d'organisation (OU) précise.

Conditions préalables

- Connectez-vous à un système vCenter Server avec vSphere Web Client.
- Si ESXi est configuré avec une adresse DHCP, configurez une plage DHCP.
- Si ESXi est configuré avec une adresse IP statique, vérifiez que son profil associé est configuré pour utiliser le service vSphere Authentication Proxy pour rejoindre un domaine afin que le serveur proxy d'authentification puisse faire confiance à l'adresse IP ESXi.
- Si ESXi utilise un certificat signé par VMCA, vérifiez que l'hôte a été ajouté à vCenter Server. Ainsi, le serveur proxy d'authentification peut faire confiance à ESXi.
- Si ESXi utilise un certificat signé par une autorité de certification et qu'il n'est pas provisionné par Auto Deploy, vérifiez que le certificat de l'autorité de certification a été ajouté au magasin local des certificats de confiance du serveur proxy d'authentification, comme décrit dans [Configurer un hôte pour utiliser vSphere Authentication Proxy pour l'authentification](#).
- Authentifiez le serveur vSphere Authentication Proxy sur l'hôte.

Procédure

- 1 Accédez à l'hôte dans vSphere Web Client et cliquez sur l'onglet **Gérer**.
- 2 Cliquez sur **Paramètres** et sélectionnez **Services d'authentification**.
- 3 Cliquez sur **Joindre le domaine**.
- 4 Entrez un domaine.
Utilisez le format **name.tld** ou **name.tld/container/path**.
- 5 Sélectionnez **Utilisation du serveur proxy**.
- 6 Entrez l'adresse IP du serveur proxy d'authentification.
- 7 Cliquez sur **OK**.

Remplacer le certificat du serveur proxy d'authentification de l'hôte ESXi

Vous pouvez importer le certificat d'une autorité de certification approuvée à partir de vSphere Web Client

Conditions préalables

- Téléchargez le fichier de certificat du serveur proxy d'authentification sur l'hôte ESXi.

Procédure

- 1 Dans vSphere Web Client, sélectionnez l'hôte ESXi.
- 2 Dans l'onglet **Paramètres**, sélectionnez **Services d'authentification** dans la zone **Système**.
- 3 Cliquez sur **Importer un certificat**.
- 4 Entrez le chemin du certificat SSL et le serveur vSphere Authentication Proxy.

Meilleures pratiques de sécurité de ESXi

Suivez les recommandations de sécurité ESXi pour garantir l'intégrité de votre déploiement vSphere. Pour plus d'informations, consultez le *Guide de sécurisation renforcée*.

Vérifier le support d'installation

Vérifiez toujours le hachage du fichier après le téléchargement d'une offre groupée hors ligne ISO ou d'un correctif pour garantir l'intégrité et l'authenticité des fichiers téléchargés. Si vous obtenez des supports physiques de VMware et si le sceau de sécurité a été rompu, retournez le logiciel à VMware en demandant son remplacement.

Après avoir téléchargé le support, utilisez la somme MD5 pour vérifier l'intégrité du téléchargement. Comparez la somme MD5 à la valeur diffusée sur le site Web de VMware. Chaque système d'exploitation a une méthode et un outil différents pour vérifier les sommes MD5. Pour Linux, utilisez la commande « md5sum ». Pour Microsoft Windows, vous pouvez télécharger un produit complémentaire

Vérifier les CRL manuellement

Par défaut, un hôte ESXi ne prend pas en charge la vérification des listes de révocation de certificats (CRL). Vous devez rechercher et supprimer manuellement les certificats révoqués. Ces certificats sont généralement des certificats personnalisés générés à partir d'une autorité de certification d'entreprise ou d'une autorité de certification tierce. De nombreuses entreprises utilisent des scripts pour trouver et remplacer les certificats SSL révoqués sur des hôtes ESXi.

Surveiller le groupe Active Directory ESX Admins

Le groupe Active Directory utilisé par vSphere est défini par le paramètre système avancé `plugins.hostsvc.esxAdminsGroup`. Par défaut, cette option est définie sur ESX Admins. Tous les membres du groupe ESX Admins obtiennent un accès administratif complet à tous les hôtes ESXi du domaine. Surveillez Active Directory pour la création de ce groupe et limitez l'appartenance aux utilisateurs et aux groupes hautement approuvés.

Surveiller les fichiers de configuration

Bien que la plupart des paramètres de configuration ESXi soient contrôlés par une API, un nombre limité de fichiers de configuration affecte l'hôte directement. Ces fichiers sont exposés par l'API de transfert de fichiers vSphere qui utilise HTTPS. Si vous apportez des modifications à ces fichiers, vous devez également effectuer l'action administrative correspondante (par exemple, apporter une modification de configuration).

Note Ne tentez pas de surveiller des fichiers qui ne sont pas exposés via cette API de transfert de fichiers.

Utiliser vmkfstools pour effacer les données sensibles

Lorsque vous supprimez un fichier VMDK contenant des données sensibles, éteignez ou arrêtez la machine virtuelle, puis exécutez la commande vCLI `vmkfstools --writezeros` sur ce fichier. Vous pouvez ensuite supprimer le fichier de la banque de données.

Périphériques PCI et PCIe et ESXi

L'utilisation de la fonctionnalité de VMware DirectPath I/O pour relayer un périphérique PCI ou PCIe vers une machine virtuelle crée une vulnérabilité de sécurité potentielle. La vulnérabilité peut être déclenchée par un code bogué ou malveillant tel qu'un pilote de périphérique qui s'exécuterait en mode privilégié dans le système d'exploitation invité. Le matériel et les microprogrammes standard actuels n'assurent pas un niveau suffisant de confinement des erreurs suffisant pour permettre à ESXi d'entièrement neutraliser la vulnérabilité.

VMware recommande d'utiliser un relais PCI ou PCIe vers une machine virtuelle uniquement si la machine virtuelle est détenue et administrée par une entité approuvée. Vous devez vous assurer que cette entité ne tente pas de bloquer ou d'exploiter l'hôte depuis la machine virtuelle.

Votre hôte peut être compromis de l'une des manières suivantes.

- Le système d'exploitation invité peut générer une erreur PCI ou PCIe irrécupérable. Une telle erreur n'altère pas les données, mais peut bloquer l'hôte ESXi. De telles erreurs peuvent se produire en raison de bogues et d'incompatibilités dans les périphériques matériels qui sont relayés, ou en raison de problèmes de pilotes du système d'exploitation invité.
- Le système d'exploitation invité peut générer une opération DMA (Direct Memory Access) qui provoque une erreur de page IOMMU sur l'hôte ESXi, par exemple, si l'opération DMA cible une adresse située hors de la mémoire de la machine virtuelle. Sur certaines machines, le microprogramme de l'hôte configure les fautes IOMMU pour signaler une erreur irrémédiable via une interruption non-masquable (NMI), ce qui entraîne le blocage de l'hôte ESXi. Ce problème peut être dû à des dysfonctionnements de pilotes du système d'exploitation invité.
- Si le système d'exploitation sur l'hôte ESXi n'utilise pas le remappage d'interruption, le système d'exploitation invité peut injecter une interruption fallacieuse dans l'hôte ESXi sur n'importe quel vecteur. ESXi utilise actuellement le remappage d'interruptions sur les plates-

formes Intel offrant cette possibilité ; le remappage d'interruption fait partie de l'ensemble de fonctionnalités Intel VT-d. ESXi n'utilise pas le mappage d'interruptions sur les plates-formes AMD. Une interruption fallacieuse est susceptible de provoquer le blocage de l'hôte ESXi ; cependant, il peut théoriquement exister d'autres manières d'exploiter ces interruptions.

Configuration de l'authentification par carte à puce pour ESXi

Vous pouvez utiliser l'authentification par carte à puce pour vous connecter à l'interface utilisateur de la console directe (DCUI, Direct Console User Interface) ESXi à l'aide d'une carte à puce PIV (Personal Identity Verification), CAC (Common Access Card) ou SC650 au lieu de l'invite par défaut permettant d'entrer un nom d'utilisateur et un mot de passe.

Une carte à puce est une petite carte en plastique dotée d'une puce de circuit intégré. Beaucoup d'organismes publics et de grandes entreprises utilisent l'authentification à deux facteurs basée sur carte à puce pour renforcer la sécurité de leurs systèmes et respecter les réglementations de sécurité.

Lorsque l'authentification par carte à puce est activée sur un hôte ESXi, l'interface DCUI vous invite à entrer une combinaison valide de carte à puce et de PIN au lieu de l'invite par défaut qui vous demande d'entrer un nom d'utilisateur et un mot de passe.

- 1 Lorsque vous insérez la carte à puce dans le lecteur de carte à puce, l'hôte ESXi lit les informations d'identification qui s'y trouvent.
- 2 L'interface DCUI ESXi affiche votre ID de connexion et vous invite à entrer votre PIN.
- 3 Une fois que vous avez entré le PIN, l'hôte ESXi établit la correspondance entre celui-ci et le PIN stocké sur la carte à puce et vérifie le certificat de la carte à puce à l'aide d'Active Directory.
- 4 Une fois le certificat de la carte à puce vérifié, ESXi vous connecte à l'interface DCUI.

Si vous préférez passer à l'authentification par nom d'utilisateur et mot de passe via l'interface DCUI, appuyez sur F3.

La puce de la carte se verrouille si vous entrez plusieurs codes PIN incorrects consécutifs (trois, en général). Si une carte à puce est verrouillée, seul le personnel sélectionné peut la déverrouiller.

Activer l'authentification par carte à puce

Activez l'authentification par carte à puce afin de demander aux utilisateurs d'entrer une combinaison de carte à puce et de PIN pour se connecter à l'interface DCUI ESXi.

Conditions préalables

- Configurez l'infrastructure de manière à prendre en charge l'authentification par carte à puce, avec par exemple des comptes dans le domaine Active Directory, des lecteurs de cartes à puce et des cartes à puce.

- Configurez ESXi pour joindre un domaine Active Directory qui prend en charge l'authentification par carte à puce. Pour plus d'informations, consultez [Utilisation d'Active Directory pour gérer des utilisateurs ESXi](#).
- Utilisez vSphere Web Client pour ajouter des certificats racines. Reportez-vous à [Gestion de certificats pour les hôtes ESXi](#).

Procédure

- 1 Dans vSphere Web Client, accédez à l'hôte
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sous Système, sélectionnez **Services d'authentification**.
Vous voyez l'état actuel de l'authentification par carte à puce et la liste des certificats importés.
- 4 Dans le panneau Authentification par carte à puce, cliquez sur **Modifier**.
- 5 Dans la boîte de dialogue Modifier les paramètres d'authentification par carte à puce, sélectionnez la page Certificats.
- 6 Ajoutez des certificats d'autorité de certification (CA) approuvés (certificats CA racines et intermédiaires, par exemple).
- 7 Ouvrez la page Authentification par carte à puce, cochez la case **Activer l'authentification par carte à puce** et cliquez sur **OK**.

Désactiver l'authentification par carte à puce

Désactiver l'authentification par carte à puce pour revenir à l'authentification par nom d'utilisateur et mot de passe par défaut pour la connexion à l'interface DCUI d'ESXi.

Procédure

- 1 Dans vSphere Web Client, accédez à l'hôte
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Sous Système, sélectionnez **Services d'authentification**.
Vous voyez l'état actuel de l'authentification par carte à puce et la liste des certificats importés.
- 4 Dans le panneau Authentification par carte à puce, cliquez sur **Modifier**.
- 5 Sur la page Authentification par carte à puce, décochez la case **Activer l'authentification par carte à puce**, puis cliquez sur **OK**.

Authentification d'informations d'identification d'utilisateur en cas de problèmes de connectivité

Si le serveur de domaine Active Directory (AD) n'est pas accessible, vous pouvez vous connecter à l'interface DCUI ESXi avec l'authentification par nom d'utilisateur et mot de passe pour réaliser des opérations de secours sur l'hôte.

Exceptionnellement, il est possible que le serveur de domaine AD ne soit pas accessible pour authentifier les informations d'identification de l'utilisateur sur la carte à puce, par exemple suite à des problèmes de connectivité, à une panne de réseau ou à un sinistre. En cas de perte de connexion avec le serveur AD, vous pouvez vous connecter à l'interface DCUI ESXi à l'aide des informations d'identification de l'utilisateur ESXi local. Cela vous permet d'effectuer des diagnostics et d'autres opérations de secours. Le recours à la connexion par nom d'utilisateur et mot de passe est consigné. Une fois la connectivité avec Active Directory restaurée, l'authentification par carte à puce est réactivée.

Note La perte de connectivité réseau avec vCenter Server n'affecte pas l'authentification par carte à puce si le serveur de domaine Active Directory (AD) est disponible.

Utilisation de l'authentification par carte à puce en mode de verrouillage

Lorsqu'il est activé, le mode de verrouillage sur l'hôte ESXi renforce la sécurité de l'hôte et limite l'accès à l'interface DCUI. Le mode de verrouillage peut désactiver la fonctionnalité d'authentification par carte à puce.

En mode de verrouillage normal, seuls les utilisateurs répertoriés dans la liste des utilisateurs exceptionnels et disposant de privilèges d'administration peuvent accéder à l'interface DCUI. Les utilisateurs exceptionnels sont des utilisateurs locaux d'un hôte ou des utilisateurs Active Directory disposant d'autorisations définies localement pour l'hôte ESXi. Si vous souhaitez utiliser l'authentification par carte à puce en mode de verrouillage normal, vous devez ajouter les utilisateurs à la liste des utilisateurs exceptionnels à partir de vSphere Web Client. Lorsque l'hôte passe en mode de verrouillage normal, ces utilisateurs ne perdent pas leurs autorisations et peuvent se connecter à l'interface DCUI. Pour plus d'informations, consultez [Spécifier les utilisateurs exceptionnels du mode de verrouillage](#).

En mode de verrouillage strict, le service DCUI est interrompu. Il est donc impossible d'utiliser l'authentification par carte à puce pour accéder à l'hôte.

Clés SSH ESXi

Vous pouvez utiliser des clés SSH pour restreindre, contrôler et sécuriser l'accès à un hôte ESXi. En utilisant une clé SSH, vous pouvez permettre à des utilisateurs ou des scripts approuvés de se connecter à un hôte sans spécifier le mot de passe.

Vous pouvez copier la clé SSH sur l'hôte en utilisant la commande `vifs` de l'interface de ligne de commande vSphere. Pour obtenir des informations sur l'installation et l'utilisation de l'ensemble de commandes de l'interface de ligne de commande vSphere, reportez-vous à *Démarrage avec les interfaces de ligne de commande vSphere*. Il est également possible d'utiliser HTTPS PUT pour copier la clé SSH sur l'hôte.

Au lieu de générer les clés en externe et de les télécharger, vous pouvez les créer sur l'hôte ESXi et les télécharger. Reportez-vous à l'article [1002866](#) de la base de connaissances VMware.

L'activation de SSH et l'ajout de clés SSH à l'hôte comportent des risques inhérents et ne sont pas recommandés dans un environnement sécurisé. Reportez-vous à la section [Désactiver les clés autorisées \(SSH\)](#).

Note Dans ESXi 5.0 et versions ultérieures, un utilisateur disposant d'une clé SSH peut accéder à l'hôte même lorsque ce dernier est en mode verrouillage. Ce problème est résolu dans ESXi 5.1.

Sécurité SSH

Vous pouvez utiliser SSH pour vous connecter à distance au ESXi Shell et accomplir des tâches de dépannage pour l'hôte.

La configuration SSH d'ESXi est améliorée et offre un haut niveau de sécurité.

Désactivation de la version 1 du protocole SSH

VMware ne prend pas en charge la version 1 du protocole SSH . Il utilise désormais exclusivement la version 2. La version 2 permet d'éliminer certains problèmes de sécurité qui se produisaient dans la version 1 et offre une communication plus sûre grâce à l'interface de gestion.

Chiffrement renforcé

Pour les connexions, SSH ne prend en charge que les chiffrements AES 256 bits et 128 bits.

Ces paramètres sont destinés à assurer une protection renforcée des données transmises à l'interface de gestion via SSH. Vous ne pouvez pas modifier ces paramètres.

Charger une clé SSH à l'aide d'une commande vifs

Si vous décidez d'utiliser des clés autorisées pour vous connecter à un hôte avec SSH, vous pouvez télécharger des clés autorisées avec une commande `vifs`.

Note Du fait que les clés autorisées permettent l'accès SSH sans nécessiter l'authentification de l'utilisateur, demandez-vous vraiment si vous voulez utiliser des clés SSH dans votre environnement.

Les clés autorisées vous permettent d'authentifier un accès distant à un hôte. Lorsque des utilisateurs ou des scripts essaient d'accéder à un hôte avec SSH, la clé fournit l'authentification sans mot de passe. Les clés autorisées vous permettent d'automatiser l'authentification, ce qui est utile lorsque vous écrivez des scripts pour réaliser des tâches routinières.

Vous pouvez télécharger les types de clés SSH suivants sur un hôte.

- Fichier de clés autorisées pour un utilisateur racine
- Clé RSA
- Clé RSA publique

À partir de vSphere 6.0 Update 2, les clés DSS/DSA ne sont plus prises en charge.

Important Ne modifiez pas le fichier `/etc/ssh/sshd_config`.

Procédure

- ◆ Sur la ligne de commande ou un serveur d'administration, utilisez la commande `vifs` pour télécharger la clé SSH dans l'emplacement approprié sur l'hôte ESXi.

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

Type de clés :	Emplacement
Fichiers de clés autorisées pour un utilisateur racine	/host/ssh_root_authorized_keys Vous devez bénéficier de tous les privilèges Administrateur pour télécharger ce fichier.
Clés RSA	/host/ssh_host_rsa_key
Clés RSA publiques	/host/ssh_host_rsa_key_pub

Charger une clé SSH à l'aide de HTTPS PUT

Vous pouvez utiliser des clés autorisées pour ouvrir une session sur un hôte avec SSH. Vous pouvez charger les clés autorisées à l'aide de HTTPS PUT.

Les clés autorisées vous permettent d'authentifier un accès distant à un hôte. Lorsque des utilisateurs ou des scripts essaient d'accéder à un hôte avec SSH, la clé fournit l'authentification sans mot de passe. Les clés autorisées vous permettent d'automatiser l'authentification, ce qui est utile lorsque vous écrivez des scripts pour réaliser des tâches routinières.

Vous pouvez télécharger les types de clés SSH suivants sur un hôte à l'aide de HTTPS PUT :

- Fichier de clés autorisées pour un utilisateur racine
- Clé DSA
- Clé DSA publique
- Clé RSA
- Clé RSA publique

Important Ne modifiez pas le fichier `/etc/ssh/sshd_config`.

Procédure

- 1 Dans votre application de chargement, ouvrez le fichier de clé.

2 Publiez le fichier aux emplacements suivants.

Type de clés :	Emplacement
Fichiers de clés autorisées pour un utilisateur racine	<code>https://hostname_or_IP_address/host/ssh_root_authorized_keys</code> Vous devez disposer de tous les privilèges Administrateur sur l'hôte pour télécharger ce fichier.
Clés DSA	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key</code>
Clés DSA publiques	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key_pub</code>
Clés RSA	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
Clés RSA publiques	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

Utilisation du ESXi Shell

Le ESXi Shell est désactivé par défaut sur les hôtes ESXi. Vous pouvez activer l'accès local et distant au shell si nécessaire.

Pour réduire le risque d'accès non autorisé, activez ESXi Shell pour le dépannage uniquement.

Le ESXi Shell est indépendant du mode verrouillage. Même si l'hôte s'exécute en mode verrouillage, vous pouvez toujours vous connecter au ESXi Shell si ce service est activé.

ESXi Shell

Activez ce service pour accéder localement au ESXi Shell.

SSH

Activez ce service pour accéder à ESXi Shell à distance en utilisant SSH.

Reportez-vous à *Sécurité vSphere*.

L'utilisateur racine et les utilisateurs disposant du rôle d'administrateur peuvent accéder au ESXi Shell. Les utilisateurs du groupe Active Directory ESX Admins reçoivent automatiquement le rôle d'Administrateur. Par défaut, seul l'utilisateur racine peut exécuter des commandes système (telles que `vmware -v`) en utilisant ESXi Shell.

Note N'activez pas le ESXi Shell si n'avez pas réellement besoin d'un accès.

■ Utiliser vSphere Web Client pour activer l'accès à ESXi Shell

Vous pouvez utiliser vSphere Web Client pour activer un accès local et distant (SSH) au service ESXi Shell et pour définir le délai d'attente d'inactivité et le délai d'attente de disponibilité.

- [Utiliser l'interface utilisateur de la console directe \(DCUI\) pour activer l'accès au service ESXi Shell](#)

L'interface utilisateur de la console directe (DCUI) vous permet d'interagir avec l'hôte localement en utilisant des menus textuels. Évaluez avec soin si les exigences de votre environnement en matière de sécurité permettent l'activation de l'interface utilisateur de la console directe (DCUI).

- [Connexion au ESXi Shell pour une opération de dépannage](#)

Effectuez des tâches de configuration d'ESXi avec vSphere Web Client, vSphere CLI ou vSphere PowerCLI. Connectez-vous au ESXi Shell (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Utiliser vSphere Web Client pour activer l'accès à ESXi Shell

Vous pouvez utiliser vSphere Web Client pour activer un accès local et distant (SSH) au service ESXi Shell et pour définir le délai d'attente d'inactivité et le délai d'attente de disponibilité.

Note Accédez à l'hôte à l'aide de vSphere Web Client, d'outils de ligne de commande à distance (vCLI et PowerCLI) et d'API publiées. N'activez pas l'accès à distance à l'hôte à l'aide de SSH, sauf si des circonstances spéciales imposent l'activation de l'accès SSH.

Conditions préalables

Si vous souhaitez utiliser une clé SSH autorisée, vous pouvez la télécharger. Reportez-vous à la section [Clés SSH ESXi](#).

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans **Système**, sélectionnez **Profil de sécurité**.
- 4 Dans le panneau **Services**, cliquez sur **Modifier**.
- 5 Sélectionnez un service dans la liste.
 - ESXi Shell
 - SSH
 - IU de Direct Console
- 6 Cliquez sur **Détails du service** et sélectionnez la règle de démarrage **Démarrer et arrêter manuellement**.

Lorsque vous sélectionnez **Démarrer et arrêter manuellement**, le service ne démarre pas lorsque vous redémarrez l'hôte. Si vous voulez démarrer le service lors du redémarrage de l'hôte, sélectionnez **Démarrer et arrêter avec hôte**.
- 7 Sélectionnez **Démarrer** pour activer le service.

8 Cliquez sur **OK**.

Étape suivante

Définissez le délai d'attente de disponibilité et le délai d'inactivité pour ESXi Shell. Reportez-vous à [Créer un délai d'attente de disponibilité pour ESXi Shell dans vSphere Web Client](#) et [Créer un délai d'expiration pour les sessions ESXi Shell inactives dans vSphere Web Client](#)

Créer un délai d'attente de disponibilité pour ESXi Shell dans vSphere Web Client

ESXi Shell est désactivé par défaut. Vous pouvez paramétrer un délai d'attente de disponibilité pour ESXi Shell pour renforcer la sécurité quand vous activez le shell.

La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne sont plus autorisés à se connecter.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans Système, sélectionnez **Paramètres système avancés**.
- 4 Sélectionnez UserVars.ESXiShellTimeOut, puis cliquez sur l'icône **Modifier**.
- 5 Saisissez le paramètre de délai d'inactivité.

Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.

- 6 Cliquez sur **OK**.

Résultats

Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Cependant, une fois que vous vous êtes déconnecté ou que votre session est terminée, les utilisateurs ne sont plus autorisés à se connecter.

Créer un délai d'expiration pour les sessions ESXi Shell inactives dans vSphere Web Client

Si un utilisateur active ESXi Shell sur un hôte mais oublie de se déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion ouverte peut augmenter les possibilités qu'une personne obtienne un accès privilégié à l'hôte. Vous pouvez éviter cela en paramétrant un délai d'expiration des sessions inactives.

Le délai d'expiration d'inactivité correspond à la période au terme de laquelle un utilisateur est déconnecté d'une session interactive inactive. Vous pouvez définir ce délai pour les sessions locales et distantes (SSH) dans l'interface de la console directe (DCUI) ou dans vSphere Web Client.

Procédure

- 1 Accédez à l'hôte dans l'inventaire de vSphere Web Client.
- 2 Cliquez sur l'onglet **Gérer** puis sur **Paramètres**.
- 3 Dans Système, sélectionnez **Paramètres système avancés**.
- 4 Sélectionnez UserVars.ESXiShellInteractiveTimeOut, cliquez sur l'icône **Modifier** et saisissez le paramètre du délai d'expiration.
- 5 Redémarrez le service ESXi Shell et le service SSH pour que le délai d'expiration prenne effet.

Résultats

Si la session est inactive, les utilisateurs sont déconnectés à l'expiration du délai d'attente.

Utiliser l'interface utilisateur de la console directe (DCUI) pour activer l'accès au service ESXi Shell

L'interface utilisateur de la console directe (DCUI) vous permet d'interagir avec l'hôte localement en utilisant des menus textuels. Évaluez avec soin si les exigences de votre environnement en matière de sécurité permettent l'activation de l'interface utilisateur de la console directe (DCUI).

Vous pouvez utiliser l'interface utilisateur de la console directe pour activer l'accès local et distant au service ESXi Shell.

Note Les modifications apportées à l'hôte en utilisant l'interface utilisateur de la console directe, vSphere Web Client, ESXCLI ou d'autres outils d'administration sont enregistrées dans un stockage permanent toutes les heures ou lors d'un arrêt dans les règles. Les modifications peuvent se perdre si l'hôte échoue avant qu'elles ne soient enregistrées.

Procédure

- 1 Dans l'interface utilisateur de la console directe, appuyez sur F2 pour accéder au menu Personnalisation du système.
- 2 Sélectionnez **Options de dépannage** et appuyez sur Entrée.
- 3 Dans le menu des options de mode de dépannage, sélectionnez un service à activer.
 - Activer ESXi Shell
 - Activer SSH
- 4 Appuyez sur Entrée pour activer le service souhaité.
- 5 Appuyez sur Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de la console directe.

Étape suivante

Définissez le délai d'attente de disponibilité et le délai d'inactivité du service ESXi Shell. Voir [Créer un délai d'attente de disponibilité pour ESXi Shell dans l'interface utilisateur de console directe](#) et [Créer un délai d'expiration pour des sessions ESXi Shell inactives](#).

Créer un délai d'attente de disponibilité pour ESXi Shell dans l'interface utilisateur de console directe

ESXi Shell est désactivé par défaut. Vous pouvez paramétrer un délai d'attente de disponibilité pour ESXi Shell pour renforcer la sécurité quand vous activez le shell.

La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Procédure

- 1 Dans le menu des options de mode de dépannage, sélectionnez **Modifier les délais d'ESXi Shell et de SSH** et cliquez sur Entrée.
- 2 Entrez le délai d'attente de disponibilité.

Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.
- 3 Appuyez sur Entrée et Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.
- 4 Cliquez sur **OK**.

Résultats

Si vous avez ouvert une session au moment de l'expiration de ce délai, elle restera ouverte. Cependant, une fois que vous vous êtes déconnecté ou que votre session est terminée, les utilisateurs ne sont plus autorisés à se connecter.

Créer un délai d'expiration pour des sessions ESXi Shell inactives

Si un utilisateur active ESXi Shell sur un hôte mais oublie de se déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion ouverte peut augmenter les possibilités qu'une personne obtienne un accès privilégié à l'hôte. Vous pouvez éviter cela en paramétrant un délai d'expiration des sessions inactives.

Le délai d'inactivité correspond au temps qui peut s'écouler avant que l'utilisateur ne soit déconnecté d'une session interactive inactive. Les modifications du délai d'inactivité s'appliquent lors de la prochaine connexion de l'utilisateur à ESXi Shell et n'affectent pas les sessions existantes.

Vous pouvez spécifier le délai d'expiration en secondes dans l'interface DCUI (Direct Console User Interface) ou en minutes dans vSphere Web Client.

Procédure

- 1 Dans le menu des options de mode de dépannage, sélectionnez **Modifier les délais d'ESXi Shell et de SSH** et cliquez sur Entrée.

2 Entrez le délai d'expiration en secondes.

Vous devez redémarrer le service SSH et le service ESXi Shell pour que le délai soit pris en compte.

3 Appuyez sur Entrée et Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

Résultats

Si la session est inactive, les utilisateurs sont déconnectés à l'expiration du délai d'attente.

Connexion au ESXi Shell pour une opération de dépannage

Effectuez des tâches de configuration d'ESXi avec vSphere Web Client, vSphere CLI ou vSphere PowerCLI. Connectez-vous au ESXi Shell (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Procédure

1 Connectez-vous au ESXi Shell en utilisant l'une des méthodes suivantes.

- Si vous avez un accès direct à l'hôte, appuyez sur la combinaison de touches Alt+F1 pour ouvrir la page de connexion de la console physique de la machine.
- Si vous vous connectez à l'hôte à distance, utilisez SSH ou une autre connexion à distance pour ouvrir une session sur l'hôte.

2 Entrez un nom d'utilisateur et un mot de passe reconnus par l'hôte.

Modifier les paramètres proxy Web ESXi

Lorsque vous modifiez les paramètres proxy Web, vous devez prendre en compte plusieurs recommandations de sécurité utilisateur et de chiffrement.

Note Redémarrez le processus hôte après avoir modifié les répertoires hôtes ou les mécanismes d'authentification.

- Ne configurez aucun certificat utilisant un mot de passe ou une phrase secrète. ESXi ne prend pas en charge les proxies Web qui utilisent des mots de passe ou des phrases secrètes (également appelés « clés chiffrées »). Si vous configurez un proxy Web qui nécessite un mot de passe ou une phrase secrète, les processus ESXi ne peuvent pas démarrer correctement.
- Pour assurer la prise en charge du chiffrement des noms d'utilisateur, des mots de passe et des paquets, SSL est activé par défaut pour les connexions vSphere Web Services SDK. Si vous souhaitez configurer ces connexions afin qu'elles ne chiffrent pas les transmissions, désactivez SSL pour votre connexion vSphere Web Services SDK en remplaçant le paramètre de connexion HTTPS par HTTP.

Envisagez de mettre hors tension SSL uniquement si vous avez créé un environnement parfaitement fiable pour ces clients, avec des pare-feu et des transmissions depuis/vers l'hôte totalement isolées. La désactivation de SSL peut améliorer les performances car vous évitez le traitement requis pour l'exécution du chiffrement.

- Pour vous protéger contre les utilisations abusives des services ESXi, la plupart des services ESXi internes sont uniquement accessibles via le port 443, qui est utilisé pour la transmission HTTPS. Le port 443 agit comme proxy inversé pour ESXi. Vous pouvez consulter la liste de services sur ESXi via une page d'accueil HTTP, mais vous ne pouvez pas directement accéder aux services d'Adaptateurs de stockage sans autorisation.

Vous pouvez modifier cette configuration afin que des services individuels soient directement accessibles via des connexions HTTP. N'effectuez pas ce changement à moins d'utiliser ESXi dans un environnement parfaitement fiable.

- Lorsque vous mettez votre environnement à niveau, le certificat est conservé.

Considérations relatives à la sécurité dans vSphere Auto Deploy

Pour protéger au mieux votre environnement, vous devez connaître les risques de sécurité potentiels lorsque vous utilisez Auto Deploy avec des profils d'hôte.

Sécurité de la mise en réseau

Protégez le réseau comme vous le feriez pour toute autre méthode de déploiement PXE. vSphere Auto Deploy transfère les données sur SSL pour éviter les interférences et les risques d'écoute. Toutefois, l'authenticité du client ou du serveur Auto Deploy n'est pas vérifiée au cours d'un démarrage PXE.

Vous pouvez considérablement réduire le risque de sécurité d'Auto Deploy en isolant complètement le réseau lorsqu'Auto Deploy est utilisé.

Sécurité concernant l'image de démarrage et le profil d'hôte

L'image de démarrage que le serveur vSphere Auto Deploy télécharge sur une machine peut contenir les composants suivants.

- Les modules VIB qui constituent le profil d'image sont toujours inclus dans l'image de démarrage.
- Le profil d'hôte et la personnalisation de l'hôte sont inclus dans l'image de démarrage si les règles Auto Deploy sont configurées pour provisionner l'hôte avec un profil d'hôte ou un paramétrage de personnalisation d'hôte.
 - Le mot de passe administrateur (racine) et les mots de passe utilisateur qui sont inclus dans le profil d'hôte et la personnalisation d'hôte sont cryptés en MD5.

- Tous les autres mots de passe associés aux profils sont en clair. Si vous paramétrez Active Directory en utilisant des profils d'hôte, les mots de passe ne sont pas protégés.

Utilisez vSphere Authentication Service pour paramétrer Active Directory afin d'éviter d'exposer les mots de passe. Si vous paramétrez Active Directory en utilisant des profils d'hôte, les mots de passe sont protégés.

- La clé SSL publique et privée et le certificat de l'hôte sont inclus dans l'image de démarrage.

Gestion des fichiers journaux ESXi

Les fichiers journaux constituent un élément important dans le dépannage des attaques et l'obtention d'informations relatives aux failles de sécurité de l'hôte. Une journalisation effectuée sur un serveur dédié centralisé et sécurisé peut contribuer à éviter la falsification des journaux. La journalisation à distance fournit également un enregistrement des contrôles à long terme.

Prenez les mesures suivantes pour renforcer la sécurité de l'hôte.

- Configurez la journalisation permanente d'une banque de données. Les journaux des hôtes ESXi sont stockés par défaut dans le système de fichiers in-memory. Par conséquent, ils sont perdus lorsque vous redémarrez l'hôte et seules 24 heures de données de journalisation sont stockées. Lorsque vous activez la journalisation permanente, vous obtenez un enregistrement dédié de l'activité du serveur, disponible pour l'hôte.
- La journalisation à distance vers un hôte central vous permet de collecter des fichiers journaux sur un hôte central, où vous pouvez surveiller tous les hôtes à l'aide d'un outil unique. Vous pouvez également effectuer une analyse cumulée et une recherche de données de journalisation, pouvant révéler des informations concernant des choses comme des attaques coordonnées sur plusieurs hôtes.
- Configurez un syslog à distance sécurisé sur les hôtes ESXi utilisant une ligne de commande distante (comme vCLI ou PowerCLI) ou une API client.
- Interrogez la configuration syslog pour vous assurer qu'un serveur syslog valide a été configuré, y compris le port correct.

Configurer Syslog sur des hôtes ESXi

Tous les hôtes ESXi exécutent un service syslog (`vmssyslogd`) qui enregistre les messages venant de VMkernel et d'autres composants système dans des fichiers journaux.

Vous pouvez utiliser vSphere Web Client ou la commande vCLI `esxcli system syslog` pour configurer le service syslog.

Pour plus d'informations sur l'utilisation de commandes vCLI, reportez-vous à *Démarrage avec vSphere Command-Line Interfaces*.

Procédure

- 1 Dans l'inventaire de vSphere Web Client, sélectionnez l'hôte.

- 2 Cliquez sur l'onglet **Gérer**.
- 3 Dans le panneau système, cliquez sur **Paramètres système avancés**.
- 4 Recherchez la section **Syslog** dans la liste des Paramètres système avancés.
- 5 Pour configurer la journalisation de façon globale, sélectionnez le paramètre à modifier et cliquez sur l'icône Modifier.

Option	Description
Syslog.global.defaultRotate	Définit le nombre maximum d'archives à conserver. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.
Syslog.global.defaultSize	Définit la taille par défaut du journal, en Ko, avant que le système n'effectue la rotation des journaux. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.
Syslog.global.LogDir	Répertoire dans lequel sont stockés les journaux. Le répertoire peut se trouver sur des volumes NFS ou VMFS montés. Seul le répertoire <code>/scratch</code> situé sur le système de fichiers local subsiste après des redémarrages. Le répertoire doit être défini sous la forme <code>[nom_banque_de_données]chemin_du_fichier</code> , le chemin se rapportant à la racine du volume qui assure la sauvegarde de la banque de données. Par exemple, le chemin <code>[storage1] /systemlogs</code> crée un mappage vers le chemin <code>/vmfs/volumes/storage1/systemlogs</code> .
Syslog.global.logDirUnique	Lorsque vous sélectionnez cette option, un sous-répertoire est créé portant le nom de l'hôte ESXi dans le répertoire spécifié par Syslog.global.LogDir . Il est utile d'avoir un répertoire unique si le même répertoire NFS est utilisé par plusieurs hôtes ESXi.
Syslog.global.LogHost	Hôte distant vers lequel les messages syslog sont transférés et port sur lequel l'hôte distant reçoit les messages syslog. Vous pouvez inclure le protocole et le port, par exemple, <code>ssl://hostName1:1514</code> . Les protocoles UDP (par défaut), TCP et SSL sont pris en charge. L'hôte distant doit avoir un syslog installé et correctement configuré pour recevoir les messages syslog transférés. Consultez la documentation du service syslog installé sur l'hôte distant pour plus d'informations sur la configuration.

- 6 (Facultatif) Pour remplacer la taille par défaut et la rotation des journaux d'un journal quelconque.
 - a Cliquez sur le nom du journal que vous souhaitez personnaliser.
 - b Cliquez sur l'icône Modifier et entrez le nombre de rotations et la taille de journal souhaités.
- 7 Cliquez sur **OK**.

Résultats

Les modifications apportées aux options syslog prennent effet immédiatement.

Emplacements des fichiers journaux ESXi

ESXi enregistre l'activité de l'hôte dans des fichiers journaux en utilisant un outil syslog.

Composant	Emplacement	Objectif
VMkernel	<code>/var/log/vmkernel.log</code>	Enregistre les activités relatives aux machines virtuelles et à ESXi.
Avertissements VMkernel	<code>/var/log/vmkwarning.log</code>	Enregistre les activités relatives aux machines virtuelles.
Résumé VMkernel	<code>/var/log/vmksummary.log</code>	Utilisé pour déterminer les statistiques de temps de fonctionnement et de disponibilité pour ESXi (virgule séparée).
Journal de l'agent hôte ESXi	<code>/var/log/hostd.log</code>	Contient des informations sur l'agent gérant et configurant les hôtes ESXi et leurs machines virtuelles.
Journal de l'agent vCenter	<code>/var/log/vpxa.log</code>	Contient des informations sur l'agent communiquant avec vCenter Server (si l'hôte est géré par vCenter Server).
Journal du shell	<code>/var/log/shell.log</code>	Contient un enregistrement de toutes les commandes tapées dans ESXi Shell, ainsi que les événements de shell (par exemple, le moment où le shell a été activé).
Authentification	<code>/var/log/auth.log</code>	Contient tous les événements relatifs à l'authentification pour le système local.
Messages système	<code>/var/log/syslog.log</code>	Contient tous les messages généraux du journal et peut être utilisé en cas de dépannage. Ces informations étaient précédemment situées dans le fichier journal des messages.
Machines virtuelles	Le même répertoire que les fichiers de configuration de la machine virtuelle, appelés <code>vmware.log</code> et <code>vmware*.log</code> . Par exemple, <code>/vmfs/volumes/datastore/virtual machine/vmware.log</code>	Contient les événements d'alimentation de la machine virtuelle, les informations relatives aux défaillances système, la synchronisation horaire, les modifications virtuelles du matériel, les migrations vMotion, les clones de machines, etc.

Trafic de la journalisation de la tolérance aux pannes

Lorsque vous activez Fault Tolerance (FT), VMware vLockstep capture les entrées et les événements qui se produisent sur une machine virtuelle principale et les transmet à la machine virtuelle secondaire qui est exécutée sur un autre hôte.

Le trafic de la journalisation entre les machines virtuelles primaires et secondaires est chiffré et contient un réseau client et des données E/S de stockage, ainsi que le contenu de la mémoire du système d'exploitation invité. Ce trafic peut inclure des données sensibles telles que des mots de passe en texte brut. Pour éviter que ces données ne soient divulguées, assurez-vous que ce réseau est sécurisé, notamment pour éviter les « attaques de l'intercepteur ». Par exemple, vous pouvez utiliser un réseau privé pour le trafic de la journalisation de la tolérance aux pannes.

Sécurisation des systèmes vCenter Server

6

La sécurisation de vCenter Server comporte notamment le fait de veiller à la sécurité de l'hôte sur lequel vCenter Server fonctionne, en respectant les meilleures pratiques en matière d'attribution des privilèges et des rôles, et en vérifiant l'intégrité des clients qui se connectent au vCenter Server.

Ce chapitre contient les rubriques suivantes :

- [Meilleures pratiques de sécurité de vCenter Server](#)
- [Vérifier les empreintes des hôtes ESXi hérités](#)
- [Vérifier que la validation des certificats SSL sur Network File Copy est activée](#)
- [Ports TCP et UDP pour vCenter Server](#)
- [Accès à l'outil de surveillance du matériel basé sur la surveillance CIM](#)

Meilleures pratiques de sécurité de vCenter Server

Le respect des meilleures pratiques de sécurité de vCenter Server vous aide à garantir l'intégrité de votre environnement vSphere.

Meilleures pratiques pour le contrôle d'accès à vCenter Server

Contrôlez strictement l'accès aux différents composants de vCenter Server pour augmenter la sécurité du système.

Les directives suivantes contribuent à garantir la sécurité de votre environnement.

Utiliser des comptes nommés

- Si le compte d'administrateur Windows local dispose actuellement de droits administratifs complets sur vCenter Server, supprimez ces droits d'accès et accordez-les à un ou plusieurs comptes d'administrateurs nommés de vCenter Server. Accordez des droits administratifs complets aux administrateurs qui doivent en disposer. N'accordez pas ce privilège à un groupe dont la composition ne fait pas l'objet d'un contrôle strict.

Note À partir de vSphere 6.0, l'administrateur local n'a plus de droits administratifs complets sur vCenter Server par défaut. L'emploi d'utilisateurs du système d'exploitation local n'est pas recommandé.

- Installez vCenter Server en utilisant un compte de service plutôt qu'un compte Windows. Le compte de service doit être un administrateur sur la machine locale.
- Assurez-vous que les applications utilisent des comptes de service uniques lors d'une connexion à un système vCenter Server.

Minimiser l'accès

Évitez d'autoriser les utilisateurs à se connecter directement à la machine hôte vCenter Server. Les utilisateurs qui sont connectés à vCenter Server peuvent potentiellement provoquer des dommages, intentionnellement ou non, en modifiant les paramètres et les processus. Ils ont également un accès potentiel aux informations d'identification de vCenter (par exemple, le certificat SSL). Autorisez uniquement les utilisateurs ayant des tâches légitimes à effectuer à se connecter au système et assurez-vous que les événements de connexion sont suivis.

Surveillez les privilèges des utilisateurs administrateurs de vCenter Server

Certains utilisateurs administrateurs ne doivent pas avoir le rôle Administrateur. Créez plutôt un rôle personnalisé disposant de l'ensemble approprié de privilèges et attribuez-le aux autres administrateurs.

Les utilisateurs disposant du rôle Administrateur de vCenter Server disposent de privilèges sur tous les objets de la hiérarchie. Par exemple, le rôle Administrateur permet par défaut aux utilisateurs d'interagir avec les fichiers et les programmes du système d'exploitation invité de la machine virtuelle. L'attribution de ce rôle à un trop grand nombre d'utilisateurs peut compromettre la confidentialité, la disponibilité ou l'intégrité des données. Créez un rôle qui donne aux administrateurs les privilèges dont ils ont besoin, mais supprimez certains privilèges de gestion de machines virtuelles.

Accordez des privilèges minimaux aux utilisateurs de base de données vCenter Server

L'utilisateur de la base de données n'a besoin que de quelques privilèges spécifiques à l'accès à la base de données. En outre, certains privilèges ne sont nécessaires que pour l'installation et la mise à niveau. Ces privilèges peuvent être supprimés après l'installation ou la mise à niveau du produit.

Restreindre l'accès au navigateur de la banque de données

La fonctionnalité de navigateur de banques de données permet aux utilisateurs possédant les privilèges appropriés d'afficher et de télécharger des fichiers depuis et vers les banques de données associées au déploiement de vSphere au moyen du navigateur web ou de vSphere Web Client. Attribuer le privilège **Banque de données.Parcourir la banque de données** uniquement aux utilisateurs ou aux groupes qui ont réellement besoin de ces privilèges.

Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle

Par défaut, un utilisateur avec le rôle d'administrateur vCenter Server peut interagir avec les fichiers et programmes au sein du système d'exploitation invité d'une machine virtuelle. Afin de réduire les risques d'atteinte à la confidentialité, la disponibilité et l'intégrité de l'invité, créez un rôle d'accès non-invité, dépourvu du privilège **Opérations client**. Reportez-vous à [Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle](#).

Vérifier la stratégie de mot de passe de vpxuser

Par défaut, vCenter Server modifie le mot de passe de vpxuser automatiquement tous les 30 jours. Assurez-vous que ce paramètre est conforme à vos stratégies ou configurez la stratégie pour répondre aux stratégies d'expiration de mot de passe de l'entreprise. Reportez-vous à [Configurer la stratégie de mot de passe de vCenter Server](#).

Note Assurez-vous que la stratégie d'expiration du mot de passe n'est pas trop courte.

Vérifiez les privilèges après le redémarrage de vCenter Server

Vérifiez la réaffectation des privilèges lorsque vous redémarrez vCenter Server. Si l'utilisateur ou le groupe d'utilisateurs ayant obtenu le rôle Administrateur sur le dossier racine ne peut pas être vérifié comme utilisateur ou groupe valide pendant un redémarrage, le rôle est retiré de cet utilisateur ou de ce groupe. À la place, vCenter Server accorde le rôle Administrateur au compte administrator@vsphere.local de vCenter Single Sign-On. Ce compte peut alors agir en tant qu'administrateur.

Rétablissez un compte d'administrateur nommé et attribuez-lui le rôle Administrateur pour éviter d'utiliser le compte administrator@vsphere.local anonyme.

Utiliser des niveaux de chiffrement RDP élevés

Sur chaque ordinateur Windows de l'infrastructure, vérifiez que les paramètres de configuration d'hôte des services Bureau à distance sont définis afin de garantir le niveau de chiffrement le plus élevé pour votre environnement.

Vérifiez les certificats vSphere Web Client

Demander aux utilisateurs d'une application vSphere Web Client ou d'autres applications client de ne jamais ignorer les avertissements de vérification de certificat. Sans vérification de certificat, l'utilisateur peut être sujet à une attaque MiTM.

Configurer la stratégie de mot de passe de vCenter Server

Par défaut, vCenter Server modifie automatiquement le mot de passe vpxuser tous les 30 jours. Vous pouvez modifier cette valeur dans vSphere Web Client.

Procédure

- 1 Sélectionnez vCenter Server dans la hiérarchie des objets vSphere Web Client.

- 2 Cliquez sur l'onglet **Gérer**, puis sur le sous-onglet **Paramètres**.
- 3 Cliquez sur **Paramètres avancés** et entrez **VimPasswordExpirationInDays** dans la case des filtres.
- 4 Configurez `VirtualCenter.VimPasswordExpirationInDays` pour qu'il soit conforme à vos exigences.

Protection de l'hôte Windows vCenter Server

Protégez l'hôte Windows contre les vulnérabilités et les attaques lors de l'exécution de vCenter Server en s'assurant que l'environnement de l'hôte est aussi sécurisé que possible.

- Gérez un système d'exploitation, une base de données ou un matériel pris en charge pour le système vCenter Server. Si vCenter Server ne s'exécute pas sur un système d'exploitation pris en charge, il est possible qu'il ne fonctionne pas correctement, ce qui le rend vulnérable aux attaques vCenter Server.
- Veillez à ce que les correctifs soient correctement installés sur le système vCenter Server. Le serveur est moins vulnérable aux attaques si les correctifs du système d'exploitation sont mis à jour régulièrement.
- Protégez le système d'exploitation sur l'hôte vCenter Server. La protection comprend un logiciel antivirus et un logiciel anti-programme malveillant.
- Sur chaque ordinateur Windows de l'infrastructure, vérifiez que les paramètres de configuration d'hôte des services Bureau à distance (RDP) sont définis afin de garantir le niveau de chiffrement le plus élevé conformément aux directives standard du marché ou aux instructions internes.

Pour obtenir des informations sur la compatibilité des systèmes d'exploitation et des bases de données, reportez-vous à *Matrices de compatibilité vSphere*.

Suppression de certificats expirés ou révoqués et de journaux d'installations ayant échoué

La conservation de certificats expirés ou révoqués ou des journaux d'installation de vCenter Server générés lors de l'échec d'une installation sur votre système vCenter Server peut compromettre la sécurité de votre environnement.

La suppression des certificats expirés ou révoqués est nécessaire pour les raisons suivantes.

- Si les certificats expirés ou révoqués ne sont pas supprimés du système vCenter Server, l'environnement peut être exposé à une attaque MiTM.
- Dans certains cas, un fichier journal contenant le mot de passe d'une base de données en texte clair est créé sur le système lors d'un échec d'installation de vCenter Server. Un attaquant qui s'introduit dans le système vCenter Server peut réussir à accéder à ce mot de passe et, en même temps, à la base de données vCenter Server.

Limitation de la connectivité réseau vCenter Server

Pour plus de sécurité, évitez d'installer le système vCenter Server sur un réseau autre qu'un réseau de gestion et assurez-vous que le trafic de gestion vSphere circule sur un réseau restreint. En limitant la connectivité du réseau, vous limitez l'éventualité de certains types d'attaque.

vCenter Server requiert uniquement l'accès à un réseau de gestion. Évitez de placer le système vCenter Server sur d'autres réseaux tels que vos réseaux de production ou de stockage, ou sur tout réseau ayant accès à Internet. vCenter Server n'a pas besoin d'un accès au réseau sur lequel vMotion fonctionne.

vCenter Server requiert une connectivité réseau vers les systèmes suivants.

- Tous les hôtes ESXi.
- La base de données vCenter Server.
- D'autres systèmes vCenter Server (si les systèmes vCenter Server appartiennent à un domaine vCenter Single Sign-On commun, à des fins de réplication des balises, des autorisations, etc.)
- Des systèmes autorisés à exécuter des clients de gestion. Par exemple, vSphere Web Client, un système Windows sous lequel vous utilisez PowerCLI ou tout autre client SDK.
- Des systèmes qui exécutent des composants complémentaires, tels que VMware vSphere Update Manager.
- Des services d'infrastructure, tels que DNS, Active Directory et NTP.
- D'autres systèmes qui exécutent des composants essentiels à la fonctionnalité du système vCenter Server.

Utilisez un pare-feu local sur le système Windows sur lequel le système vCenter Server s'exécute ou utilisez un pare-feu de réseau. Incluez des restrictions d'accès basées sur l'IP, afin que seuls les composants nécessaires puissent communiquer avec le système vCenter Server.

Envisager la restriction d'utilisation de clients Linux

Les communications entre les composants clients et un système vCenter Server ou des hôtes ESXi sont protégées par défaut par un chiffrement SSL. Les versions Linux de ces composants n'effectuent pas de validation de certificats. Envisagez de restreindre l'utilisation de ces clients.

Même si vous avez remplacé les certificats signés par VMCA sur le système vCenter Server et sur les hôtes ESXi par des certificats qui sont signés par une autorité de certification tierce, certaines communications avec les clients Linux sont toujours vulnérables aux attaques de l'intercepteur. Les composants suivants sont vulnérables lorsqu'ils fonctionnent sur le système d'exploitation Linux.

- Commandes vCLI
- Scripts vSphere SDK pour Perl
- Programmes écrits à l'aide de vSphere Web Services SDK

Vous pouvez assouplir la restriction de l'utilisation des clients Linux à condition d'assurer un contrôle adéquat.

- Limitez l'accès au réseau de gestion exclusivement aux systèmes autorisés.
- Utilisez des pare-feux pour vous assurer que seuls les hôtes autorisés peuvent accéder à vCenter Server.
- Utilisez les systèmes JumpBox afin de vous assurer que les clients Linux se trouvent derrière le saut.

Vérifier les plug-in installés

Les extensions vSphere Web Client sont exécutées avec le même niveau de privilège que l'utilisateur qui est connecté. Une extension malveillante peut se faire passer pour un plug-in utile et effectuer des opérations nuisibles, notamment le vol d'informations d'identification ou la modification de la configuration système. Pour augmenter la sécurité, utilisez une installation vSphere Web Client qui comporte uniquement des extensions autorisées provenant de sources fiables.

Une installation vCenter comprend l'infrastructure d'extensibilité vSphere Web Client qui offre la possibilité d'étendre vSphere Web Client à l'aide de sélections de menu ou d'icônes de la barre d'outils qui donnent accès aux composants complémentaires de vCenter ou à des fonctionnalités Web externes. Cette flexibilité s'accompagne du risque d'introduire des fonctionnalités non souhaitées. Par exemple, si un administrateur installe un plug-in dans une instance de vSphere Web Client, le plug-in peut alors exécuter des commandes arbitraires grâce au niveau de privilège de cet administrateur.

Pour protéger votre vSphere Web Client de tout risque éventuel, vous pouvez examiner périodiquement tous les plug-ins installés et vous assurer qu'ils proviennent d'une source fiable.

Conditions préalables

Vous devez disposer de privilèges pour accéder au service vCenter Single Sign-On. Ces privilèges diffèrent des privilèges vCenter Server.

Procédure

- 1 Connectez-vous à vSphere Web Client en tant qu'`administrator@vsphere.local` ou utilisateur avec des privilèges vCenter Single Sign-On.
- 2 Sur la page d'accueil, sélectionnez **Administration**, puis **Plug-ins des clients** dans **Solutions**
- 3 Examinez la liste de plug-ins des clients.

Meilleures pratiques en matière de sécurité de vCenter Server Appliance

Suivez toutes les meilleures pratiques de sécurisation d'un système vCenter Server pour sécuriser vCenter Server Appliance. Les étapes supplémentaires vous permettent de renforcer la sécurité de votre environnement.

Configurer NTP

Assurez-vous que tous les systèmes utilisent la même source d'heure relative (en tenant compte du décalage de localisation pertinent), et que la source d'heure relative peut être mise en corrélation avec une heure standard convenue, telle que le Temps universel coordonné (UTC). La synchronisation des systèmes est essentielle pour assurer la validité des certificats. 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 [Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP](#).

Limiter l'accès au réseau de vCenter Server Appliance

Autorisez l'accès uniquement aux composants absolument essentiels pour communiquer avec vCenter Server Appliance. En bloquant l'accès des systèmes non essentiels, vous réduisez les risques d'attaque générale sur le système d'exploitation. Si vous autorisez l'accès uniquement aux composants essentiels, les risques diminuent.

Vérifier les empreintes des hôtes ESXi hérités

Dans vSphere 6 et versions ultérieures, des certificats VMCA sont attribués aux hôtes par défaut. Si vous passez au mode de certificat d'empreinte, vous pouvez continuer à utiliser le mode d'empreinte pour les hôtes hérités. Vous pouvez vérifier les empreintes dans vSphere Web Client.

Note Les certificats sont conservés par défaut entre les mises à niveau.

Procédure

- 1 Accédez au système vCenter Server dans le navigateur d'objets de vSphere Web Client.
- 2 Sélectionnez l'onglet **Gérer**, cliquez sur **Paramètres**, puis cliquez sur **Général**.
- 3 Cliquez sur **Edit**.
- 4 Cliquez sur **Paramètres SSL**.

- 5 Si l'un de vos hôtes ESXi 5.5 ou version antérieure nécessite une validation manuelle, comparez les empreintes répertoriées pour les hôtes aux empreintes de la console hôte.
Pour obtenir l'empreinte de l'hôte, utilisez l'interface utilisateur de console directe (DCUI).
 - a Connectez-vous à la console directe et appuyez sur F2 pour accéder au menu de Personnalisation du système.
 - b Sélectionnez **Voir les informations de support**.
L'empreinte hôte figure dans la colonne de droite.
- 6 Si l'empreinte correspond, cochez la case **Vérifier** à côté de l'hôte.
Les hôtes non sélectionnés sont déconnectés après avoir cliqué sur **OK**.
- 7 Cliquez sur **OK**.

Vérifier que la validation des certificats SSL sur Network File Copy est activée

La NFC (Network File Copy, copie de fichiers réseau) fournit un service FTP capable de reconnaître les types de fichiers pour les composants vSphere. À partir de vSphere 5.5, ESXi utilise par défaut NFC pour les opérations telles que la copie et le déplacement de données entre les banques de données, mais si la fonction est désactivée, vous devrez l'activer.

Lorsque SSL sur NFC est activé, les connexions entre les composants de vSphere via le protocole NFC sont sécurisées. Cette connexion permet d'éviter des « attaques de l'intercepteur » au sein d'un centre de données.

Dans la mesure où l'utilisation de NFC via SSL entraîne une dégradation des performances, vous pouvez envisager de désactiver ce paramètre avancé dans certains environnements de développement.

Note Définissez explicitement cette valeur sur true si vous utilisez des scripts pour vérifier la valeur.

Procédure

- 1 Connectez-vous à vCenter Server avec vSphere Web Client.
- 2 Sélectionnez l'onglet **Paramètres**, puis cliquez sur **Paramètres avancés**.
- 3 Cliquez sur **Modifier**.
- 4 Dans le bas de la boîte de dialogue, entrez la clé et la valeur suivantes.

Champ	Valeur
Touche	config.nfc.useSSL
Valeur	vrai

- 5 Cliquez sur **OK**.

Ports TCP et UDP pour vCenter Server

vCenter Server est accessible par le biais de ports TCP et UDP prédéterminés. Si vous gérez des composants réseau à partir de l'extérieur d'un pare-feu, vous pouvez être invité à reconfigurer le pare-feu pour autoriser l'accès sur les ports appropriés.

Le tableau répertorie les ports TCP et UDP et l'objectif et le type de chaque port. Les ports qui sont ouverts par défaut lors de l'installation sont suivis de la mention « (par défaut) ». Pour obtenir une liste actualisée des ports de tous les composants vSphere pour les différentes versions de vSphere, reportez-vous à l'[article 1012382 de la base de connaissances VMware](#).

Tableau 6-1. Ports TCP et UDP pour vCenter Server

Port	Objectif
80 (par défaut)	Accès HTTP vCenter Server nécessite le port 80 pour les connexions HTTP directes. Le port 80 redirige les demandes vers le port HTTPS 443. Cette redirection est utile si vous utilisez accidentellement <code>http://server</code> au lieu de <code>https://server</code> WS-Management (nécessite également l'ouverture du port 443)
88, 2013	Interface de contrôle RPC pour Kerberos, utilisée par vCenter Single Sign-On.
123	Client NTP
135 (par défaut)	Pour vCenter Server Appliance, ce port est désigné pour l'authentification Active Directory. Pour une installation de vCenter Server sur Windows, ce port est utilisé pour Linked mode et le port 88 est utilisé pour l'authentification Active Directory.
161 (par défaut)	Serveur SNMP. Il s'agit du port par défaut sur un hôte ESXi et sur un vCenter Server Appliance.
389	vCenter Single Sign-On LDAP (6.0 et ultérieur)
636	vCenter Single Sign-On LDAPS (6.0 et ultérieur)
443 (par défaut)	Les systèmes vCenter Server utilisent le port 443 pour surveiller les transferts de données à partir des clients SDK. Ce port est également utilisé pour les services suivants : <ul style="list-style-type: none"> ■ WS-Management (nécessite également l'ouverture du port 80) ■ Connexions clients de gestion de réseau tiers à vCenter Server ■ Accès clients de gestion de réseau tiers à des hôtes
2012	Port RPC de VMware Directory Service (vmdir).
2014	Port RPC du service VMware Certificate Authority (VMCA).
2020	Port RPC du service VMware Authentication Framework (vmafd).
31031, 44046 (par défaut)	vSphere Replication
7444	vCenter Single Sign-On HTTPS.
8093	Le plug-in d'intégration de client utilise un nom d'hôte de boucle local, et emploie le port 8093 et des ports aléatoires dans la plage 50100 à 60099. Le plug-in d'intégration de client utilise le port 8093 uniquement pour les communications locales. Le port peut rester bloqué par le pare-feu.

Tableau 6-1. Ports TCP et UDP pour vCenter Server (suite)

Port	Objectif
8109	VMware Syslog Collector.
9443	Accès HTTP vSphere Web Client aux hôtes ESXi.
10080	Inventory Service.
11711	vCenter Single Sign-On LDAP (environnements mis à niveau depuis vSphere 5.5)
11712	vCenter Single Sign-On LDAPS (environnements mis à niveau depuis vSphere 5.5)
12721	VMware Identity Management Service.
15005	Gestionnaire d'agent ESX (EAM). Un agent ESX peut être une machine virtuelle ou un VIB optionnel. L'agent étend les fonctions d'un hôte ESXi pour fournir les services additionnels que requiert une solution vSphere telle que NSX-v ou vRealize Automation.
15007	vService Manager (VSM). Ce service enregistre les extensions de vCenter Server. Ouvrez ce port uniquement si cela est requis par les extensions que vous prévoyez d'utiliser.
50100-60099	Le plug-in d'intégration de client utilise un nom d'hôte de boucle local, et emploie le port 8093 et des ports aléatoires dans la plage 50100 à 60099. Le plug-in d'intégration de client utilise cette plage de ports uniquement pour les communications locales. Le port peut rester bloqué par le pare-feu.

En plus de ces ports, vous pouvez configurer d'autres ports en fonction de vos besoins.

Accès à l'outil de surveillance du matériel basé sur la surveillance CIM

Le système CIM (Modèle de données unifié, Common Information Model) fournit une interface permettant la gestion au niveau du matériel à partir d'applications distantes utilisant un ensemble d'API standard. Pour assurer la sécurisation de l'interface CIM, ne fournissez que le niveau d'accès minimal nécessaire à ces applications. Si une application, qui a été provisionnée avec un compte racine ou un compte administrateur complet, est compromise, l'ensemble de l'environnement virtuel peut l'être aussi.

Le modèle CIM est une norme ouverte qui définit une architecture pour la surveillance des ressources matérielles sans agent et basée sur des règles pour ESXi. Cette structure se compose d'un gestionnaire d'objet CIM, généralement appelé courtier CIM, et d'un ensemble de fournisseurs CIM.

Les fournisseurs CIM sont utilisés comme mécanisme pour fournir un accès de gestion aux pilotes de périphériques et au matériel sous-jacent. Les fabricants de matériel, notamment les fabricants de serveurs et les fournisseurs de périphériques spécifiques, peuvent créer ce type de fournisseurs afin d'assurer la surveillance et la gestion de leurs périphériques spécifiques. VMware crée également des fournisseurs qui mettent en œuvre la surveillance du matériel serveur, l'infrastructure de stockage ESXi et des ressources spécifiques à la virtualisation. Ces fournisseurs

s'exécutent au sein même du système ESXi. Ils sont donc conçus pour être extrêmement légers et dédiés à des tâches de gestion spécifiques. Le courtier CIM recueille des informations auprès de tous les fournisseurs CIM et les diffuse à l'extérieur par le biais d'API standards, la plus commune d'entre elles étant WS-MAN.

Ne fournissez pas aux applications distantes des informations d'identification racine permettant d'accéder à l'interface CIM. Créez plutôt un compte de service spécifique à ces applications et accordez un accès en lecture seule aux informations CIM à tous les comptes locaux définis sur le système ESXi, ainsi qu'à tous les rôles définis dans vCenter Server.

Procédure

- 1 Créez un compte de service spécifique aux applications CIM.
- 2 Accordez un accès en lecture seule aux informations CIM à tous les comptes locaux définis sur le système ESXi, ainsi qu'à tous les rôles définis dans vCenter Server.
- 3 (Facultatif) Si l'application requiert un accès en écriture à l'interface CIM, créez un rôle s'appliquant au compte de service avec seulement deux privilèges :
 - **Hôte.Config.SystemManagement (Gestion du système)**
 - **Hôte.CIM.CIMInteraction (Interaction CIM)**

Ce rôle peut être local pour l'hôte ou défini centralement sur vCenter Server, selon le mode de fonctionnement de l'application de contrôle.

Résultats

Lorsqu'un utilisateur se connecte à l'hôte avec le compte de service créé pour les applications CIM, l'utilisateur dispose uniquement des privilèges **SystemManagement (Gestion du système)** et **CIMInteraction (Interaction CIM)** ou d'un accès en lecture seule.

Sécurisation des machines virtuelles

7

Le système d'exploitation client qui est exécuté dans la machine virtuelle est exposé aux mêmes risques de sécurité qu'une machine physique. Sécurisez les machines virtuelles comme vous le feriez pour des machines physiques.

Ce chapitre contient les rubriques suivantes :

- [Limiter les messages d'information entre les machines virtuelles et les fichiers VMX](#)
- [Empêcher la réduction de disque virtuel](#)
- [Recommandations en matière de sécurité des machines virtuelles](#)

Limiter les messages d'information entre les machines virtuelles et les fichiers VMX

Limitez les messages d'information de la machine virtuelle vers le fichier VMX, afin d'éviter de remplir la banque de données et de causer un déni de service (DoS). Un déni de service peut survenir quand vous ne contrôlez pas la taille du fichier VMX d'une machine virtuelle et que la somme d'informations excède la capacité de la banque de données.

Le fichier de configuration contenant les paires d'informations nom-valeur est limité par défaut à 1 Mo. Cette capacité est suffisante dans la plupart des cas, mais vous pouvez modifier cette valeur si nécessaire. Vous pouvez par exemple augmenter la limite si de grandes quantités d'informations personnalisées sont stockées dans le fichier de configuration.

Note Étudiez soigneusement le volume d'informations dont vous avez besoin. Si le volume d'informations excède la capacité de la banque de données, un déni de service peut se produire.

La limite par défaut de 1 Mo s'applique même si le paramètre `tools.setInfo.sizeLimit` n'est pas répertorié dans les options avancées.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.

- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Ajoutez ou modifiez le paramètre `tools.setInfo.sizeLimit`.

Empêcher la réduction de disque virtuel

Les utilisateurs non administratifs du système d'exploitation client peuvent réduire les disques virtuels. La réduction d'un disque virtuel exige de l'espace inutilisé sur le disque. Cependant, si vous réduisez un disque virtuel de façon répétée, le disque peut devenir indisponible et provoquer un déni de service. Pour éviter cela, désactivez la possibilité de réduction des disques virtuels.

Conditions préalables

- Désactivez la machine virtuelle.
- Vérifiez que vous disposez des privilèges racine ou d'administrateur sur la machine virtuelle.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Ajoutez ou modifiez les paramètres suivants.

Nom	Valeur
<code>isolation.tools.diskWiper.disable</code>	TRUE
<code>isolation.tools.diskShrink.disable</code>	TRUE

- 6 Cliquez sur **OK**.

Résultats

Lorsque vous désactivez cette fonction, vous ne pouvez plus réduire des disques de machines virtuelles lorsqu'une banque de données vient à manquer d'espace.

Recommandations en matière de sécurité des machines virtuelles

Suivez les recommandations suivantes pour garantir l'intégrité de votre déploiement vSphere.

- **Protection générale d'une machine virtuelle**

Une machine virtuelle est, pour l'essentiel, l'équivalent d'un serveur physique. Il convient de prendre les mêmes mesures de sécurité pour les machines virtuelles et les systèmes physiques.

- **Utiliser des modèles pour déployer des machines virtuelles**

Lorsque vous installez manuellement des systèmes d'exploitation clients et des applications sur une machine virtuelle, le risque existe que votre configuration soit incorrecte. Grâce à l'utilisation d'un modèle pour capturer une image sécurisée du système d'exploitation de base sans applications installées, vous pouvez vous assurer que toutes les machines virtuelles sont créées avec une ligne de base connue du niveau de sécurité.

- **Réduire l'utilisation de la console de machine virtuelle**

La console de machine virtuelle joue pour la machine virtuelle le même rôle qu'un moniteur sur un serveur physique. Les utilisateurs qui accèdent à une console de machine virtuelle disposent d'un accès aux commandes de gestion de l'alimentation et de connectivité des périphériques amovibles des machines virtuelles, ce qui peut permettre une attaque malveillante sur ces dernières.

- **Empêcher les machines virtuelles de récupérer les ressources**

Lorsqu'une machine virtuelle consomme une telle proportion des ressources de l'hôte que les autres machines virtuelles de l'hôte ne peuvent accomplir les fonctions pour lesquelles elles sont prévues, un déni de service (DoS) peut survenir. Pour empêcher une machine virtuelle de provoquer un DoS, utilisez les fonctions de gestion des ressources de l'hôte, telles que le paramétrage des partages, et utilisez des pools de ressources.

- **Désactiver les fonctions inutiles à l'intérieur des machines virtuelles**

Tout service fonctionnant sur une machine virtuelle fournit une possibilité d'attaque. En désactivant des composants système inutiles à la prise en charge de l'application ou du service fonctionnant sur le système, vous réduisez le nombre de composants susceptibles d'être attaqués.

Protection générale d'une machine virtuelle

Une machine virtuelle est, pour l'essentiel, l'équivalent d'un serveur physique. Il convient de prendre les mêmes mesures de sécurité pour les machines virtuelles et les systèmes physiques.

Respectez ces recommandations pour protéger votre machine virtuelle :

Correctifs et autres protections

Maintenez toutes vos mesures de sécurité à jour, y compris en appliquant les correctifs appropriés. Il est tout particulièrement important de ne pas négliger les machines virtuelles dormantes désactivées et de suivre les mises à jour les concernant. Par exemple, assurez-vous que le logiciel antivirus, les produits anti-spyware, la détection d'intrusion et toute autre protection sont activés pour chaque machine virtuelle dans votre infrastructure virtuelle. Vous devez également vous assurer de disposer de suffisamment d'espace pour les journaux des machines virtuelles.

Analyses antivirus

Comme chaque machine virtuelle héberge un système d'exploitation standard, vous devez le protéger des virus en installant antivirus. En fonction de votre utilisation habituelle de la machine virtuelle, vous pouvez installer également un pare-feu.

Planifiez l'exécution de scan de virus, tout particulièrement en cas de déploiement incluant un grand nombre de machines virtuelles. Si vous scannez toutes les machines virtuelles simultanément, les performances des systèmes de votre environnement enregistrent une baisse importante. Les pare-feu et les logiciels anti-virus peuvent exiger une grande quantité de virtualisation ; par conséquent, vous pouvez équilibrer ces deux mesures en fonction des performances souhaitées au niveau des machines virtuelles (et tout particulièrement si vous pensez que vos machines virtuelles se trouvent dans un environnement totalement sécurisé).

Ports série

Les ports série sont des interfaces permettant de connecter des périphériques à la machine virtuelle. Ils sont souvent utilisés sur les systèmes physiques pour fournir une connexion directe, de bas niveau à la console d'un serveur. Un port série virtuel autorise le même accès à une machine virtuelle. Les ports série permettent un accès de bas niveau, qui n'offre souvent pas de contrôle renforcé, tel que journalisation ou privilèges.

Utiliser des modèles pour déployer des machines virtuelles

Lorsque vous installez manuellement des systèmes d'exploitation clients et des applications sur une machine virtuelle, le risque existe que votre configuration soit incorrecte. Grâce à l'utilisation d'un modèle pour capturer une image sécurisée du système d'exploitation de base sans applications installées, vous pouvez vous assurer que toutes les machines virtuelles sont créées avec une ligne de base connue du niveau de sécurité.

Vous pouvez utiliser des modèles qui contiennent un système d'exploitation sécurisé doté de correctifs et correctement configuré pour créer d'autres modèles propres à des applications ou utiliser le modèle d'application pour déployer des machines virtuelles.

Procédure

- ◆ Fournissez des modèles pour la création de machines virtuelles qui comportent des déploiements de systèmes d'exploitation sécurisés, corrigés et correctement configurés.

Si possible, déployez également les applications dans les modèles. Assurez-vous que les applications ne dépendent pas d'informations spécifiques à la machine virtuelle à déployer.

Étape suivante

Pour plus d'informations sur les modèles, reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Réduire l'utilisation de la console de machine virtuelle

La console de machine virtuelle joue pour la machine virtuelle le même rôle qu'un moniteur sur un serveur physique. Les utilisateurs qui accèdent à une console de machine virtuelle disposent d'un accès aux commandes de gestion de l'alimentation et de connectivité des périphériques amovibles des machines virtuelles, ce qui peut permettre une attaque malveillante sur ces dernières.

Procédure

- 1 Utilisez des services natifs de gestion à distance, tels que des services de terminaux et SSH, pour interagir avec les machines virtuelles.

Autorisez l'accès à la console de machine virtuelle uniquement lorsque cela est nécessaire.
- 2 Limitez les connexions à la console au nombre de connexions strictement nécessaires.

Par exemple, dans un environnement hautement sécurisé, limitez ce nombre à une connexion. Dans certains environnements, vous pouvez augmenter cette limite en fonction du nombre de connexions simultanées requises pour effectuer des tâches normales.

Empêcher les machines virtuelles de récupérer les ressources

Lorsqu'une machine virtuelle consomme une telle proportion des ressources de l'hôte que les autres machines virtuelles de l'hôte ne peuvent accomplir les fonctions pour lesquelles elles sont prévues, un déni de service (DoS) peut survenir. Pour empêcher une machine virtuelle de provoquer un DoS, utilisez les fonctions de gestion des ressources de l'hôte, telles que le paramétrage des partages, et utilisez des pools de ressources.

Par défaut, toutes les machines virtuelles d'un hôte ESXi partagent équitablement les ressources. Vous pouvez utiliser les partages et les pools de ressources pour empêcher une attaque par déni de service amenant une machine virtuelle à consommer une quantité si importante des ressources de l'hôte que les autres machines virtuelles sur le même hôte ne peuvent pas remplir les fonctions prévues.

N'utilisez pas de limites si vous n'en comprenez pas complètement l'impact.

Procédure

- 1 Fournissez à chaque machine virtuelle juste ce qu'il faut de ressources (CPU et mémoire) pour fonctionner correctement.
- 2 Utilisez les partages pour assurer des ressources suffisantes aux machines virtuelles essentielles.
- 3 Regroupez les machines virtuelles dont les exigences sont identiques dans des pools de ressources.

- 4 Dans chaque pool de ressources, conservez la configuration par défaut des partages pour veiller à ce que chaque machine virtuelle du pool bénéficie d'à peu près la même priorité face aux ressources.

Avec ce paramètre, une machine virtuelle individuelle ne peut pas utiliser plus de ressources que les autres machines virtuelles du pool de ressources.

Étape suivante

Consultez la documentation *Gestion des ressources vSphere* pour de plus amples informations sur les partages et les limites.

Désactiver les fonctions inutiles à l'intérieur des machines virtuelles

Tout service fonctionnant sur une machine virtuelle fournit une possibilité d'attaque. En désactivant des composants système inutiles à la prise en charge de l'application ou du service fonctionnant sur le système, vous réduisez le nombre de composants susceptibles d'être attaqués.

En règle générale, les machines virtuelles n'exigent pas autant de services et de fonctions que les serveurs physiques. Lorsque vous virtualisez un système, évaluez si une fonction ou un service est nécessaire.

Procédure

- ◆ Désactivez les services inutilisés dans le système d'exploitation.
Par exemple, si le système exécute un serveur de fichiers, désactivez tous les services Web.
- ◆ Déconnectez les périphériques physiques inutilisés, tels que les lecteurs CD/DVD, les lecteurs de disquette et les adaptateurs USB.
- ◆ Désactivez toute fonctionnalité inutilisée (par exemple, les fonctionnalités d'affichage inutilisées ou HGFS (Host Guest File System)).
- ◆ Désactivez les écrans de veille.
- ◆ N'exécutez pas le système X Window sous des systèmes d'exploitation client Linux, BSD ou Solaris, à moins que ce ne soit nécessaire.

Supprimer les périphériques matériels inutiles

Tout périphérique activé ou connecté représente un canal d'attaque potentiel. Les utilisateurs et les processus ne disposant pas de privilèges d'accès sur une machine virtuelle peuvent connecter ou déconnecter des périphériques matériels (adaptateurs réseau et lecteurs de CD-ROM, par exemple). Les agresseurs peuvent utiliser ce moyen pour déjouer la sécurité des machines virtuelles. La suppression des périphériques matériels inutiles permet de prévenir les attaques.

Un agresseur ayant accès à une machine virtuelle peut se connecter à un périphérique matériel et ainsi accéder à des informations sensibles figurant sur le support laissé dans le lecteur. Il peut également déconnecter un adaptateur réseau pour isoler la machine virtuelle de son réseau, provoquant de la sorte un déni de service.

- Assurez-vous que des périphériques non autorisés ne sont pas connectés et supprimez les périphériques inutiles ou inutilisés.
- Désactivez les périphériques virtuels inutiles au sein d'une machine virtuelle.
- Assurez-vous qu'aucun périphérique n'est connecté sans nécessité à une machine virtuelle. Les ports série et parallèles sont rarement utilisés pour les machines virtuelles dans un centre de données. Quant aux lecteurs CD/DVD, ils ne sont généralement connectés que lors de l'installation du logiciel.

Procédure

- 1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Web Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Vérifiez chaque périphérique matériel et assurez-vous que vous souhaitez qu'il soit connecté. Vérifiez notamment les périphériques suivants :

- Lecteurs de disquettes
- Ports série
- Ports parallèles
- contrôleurs USB
- lecteurs de CD-ROM

Désactiver les fonctionnalités d'affichage inutilisées

Les pirates peuvent utiliser une fonctionnalité d'affichage inutilisée comme vecteur d'insertion de code malveillant dans votre environnement. Désactivez les fonctionnalités qui ne sont pas utilisées dans votre environnement.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.

- 5 Si cela est approprié, définissez les paramètres suivants en les ajoutant ou en les modifiant.

Option	Description
<code>svga.vgaonly</code>	Si vous définissez ce paramètre sur TRUE, les fonctions graphiques avancées ne fonctionnent plus. Seul le mode de console en cellule de caractère sera disponible. Si vous utilisez ce paramètre, <code>mks.enable3d</code> n'a aucun effet.
Note Appliquez ces paramètres uniquement aux machines virtuelles n'ayant pas besoin d'une carte vidéo virtualisée.	
<code>mks.enable3d</code>	Définissez ce paramètre sur FALSE sur les machines virtuelles n'ayant pas besoin d'une fonctionnalité 3D.

Désactiver les fonctions non exposées

Les machines virtuelles VMware sont conçues pour fonctionner sur les deux systèmes vSphere et sur des plateformes de virtualisation hébergées comme Workstation et Fusion. Certains paramètres de machine virtuelle ne nécessitent pas d'être activés lorsque vous exécutez une machine virtuelle sur un système vSphere. Désactivez ces paramètres afin de réduire les possibilités de faille.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Définissez les paramètres suivants sur TRUE en les ajoutant ou en les modifiant.
 - `isolation.tools.unity.push.update.disable`
 - `isolation.tools.ghi.launchmenu.change`
 - `isolation.tools.memSchedFakeSampleStats.disable`
 - `isolation.tools.getCreds.disable`
 - `isolation.tools.ghi.autologon.disable`
 - `isolation.bios.bbs.disable`
 - `isolation.tools.hgfsServerSet.disable`

6 Cliquez sur **OK**.

Désactiver les transferts de fichiers HGFS

Certaines opérations telles que les mises à niveau d'outils automatisées utilisent le composant HGFS (host guest file system) de l'hyperviseur. Dans les environnement hautement sécurisés, vous pouvez désactiver ce composant pour minimiser le risque d'utilisation du système HGFS par un pirate pour transférer des fichiers dans le système d'exploitation invité.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Vérifiez que le paramètre `isolation.tools.hgfsServerSet.disable` est défini sur **TRUE**.

Résultats

Lorsque vous apportez cette modification, le processus VMX ne répond plus aux commandes du processus tools. Les API qui utilisent HGFS pour transférer des fichiers vers et depuis le système d'exploitation invité, telles que certaines commandes VIX ou l'utilitaire de mise à niveau automatique de VMware Tools, ne fonctionnent plus.

Désactiver les opérations Copier et Coller entre le système d'exploitation client et la console distante

Les opérations Copier et Coller entre le système d'exploitation hôte et la console distante sont désactivées par défaut. Pour un environnement sécurisé, conservez ce paramétrage par défaut. Si vous avez besoin d'effectuer des opérations Copier et Coller, vous devez les activer en utilisant vSphere Web Client.

Ces options sont réglées sur la valeur recommandée par défaut. Toutefois, vous devez les régler sur vrai explicitement si vous souhaitez activer des outils d'audit pour vérifier que le réglage est correct.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

- 1 Ouvrez une session sur un système vCenter Server au moyen de vSphere Web Client.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.

- 3 Cliquez sur **Options VM**, puis cliquez sur **Modifier la configuration**.
- 4 Assurez-vous que les valeurs suivantes sont dans les colonnes de nom et de valeur, ou cliquez sur **Ajouter ligne** pour les ajouter.

Nom	Valeur recommandée
isolation.tools.copy.disable	vrai
isolation.tools.paste.disable	vrai
isolation.tools.setGUIOptions.enable	false

Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.

- 5 Cliquez sur **OK**.
- 6 (Facultatif) Si vous avez modifié les paramètres de configuration, redémarrez la machine virtuelle.

Limitation de l'exposition des données sensibles copiées dans le presse-papiers

Par défaut, les opérations Copier et Coller sont désactivées pour les hôtes, afin d'éviter d'exposer les données sensibles copiées dans le presse-papiers.

Lorsque les opérations Copier et Coller sont activées sur une machine virtuelle utilisant VMware Tools, vous pouvez copier et coller des données entre le système d'exploitation invité et la console distante. Dès que la fenêtre de la console s'affiche, les utilisateurs et les processus ne disposant pas de privilèges d'accès et utilisant la machine virtuelle peuvent accéder au presse-papiers de sa console. Si un utilisateur copie des informations sensibles dans le presse-papiers avant d'utiliser la console, il expose (involontairement) des données sensibles au niveau de la machine virtuelle. Pour éviter ce problème, les opérations Copier et Coller sont par défaut désactivées sur le système d'exploitation invité.

En cas de besoin, vous pouvez activer ces opérations pour les machines virtuelles.

Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle

Par défaut, un utilisateur avec le rôle d'administrateur vCenter Server peut interagir avec les fichiers et programmes au sein du système d'exploitation invité d'une machine virtuelle. Afin de réduire les risques d'atteinte à la confidentialité, la disponibilité et l'intégrité de l'invité, créez un rôle d'accès non-invité, dépourvu du privilège **Opérations client**.

Pour garantir la sécurité, appliquez les mêmes restrictions pour l'accès au centre de données virtuel que pour l'accès au centre de données physique. Pour éviter d'octroyer un accès administrateur complet aux utilisateurs, créez un rôle personnalisé qui désactive l'accès invité et appliquez ce rôle aux utilisateurs qui ont besoin de disposer de privilèges d'administrateur, mais qui ne sont pas autorisés à interagir avec les fichiers et les programmes au sein du système d'exploitation invité.

Prenons, par exemple, une configuration composée d'une machine virtuelle placée dans une infrastructure contenant des informations sensibles. Pour des tâches telles que la migration avec vMotion et Storage vMotion, le responsable informatique doit avoir accès à la machine virtuelle. Dans ce cas, désactivez certaines opérations distantes au sein du système d'exploitation invité afin de vous assurer que le responsable informatique n'a pas accès aux informations sensibles.

Conditions préalables

Vérifiez que vous avez les privilèges **Administrateur** sur le système vCenter Server sur lequel vous créez le rôle.

Procédure

- 1 Connectez-vous à vSphere Web Client en tant qu'utilisateur possédant des privilèges **Administrateur** sur le système vCenter Server sur lequel vous créez le rôle.
- 2 Cliquez sur **Administration** et sélectionnez **Rôles**.
- 3 Cliquez sur l'icône **Créer une action de rôle** et tapez le nom que vous souhaitez attribuer au rôle.
Par exemple, entrez **Accès non-invité administrateur**.
- 4 Sélectionnez **Tous les privilèges**.
- 5 Désélectionnez **Tous les privilèges.Machine virtuelle.Opérations client** pour supprimer l'ensemble des privilèges Opérations client.
- 6 Cliquez sur **OK**.

Étape suivante

Sélectionnez le système vCenter Server ou l'hôte et attribuez une autorisation qui couple l'utilisateur ou le groupe requérant les nouveaux privilèges avec le rôle que vous venez de créer. Supprimez ces utilisateurs du rôle d'administrateur par défaut.

Interdiction pour les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques

Les utilisateurs et processus sans privilèges racine ou administrateur au sein d'une machine virtuelle ont la possibilité de connecter ou déconnecter des périphériques, comme les adaptateurs réseau et les lecteurs de CD-ROM, ainsi que la capacité de modifier les paramètres des périphériques. Afin de renforcer la sécurité des machines virtuelles, supprimez ces périphériques. Si vous ne souhaitez pas supprimer en permanence un périphérique, vous pouvez empêcher un utilisateur ou un processus de machine virtuelle de déconnecter ce périphérique du système d'exploitation invité.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Vérifiez que les valeurs suivantes sont dans les colonnes de nom et de valeur, ou cliquez sur **Ajouter ligne** pour les ajouter.

Nom	Valeur
<code>isolation.device.connectable.disable</code>	true
<code>isolation.device.edit.disable</code>	true

Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.

- 6 Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de configuration, puis cliquez de nouveau sur **OK**.

Modification de la limite de mémoire variable du système d'exploitation invité

Vous pouvez augmenter la limite de mémoire variable du système d'exploitation invité si de grandes quantités d'informations personnalisées sont stockées dans le fichier de configuration.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM > Avancées**, puis cliquez sur **Modifier la configuration**.
- 4 Ajoutez ou modifiez le paramètre `tools.setInfo.sizeLimit` et définissez la valeur en nombre d'octets.
- 5 Cliquez sur **OK**.

Empêcher les processus du système d'exploitation invité d'envoyer des messages de configuration à l'hôte

Vous pouvez empêcher les invités d'écrire des paires nom/valeur dans le fichier de configuration. Cette mesure est appropriée lorsque les systèmes d'exploitation invités ne doivent pas être autorisés à modifier les paramètres de configuration.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

- 1 Trouvez la machine virtuelle dans l'inventaire vSphere Web Client.
 - a Sélectionnez un centre de données, un dossier, un cluster, un pool de ressources ou un hôte.
 - b Cliquez sur l'onglet **Objets associés**, puis cliquez sur **Machines virtuelles**.
- 2 Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
- 3 Sélectionnez **Options VM**.
- 4 Cliquez sur **Avancées**, puis cliquez sur **Modifier la configuration**.
- 5 Cliquez sur **Ajouter ligne** et tapez les valeurs suivantes dans les colonnes de nom et de valeur.
 - Dans la colonne de nom : `isolation.tools.setinfo.disable`
 - Dans la colonne de valeur : `vrai`
- 6 Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de configuration, puis cliquez de nouveau sur **OK**.

Éviter d'utiliser des disques indépendants non persistants

Lorsque vous utilisez des disques indépendants non permanents, des pirates peuvent supprimer toute évidence que la machine a été compromise en arrêtant ou en redémarrant le système. Sans un enregistrement permanent des activités sur une machine virtuelle, une attaque risque de ne pas être décelée par les administrateurs. Il convient donc d'éviter d'utiliser des disques indépendants non permanents.

Procédure

- ◆ Assurez-vous que l'activité de la machine virtuelle est consignée à distance sur un serveur séparé, par exemple un serveur syslog ou un collecteur d'événements Windows équivalent.
- Si la journalisation à distance des événements n'est pas configurée pour l'invité, scsiX:Y.mode doit prendre l'une des valeurs suivantes :
- Pas présent
 - Non défini sur indépendant non permanent

Résultats

Lorsque le mode non permanent n'est pas activé, vous ne pouvez pas remettre une machine virtuelle à un état connu lors du redémarrage du système.

Sécurisation de la mise en réseau vSphere



La sécurisation de la mise en réseau vSphere constitue une part essentielle de la protection de votre environnement. Vous sécurisez différents composants vSphere de différentes manières. Pour plus d'informations sur la mise en réseau dans l'environnement vSphere, reportez-vous à la documentation *Mise en réseau vSphere*.

Ce chapitre contient les rubriques suivantes :

- Introduction à la sécurité du réseau vSphere
- Sécurisation du réseau avec des pare-feu
- Sécuriser le commutateur physique
- Sécurisation des ports du commutateur standard à l'aide de stratégies de sécurité
- Sécuriser les commutateurs standard vSphere
- Sécuriser les commutateurs distribués vSphere et les groupes de ports distribués
- Sécurisation des machines virtuelles avec des VLAN
- Créer une DMZ réseau sur un hôte ESXi
- Création de plusieurs réseaux sur un hôte ESXi
- Sécurité du protocole Internet
- Garantir une configuration SNMP appropriée
- Utiliser des commutateurs virtuels avec l'API vSphere Network Appliance, uniquement si nécessaire
- Meilleures pratiques en matière de sécurité de la mise en réseau vSphere

Introduction à la sécurité du réseau vSphere

La sécurité du réseau dans l'environnement vSphere partage de nombreuses caractéristiques de sécurisation d'un environnement de réseau physique, mais inclut également des caractéristiques qui s'appliquent uniquement aux machines virtuelles.

Pare-feu

Ajoutez une protection par pare-feu à votre réseau virtuel en installant et en configurant des pare-feu hébergés sur hôte sur certaines ou la totalité de ses machines virtuelles.

Pour une plus grande efficacité, vous pouvez configurer des réseaux Ethernet privés de machines virtuelles ou des réseaux virtuels. Avec les réseaux virtuels, vous installez un pare-feu hébergé sur hôte sur une machine virtuelle à la tête du réseau virtuel. Ce pare-feu sert de tampon de protection entre l'adaptateur réseau physique et les machines virtuelles restantes du réseau virtuel.

Étant donné que les pare-feu hébergés sur hôte peuvent ralentir les performances, équilibrez vos besoins en sécurité par rapport aux objectifs de performances avant d'installer des pare-feu hébergés sur hôte sur des machines virtuelles ailleurs dans le réseau virtuel.

Reportez-vous à la section [Sécurisation du réseau avec des pare-feu](#).

Segmentation

Conservez différentes zones de machines virtuelles au sein d'un hôte sur différents segments du réseau. Si vous isolez chaque zone de machines virtuelles sur leur propre segment de réseau, vous réduisez le risque de fuite de données d'une zone de machines virtuelles à la suivante. La segmentation empêche diverses menaces, y compris l'usurpation d'adresse ARP (Address Resolution Protocol), dans laquelle un attaquant manipule la table ARP pour remapper les adresses MAC et IP, obtenant ainsi accès au trafic réseau de et vers un hôte. Les pirates utilisent la falsification de la réponse ARP (ARP spoofing) pour générer des attaques « Man in the Middle » (MITM), effectuer des attaques par déni de service (DoS), pirater le système cible ou perturber le réseau virtuel.

La planification soignée de la segmentation réduit les chances de transmissions de paquets entre les zones de machines virtuelles, ce qui empêche les attaques de reniflement qui nécessitent l'envoi de trafic réseau à la victime. Par conséquent, un attaquant ne peut pas utiliser un service non sécurisé sur une zone de machines virtuelles pour accéder aux autres zones de machines virtuelles de l'hôte. Vous pouvez implémenter la segmentation à l'aide de l'une des deux approches suivantes, chacune d'entre elles ayant des avantages différents.

- Utilisez des adaptateurs réseau physiques séparés pour des zones de machines virtuelles afin de garantir que les zones sont isolées. Conserver des adaptateurs réseau physiques séparés pour des zones de machines virtuelles est probablement la méthode la plus sécurisée et moins susceptible de subir une configuration incorrecte après la création des segments initiaux.
- Configurez des réseaux locaux virtuels (VLAN) pour protéger votre réseau. Comme les VLAN disposent de presque tous les avantages de sécurité inhérents à l'implémentation de réseaux séparés physiquement sans surcharge matérielle, ils offrent une solution viable pouvant vous économiser les coûts de déploiement et d'entretien de périphériques, câblages, etc. supplémentaires. Reportez-vous à la section [Sécurisation des machines virtuelles avec des VLAN](#).

Prévention de l'accès non autorisé

Si votre réseau de machines virtuelles est connecté à un réseau physique, il peut être soumis à des défaillances tout comme un réseau constitué de machines physiques. Même si le réseau de machines virtuelles est isolé de tout réseau physique, les machines virtuelles du réseau peuvent être soumises à des attaques d'autres machines virtuelles du réseau. Les contraintes de sécurisation des machines virtuelles sont souvent identiques à celles des machines physiques.

Les machines virtuelles sont isolées les unes des autres. Une machine virtuelle ne peut pas lire ou écrire sur la mémoire d'une autre machine virtuelle, accéder à ses données, utiliser ses applications, etc. Cependant, dans le réseau, toute machine virtuelle ou groupes de machines virtuelles peut toujours être la cible d'un accès non autorisé à partir d'autres machines virtuelles et peut nécessiter une protection supplémentaire par des moyens externes.

Sécurisation du réseau avec des pare-feu

Les administrateurs de sécurité utilisent des pare-feu pour protéger le réseau ou les composants sélectionnés dans le réseau des intrusions.

Les pare-feu contrôlent l'accès aux périphériques dans leur périmètre en fermant tous les ports, excepté pour ceux que l'administrateur désigne explicitement ou implicitement comme autorisés. Les ports que les administrateurs ouvrent permettent le trafic entre les périphériques sur différents côtés du pare-feu.

Important Le pare-feu ESXi d'ESXi 5.5 et versions ultérieures n'autorise pas le filtrage par réseau du trafic vMotion. Par conséquent, vous devez établir des règles sur votre pare-feu externe pour vous assurer qu'aucune connexion entrante ne peut être réalisée vers le socket vMotion.

Dans un environnement de machines virtuelles, vous pouvez planifier la disposition des pare-feu entre les composants.

- Pare-feu entre machines physiques telles que des systèmes vCenter Server et des hôtes ESXi.
- Pare-feu entre une machine virtuelle et une autre, par exemple entre une machine virtuelle agissant comme serveur Web externe et une machine virtuelle connectée au réseau interne de votre entreprise.
- Pare-feu entre une machine physique et une machine virtuelle, par exemple lorsque vous placez un pare-feu entre une carte réseau physique et une machine virtuelle.

L'utilisation des pare-feu dans une configuration ESXi dépend de la manière dont vous planifiez l'utilisation du réseau et du niveau de sécurité dont certains composants ont besoin. Par exemple, si vous créez un réseau virtuel où chaque machine virtuelle est dédiée à l'exécution d'une suite de tests de référence différents pour le même service, le risque d'accès non autorisé d'une machine virtuelle à une autre est minime. Par conséquent, une configuration où des pare-feu sont présents entre les machines virtuelles n'est pas nécessaire. Cependant, pour empêcher l'interruption d'un test exécuté à partir d'un hôte externe, vous pouvez configurer un pare-feu au point d'entrée du réseau virtuel pour protéger tout l'ensemble de machines virtuelles.

Pour un diagramme des ports de pare-feu, reportez-vous à l'article [2131180](#) de la base de connaissances VMware.

Pare-feux pour configurations avec vCenter Server

Si vous accédez aux hôtes ESXi par l'intermédiaire de vCenter Server, vous protégez généralement vCenter Server à l'aide d'un pare-feu. Ce pare-feu fournit une protection de base à votre réseau.

Il peut y avoir un pare-feu entre les clients et vCenter Server. En fonction de votre déploiement, il se peut aussi que vCenter Server et les clients se trouvent tous les deux derrière le pare-feu. L'important est de s'assurer qu'un pare-feu est présent sur ce que vous considérez être un point d'entrée pour le système.

Pour obtenir la liste complète des ports TCP et UDP, y compris ceux de vSphere vMotion™ et vSphere Fault Tolerance, consultez [Ports TCP et UDP pour vCenter Server](#).

Les réseaux configurés avec vCenter Server peuvent recevoir des communications par l'intermédiaire de vSphere Web Client ou de clients de gestion de réseau tiers qui utilisent SDK pour communiquer avec l'hôte. Pendant le fonctionnement normal, vCenter Server écoute les données de ses hôtes et clients gérés sur les ports désignés. vCenter Server suppose aussi que ces hôtes gérés écoutent les données de vCenter Server sur les ports désignés. Si un pare-feu est présent entre l'un de ces éléments, vous devez vous assurer que le pare-feu a des ports ouverts pour prendre en charge le transfert des données.

Vous pouvez également inclure des pare-feu à un grand nombre d'autres points d'accès du réseau, en fonction de la manière dont vous envisagez d'utiliser le réseau et du niveau de sécurité nécessaire aux différents périphériques. Sélectionnez les emplacements de vos pare-feu en fonction des risques de sécurité que vous avez identifiés pour votre configuration réseau. Vous trouverez ci-après une liste des emplacements de pare-feu commune aux implémentations ESXi.

- Entre vSphere Web Client ou un client de gestion de réseau tiers et vCenter Server.
- Si vos utilisateurs accèdent aux machines virtuelles via un navigateur Web, entre le navigateur Web et l'hôte ESXi.
- Si vos utilisateurs accèdent à des machines virtuelles par l'intermédiaire de vSphere Web Client, entre vSphere Web Client et l'hôte ESXi. Cette connexion s'ajoute à la connexion entre vSphere Web Client et vCenter Server et elle nécessite un port différent.
- Entre vCenter Server et les hôtes ESXi.
- Entre les hôtes ESXi de votre réseau. Bien que le trafic entre les hôtes soit généralement considéré comme sécurisé, vous pouvez ajouter des pare-feu entre eux si vous vous inquiétez des défaillances de sécurité de machine à machine.

Si vous ajoutez des pare-feu entre les hôtes ESXi et envisagez de migrer les machines virtuelles entre les serveurs, faites un clonage ou utilisez vMotion. Vous devez également ouvrir des ports dans les pare-feu qui divisent l'hôte source des hôtes cibles afin que la source et les cibles puissent communiquer.

- Entre les hôtes ESXi et le stockage réseau tel que le stockage NFS ou iSCSI. Ces ports ne sont pas spécifiques à VMware et vous pouvez les configurer en fonction des spécifications de votre réseau.

Connexion à vCenter Server via un pare-feu

vCenter Server utilise le port TCP 443 pour surveiller les transferts de données à partir de ses clients. Si vous disposez d'un pare-feu placé entre vCenter Server et ses clients, vous devez configurer la connexion par l'intermédiaire de laquelle vCenter Server peut recevoir des données des clients.

Ouvrez le port TCP 443 dans le pare-feu pour permettre à vCenter Server de recevoir des données de vSphere Web Client. La configuration du pare-feu dépend de ce qui est utilisé sur votre site. Renseignez-vous auprès de l'administrateur système de votre pare-feu local.

Si vous ne souhaitez pas utiliser le port 443 comme port pour la communication entre vSphere Web Client et vCenter Server, vous pouvez basculer sur un autre port en modifiant les paramètres de vCenter Server à partir de vSphere Web Client. Consultez la documentation de *Gestion de vCenter Server et des hôtes*.

Si vous utilisez encore vSphere Client, consultez la *documentation Administration de vSphere avec vSphere Client*.

Pare-feu pour configurations sans vCenter Server

Vous pouvez connecter des clients directement à votre réseau ESXi au lieu d'utiliser vCenter Server.

Les réseaux configurés sans vCenter Server reçoivent des communications via vSphere Client, l'une des interfaces de ligne de commande de vSphere, les vSphere Web Services SDK ou des clients tiers. Les besoins de pare-feu sont en majeure partie les mêmes qu'en présence de vCenter Server, mais il y a plusieurs différences clés.

- Tout comme pour les configurations comprenant vCenter Server, assurez-vous qu'un pare-feu est présent pour protéger votre couche ESXi, en fonction de votre configuration, vos clients et votre couche ESXi. Ce pare-feu fournit une protection de base à votre réseau.
- La licence pour ce type de configuration fait partie du module ESXi que vous installez sur chacun des hôtes. Comme la licence réside sur le serveur, un serveur de licences distinct n'est pas nécessaire. Un pare-feu entre le serveur de licences et le réseau ESXi n'est donc pas nécessaire.

Vous pouvez configurer des ports de pare-feu à l'aide d'ESXCLI en utilisant vSphere Client ou des règles de pare-feu. Reportez-vous à [Configuration du pare-feu ESXi](#).

Connexion des hôtes ESXi via des pare-feu

Si un pare-feu se trouve entre deux hôtes ESXi et que vous souhaitez autoriser des transactions entre les hôtes ou utiliser vCenter Server pour effectuer des activités sources ou cibles, telles que

du trafic vSphere High Availability (vSphere HA), une migration, un clonage ou vMotion, vous devez configurer une connexion par laquelle les hôtes gérés peuvent recevoir des données.

Pour configurer une connexion pour recevoir des données, ouvrez les ports au trafic des services tels que vSphere High Availability, vMotion, et vSphere Fault Tolerance. Reportez-vous à [Configuration du pare-feu ESXi](#) pour consulter une description des fichiers de configuration, de l'accès à vSphere Web Client et des commandes de pare-feu. Reportez-vous à [Ports de pare-feu entrants et sortants pour les hôtes ESXi](#) pour obtenir une liste de ports. Consultez l'administrateur système du pare-feu pour plus d'informations sur la configuration des ports.

Connexion à la console de la machine virtuelle via un pare-feu

Certains ports doivent être ouverts pour la communication utilisateur et administrateur avec la console de machine virtuelle. Les ports nécessitant d'être ouverts varient selon le type de console de machine virtuelle et si vous vous connectez via vCenter Server avec vSphere Web Client ou directement à l'hôte ESXi depuis vSphere Client.

Connexion à une console de machine virtuelle basée sur une interface de navigation au moyen vSphere Web Client

Lorsque vous vous connectez avec vSphere Web Client, vous vous connectez toujours au système vCenter Server qui gère l'hôte ESXi et accédez à la console de machine virtuelle depuis là.

Si vous utilisez vSphere Web Client et que vous vous connectez à une console de machine virtuelle basée sur une interface de navigation, l'accès suivant doit être possible :

- Le pare-feu doit autoriser vSphere Web Client à accéder à vCenter Server par le port 9443.
- Le pare-feu doit autoriser vCenter Server à accéder à ESXi par le port 902.

Connexion à une console de machine virtuelle autonome au moyen vSphere Web Client

Si vous utilisez vSphere Web Client et que vous vous connectez à une console de machine virtuelle autonome, l'accès suivant doit être possible :

- Le pare-feu doit autoriser vSphere Web Client à accéder à vCenter Server par le port 9443.
- Le pare-feu doit autoriser la console de machine virtuelle à accéder à vCenter Server par le port 9443 et à l'hôte ESXi par le port 902.

Connexion aux hôtes ESXi directement avec vSphere Client

Vous pouvez utiliser la console de machine virtuelle vSphere Client si vous vous connectez directement à un hôte ESXi.

Note N'utilisez pas vSphere Client pour vous connecter directement aux hôtes gérés par un système vCenter Server. Si vous apportez des modifications à de tels hôtes depuis vSphere Client, votre environnement devient instable.

Le pare-feu doit autoriser l'accès à l'hôte ESXi sur les ports 443 et 902

vSphere Client utilise le port 902 pour fournir une connexion pour les activités MKS du système d'exploitation invité sur les machines virtuelles. C'est par ce port que les utilisateurs interagissent avec les systèmes d'exploitation et les applications invités de la machine virtuelle. VMware ne prend pas en charge la configuration d'un port différent pour cette fonction.

Sécuriser le commutateur physique

Sécurisez le commutateur physique sur chaque hôte ESXi pour empêcher les pirates d'obtenir accès à l'hôte et à ses machines virtuelles.

Pour garantir la meilleure protection de vos hôtes, assurez-vous que la configuration des ports du commutateur physique désactive le protocole STP (Spanning Tree Protocol) et que l'option de non-négociation est configurée pour les liaisons de jonction entre les commutateurs physiques externes et les commutateurs virtuels en mode VST (Virtual Switch Tagging).

Procédure

- 1 Connectez-vous au commutateur physique et assurez-vous que le protocole Spanning Tree est désactivé ou que PortFast est configuré pour tous les ports de commutateur physique qui sont connectés aux hôtes ESXi.
- 2 Pour des machines virtuelles qui effectuent un pontage ou un routage, vérifiez périodiquement que la configuration du premier port de commutateur physique en amont désactive BPDU Guard et PortFast et active le protocole Spanning Tree.

Dans vSphere 5.1 et versions ultérieures, pour protéger le commutateur physique des attaques de déni de service (DoS), vous pouvez activer le filtrage BPDU invité sur les hôtes ESXi.
- 3 Connectez-vous au commutateur physique et assurez-vous que le protocole DTP (Dynamic Trunking Protocol) n'est pas activé sur les ports du commutateur physique qui sont connectés aux hôtes ESXi.
- 4 Vérifiez régulièrement les ports du commutateur physique pour vous assurer qu'ils sont correctement configurés comme ports de jonction s'ils sont connectés à des ports de jonction VLAN d'un commutateur virtuel.

Sécurisation des ports du commutateur standard à l'aide de stratégies de sécurité

Tout comme pour les adaptateurs réseau physiques, un adaptateur réseau de machine virtuelle peut envoyer des trames qui semblent provenir d'une autre machine ou emprunter l'identité d'une autre machine afin de pouvoir recevoir des trames réseau destinées à cette machine. Par conséquent, tout comme les adaptateurs réseau physiques, un adaptateur réseau de machine virtuelle peut être configuré afin de recevoir des trames destinées à d'autres machines. Ces deux scénarios représentent un risque pour la sécurité.

Lorsque vous créez un commutateur standard pour votre réseau, vous ajoutez des groupes de ports dans vSphere Web Client pour imposer aux machines virtuelles et aux adaptateurs VMkernel une stratégie concernant le trafic système lié au commutateur.

Dans le cadre de l'ajout d'un groupe de ports VMkernel ou d'un groupe de ports de machine virtuelle à un commutateur standard, ESXi configure une stratégie de sécurité pour les ports du groupe. Vous pouvez utiliser ce profil de sécurité pour garantir que l'hôte empêche les systèmes d'exploitation invités de ses machines virtuelles d'emprunter l'identité d'autres machines sur le réseau. Cette fonction de sécurité est implémentée afin que le système d'exploitation invité responsable de l'emprunt d'identité ne détecte pas que l'emprunt d'identité a été empêché.

La stratégie de sécurité détermine le niveau d'intensité avec lequel vous appliquez la protection contre l'emprunt d'identité et les attaques d'interception sur les machines virtuelles. Pour utiliser correctement les paramètres du profil de sécurité, vous devez comprendre comment les adaptateurs réseau de machines virtuelles contrôlent les transmissions et la manière dont les attaques sont contrées à ce niveau. Consultez la section Stratégies de sécurité dans *Mise en réseau vSphere*.

Sécuriser les commutateurs standard vSphere

Vous pouvez sécuriser le trafic de commutation standard contre les attaques de couche 2 en limitant certains modes d'adresses MAC à l'aide des paramètres de sécurité des commutateurs.

Chaque adaptateur réseau de la machine virtuelle dispose d'une adresse MAC initiale et d'une adresse MAC effective.

Adresse MAC initiale

L'adresse MAC initiale est attribuée lors de la création de l'adaptateur. Bien que l'adresse MAC initiale puisse être reconfigurée à partir de l'extérieur du système d'exploitation invité, elle ne peut pas être modifiée par le système d'exploitation invité.

Adresse MAC effective

Chaque adaptateur dispose d'une adresse MAC effective qui filtre le trafic réseau entrant avec une adresse MAC de destination différente de l'adresse MAC effective. Le système d'exploitation invité est responsable de la définition de l'adresse MAC effective et fait généralement correspondre l'adresse MAC effective à l'adresse MAC initiale.

Lors de la création de l'adaptateur réseau d'une machine virtuelle, l'adresse MAC effective et l'adresse MAC initiale sont identiques. Le système d'exploitation invité peut à tout moment remplacer l'adresse MAC effective par une autre valeur. Si un système d'exploitation modifie l'adresse MAC effective, son adaptateur réseau reçoit le trafic réseau destiné à la nouvelle adresse MAC.

Lors de l'envoi de paquets via un adaptateur réseau, le système d'exploitation invité place généralement sa propre adresse MAC effective de l'adaptateur dans la zone de l'adresse MAC source des trames Ethernet. Il place l'adresse MAC de l'adaptateur réseau récepteur dans la zone d'adresse MAC de destination. L'adaptateur récepteur accepte les paquets uniquement si l'adresse MAC de destination du paquet correspond à sa propre adresse MAC effective.

Un système d'exploitation peut envoyer des trames avec une adresse MAC source usurpée. Cela signifie qu'un système d'exploitation peut bloquer les attaques nuisibles sur les périphériques dans un réseau en empruntant l'identité d'un adaptateur réseau que le réseau récepteur autorise.

Protégez le trafic virtuel contre l'emprunt d'identité et les attaques de couche 2 d'interception en configurant une stratégie de sécurité sur les groupes de ports ou les ports.

La stratégie de sécurité sur les groupes de ports distribués et les ports inclut les options suivantes :

- Mode promiscuité (reportez-vous à [Fonctionnement en mode promiscuité](#))
- Modifications d'adresse MAC (reportez-vous à [Modifications d'adresse MAC](#))
- Transmissions forgées (reportez-vous à [Transmissions forgées](#))

Vous pouvez afficher et modifier les paramètres par défaut en sélectionnant le commutateur virtuel associé à l'hôte dans vSphere Web Client. Consultez la documentation de *Mise en réseau vSphere*.

Modifications d'adresse MAC

La règle de sécurité d'un commutateur virtuel inclut une option **Modifications d'adresse MAC**. Cette option affecte le trafic qu'une machine virtuelle reçoit.

Lorsque l'option **Modifications d'adresse Mac** est définie sur **Accepter**, ESXi accepte les demandes de modification de l'adresse MAC effective en une adresse différente de l'adresse MAC initiale.

Lorsque l'option **Modifications d'adresse Mac** est définie sur **Rejeter**, ESXi n'honore pas les demandes de modification de l'adresse MAC effective en une adresse différente de l'adresse MAC initiale. Ce paramètre protège l'hôte contre l'emprunt d'identité MAC. Le port que l'adaptateur de machine virtuelle a utilisé pour envoyer la demande est désactivé et l'adaptateur de machine virtuelle ne reçoit plus de trames jusqu'à ce que l'adresse MAC effective corresponde à l'adresse MAC initiale. Le système d'exploitation invité ne détecte pas que la demande de modification d'adresse MAC n'a pas été honorée.

Note L'initiateur iSCSI repose sur la capacité à obtenir les modifications d'adresse MAC de certains types de stockage. Si vous utilisez iSCSI ESXi avec un stockage iSCSI, définissez l'option **Modifications d'adresse MAC** sur **Accepter**.

Dans certaines situations, vous pouvez avoir un besoin légitime d'attribuer la même adresse MAC à plusieurs adaptateurs, par exemple, si vous utilisez l'équilibrage de la charge réseau Microsoft en mode monodiffusion. Lorsque l'équilibrage de la charge réseau Microsoft est utilisé en mode multidiffusion standard, les adaptateurs ne partagent pas les adresses MAC.

Transmissions forgées

L'option **Transmissions forgées** affecte le trafic transmis à partir d'une machine virtuelle.

Lorsque l'option **Transmissions forgées** est définie sur **Accepter**, ESXi ne compare les adresses MAC source et effective.

Pour se protéger d'un emprunt d'identité MAC, vous pouvez définir l'option **Transmissions forgées** sur **Rejeter**. Dans ce cas, l'hôte compare l'adresse MAC source que transmet le système d'exploitation invité avec l'adresse MAC effective de son adaptateur de machine virtuelle pour déterminer si elles correspondent. Si elles ne correspondent pas, l'hôte ESXi abandonne le paquet.

Le système d'exploitation invité ne détecte pas que son adaptateur de machine virtuelle ne peut pas envoyer de paquets à l'aide de l'adresse MAC usurpée. L'hôte ESXi intercepte les paquets avec des adresses usurpées avant leur livraison, et le système d'exploitation invité peut supposer que les paquets sont rejetés.

Fonctionnement en mode promiscuité

Le mode promiscuité élimine tout filtrage de réception que l'adaptateur de machine virtuelle peut effectuer afin que le système d'exploitation invité reçoive tout le trafic observé sur le réseau. Par défaut, l'adaptateur de machine virtuelle ne peut pas fonctionner en mode promiscuité.

Bien que le mode promiscuité puisse être utile pour le suivi de l'activité réseau, c'est un mode de fonctionnement non sécurisé, car les adaptateurs en mode promiscuité ont accès aux paquets, même si certains de ces paquets sont reçus uniquement par un adaptateur réseau spécifique. Cela signifie qu'un administrateur ou un utilisateur racine dans une machine virtuelle peut potentiellement voir le trafic destiné à d'autres systèmes d'exploitation hôtes ou invités.

Note Dans certaines situations, vous pouvez avoir une raison légitime de configurer un commutateur virtuel standard ou distribué pour fonctionner en mode promiscuité ; par exemple, si vous exécutez un logiciel de détection des intrusions réseau ou un renifleur de paquets.

Sécuriser les commutateurs distribués vSphere et les groupes de ports distribués

Les administrateurs disposent de plusieurs options pour sécuriser un vSphere Distributed Switch dans leur environnement vSphere.

Procédure

- 1 Pour les groupes de ports distribués avec une liaison statique, vérifiez que la fonction Extension automatique est désactivée.

Extension automatique est activée par défaut dans vSphere 5.1 et versions ultérieures.

Pour désactiver Extension automatique, configurez la propriété `autoExpand` sous le groupe de ports distribués avec vSphere Web Services SDK ou avec une interface de ligne de commande. Reportez-vous à la documentation *vSphere Web Services SDK*.

- 2 Assurez-vous que tous les ID VLAN privés de tout vSphere Distributed Switch sont entièrement documentés.
- 3 Si vous utilisez le balisage VLAN sur un dvPortgroup, les ID de VLAN doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID de VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De la même manière, si des ID de VLAN sont incorrects ou manquants, le trafic risque de ne pas être transmis entre les machines physiques et virtuelles.
- 4 Vérifiez l'absence de ports inutilisés sur un groupe de ports virtuels associé à un vSphere Distributed Switch.
- 5 Attribuez un libellé à chaque vSphere Distributed Switch.

Les vSphere Distributed Switches associés à un hôte ESXi nécessitent un champ pour le nom du commutateur. Ce libellé sert de descripteur fonctionnel du commutateur, de même qu'un nom d'hôte associé à un commutateur physique. Le libellé du vSphere Distributed Switch indique la fonction ou le sous-réseau IP du commutateur. Par exemple, vous pouvez attribuer le libellé « interne » au commutateur pour indiquer qu'il est destiné uniquement à la mise en réseau interne d'un commutateur virtuel privé de machine virtuelle, sans liaison avec des adaptateurs réseau physiques.

- 6 Désactivez le contrôle de santé du réseau pour vos vSphere Distributed Switches si vous ne l'utilisez pas activement.

Le contrôle de santé du réseau est désactivé par défaut. Une fois qu'il est activé, les paquets de contrôle de santé contiennent des informations sur l'hôte, le commutateur et le port, susceptibles d'être utilisées par un pirate. N'utilisez le contrôle de santé du réseau que pour le dépannage et désactivez-le lorsque le dépannage est terminé.

- 7 Protégez le trafic virtuel contre l'emprunt d'identité et les attaques de couche 2 d'interception en configurant une stratégie de sécurité sur les groupes de ports ou les ports.

La stratégie de sécurité sur les groupes de ports distribués et les ports inclut les options suivantes :

- Mode promiscuité (reportez-vous à [Fonctionnement en mode promiscuité](#))
- Modifications d'adresse MAC (reportez-vous à [Modifications d'adresse MAC](#))
- Transmissions forgées (reportez-vous à [Transmissions forgées](#))

Pour consulter les paramètres actuels et les modifier, sélectionnez **Gérer des groupes de ports distribués** dans le menu contextuel (bouton droit de la souris) du Distributed Switch, puis sélectionnez **Sécurité** dans l'assistant. Consultez la documentation de *Mise en réseau vSphere*.

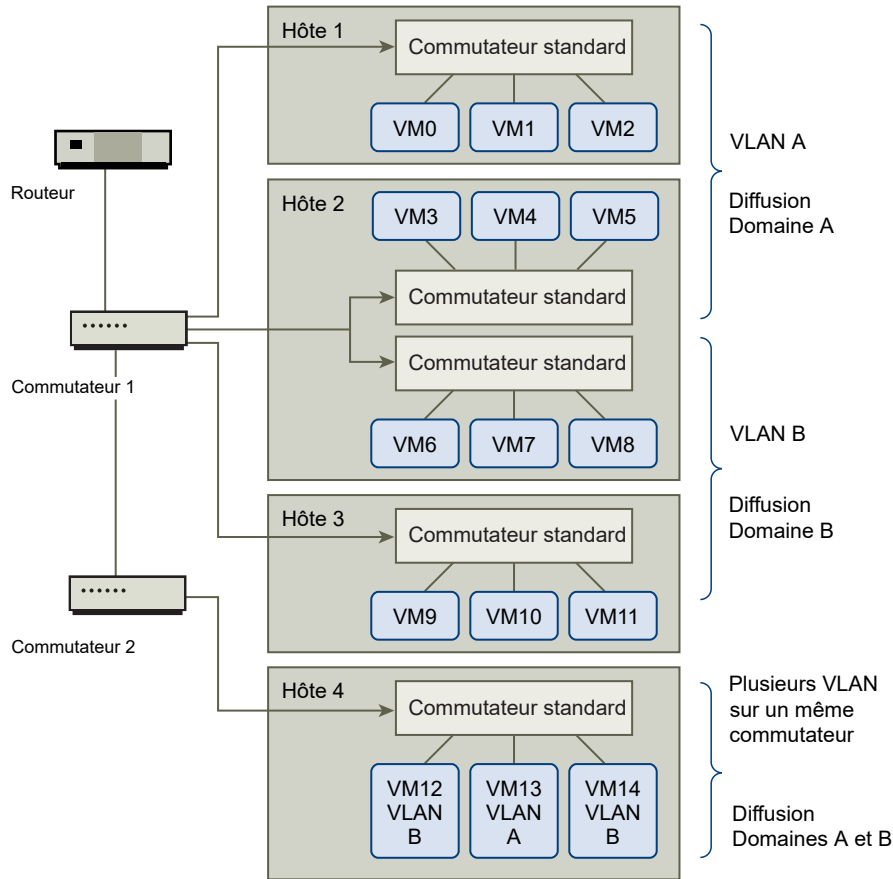
Sécurisation des machines virtuelles avec des VLAN

Le réseau peut être l'une des parties les plus vulnérables d'un système. Votre réseau de machines virtuelles nécessite autant de protection que votre réseau physique. L'utilisation des VLAN peut permettre d'améliorer la sécurité réseau dans votre environnement.

Les VLAN sont un schéma de réseau standard IEEE avec des méthodes de balisage spécifiques qui permettent le routage des paquets uniquement vers les ports faisant partie du VLAN. S'ils sont configurés correctement, les VLAN fournissent un moyen fiable pour protéger un ensemble de machines virtuelles des intrusions accidentelles et nuisibles.

Les VLAN vous permettent de segmenter un réseau physique afin que deux machines du réseau ne puissent pas transmettre et recevoir des paquets à moins de faire partie du même VLAN. Par exemple, les enregistrements de comptabilité et les transactions font partie des informations internes les plus sensibles d'une entreprise. Dans une entreprise dont les employés des ventes, des expéditions et de la comptabilité utilisent tous des machines virtuelles sur le même réseau physique, vous pouvez protéger les machines virtuelles du service de comptabilité en configurant des VLAN.

Figure 8-1. Exemple de disposition de VLAN



Dans cette configuration, tous les employés du service de comptabilité utilisent des machines virtuelles dans un VLAN A et les employés des ventes utilisent des machines virtuelles dans VLAN B.

Le routeur transmet les paquets contenant les données de comptabilité aux commutateurs. Ces paquets sont balisés pour une distribution sur le VLAN A uniquement. Par conséquent, les données sont confinées à une diffusion dans le domaine A et ne peuvent pas être acheminées pour une diffusion dans le domaine B à moins que le routeur ne soit configuré pour le faire.

Cette configuration de VLAN empêche les forces de vente d'intercepter les paquets destinés au service de comptabilité. Elle empêche également le service de comptabilité de recevoir des paquets destinés au groupes de ventes. Les machines virtuelles prises en charge par un seul commutateur virtuel peuvent se trouver sur des VLAN différents.

Considérations relatives à la sécurité pour les VLAN

La manière dont vous configurez les VLAN pour sécuriser des parties du réseau dépend de facteurs tels que le système d'exploitation invité et la façon dont votre équipement réseau est configuré.

ESXi dispose d'une implémentation VLAN complète conforme IEEE 802.1q. VMware ne peut pas faire de recommandations spécifiques sur la manière de configurer des VLAN, mais il existe des facteurs à prendre en compte lors de l'utilisation d'un déploiement VLAN dans le cadre de votre stratégie d'application de la sécurité.

Sécuriser les VLAN

Les administrateurs disposent de plusieurs options permettant de sécuriser les réseaux VLAN dans leur environnement vSphere.

Procédure

- 1 Assurez-vous que les groupes de ports ne sont pas configurés pour des valeurs VLAN réservées par les commutateurs physiques en amont

Ne définissez pas de valeurs ID VLAN réservées au commutateur physique.

- 2 Assurez-vous que les groupes de ports ne sont pas configurés sur VLAN 4095, sauf si vous utilisez le balisage d'invité virtuel (VGT).

Il existe trois types de balisage VLAN dans vSphere :

- Balisage de commutateur externe (EST)
- Balisage de commutateur virtuel (VST) - Le commutateur virtuel marque avec l'ID de VLAN le trafic qui entre dans les machines virtuelles attachées et supprime la balise VLAN du trafic qui les quitte. Pour configurer le mode VST, attribuez un ID VLAN compris entre 1 et 4095.
- Balisage d'invité virtuel (VGT) - Les machines virtuelles gèrent le trafic VLAN. Pour activer le mode VGT, définissez l'ID VLAN sur 4095. Sur un commutateur distribué, vous pouvez également autoriser le trafic d'une machine virtuelle en fonction de son réseau VLAN à l'aide de l'option **Jonction VLAN**.

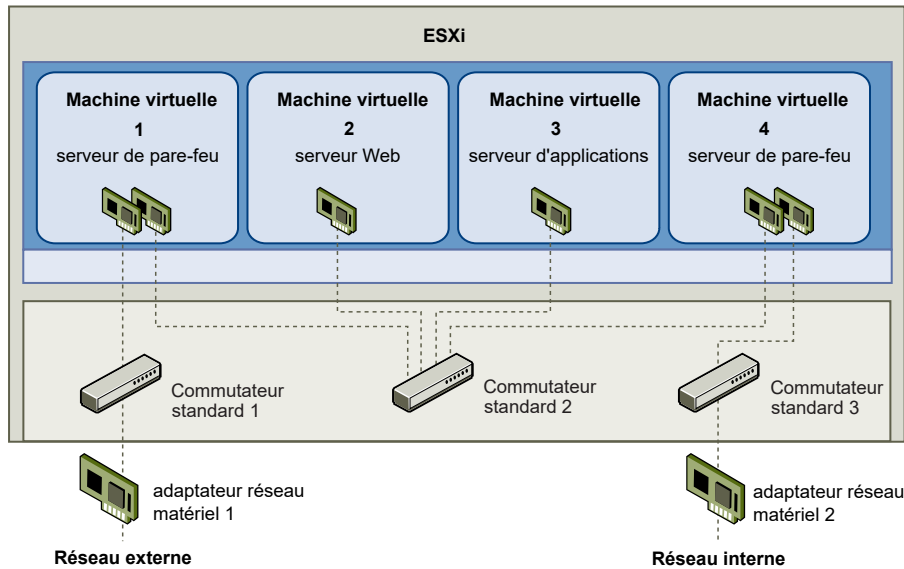
Sur un commutateur standard, vous pouvez configurer le mode de mise en réseau VLAN au niveau du commutateur ou du groupe de ports, et sur un commutateur distribué au niveau du groupe de ports distribués ou du port.

- 3 Assurez-vous que tous les réseaux VLAN de chaque commutateur virtuel sont pleinement documentés et que chaque commutateur virtuel dispose de tous les VLAN requis et des VLAN seulement nécessaires.

Créer une DMZ réseau sur un hôte ESXi

La création d'une zone démilitarisée (DMZ) réseau sur un hôte est un exemple d'utilisation des fonctions d'isolation et de mise en réseau virtuel d'ESXi pour configurer un environnement sécurisé.

Figure 8-2. DMZ configurée sur un hôte ESXi



Dans cet exemple, quatre machines virtuelles sont configurées en vue de créer une zone démilitarisée virtuelle sur le commutateur standard 2 :

- La machine virtuelle 1 et la machine virtuelle 4 exécutent des pare-feux et sont connectées aux adaptateurs réseau physiques par l'intermédiaire de commutateurs standard. Ces deux machines virtuelles utilisent plusieurs commutateurs.
- La machine virtuelle 2 s'exécute en tant que serveur Web, tandis que la machine virtuelle 3 s'exécute en tant que serveur d'applications. Ces deux machines virtuelles sont connectées à un commutateur virtuel.

Le serveur Web et le serveur d'applications occupent la DMZ entre les deux pare-feu. Le passage entre ces deux éléments est le commutateur standard 2, qui connecte les pare-feu aux serveurs. Ce commutateur ne possède pas de connexion directe aux éléments situés hors de la zone démilitarisée ; il est isolé du trafic externe via les deux pare-feu.

D'un point de vue opérationnel, le trafic externe Internet entre dans la machine virtuelle 1 via l'adaptateur réseau 1 (acheminé par le commutateur standard 1) ; il est alors vérifié par le pare-feu installé sur cette machine. Si le pare-feu autorise le trafic, celui-ci est acheminé vers le commutateur standard situé au sein de la zone démilitarisée (commutateur standard 2). Étant donné que le serveur Web et le serveur d'applications sont également connectés à ce commutateur, ils peuvent traiter des requêtes externes.

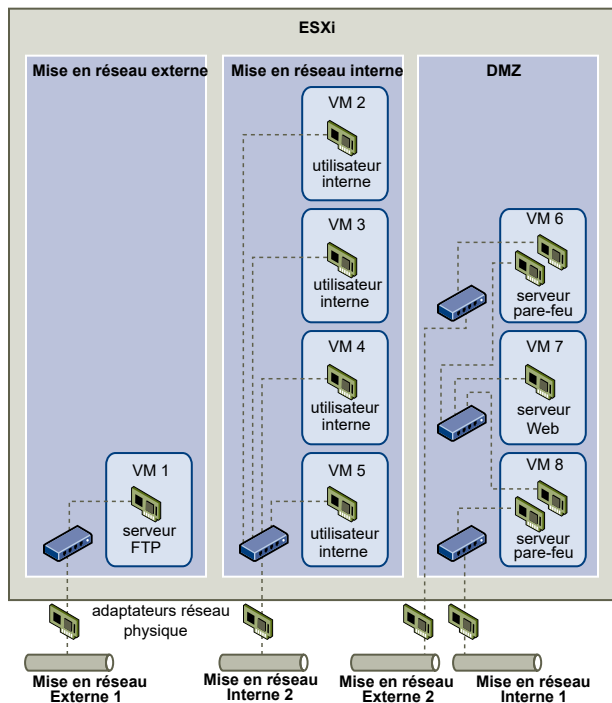
Le commutateur standard 2 est également connecté à la machine virtuelle 4. Cette machine virtuelle permet de bénéficier d'un pare-feu entre la DMZ et le réseau interne de l'entreprise. Ce pare-feu filtre les paquets en provenance du serveur Web et du serveur d'applications. Si un paquet est vérifié, il est acheminé vers l'adaptateur réseau 2 via le commutateur standard 3. L'adaptateur réseau 2 est connecté au réseau interne de l'entreprise.

Lorsque vous créez une DMZ sur un seul hôte, vous pouvez utiliser des pare-feu assez légers. Dans cette configuration, une machine virtuelle ne peut pas exercer un contrôle direct sur une autre machine virtuelle, ni accéder à sa mémoire ; toutefois, toutes les machines virtuelles restent connectées via un réseau virtuel. Or, ce réseau peut être utilisé pour la propagation de virus ou être la cible d'autres types d'attaques. La sécurité des machines virtuelles dans la zone démilitarisée revient donc à séparer des machines physiques connectées à un même réseau.

Création de plusieurs réseaux sur un hôte ESXi

Le système ESXi a été conçu pour vous permettre de connecter certains groupes de machines virtuelles au réseau interne, ainsi que d'autres groupes au réseau externe, et enfin d'autres groupes aux deux réseaux, le tout sur le même hôte. Cette capacité est une extension de l'isolation de machines virtuelles ; elle est associée à une optimisation de la planification d'utilisation des fonctions de réseau virtuel.

Figure 8-3. Réseaux externes, réseaux internes et DMZ configurée sur un hôte ESXi unique



Dans la figure, l'administrateur système a configuré un hôte dans trois zones différentes de machine virtuelle : sur le serveur FTP, dans les machines virtuelles et dans la zone démilitarisée (DMZ). Chacune de ces zones a une fonction spécifique.

Serveur FTP

La machine virtuelle 1 est configurée avec logiciel FTP et sert de zone de rétention des données envoyées de et vers des ressources extérieures (formulaires et collatéraux localisés par un fournisseur, par exemple).

Cette machine virtuelle est associée à un réseau externe uniquement. Elle possède son propre commutateur virtuel et sa propre carte de réseau physique, qui lui permettent de se connecter au réseau externe 1. Ce réseau est réservé aux serveurs utilisés par l'entreprise pour la réception de données issues de sources externes. Par exemple, l'entreprise peut utiliser le réseau externe 1 pour recevoir un trafic FTP en provenance de leurs fournisseurs, et pour permettre à ces derniers d'accéder aux données stockées sur des serveurs externes via FTP. Outre la machine virtuelle 1, le réseau externe 1 sert les serveurs FTP configurés sur différents hôtes ESXi du site.

La machine virtuelle 1 ne partage pas de commutateur virtuel ou de carte de réseau physique avec les machines virtuelles de l'hôte ; par conséquent, les autres machines virtuelles ne peuvent pas acheminer de paquets de et vers le réseau de la machine virtuelle 1. Cette restriction évite les intrusions, qui nécessitent l'envoi de trafic réseau à la victime. Plus important encore : un pirate ne peut pas exploiter la vulnérabilité naturelle du protocole FTP pour accéder aux autres machines virtuelles de l'hôte.

Machines virtuelles internes

Les machines virtuelles 2 à 5 sont réservées à une utilisation interne. Ces machines virtuelles traitent et stockent les données confidentielles des entreprises (dossiers médicaux, jugements ou enquêtes sur la fraude, par exemple). Les administrateurs systèmes doivent donc leur associer un niveau maximal de protection.

Elles se connectent au réseau interne 2 via leur propre commutateur virtuel et leur propre carte réseau. Le réseau interne 2 est réservé à une utilisation interne par le personnel approprié (responsables de dossiers d'indemnisation ou juristes internes, par exemple).

Les machines virtuelles 2 à 5 peuvent communiquer entre elles via le commutateur virtuel ; elles peuvent aussi communiquer avec les machines virtuelles du réseau interne 2 via la carte réseau physique. En revanche, elles ne peuvent pas communiquer avec des machines externes. Comme pour le serveur FTP, ces machines virtuelles ne peuvent pas acheminer des paquets vers ou les recevoir depuis les réseaux des autres machines virtuelles. De la même façon, les autres machines virtuelles de l'hôte ne peuvent pas acheminer des paquets vers ou les recevoir depuis les machines virtuelles 2 à 5.

DMZ

Les machines virtuelles 6 à 8 sont configurées en tant que zone démilitarisée (DMZ) ; le groupe marketing les utilise pour publier le site Web externe de l'entreprise.

Ce groupe de machines virtuelles est associé au réseau externe 2 et au réseau interne 1. L'entreprise utilise le réseau externe 2 pour les serveurs Web qui hébergent le site Web de l'entreprise et d'autres outils Web destinés à des utilisateurs externes. Le réseau interne 1 est utilisé par le service marketing pour publier le contenu du site Web de l'entreprise, pour effectuer des téléchargements et pour gérer des services tels que des forums utilisateur.

Puisque ces réseaux sont séparés du réseau externe 1 et du réseau interne 2, et que les machines virtuelles n'ont pas de point de contact partagé (commutateurs ou adaptateurs), il

n'y a aucun risque d'attaque de ou vers le serveur FTP ou le groupe de machines virtuelles internes.

Grâce à l'isolation des machines virtuelles, à la bonne configuration des commutateurs virtuels et à la séparation des réseaux, l'administrateur système peut inclure les trois zones de machines virtuelles sur le même hôte ESXi et être rassuré quant à l'absence de violations de données ou de ressources.

L'entreprise met en œuvre l'isolation au sein des groupes de machines virtuelles via l'utilisation de plusieurs réseaux internes et externes, et via la séparation des commutateurs virtuels et des adaptateurs réseau physiques de chaque groupe.

Aucun des commutateurs virtuels ne fait le lien entre les différentes zones de machines virtuelles ; l'administrateur système peut donc éliminer tout risque de fuite de paquets d'une zone à l'autre. Au niveau de sa conception même, un commutateur virtuel ne peut pas transmettre directement des paquets vers un autre commutateur virtuel. Pour acheminer des paquets d'un commutateur virtuel vers un autre, les conditions suivantes doivent être réunies :

- Les commutateurs virtuels doivent être connectés au même réseau local physique.
- Les commutateurs virtuels doivent se connecter à une machine virtuelle commune, qui peut être utilisée pour la transmission de paquets.

Or, aucune de ces situations ne se vérifie dans l'exemple de configuration. Si les administrateurs système souhaitent vérifier l'absence de chemin commun de commutateur virtuel, ils peuvent rechercher les éventuels points de contact partagés en examinant la disposition des commutateurs réseau dans vSphere Web Client.

Pour protéger les ressources des machines virtuelles, l'administrateur système diminue le risque d'attaque DoS et DDoS en configurant une réservation de ressources, ainsi qu'une limite applicable à chaque machine virtuelle. Il renforce la protection de l'hôte ESXi et des machines virtuelles en installant des pare-feu sur la partie frontale et la partie principale de la zone démilitarisée (DMZ), en vérifiant que l'hôte est protégé par un pare-feu physique et en configurant les ressources de stockage réseau de telle sorte qu'elles bénéficient toutes de leur propre commutateur virtuel.

Sécurité du protocole Internet

La sécurité du protocole Internet (IPsec) sécurise les communications IP provenant de et arrivant sur l'hôte. Les hôtes ESXi prennent en charge IPsec utilisant IPv6.

Lorsque vous configurez IPsec sur un hôte, vous activez l'authentification et le chiffrement des paquets entrants et sortants. Le moment et la manière dont le trafic IP est chiffré dépendent de la façon dont vous avez configuré les associations de sécurité et les règles de sécurité du système.

Une association de sécurité détermine comment le système chiffre le trafic. Lorsque vous créez une association de sécurité, vous indiquez la source et la destination, les paramètres de chiffrement et le nom de l'association de sécurité.

Une stratégie de sécurité détermine le moment auquel le système doit chiffrer le trafic. La stratégie de sécurité comprend les informations de source et de destination, le protocole et la direction du trafic à chiffrer, le mode (transport ou tunnel) et l'association de sécurité à utiliser.

Liste des associations de sécurité disponibles

ESXi peut fournir une liste de toutes les associations de sécurité disponibles pour l'utilisation par les règles de sécurité. Cette liste inclut les associations de sécurité créées par l'utilisateur et les associations de sécurité que VMkernel a installées à l'aide d'Internet Key Exchange.

Vous pouvez obtenir une liste des associations de sécurité disponibles à l'aide de la commande vSphere CLI `esxcli`.

Procédure

- ◆ Dans l'invite de commande, entrez la commande **`esxcli network ip ipsec sa list`**.

Résultats

ESXi affiche une liste de toutes les associations de sécurité disponibles.

Ajouter une association de sécurité IPsec

Ajoutez une association de sécurité pour définir des paramètres de chiffrement pour le trafic IP associé.

Vous pouvez ajouter une association de sécurité avec la commande vSphere CLI `esxcli`.

Procédure

- ◆ Dans l'invite de commande, saisissez la commande **`esxcli network ip ipsec sa add`** avec une ou plusieurs des options suivantes.

Option	Description
<code>--sa-source= <i>source address</i></code>	Requis. Spécifiez l'adresse source.
<code>--sa-destination= <i>destination address</i></code>	Requis. Spécifiez l'adresse de destination.
<code>--sa-mode= <i>mode</i></code>	Requis. Spécifiez le mode, soit <code>transport</code> ou <code>tunnel</code> .
<code>--sa-spi= <i>security parameter index</i></code>	Requis. Spécifiez l'index des paramètres de sécurité. Celui-ci identifie l'association de sécurité à l'hôte. Ce doit être un hexadécimal avec un préfixe 0x. Chaque association de sécurité que vous créez doit disposer d'une combinaison unique de protocole et d'index de paramètres de sécurité.
<code>--encryption-algorithm= <i>encryption algorithm</i></code>	Requis. Spécifiez l'algorithme de chiffrement à l'aide d'un des paramètres suivants. <ul style="list-style-type: none"> ■ <code>3des-cbc</code> ■ <code>aes128-cbc</code> ■ <code>null</code> (n'assure aucun chiffrement)

Option	Description
--encryption-key= <i>encryption key</i>	Requis lorsque vous spécifiez un algorithme de chiffrement. Spécifiez la clé de chiffrement. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
--integrity-algorithm= <i>authentication algorithm</i>	Requis. Spécifiez l'algorithme d'authentification, soit <code>hmac-sha1</code> ou <code>hmac-sha2-256</code> .
--integrity-key= <i>authentication key</i>	Requis. Spécifiez la clé d'authentification. Vous pouvez entrer des clés en tant que texte ASCII ou en tant qu'hexadécimal avec un préfixe 0x.
--sa-name= <i>name</i>	Requis. Indiquez un nom pour l'association de sécurité.

Exemple : Commande de nouvelle association de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

Supprimer une association de sécurité IPsec

Vous pouvez supprimer une association de sécurité avec la commande vSphere CLI ESXCLI.

Conditions préalables

Vérifiez que l'association de sécurité que vous souhaitez employer n'est pas actuellement utilisée. Si vous essayez de supprimer une association de sécurité en cours d'utilisation, l'opération de suppression échoue.

Procédure

- ◆ À la suite de l'invite de commande, entrez la commande **esxcli network ip ipsec sa remove --sa-name *security_association_name***.

Répertorier les stratégies de sécurité IPsec disponibles

Vous pouvez répertorier les stratégies de sécurité disponibles à l'aide de la commande vSphere CLI ESXCLI.

Procédure

- ◆ À la suite de l'invite de commande, entrez la commande **esxcli network ip ipsec sp list**.

Résultats

L'hôte affiche une liste de toutes les règles de sécurité disponibles.

Créer une stratégie de sécurité IPSec

Créez une règle de sécurité pour déterminer le moment auquel utiliser les paramètres d'authentification et de chiffrement définis dans une association de sécurité. Vous pouvez ajouter une stratégie de sécurité à l'aide de la commande vSphere CLI ESXCLI.

Conditions préalables

Avant de créer une règle de sécurité, ajoutez une association de sécurité comportant les paramètres d'authentification et de chiffrement appropriés décrits dans [Ajouter une association de sécurité IPSec](#).

Procédure

- ◆ Dans l'invite de commande, saisissez la commande **esxcli network ip ipsec sp add** avec une ou plusieurs des options suivantes.

Option	Description
--sp-source= <i>source address</i>	Requis. Spécifiez l'adresse IP source et la longueur du préfixe.
--sp-destination= <i>destination address</i>	Requis. Spécifiez l'adresse de destination et la longueur du préfixe.
--source-port= <i>port</i>	Requis. Spécifiez le port source. Le port source doit être un nombre compris entre 0 et 65 535.
--destination-port= <i>port</i>	Requis. Spécifiez le port de destination. Le port source doit être un nombre compris entre 0 et 65 535.
--upper-layer-protocol= <i>protocol</i>	Spécifiez le protocole de couche supérieure à l'aide d'un des paramètres suivants. <ul style="list-style-type: none"> ■ tcp ■ udp ■ icmp6 ■ toutes
--flow-direction= <i>direction</i>	Spécifiez la direction dans laquelle vous souhaitez surveiller le trafic à l'aide de <i>in</i> ou <i>out</i> .
--action= <i>action</i>	Définissez l'action à prendre lorsque le trafic avec les paramètres spécifiés est rencontré à l'aide des paramètres suivants. <ul style="list-style-type: none"> ■ none : Ne faites rien ■ discard : Ne permettez pas l'entrée ou la sortie de données. ■ ipsec : Utilisez les informations d'authentification et de chiffrement fournies dans l'association de sécurité pour déterminer si les données proviennent d'une source de confiance.
--sp-mode= <i>mode</i>	Spécifiez le mode, soit <i>tunnel</i> ou <i>transport</i> .

Option	Description
<code>--sa-name=security association name</code>	Requis. Indiquez le nom de l'association de sécurité pour la règle de sécurité à utiliser.
<code>--sp-name=name</code>	Requis. Indiquez un nom pour la règle de sécurité.

Exemple : Commande de nouvelle règle de sécurité

L'exemple suivant contient des sauts de ligne supplémentaires pour des raisons de lisibilité.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sal
--sp-name=sp1
```

Supprimer une stratégie de sécurité IPsec

Vous pouvez supprimer une stratégie de sécurité de l'hôte ESXi à l'aide de la commande vSphere CLI ESXCLI.

Conditions préalables

Vérifiez que la stratégie de sécurité que vous souhaitez utiliser n'est pas actuellement utilisée. Si vous essayez de supprimer une règle de sécurité en cours d'utilisation, l'opération de suppression échoue.

Procédure

- ◆ Dans l'invite de commande, entrez la commande **esxcli network ip ipsec sp remove --sa-name security policy name**.

Pour supprimer toutes les règles de sécurité, entrez la commande **esxcli network ip ipsec sp remove --remove-all**.

Garantir une configuration SNMP appropriée

Si SNMP n'est pas configuré correctement, les informations de surveillance peuvent être envoyées à un hôte malveillant. L'hôte malveillant peut ensuite utiliser ces informations pour planifier une attaque.

Procédure

- 1 Exécutez **esxcli system snmp get** pour déterminer si SNMP est actuellement utilisé.

- 2 Si votre système ne requiert pas SNMP, assurez-vous qu'il est en cours d'exécution en exécutant la commande `esxcli system snmp set --enable true`.
- 3 Si votre système utilise SNMP, consultez la publication *Surveillance et performances* pour obtenir des informations sur la configuration de SNMP 3.

SNMP doit être configuré sur chaque hôte ESXi. Vous pouvez utiliser vCLI, PowerCLI ou vSphere Web Services SDK pour la configuration.

Utiliser des commutateurs virtuels avec l'API vSphere Network Appliance, uniquement si nécessaire

Si vous n'utilisez pas de produits faisant appel à l'API vSphere Network Appliance (DvFilter), ne configurez pas votre hôte pour envoyer des informations sur le réseau à une machine virtuelle. Si l'API vSphere Network Appliance est activée, un pirate peut tenter de connecter une machine virtuelle au filtre. Cette connexion risque de donner à d'autres machines virtuelles sur l'hôte un accès au réseau.

Si vous utilisez un produit qui fait appel à cette API, vérifiez que l'hôte est correctement configuré. Reportez-vous aux sections sur DvFilter dans *Développement et déploiement des solutions vSphere, des vServices et des agents ESX*. Si votre hôte est configuré pour utiliser l'API, assurez-vous que la valeur du paramètre `Net.DVFilterBindIpAddress` correspond au produit qui utilise l'API.

Procédure

- 1 Pour s'assurer que le paramètre de noyau `Net.DVFilterBindIpAddress` a la valeur appropriée, localisez le paramètre à l'aide de vSphere Web Client.
 - a Sélectionnez l'hôte et cliquez sur l'onglet **Gérer**.
 - b Dans Système, sélectionnez **Paramètres système avancés**.
 - c Faites défiler jusqu'à `Net.DVFilterBindIpAddress` et vérifiez que le paramètre a une valeur vide.

L'ordre des paramètres n'est pas strictement alphabétique. Tapez **DVFilter** dans le champ Filtre pour afficher tous les paramètres associés.
- 2 Si vous n'utilisez pas les paramètres DvFilter, assurez-vous que la valeur est vide.
- 3 Si vous utilisez des paramètres DvFilter, assurez-vous que la valeur du paramètre correspond à celle qu'emploie le produit qui utilise DvFilter.

Meilleures pratiques en matière de sécurité de la mise en réseau vSphere

L'observation des recommandations en matière de sécurité contribue à garantir l'intégrité de votre déploiement vSphere.

Recommandations générales de sécurité pour la mise en réseau

En matière de sécurisation de votre environnement réseau, la première étape consiste à respecter les recommandations de sécurité générales s'appliquant aux réseaux. Vous pouvez ensuite vous concentrer sur des points spéciaux, comme la sécurisation du réseau à l'aide de pare-feu ou du protocole IPsec.

- Assurez-vous que les ports du commutateur physique sont configurés avec Portfast si le protocole STP (Spanning Tree Protocol) est activé. Étant donné que les commutateurs virtuels VMware ne prennent pas en charge le STP, Portfast doit être configuré sur les ports de commutateur physique connectés à un hôte ESXi si le protocole Spanning Tree est activé afin d'éviter les boucles au sein du réseau de commutateurs physiques. Si le protocole Portfast n'est pas configuré, des problèmes de performance et de connectivité sont potentiellement à craindre.
- Assurez-vous que le trafic réseau d'un Distributed Virtual Switch est envoyé uniquement aux adresses IP de collecteurs autorisés. Les exportations Netflow ne sont pas chiffrées et peuvent contenir des informations sur le réseau virtuel, ce qui accroît le risque de succès d'une attaque de l'intercepteur. Si une exportation Netflow est nécessaire, assurez-vous que toutes les adresses IP Netflow cibles sont correctes.
- Assurez-vous que seuls les administrateurs autorisés ont accès aux composants de mise en réseau en utilisant des contrôles d'accès basés sur rôles. Par exemple, les administrateurs de machines virtuelles ne devraient pouvoir accéder qu'aux groupes de ports dans lesquels leurs machines virtuelles résident. Les administrateurs réseau doivent disposer d'autorisations pour tous les composants du réseau virtuel mais pas d'un accès aux machines virtuelles. Le fait de limiter l'accès réduit le risque d'erreur de configuration, qu'elle soit accidentelle ou délibérée, et renforce les concepts essentiels de sécurité que sont la séparation des devoirs et le moindre privilège.
- Assurez-vous que les groupes de ports ne sont pas configurés sur la valeur du VLAN natif. Les commutateurs physiques utilisent VLAN 1 comme VLAN natif. Les trames sur un VLAN natif ne sont pas balisées avec un 1. ESXi n'a pas de VLAN natif. Les trames pour lesquelles le VLAN est spécifié dans le groupe de ports comportent une balise, mais les trames pour lesquelles le VLAN n'est pas spécifié dans le groupe de ports ne sont pas balisées. Ceci peut créer un problème, car les machines virtuelles balisées avec un 1 appartiendront au VLAN natif du commutateur physique.

Par exemple, les trames sur le VLAN 1 d'un commutateur physique Cisco ne sont pas balisées car VLAN1 est le VLAN natif sur ce commutateur physique. Cependant, les trames de l'hôte ESXi spécifiées comme VLAN 1 sont balisées avec un 1 ; le trafic de l'hôte ESXi destiné au VLAN natif n'est donc pas acheminé correctement, car il porte la balise 1 au lieu de ne pas être balisé. Le trafic du commutateur physique provenant du VLAN natif n'est pas visible car il n'est pas balisé. Si le groupe de ports du commutateur virtuel ESXi utilise l'ID du VLAN natif, le trafic provenant des machines virtuelles sur ce port n'est pas visible pour le VLAN natif sur le commutateur car le commutateur attend un trafic non balisé.

- Assurez-vous que les groupes de ports ne sont pas configurés sur des valeurs VLAN réservées par les commutateurs physiques en amont. Les commutateurs physiques réservent certains ID de VLAN à des fins internes, et n'autorisent souvent pas le trafic configuré sur ces valeurs. Par exemple, les commutateurs Cisco Catalyst réservent généralement les VLAN 1001 à 1024 et 4094. Utiliser un VLAN réservé peut entraîner un déni de service sur le réseau.
- Assurez-vous que les groupes de ports ne sont pas configurés sur VLAN 4095, sauf si vous utilisez le balisage d'invité virtuel (VGT). Définir un groupe de ports sur VLAN 4095 active le mode VGT. Dans ce mode, le commutateur virtuel transmet toutes les trames du réseau à la machine virtuelle sans modifier les balises VLAN, en laissant la machine virtuelle les traiter.
- Restreignez les remplacements de configuration de niveau de port sur un commutateur virtuel distribué. Les remplacements de configuration de niveau de port sont désactivés par défaut. Une fois activés, les remplacements permettent différents paramètres de sécurité pour une machine virtuelle que les paramètres au niveau du groupe de ports. Certaines machines virtuelles requièrent des configurations uniques, mais la surveillance est essentielle. Si les remplacements ne sont pas surveillés, n'importe quel utilisateur parvenant à accéder à une machine virtuelle avec une configuration de commutateur virtuel distribué peut tenter d'exploiter cet accès.
- Assurez-vous que le trafic en miroir du port du commutateur virtuel distribué est envoyé uniquement aux ports du collecteur ou aux VLAN autorisés. Un vSphere Distributed Switch peut mettre en miroir le trafic provenant d'un port vers un autre pour permettre aux périphériques de capture de paquets de collecter des flux de trafic spécifiques. La mise en miroir des ports envoie une copie de tout le trafic spécifié dans un format non-chiffré. Ce trafic mis en miroir contient les données complètes dans les paquets capturés, et ceci peut compromettre les données s'il est mal dirigé. Si la mise en miroir des ports est requise, vérifiez que tous les ID de VLAN, de port et de liaison montante de destination de la mise en miroir des ports sont corrects.

Étiquetage de composants de mise en réseau

L'identification des différents composants de votre architecture de mise en réseau est critique et contribue à garantir qu'aucune erreur n'est introduite lors de l'extension de votre réseau.

Suivez ces recommandations :

- Assurez-vous que les groupes de ports sont configurés avec une étiquette réseau claire et évidente. Ces étiquettes servent de descripteur fonctionnel du groupe de ports et vous aident à identifier la fonction de chaque groupe de ports lorsque le réseau devient plus complexe.
- Assurez-vous que chaque vSphere Distributed Switch dispose d'une étiquette réseau qui indique clairement la fonction ou le sous-réseau IP du commutateur. Cette étiquette sert de descripteur fonctionnel du commutateur, tout comme un commutateur physique nécessite un nom d'hôte. Par exemple, vous pouvez étiqueter le commutateur comme étant interne pour indiquer qu'il est dédié à la mise en réseau interne. Vous ne pouvez pas modifier l'étiquette d'un commutateur virtuel standard.

Documenter et vérifier l'environnement VLAN vSphere

Vérifiez votre environnement VLAN régulièrement pour éviter les problèmes. Documentez entièrement l'environnement VLAN et assurez-vous que les ID VLAN ne sont utilisés qu'une seule fois. Votre documentation peut simplifier le dépannage et est essentielle lorsque vous souhaitez développer l'environnement.

Procédure

1 Assurez-vous que tous les vSwitch et ID VLAN sont entièrement documentés

Si vous utilisez le balisage VLAN sur un commutateur virtuel, les ID doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si les ID VLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué à un endroit où le trafic devrait normalement passer.

2 Assurez-vous que les ID VLAN de tous les groupes de ports virtuels distribués (instances de dvPortgroup) sont entièrement documentés.

Si vous utilisez le balisage VLAN sur un dvPortgroup, les ID doivent correspondre aux ID des commutateurs VLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si les ID VLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué à un endroit où le trafic devrait normalement passer.

3 Assurez-vous que les ID VLAN de tous les commutateurs virtuels distribués sont entièrement documentés.

Les VLAN privés (PVLAN) des commutateurs virtuels distribués nécessitent des ID VLAN principaux et secondaires. Ces ID doivent correspondre aux ID des commutateurs PVLAN externes en amont. Si les ID VLAN ne sont pas entièrement suivis, une réutilisation erronée d'ID peut permettre l'établissement de trafic entre des machines physiques et virtuelles non appropriées. De même, si des ID PVLAN sont erronés ou manquants, le trafic entre les machines physiques et virtuelles peut être bloqué là où vous souhaitez faire passer le trafic.

4 Vérifiez que les liaisons de jonction VLAN sont connectées uniquement à des ports de commutateur physiques qui fonctionnent comme des liaisons de jonction.

Lorsque vous connectez un commutateur virtuel à un port de jonction VLAN, vous devez configurer correctement le commutateur virtuel et le commutateur physique au port de liaison montante. Si le commutateur physique n'est pas configuré correctement, les trames avec l'en-tête VLAN 802.1q sont renvoyées vers un commutateur qui n'attend pas leur arrivée.

Adoption de solides pratiques d'isolation de réseau

L'adoption de solides pratiques d'isolation réseau améliore de façon significative la sécurité réseau de l'environnement vSphere.

Isoler le réseau de gestion

Le réseau de gestion vSphere donne accès à l'interface de gestion vSphere sur chaque composant. Les services s'exécutant sur l'interface de gestion offrent la possibilité pour un pirate d'obtenir un accès privilégié aux systèmes. Les attaques à distance sont susceptibles de commencer par l'obtention d'un accès à ce réseau. Si un pirate obtient accès au réseau de gestion, cela lui fournit une base pour mener d'autres intrusions.

Contrôlez strictement l'accès au réseau de gestion en le protégeant au niveau de sécurité de la machine virtuelle la plus sécurisée s'exécutant sur un hôte ou un cluster ESXi. Quelle que soit la restriction du réseau de gestion, les administrateurs doivent avoir accès à ce réseau pour configurer les hôtes ESXi et le système vCenter Server.

Placez le groupe de ports de gestion vSphere dans un VLAN dédié sur un commutateur commun. vSwitch peut être partagé avec le trafic de production (machine virtuelle), à condition que le VLAN du groupe de ports de gestion de vSphere ne soit pas utilisé par les machines virtuelles de production. Vérifiez que le segment réseau n'est pas routé, à l'exception éventuellement des réseaux hébergeant d'autres entités de gestion, par exemple en liaison avec vSphere Replication. Assurez-vous notamment que le trafic des machines virtuelles de production ne peut pas être routé vers ce réseau.

Autorisez l'accès à la fonctionnalité de gestion d'une manière strictement contrôlée en utilisant l'une des approches suivantes.

- Pour les environnements particulièrement sensibles, configurez une passerelle contrôlée ou une autre méthode contrôlée pour accéder au réseau de gestion. Par exemple, obligez les administrateurs à se connecter au réseau de gestion via un réseau VPN, et autorisez l'accès uniquement aux administrateurs approuvés.
- Configurez des systèmes JumpBox qui exécutent des clients de gestion.

Isoler le trafic de stockage

Assurez-vous que le trafic de stockage IP est isolé. Le stockage IP inclut iSCSI et NFS. Les machines virtuelles peuvent partager des commutateurs virtuels et des VLAN avec des configurations de stockage IP. Ce type de configuration peut exposer du trafic de stockage IP à des utilisateurs de machine virtuelle non autorisés.

Le stockage IP est fréquemment non chiffré ; toute personne ayant accès à ce réseau peut le voir. Pour empêcher les utilisateurs non autorisés à voir le trafic de stockage IP, séparez logiquement le trafic du réseau de stockage IP du trafic de production. Configurez les adaptateurs de stockage IP sur des VLAN ou des segments de réseau séparés du réseau de gestion VMkernel pour empêcher les utilisateurs non autorisés d'afficher le trafic.

Isoler le trafic VMotion

Les informations de migration VMotion sont transmises en texte brut. Toute personne ayant accès au réseau sur lequel ces informations circulent peut les voir. Les pirates potentiels peuvent intercepter du trafic vMotion pour obtenir le contenu de la mémoire d'une machine virtuelle. Ils peuvent également préparer une attaque MiTM dans laquelle le contenu est modifié pendant la migration.

Séparez le trafic VMotion du trafic de production sur un réseau isolé. Configurez le réseau de manière qu'il soit non routable, c'est-à-dire assurez-vous qu'aucun routeur de niveau 3 n'étend ce réseau et d'autres réseaux, pour empêcher un accès au réseau de l'extérieur.

Le groupe de ports VMotion doit se trouver dans un réseau VLAN dédié sur un vSwitch commun. vSwitch peut être partagé avec le trafic de production (machine virtuelle), à condition que le VLAN du groupe de ports VMotion ne soit pas utilisé par des machines virtuelles de production.

Meilleures pratiques concernant plusieurs composants vSphere

9

Certaines meilleures pratiques en matière de sécurité, telles que la configuration de NTP dans votre environnement, affectent plusieurs composants vSphere. Tenez compte des recommandations suivantes lorsque vous configurez votre environnement.

Reportez-vous à [Chapitre 5 Sécurisation des hôtes ESXi](#) et à [Chapitre 7 Sécurisation des machines virtuelles](#) pour consulter des informations associées.

Ce chapitre contient les rubriques suivantes :

- [Synchronisation des horloges sur le réseau vSphere](#)
- [Meilleures pratiques en matière de sécurité du stockage](#)
- [Vérifier que l'envoi des données de performances de l'hôte aux invités est désactivé](#)
- [Configuration de délais d'expiration pour ESXi Shell et vSphere Web Client](#)

Synchronisation des horloges sur le réseau vSphere

Assurez-vous que les horloges de tous les composants sur le réseau vSphere sont synchronisées. Si les horloges des machines sur votre réseau vSphere ne sont pas synchronisées, les certificats SSL, pour lesquels le temps est important, peuvent ne pas être reconnus comme valides dans les communications entre les machines du réseau.

Des horloges non synchronisées peuvent entraîner des problèmes d'authentification, ce qui peut causer l'échec de l'installation ou empêcher le démarrage du service vpxd de vCenter Server Appliance.

Assurez-vous que toute machine hôte Windows sur laquelle un composant vCenter s'exécute est synchronisée avec le serveur NTP. Voir l'article de la base de connaissances <http://kb.vmware.com/kb/1318>.

- [Synchroniser les horloges ESXi avec un serveur de temps réseau](#)
Avant d'installer vCenter Server ou de déployer vCenter Server Appliance, assurez-vous que toutes les horloges des machines de votre réseau vSphere sont synchronisées.
- [Configuration des paramètres de synchronisation horaire dans vCenter Server Appliance](#)
Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server Appliance après le déploiement.

Synchroniser les horloges ESXi avec un serveur de temps réseau

Avant d'installer vCenter Server ou de déployer vCenter Server Appliance, assurez-vous que toutes les horloges des machines de votre réseau vSphere sont synchronisées.

Cette tâche explique comment configurer NTP depuis vSphere Client. Vous pouvez également utiliser la commande vCLI `vicfg-ntp`. Reportez-vous à la *Référence de l'interface de ligne de commande de vSphere*.

Procédure

- 1 Démarrez vSphere Client et connectez-vous à l'hôte ESXi.
- 2 Dans l'onglet **Configuration**, cliquez sur **Configuration de temps**.
- 3 Cliquez sur **Propriétés**, puis sur **Options**.
- 4 Sélectionnez **Paramètres NTP**.
- 5 Cliquez sur **Add**.
- 6 Dans la boîte de dialogue Ajouter serveur NTP, saisissez l'adresse IP ou le nom de domaine complet du serveur NTP avec lequel effectuer la synchronisation.
- 7 Cliquez sur **OK**.

L'hôte se synchronise avec le serveur NTP.

Configuration des paramètres de synchronisation horaire dans vCenter Server Appliance

Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server Appliance après le déploiement.

Lorsque vous déployez vCenter Server Appliance, vous pouvez définir la méthode de synchronisation horaire en utilisant un serveur NTP ou VMware Tools. En cas de modification de vos paramètres d'heure dans votre réseau vSphere, vous pouvez modifier vCenter Server Appliance et configurer les paramètres de synchronisation horaire à l'aide des commandes dans l'interpréteur de commande du dispositif.

Lorsque vous activez la synchronisation horaire régulière, VMware Tools définit l'heure de l'hôte sur le système d'exploitation invité.

Après la synchronisation horaire, VMware Tools vérifie toutes les minutes que les horloges des systèmes d'exploitation invité et de l'hôte correspondent toujours. Si tel n'est pas le cas, l'horloge du système d'exploitation client est synchronisé pour qu'elle corresponde à celle de l'hôte.

Un logiciel natif de synchronisation horaire, tel que Network Time Protocol (NTP), est généralement plus précis que la synchronisation horaire régulière de VMware Tools et il est donc préférable d'utiliser un tel logiciel. Vous pouvez utiliser une seule méthode de synchronisation horaire dans vCenter Server Appliance. Si vous décidez d'utiliser le logiciel natif de synchronisation horaire, la synchronisation horaire régulière de VMware Tools dans vCenter Server Appliance est désactivée, et l'inverse.

Utiliser la synchronisation de l'heure de VMware Tools

Vous pouvez configurer vCenter Server Appliance de manière à utiliser la synchronisation de l'heure de VMware Tools.

Procédure

- 1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

- 2 Exécutez la commande pour activer la synchronisation de l'heure de VMware Tools.

```
timesync.set --mode host
```

- 3 (Facultatif) Exécutez la commande pour vérifier que vous avez réussi à appliquer la synchronisation de l'heure de VMware Tools.

```
timesync.get
```

La commande renvoie l'indication que la synchronisation de l'heure est en mode hôte.

Résultats

L'heure du dispositif est synchronisée avec celle de l'hôte ESXi.

Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server Appliance

Pour configurer vCenter Server Appliance de manière à utiliser une synchronisation de l'heure basée sur NTP, vous devez ajouter les serveurs NTP à la configuration vCenter Server Appliance.

Procédure

- 1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

- 2 Ajoutez des serveurs NTP à la configuration de vCenter Server Appliance en exécutant la commande `ntp.server.add`.

Par exemple, exécutez la commande suivante :

```
ntp.server.add --servers IP-addresses-or-host-names
```

IP-addresses-or-host-names est une liste séparée par des virgules des adresses IP ou noms d'hôtes des serveurs NTP.

Cette commande ajoute des serveurs NTP à la configuration. Si la synchronisation horaire est basée sur un serveur NTP, le démon NTP est redémarré pour recharger les nouveaux serveurs NTP. Sinon, cette commande ajoute simplement de nouveaux serveurs NTP à la configuration NTP existante.

- 3 (Facultatif) Pour supprimer d'anciens serveurs NTP et les remplacer par de nouveaux dans la configuration de vCenter Server Appliance, exécutez la commande `ntp.server.set`.

Par exemple, exécutez la commande suivante :

```
ntp.server.set --servers IP-addresses-or-host-names
```

IP-addresses-or-host-names est une liste séparée par des virgules des adresses IP ou noms d'hôtes des serveurs NTP.

Cette commande supprime les anciens serveurs NTP de la configuration et définit les serveurs NTP d'entrée dans la configuration. Si la synchronisation horaire est basée sur un serveur NTP, le démon NTP est redémarré pour recharger la nouvelle configuration NTP. Sinon, cette commande remplace simplement les serveurs de la configuration NTP avec les serveurs que vous fournissez.

- 4 (Facultatif) Exécutez la commande pour vérifier que vous avez appliqué les nouveaux paramètres de la configuration NTP.

```
ntp.get
```

La commande renvoie une liste séparée par des espaces des serveurs configurés pour la synchronisation NTP. Si la synchronisation NTP est activée, la commande renvoie l'information précisant que la configuration NTP a l'état Actif. Si la synchronisation NTP est désactivée, la commande renvoie l'information précisant que la configuration NTP a l'état Inactif.

Étape suivante

Si la synchronisation NTP est désactivée, vous pouvez configurer les paramètres de synchronisation de l'heure de vCenter Server Appliance de façon à la baser sur un serveur NTP. Reportez-vous à [Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP](#).

Synchroniser l'heure dans vCenter Server Appliance avec un serveur NTP

Vous pouvez configurer les paramètres de synchronisation de l'heure dans vCenter Server Appliance pour qu'ils soient basés sur un serveur NTP.

Conditions préalables

Configurez un ou plusieurs serveurs NTP (Network Time Protocol) dans la configuration de vCenter Server Appliance. Reportez-vous à [Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server Appliance](#).

Procédure

- 1 Accédez à l'interpréteur de commande du dispositif et connectez-vous en tant qu'utilisateur disposant du rôle d'administrateur ou de super administrateur.

L'utilisateur par défaut ayant le rôle de super administrateur est l'utilisateur racine.

- 2 Exécutez la commande pour activer la synchronisation de l'heure basée sur un serveur NTP.

```
timesync.set --mode NTP
```

- 3 (Facultatif) Exécutez la commande pour vérifier que vous avez appliqué la synchronisation NTP.

```
timesync.get
```

La commande renvoie l'indication que la synchronisation de l'heure est en mode NTP.

Meilleures pratiques en matière de sécurité du stockage

Suivez les recommandations relatives à la sécurité de stockage, présentées par votre fournisseur de sécurité de stockage. Vous pouvez également tirer avantage du CHAP et du CHAP mutuel pour sécuriser le stockage iSCSI, masquer et affecter les ressources SAN, et configurer les informations d'identification Kerberos pour NFS 4.1.

Reportez-vous également à la documentation *Administration de VMware Virtual SAN*.

Sécurisation du stockage iSCSI

Le stockage que vous configurez pour un hôte peut comprendre un ou plusieurs réseaux de zone de stockage (SAN) utilisant iSCSI. Lorsque vous configurez iSCSI sur un hôte, vous pouvez prendre plusieurs mesures pour réduire les risques de sécurité.

iSCSI est un moyen d'accéder aux périphériques SCSI et d'échanger des enregistrements de données à l'aide du protocole TCP/IP sur un port réseau plutôt que via une connexion directe à un périphérique SCSI. Dans les transactions iSCSI, des blocs de données SCSI brutes sont encapsulés dans des enregistrements iSCSI et transmis au périphérique demandant ou à l'utilisateur.

Les SAN iSCSI vous permettent d'utiliser efficacement les infrastructures Ethernet existantes pour permettre aux hôtes d'accéder aux ressources de stockage qu'ils peuvent partager de manière dynamique. Les SAN iSCSI offrent une solution de stockage économique pour les environnements reposant sur un pool de stockage pour servir de nombreux utilisateurs. Comme pour tout système en réseau, vos SAN iSCSI peuvent être soumis à des défaillances de sécurité.

Note Les contraintes et les procédures de sécurisation d'un SAN iSCSI sont semblables à celles des adaptateurs iSCSI matériels que vous pouvez utiliser avec les hôtes et à celles des iSCSI configurés directement via l'hôte.

Sécurisation des périphériques iSCSI

Un moyen permettant de sécuriser les périphériques iSCSI des intrusions indésirables consiste à demander que l'hôte, ou l'initiateur, soit authentifié par le périphérique iSCSI, ou la cible, à chaque fois que l'hôte tente d'accéder aux données sur la LUN cible.

L'objectif de l'authentification consiste à prouver que l'initiateur a le droit d'accéder à une cible, ce droit étant accordé lorsque vous configurez l'authentification.

ESXi ne prend en charge ni Secure Remote Protocol (SRP), ni les méthodes d'authentification par clé publique d'iSCSI. L'authentification Kerberos ne peut s'utiliser qu'avec NFS 4.1.

ESXi prend en charge l'authentification CHAP ainsi que l'authentification CHAP mutuel.

La documentation *Stockage vSphere* explique comment sélectionner la meilleure méthode d'authentification pour votre périphérique iSCSI et comment configurer CHAP.

Assurez-vous que les secrets CHAP sont uniques. Le secret d'authentification mutuelle de chaque hôte doit être différent. Dans la mesure du possible, le secret doit également être différent pour chaque client s'authentifiant auprès du serveur. De la sorte, si un hôte unique est compromis, le pirate ne peut pas créer un autre hôte arbitraire et s'authentifier auprès du périphérique de stockage. Lorsqu'il existe un secret partagé unique, la compromission d'un hôte peut permettre à un pirate de s'authentifier auprès du périphérique de stockage.

Protection d'un SAN iSCSI

Lorsque vous planifiez la configuration iSCSI, prenez des mesures pour optimiser la sécurité globale de votre SAN iSCSI. Votre configuration iSCSI présente le même niveau de sécurité que votre réseau IP. Par conséquent, en appliquant de bonnes normes de sécurité lors de la configuration de votre réseau, vous aidez à la protection de votre stockage iSCSI.

Vous trouverez ci-dessous des suggestions spécifiques pour appliquer de bonnes normes de sécurité.

Protection des données transmises

Le premier risque de sécurité dans les SAN iSCSI est qu'un attaquant puisse renifler les données de stockage transmises.

Prenez des mesures supplémentaires pour empêcher les attaquants de voir aisément les données iSCSI. Ni l'adaptateur iSCSI du matériel, ni l'initiateur iSCSI d'ESXi ne chiffre les données qu'ils transmettent vers les cibles et obtiennent de celles-ci, rendant ainsi les données plus vulnérables aux attaques par reniflage.

Permettre à vos machines virtuelles de partager des commutateurs standard et des VLAN avec votre configuration iSCSI expose potentiellement le trafic iSCSI à une mauvaise utilisation par un attaquant de machine virtuelle. Afin de garantir que les intrus ne peuvent pas écouter les transmissions iSCSI, assurez-vous qu'aucune des machines virtuelles ne peut voir le réseau de stockage iSCSI.

Si vous utilisez un adaptateur iSCSI matériel, vous pouvez effectuer cette opération en vous assurant que l'adaptateur iSCSI et l'adaptateur de réseau physique ESXi ne sont pas connectés par inadvertance en dehors de l'hôte pour partager un commutateur ou un autre élément. Si vous configurez iSCSI directement via l'hôte ESXi, vous pouvez effectuer cette opération en configurant le stockage iSCSI via un commutateur standard différent de celui utilisé par vos machines virtuelles.

En plus de protéger le SAN iSCSI en lui attribuant un commutateur standard, vous pouvez configurer votre SAN iSCSI avec son propre VLAN pour améliorer les performances et la sécurité. Le placement de votre configuration iSCSI sur un VLAN séparé garantit qu'aucun périphérique autre que l'adaptateur iSCSI n'a de visibilité sur les transmissions au sein du SAN iSCSI. Par conséquent, aucun blocage réseau provenant d'autres sources ne peut interférer avec le trafic iSCSI.

Sécurisation des ports iSCSI

Lorsque vous exécutez des périphériques iSCSI, ESXi n'ouvre pas de port écoutant les connexions réseau. Cette mesure réduit le risque qu'un intrus puisse pénétrer dans ESXi par des ports disponibles et prenne le contrôle de l'hôte. Par conséquent, l'exécution iSCSI ne présente pas de risques de sécurité supplémentaires sur le côté hôte ESXi de la connexion.

Tout périphérique cible iSCSI que vous exécutez doit disposer d'un ou plusieurs ports TCP ouverts pour écouter les connexions iSCSI. Si des vulnérabilités de sécurité existent dans le logiciel du périphérique iSCSI, vos données peuvent courir un risque en raison d'une panne d'ESXi. Pour réduire ce risque, installez tous les correctifs de sécurité que le fournisseur de votre équipement de stockage fournit et limitez le nombre de périphériques connectés au réseau iSCSI.

Masquage et zonage des ressources SAN

Vous pouvez utiliser le zonage et le masquage LUN pour séparer l'activité SAN et restreindre l'accès aux périphériques de stockage.

Vous pouvez protéger l'accès au stockage dans votre environnement vSphere en utilisant le zonage et le masquage LUN avec vos ressources SAN. Par exemple, vous pouvez gérer des zones définies pour des tests indépendamment dans le réseau SAN afin qu'elles n'interfèrent pas avec l'activité des zones de production. De même, vous pouvez configurer différentes zones pour différents services.

Lorsque vous configurez des zones, tenez compte des groupes d'hôtes qui sont configurés sur le périphérique SAN.

Les possibilités de zonage et de masquage pour chaque commutateur et baie de disques SAN, ainsi que les outils de gestion du masquage LUN sont spécifiques du fournisseur.

Consultez la documentation de votre fournisseur SAN ainsi que la documentation *Stockage vSphere*.

Utilisation d'informations d'identification Kerberos pour NFS 4.1

Avec NFS version 4.1, ESXi prend en charge le mécanisme d'authentification Kerberos.

Kerberos est un service d'authentification qui permet à un client NFS 4.1 installé sur ESXi de démontrer son identité à un serveur NFS, préalablement au montage d'un partage NFS. Grâce au chiffrement, Kerberos permet de travailler sur une connexion réseau non sécurisée. L'implémentation vSphere de Kerberos pour NFS 4.1 prend en charge uniquement la vérification d'identité pour le client et le serveur. Il n'assure pas l'intégrité des données et ne fournit aucun service de confidentialité.

Lorsque vous utilisez l'authentification Kerberos, les considérations suivantes s'appliquent :

- ESXi utilise Kerberos version 5 avec le domaine Active Directory et KDC (Key Distribution Center).
- En tant qu'administrateur vSphere, vous spécifiez les informations d'identification Active Directory requises pour octroyer l'accès aux banques de données NFS 4.1 Kerberos à un utilisateur NFS. Le même ensemble d'informations d'identification est utilisé pour accéder à toutes les banques de données Kerberos montées sur cet hôte.
- Lorsque plusieurs hôtes ESXi partagent la même banque de données NFS 4.1, vous devez utiliser les mêmes informations d'identification Active Directory pour tous les hôtes qui accèdent à la banque de données partagée. Vous pouvez automatiser cela en définissant l'utilisateur dans les profils d'hôte et en appliquant le profil à tous les hôtes ESXi.
- NFS 4.1 ne prend pas en charge les montages AUTH_SYS et Kerberos simultanés.
- NFS 4.1 avec Kerberos ne prend pas en charge IPv6. Seul IPv4 est pris en charge.

Vérifier que l'envoi des données de performances de l'hôte aux invités est désactivé

vSphere comprend des compteurs de performance de machine virtuelle lorsque VMware Tools est installé sous des systèmes d'exploitation Windows. Les compteurs de performance permettent aux personnes en charge des machines virtuelles d'effectuer des analyses de performance précises à l'intérieur du système d'exploitation client. Par défaut, vSphere n'expose pas les informations relatives à l'hôte à la machine virtuelle invitée.

La possibilité d'envoyer des données de performance relatives à l'hôte à une machine virtuelle cliente est désactivée par défaut. Ce paramétrage par défaut empêche une machine virtuelle d'obtenir des informations détaillées sur l'hôte physique et rend les données de l'hôte indisponibles si une faille de la sécurité de la machine virtuelle se produit.

Note La procédure ci-dessous illustre le processus simple. Utilisez plutôt vSphere ou l'une des interfaces de ligne de commande vSphere (vCLI, PowerCLI et ainsi de suite) pour effectuer cette tâche sur tous les hôtes simultanément.

Procédure

- 1 Sur le système ESXi hébergeant la machine virtuelle, accédez au fichier VMX.

Les fichiers de configuration des machines virtuelles se situent dans le répertoire `/vmfs/volumes/datastore`, où *datastore* correspond au nom du périphérique de stockage dans lequel sont stockés les fichiers de la machine virtuelle.

- 2 Dans le fichier VMX, vérifiez que le paramètre suivant est défini.

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 Enregistrez et fermez le fichier.

Résultats

Vous ne pouvez pas récupérer d'informations de performance relatives à l'hôte à l'intérieur de la machine virtuelle.

Configuration de délais d'expiration pour ESXi Shell et vSphere Web Client

Pour empêcher des intrus d'utiliser une session inactive, veuillez à configurer des délais d'expiration pour ESXi Shell et vSphere Web Client.

Délai d'expiration d'ESXi Shell

Pour ESXi Shell, vous pouvez configurer les délais d'expiration suivants pour vSphere Web Client à partir de l'interface utilisateur de console directe (DCUI).

Délai d'expiration de la disponibilité

La valeur du délai d'attente de disponibilité correspond au temps qui peut s'écouler avant de vous connecter suite à l'activation de ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Délai d'inactivité

Le délai d'inactivité correspond au temps qui peut s'écouler avant que l'utilisateur ne soit déconnecté d'une session interactive inactive. Les modifications du délai d'inactivité s'appliquent lors de la prochaine connexion de l'utilisateur à ESXi Shell et n'affectent pas les sessions existantes.

Délai d'expiration de vSphere Web Client

Par défaut, les sessions vSphere Web Client prennent fin après 120 minutes. Vous pouvez modifier ce paramètre par défaut dans le fichier `webclient.properties`, ainsi que cela est indiqué dans la documentation *Gestion de vCenter Server et des hôtes*.

Gestion de la Configuration du protocole TLS avec l'utilitaire de reconfiguration de TLS

10

Vous pouvez utiliser l'utilitaire de reconfiguration de TLS pour activer ou désactiver les versions de protocole TLS. Vous pouvez désactiver TLS 1.0 dans l'environnement vSphere, ou vous pouvez désactiver TLS 1.0 et 1.1. À partir de vSphere 6.5, les versions de protocole TLS 1.0, 1.1 et 1.2 sont activées par défaut.

Pour la reconfiguration, vCenter Server, Platform Services Controller, vSphere Update Manager et les hôtes ESXi de l'environnement doivent exécuter les versions de logiciel qui permettent la désactivation. Pour obtenir la liste des produits VMware qui prennent en charge la désactivation de TLS 1.0, reportez-vous à l'article de la Base de connaissances VMware [2145796](#).

Avant de désactiver TLS 1.0, vous devez également vous assurer que les autres produits VMware et les produits tiers prennent en charge un protocole TLS qui est activé. Selon votre configuration, cela peut être TLS 1.2 ou TLS 1.1 et TLS 1.2.

Ce chapitre contient les rubriques suivantes :

- [Ports prenant en charge la désactivation des versions TLS](#)
- [Désactivation des versions de TLS dans vSphere](#)
- [Installer l'utilitaire de configuration de TLS](#)
- [Effectuer une sauvegarde manuelle facultative](#)
- [Désactiver les versions TLS sur les systèmes vCenter Server](#)
- [Désactiver les versions de TLS sur les hôtes ESXi](#)
- [Désactiver les versions TLS sur les systèmes Platform Services Controller](#)
- [Restaurer les modifications de l'utilitaire de configuration TLS](#)
- [Désactiver les versions de TLS sur vSphere Update Manager](#)

Ports prenant en charge la désactivation des versions TLS

Lorsque vous exécutez l'utilitaire TLS Configurator dans l'environnement vSphere, vous pouvez désactiver TLS sur les différents ports utilisant TLS sur les hôtes vCenter Server, Platform Services Controller et ESXi. Vous pouvez désactiver TLS 1.0, ou TLS 1.0 et TLS 1.1.

Le tableau suivant contient la liste des ports. Si un port n'est pas répertorié, l'utilitaire ne l'affecte pas.

Tableau 10-1. vCenter Server et Platform Services Controller affectés par l'utilitaire TLS Configurator

Service	Nom sous Windows	Nom sous Linux	Port
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMWareDirectoryService	vmldird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
Service de jeton sécurisé VMware	VMwareSTS	vmware-stsd	7444
vSphere Update Manager Service (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMWareDirectoryService	vmldird	11712

(*) TLS est contrôlé par la liste de chiffrement pour ces services. La gestion granulaire n'est pas possible. Seuls TLS 1.2 ou toutes les versions de TLS 1.x sont prises en charge.

(*) Sur vCenter Server Appliance, vSphere Update Manager se trouve sur le même système que vCenter Server. Sur vCenter Server sous Windows, vous configurez TLS en modifiant les fichiers de configuration. Reportez-vous à [Désactiver les versions de TLS sur vSphere Update Manager](#).

Tableau 10-2. Ports ESXi affectés par l'utilitaire TLS Configurator

Service	Nom du service	Port
VMware HTTP Reverse Proxy et Host Daemon	Hostd	443
Fournisseur de distributeur VMware vSAN VASA	vSANVP	8080
VMware Fault Domain Manager	FDM	8182
VMware vSphere API for IO Filters	ioFilterVPServer	9080
VMware Authorization Daemon	vmware-authd	902

Notes et mises en garde

- Assurez-vous que les hôtes hérités ESXi qui sont gérés par vCenter Server prennent en charge une version activée de TLS (TLS 1.1 et TLS 1.2) ou uniquement TLS 1.2. Lorsque vous désactivez une version de TLS sur vCenter Server 6.5, vCenter Server ne peut plus gérer les hôtes hérités ESXi 5.x et 6.0. Mettez à niveau ces hôtes vers des versions prenant en charge TLS 1.1 ou TLS 1.2.
- Vous ne pouvez pas utiliser uniquement TLS 1.2 pour une connexion à un serveur Microsoft SQL Server externe ou à une base de données Oracle externe.
- Ne désactivez pas TLS 1.0 sur une instance vCenter Server ou Platform Services Controller qui s'exécute sous Windows Server 2008. Windows 2008 prend en charge uniquement TLS 1.0. Reportez-vous à l'article de Microsoft TechNet sur les *paramètres TLS/SSL* dans le document *Server Roles and Technologies Guide*.
- Dans les cas suivants, vous devez redémarrer les services de l'hôte après avoir appliqué les modifications de configuration TLS.
 - Si vous appliquez les modifications à l'hôte ESXi directement.
 - Si vous appliquez les modifications via la configuration du cluster à l'aide de profils d'hôte.

Désactivation des versions de TLS dans vSphere

La désactivation des versions de TLS est un processus en plusieurs étapes. La désactivation des versions de TLS dans l'ordre approprié permet de s'assurer que votre environnement reste en cours d'exécution au cours du processus.

- 1 Si votre environnement inclut vSphere Update Manager sous Windows, et que vSphere Update Manager se trouve sur un système distinct, désactivez les protocoles explicitement en modifiant les fichiers de configuration. Reportez-vous à [Désactiver les versions de TLS sur vSphere Update Manager](#).

vSphere Update Manager sur vCenter Server Appliance est toujours inclus dans le système vCenter Server et le script met à jour le port correspondant.
- 2 Installez l'utilitaire de configuration de TLS sur vCenter Server et Platform Services Controller. Si votre environnement utilise une instance intégrée de Platform Services Controller, installez l'utilitaire uniquement sur vCenter Server.
- 3 Exécutez l'utilitaire sur vCenter Server.
- 4 Exécutez l'utilitaire sur chaque hôte ESXi qui est géré par vCenter Server. Vous pouvez effectuer cette tâche pour chaque hôte ou pour tous les hôtes dans un cluster.
- 5 Si votre environnement utilise une ou plusieurs instances de Platform Services Controller, exécutez l'utilitaire sur chaque instance.

Conditions préalables

Vous effectuez cette configuration sur les systèmes qui exécutent vSphere 6.0 U3 vSphere 6.5. Deux options s'offrent à vous.

- Désactivez TLS 1.0 et activez TLS 1.1 et TLS 1.2.
- Désactivez TLS1.0 et TLS 1.1 et activez TLS 1.2.

Installer l'utilitaire de configuration de TLS

Vous pouvez télécharger l'utilitaire de configuration de TLS depuis MyVMware.com et l'installer sur votre machine locale. Après l'installation, deux scripts sont disponibles. Un script est destiné à la configuration de vCenter Server et Platform Services Controller et un script est destiné à la configuration de ESXi.

Sur vCenter Server Appliance, les ports de vSphere Update Manager sont mis à jour par le script. Sur vCenter Server, modifiez les fichiers de configuration de vSphere Update Manager. Reportez-vous à [Désactiver les versions de TLS sur vSphere Update Manager](#).

Conditions préalables

Vous avez besoin d'un compte MyVMware pour télécharger le script.

Procédure

- 1 Connectez-vous à votre compte MyVMware et accédez à vSphere.
- 2 Recherchez le produit et la version du produit pour lesquels vous possédez la licence, sélectionnez VMware vCenter Server et cliquez sur **Accéder aux téléchargements**.
- 3 Sélectionnez le programme de configuration de TLS de VMware vSphere et téléchargez le fichier suivant.

SE	Fichier
Windows	VMware-vSphereTlsReconfigurator -version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator -version-build_number.x86_64.rpm

4 Téléchargez le fichier sur vCenter Server et installez les scripts.

Dans les environnements comportant un Platform Services Controller externe, téléchargez également le fichier sur Platform Services Controller.

SE	Procédure
Windows	<ol style="list-style-type: none"> Connectez-vous en tant qu'utilisateur avec des privilèges d'administrateur. Copiez le fichier <code>VMware-vSphereTlsReconfigurator -version-numéro_de_build.x86_64.msi</code> que vous avez téléchargé. Installez le fichier MSI.
Linux	<ol style="list-style-type: none"> Connectez-vous au dispositif à l'aide de SSH en tant qu'utilisateur avec des privilèges pour exécuter des scripts. Copiez le fichier <code>VMware-vSphereTlsReconfigurator -version-numéro_de_build.x86_64.rpm</code> dans le dispositif à l'aide d'un client SCP. Si l'interpréteur de commandes de dépistage n'est pas actuellement activé, exécutez les commandes suivantes. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>shell.set --enabled true shell</pre> </div> Accédez au répertoire dans lequel se trouve le fichier rpm téléchargé et exécutez la commande suivante. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-numéro_de_build.x86_64.rpm</pre> </div>

Résultats

Une fois l'installation terminée, vous trouverez les scripts aux emplacements suivants.

SE	Emplacement
Windows	<ul style="list-style-type: none"> ■ C:\Program Files\VMware\CIS\vSphereTLsReconfigurator\VcTlsReconfigurator ■ C:\Program Files\VMware\CIS\vSphereTLsReconfigurator\EsxTlsReconfigurator
Linux	<ul style="list-style-type: none"> ■ /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator ■ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

Effectuer une sauvegarde manuelle facultative

L'utilitaire de configuration TLS effectue une sauvegarde à chaque fois que le script modifie vCenter Server, Platform Services Controller ou vSphere Update Manager. Si vous avez besoin d'effectuer une sauvegarde dans un répertoire spécifique, vous pouvez effectuer une sauvegarde manuelle.

Le répertoire par défaut est différent pour Windows et le dispositif.

SE	Répertoire de sauvegarde
Windows	<code>c:\users\current_user\appdata\local\temp\yearmonthdayTtime</code>
Linux	<code>/tmp/yearmonthdayTtime</code>

Procédure

- 1 Modifiez le répertoire pour vSphereTlsReconfigurator, puis accédez au sous-répertoire VcTlsReconfigurator.

SE	Commande
Windows	<code>C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\ cd VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/ cd VcTlsReconfigurator</code>

- 2 Exécutez la commande suivante pour effectuer une sauvegarde dans un répertoire spécifique.

SE	Commande
Windows	<code>chemin_répertoire\VcTlsReconfigurator> reconfigureVc backup -d chemin_répertoire_sauvegarde</code>
Linux	<code>chemin_répertoire/VcTlsReconfigurator> ./ reconfigureVc backup -d chemin_répertoire_sauvegarde</code>

- 3 Vérifiez que la sauvegarde s'est effectuée correctement.

Une sauvegarde réussie ressemble à l'exemple suivant.

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819"
Log file: "C:\ProgramData\VMware\VCenterServer\logs\vmware\vsphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

- 4 (Facultatif) Si vous devez par la suite effectuer une restauration, exécutez la commande suivante.

```
reconfigure restore -d répertoire tmp ou chemin d'accès du répertoire de sauvegarde personnalisé
```

Désactiver les versions TLS sur les systèmes vCenter Server

Vous pouvez utiliser l'utilitaire de configuration de TLS pour désactiver les versions TLS sur les systèmes vCenter Server. Dans le cadre du processus, vous pouvez activer TLS 1.1 et TLS 1.2, ou uniquement TLS 1.2.

Conditions préalables

Assurez-vous que les hôtes et les services gérés par vCenter Server peuvent communiquer à l'aide d'une version de TLS qui reste activée. Pour les produits qui communiquent uniquement à l'aide de TLS 1.0, la connectivité devient indisponible.

Procédure

- 1 Connectez-vous au système vCenter Server en tant qu'utilisateur autorisé à exécuter des scripts, puis accédez au répertoire dans lequel se trouve le script.

SE	Commande
Windows	<code>cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 Exécutez la commande en fonction de votre système d'exploitation et de la version de TLS que vous souhaitez utiliser.

- Pour désactiver TLS 1.0 et activer TLS 1.1 et 1.2, exécutez la commande suivante.

SE	Commande
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2, exécutez la commande suivante.

SE	Commande
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 Si votre environnement inclut d'autres systèmes vCenter Server, répétez le processus sur chaque système vCenter Server.
- 4 Répétez cette configuration sur chaque hôte ESXi et chaque Platform Services Controller.

Désactiver les versions de TLS sur les hôtes ESXi

Vous pouvez utiliser l'utilitaire de configuration de TLS pour désactiver les versions TLS sur un hôte ESXi. Dans le cadre du processus, vous pouvez activer TLS 1.1 et TLS 1.2, ou uniquement TLS 1.2.

Pour les hôtes ESXi, utilisez un script différent que pour les autres composants de votre environnement vSphere.

Note Le script désactive TLS 1.0 et 1.1, sauf si vous spécifiez l'option `-p`.

Conditions préalables

Assurez-vous que les produits ou les services associés à l'hôte ESXi peuvent communiquer à l'aide de TLS 1.1 ou TLS 1.2. Pour les produits qui communiquent uniquement à l'aide de TLS 1.0, la connectivité est perdue.

Procédure

- 1 Connectez-vous à l'hôte vCenter Server en tant qu'utilisateur pouvant exécuter des scripts et accédez au répertoire dans lequel se trouve le script.

SE	Commande
Windows	<code>C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 Pour désactiver TLS sur tous les hôtes d'un cluster, exécutez l'une des commandes suivantes.
 - Pour désactiver TLS 1.0 et activer TLS 1.1 et 1.2 sur tous les hôtes d'un cluster, exécutez la commande suivante.

SE	Commande
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2 sur tous les hôtes d'un cluster, exécutez la commande suivante.

SE	Commande
Windows	<code>reconfigureEsx vCenterCluster -c <i>Cluster_Name</i> -u <i>Administrative_User</i> -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c <i>Cluster_Name</i> -u <i>Administrative_User</i> -p TLSv1.2</code>

3 Pour désactiver TLS sur un hôte individuel, exécutez l'une des commandes suivantes.

- Pour désactiver TLS 1.0 et activer TLS 1.1 et TLS 1.2 sur un hôte individuel, exécutez la commande suivante.

SE	Commande
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u <i>Administrative_User</i> -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u <i>Administrative_User</i> -p TLSv1.1 TLSv1.2</code>

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2 sur un hôte individuel, exécutez la commande suivante.

SE	Commande
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u <i>Administrative_User</i> -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u <i>Administrative_User</i> -p TLSv1.2</code>

4 Redémarrez l'hôte ESXi pour terminer les modifications du protocole TLS.

Désactiver les versions TLS sur les systèmes Platform Services Controller

Si votre environnement comprend un ou plusieurs systèmes Platform Services Controller, vous pouvez utiliser l'utilitaire de configuration de TLS pour modifier les versions de TLS qui doivent être prises en charge.

Si votre environnement utilise uniquement une instance intégrée de Platform Services Controller, vous n'avez pas besoin d'effectuer cette tâche.

Note Poursuivez cette tâche uniquement après avoir confirmé que chaque système vCenter Server exécute une version compatible de TLS. Si des instances de vCenter Server 6.0.x ou 5.5.x sont connectées à vCenter Server, elles cessent de communiquer avec Platform Services Controller si vous désactivez les versions de TLS.

Vous pouvez désactiver TLS 1.0 et TLS 1.1 et laisser TLS 1.2 activée, ou vous pouvez désactiver uniquement TLS 1.0 et laisser TLS 1.1 et 1.2 activées.

Conditions préalables

Assurez-vous que les hôtes et les services auxquels Platform Services Controller se connecte peuvent communiquer à l'aide d'un protocole pris en charge. Étant donné que la gestion des authentifications et des certificats est gérée par Platform Services Controller, tenez compte soigneusement des services qui peuvent être affectés. Pour les services qui communiquent uniquement à l'aide de protocoles non pris en charge, la connectivité devient indisponible.

Procédure

- 1 Connectez-vous à Platform Services Controller en tant qu'utilisateur pouvant exécuter des scripts et accédez au répertoire dans lequel se trouve le script.

SE	Commande
Windows	<code>cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 Vous pouvez effectuer cette tâche sur Platform Services Controller sous Windows ou sur le dispositif Platform Services Controller.

- Pour désactiver TLS 1.0 et activer TLS 1.1 et 1.2, exécutez la commande suivante.

SE	Commande
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2, exécutez la commande suivante.

SE	Commande
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 Si votre environnement inclut d'autres systèmes Platform Services Controller, répétez le processus.

Restaurer les modifications de l'utilitaire de configuration TLS

Vous pouvez utiliser l'utilitaire de configuration TLS pour restaurer les modifications de configuration. Lorsque vous restaurez les modifications, le système active les protocoles que vous avez désactivés à l'aide de l'utilitaire TLS Configurator.

Vous pouvez effectuer une récupération uniquement si vous avez préalablement sauvegardé la configuration. La restauration des modifications n'est pas prise en charge pour les hôtes ESXi.

Effectuez la récupération dans cet ordre.

- 1 vSphere Update Manager.

Si votre environnement exécute une instance de vSphere Update Manager distincte sur un système Windows, vous devez d'abord mettre à jour vSphere Update Manager.

- 2 vCenter Server

- 3 Platform Services Controller

Procédure

- 1 Connectez-vous à la machine Windows ou au dispositif.
- 2 Connectez-vous au système sur lequel vous souhaitez restaurer les modifications.

SE	Procédure
Windows	<ol style="list-style-type: none"> 1 Connectez-vous en tant qu'utilisateur avec des privilèges d'administrateur. 2 Accédez au répertoire <code>VcTlsReconfigurator</code>. <div> <pre>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</pre> </div>
Linux	<ol style="list-style-type: none"> 1 Connectez-vous au dispositif à l'aide de SSH en tant qu'utilisateur avec des privilèges pour exécuter des scripts. 2 Si l'interpréteur de commandes de dépannage n'est pas actuellement activé, exécutez les commandes suivantes. <div> <pre>shell.set --enabled true shell</pre> </div> 3 Accédez au répertoire <code>VcTlsReconfigurator</code>. <div> <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre> </div>

3 Examinez la sauvegarde précédente.

SE	Procédure
Windows	<pre>C:\ProgramData\VMware\vCenterServer\logs\vSphere-TlsReconfigurator\VcTlsReconfigurator.log</pre> <p>Le résultat est semblable à l'exemple suivant.</p> <pre>c:\users\nom d'utilisateur\appdata\local\temp\20161108T161539 c:\users\nom d'utilisateur\appdata\local\temp\20161108T171539</pre>
Linux	<pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log</pre> <p>Le résultat est semblable à l'exemple suivant.</p> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre>

4 Exécutez l'une des commandes suivantes pour effectuer une restauration.

SE	Procédure
Windows	<pre>reconfigureVc restore -d Chemin_répertoire_étape_précédente</pre> <p>Par exemple</p> <pre>reconfigureVc restore -d c:\users\nom d'utilisateur\appdata\local\temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d Chemin_répertoire_étape_précédente</pre> <p>Par exemple</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

5 Répétez la procédure sur toutes les autres instances de vCenter Server.

6 Répétez la procédure sur toutes les autres instances de Platform Services Controller.

Désactiver les versions de TLS sur vSphere Update Manager

Dans vSphere Update Manager 6.0 Update 3 et les versions ultérieures, les versions de protocole TLS 1.0, 1.1 et 1.2 sont toutes activées par défaut. Vous pouvez désactiver TLS 1.1 et 1.0, mais vous ne pouvez pas désactiver TLS 1.2.

Vous pouvez gérer la configuration du protocole TLS des autres services à l'aide de l'utilitaire de configuration de TLS. Toutefois, pour vSphere Update Manager, vous devez reconfigurer le protocole TLS manuellement.

La modification de la configuration du protocole TLS peut impliquer les tâches suivantes.

- Désactivation de TLS 1.0, tout en laissant les versions TLS 1.1 et 1.2 activées.

- Désactivation de TLS 1.0 et 1.1, tout en laissant la version TLS 1.2 activée.
- Réactivation d'une version du protocole TLS désactivée.

Désactiver les précédentes versions de TLS pour Update Manager, port 9087

Vous pouvez désactiver les versions antérieures de TLS pour le port 9087 en modifiant le fichier de configuration `jetty-vum-ssl.xml`. Le processus est différent pour le port 8084.

Note Avant de désactiver une version de TLS, assurez-vous qu'aucun des services communiquant avec vSphere Update Manager n'utilise cette version.

Conditions préalables

Arrêtez le service vSphere Update Manager. Consultez la documentation de *Installation et administration de VMware vSphere Update Manager*.

Procédure

- 1 Arrêtez le service vSphere Update Manager.
- 2 Accédez au répertoire d'installation d'Update Manager, qui est différent pour vSphere 6.0 et vSphere 6.5.

Version	Emplacement
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 Effectuez une sauvegarde du fichier `jetty-vum-ssl.xml` et ouvrez le fichier.
- 4 Désactivez les versions antérieures de TLS en modifiant le fichier.

Option	Description
Désactivez TLS 1.0. Laissez les versions TLS 1.1 et 1.2 activées.	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> </Array> </Set></pre>
Désactivez TLS 1.1 et 1.0. Laissez la version TLS 1.2 activée.	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> <Item>TLSv1.1</Item> </Array> </Set></pre>

- 5 Enregistrez le fichier.
- 6 Redémarrez le service vSphere Update Manager.

Désactiver les précédentes versions de TLS pour le port 8084 d'Update Manager

Vous pouvez désactiver les versions antérieures de TLS pour le port 8084 en modifiant le fichier de configuration `vci-integrity.xml`. Le processus est différent pour le port 9087.

Note Avant de désactiver une version de TLS, assurez-vous qu'aucun des services qui communiquent avec vSphere Update Manager n'utilise cette version.

Conditions préalables

Arrêtez le service vSphere Update Manager. Consultez la documentation de *Installation et administration de VMware vSphere Update Manager*.

Procédure

- 1 Arrêtez le service vSphere Update Manager.
- 2 Accédez au répertoire d'installation d'Update Manager, qui est différent pour les versions 6.0 et 6.5.

Version	Emplacement
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 Effectuez une sauvegarde du fichier `vci-integrity.xml` et ouvrez le fichier.
- 4 Ajoutez une balise `<sslOptions>` dans le fichier `vci-integrity.xml`.

```
<ssl>
  <handshakeTimeoutMs>120000</handshakeTimeoutMs>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>

<ssl>
  <privateKey>ssl/rui.key</privateKey>
  <certificate>ssl/rui.crt</certificate>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

- 5 Selon la version TLS que vous souhaitez désactiver, utilisez l'une des valeurs décimales suivantes dans la balise `<sslOptions>`.
 - Pour désactiver TLS 1.0 uniquement, utilisez la valeur décimale 117587968.
 - Pour désactiver TLS 1.0 et TLS 1.1, utilisez la valeur décimale 386023424
- 6 Enregistrez le fichier.
- 7 Redémarrez le service vSphere Update Manager.

Réactiver les versions de TLS désactivées pour le port 9087 du service Update Manager

Si vous désactivez une version de TLS pour le port 9087 du service Update Manager et que vous rencontrez des problèmes, vous pouvez réactiver la version. Le processus est différent pour le port 8084.

La réactivation d'une version antérieure de TLS peut affecter la sécurité.

Procédure

- 1 Arrêtez le service vSphere Update Manager.
- 2 Accédez au répertoire d'installation d'Update Manager, qui est différent pour les versions 6.0 et 6.5.

Version	Emplacement
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 Effectuez une sauvegarde du fichier `jetty-vum-ssl.xml` et ouvrez le fichier.
- 4 Supprimez la balise TLS qui correspond à la version du protocole TLS que vous souhaitez activer.

Par exemple, supprimez `<Item>TLSv1.1</Item>` dans le fichier `jetty-vum-ssl.xml` pour activer TLS 1.1.
- 5 Enregistrez le fichier.
- 6 Redémarrez le service vSphere Update Manager.

Réactiver les versions de TLS désactivées pour le port 8084 du service Update Manager

Si vous désactivez une version de TLS pour le port 8084 du service Update Manager et que vous rencontrez des problèmes, vous pouvez réactiver la version. Le processus est différent pour le port 9087.

La réactivation d'une version antérieure de TLS peut affecter la sécurité.

Procédure

- 1 Arrêtez le service vSphere Update Manager.

- 2 Accédez au répertoire d'installation d'Update Manager, qui est différent pour les versions 6.0 et 6.5.

Version	Emplacement
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 Effectuez une sauvegarde du fichier `vci-integrity.xml` et ouvrez le fichier.
- 4 Modifiez la valeur décimale qui est utilisée dans la balise `<sslOptions>`, ou supprimez la balise pour autoriser toutes les versions de TLS.
 - Pour activer TLS 1.1, sans activer TLS 1.0, utilisez la valeur décimale 117587968.
 - Pour réactiver à la fois TLS 1.1 et TLS 1.0, supprimez la balise.
- 5 Enregistrez le fichier.
- 6 Redémarrez le service vSphere Update Manager.

Privilèges définis

11

Les tableaux suivants présentent les privilèges par défaut qui, une fois sélectionnés pour un rôle, peuvent être associés avec un utilisateur et assignés à un objet. Dans les tableaux de cette annexe, VC désigne vCenter Server et HC désigne le client de l'hôte, un hôte ESXi autonome ou un hôte de poste de travail.

En définissant des autorisations, vérifiez que tous les types d'objet sont définis avec des privilèges appropriés pour chaque action particulière. Quelques opérations exigent la permission d'accès au dossier racine ou au dossier parent en plus de l'accès à l'objet manipulé. Quelques opérations exigent l'autorisation d'accès ou de performances à un dossier parent et à un objet associé.

Les extensions de vCenter Server peuvent définir des privilèges supplémentaires non mentionnés ici. Référez-vous à la documentation concernant l'extension pour plus d'informations sur ces privilèges.

Ce chapitre contient les rubriques suivantes :

- [Privilèges d'alarmes](#)
- [Privilèges Auto Deploy et privilèges de profil d'image](#)
- [Privilèges de certificats](#)
- [Privilèges de bibliothèque de contenu](#)
- [Privilèges de centre de données](#)
- [Privilèges de banque de données](#)
- [Privilèges de cluster de banques de données](#)
- [Privilèges de Distributed Switch](#)
- [Privilèges de gestionnaire d'agent ESX](#)
- [Privilèges d'extension](#)
- [Privilèges de dossier](#)
- [Privilèges globaux](#)
- [Privilèges CIM d'hôte](#)
- [Privilèges de configuration d'hôte](#)
- [Inventaire d'hôte](#)

- Privilèges d'opérations locales d'hôte
- Privilèges de réplication d'hôte vSphere
- Privilèges de profil d'hôte
- Privilèges du fournisseur Inventory Service
- Privilèges de balisage Inventory Service
- Privilèges de réseau
- Privilèges de performances
- Privilèges d'autorisations
- Privilèges de stockage basé sur le profil
- Privilèges de ressources
- Privilèges de tâche planifiée
- Privilèges de sessions
- Privilèges de vues de stockage
- Privilèges de tâches
- Privilèges Transfer Service
- Privilèges de règle de VRM
- Privilèges de configuration de machine virtuelle
- Privilèges d'opérations d'invité de machine virtuelle
- Privilèges d'interaction de machine virtuelle
- Privilèges d'inventaire de machine virtuelle
- Privilèges de provisionnement de machine virtuelle
- Privilèges de configuration de services de machine virtuelle
- Privilèges de gestion des snapshots d'une machine virtuelle
- Privilèges vSphere Replication de machine virtuelle
- Privilèges du groupe dvPort
- Privilèges de vApp
- Privilèges vServices

Privilèges d'alarmes

Les privilèges d'alarmes contrôlent la capacité à créer et à modifier des alarmes sur des objets d'inventaire, et à y répondre.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-1. Privilèges d'alarmes

Nom de privilège	Description	Requis sur
Alarmes.Reconnaître une alarme	Permet la suppression de toutes les actions d'alarme sur toutes les alarmes déclenchées.	Objet sur lequel une alarme est définie
Alarmes.Créer une alarme	Permet la création d'une alarme. En créant des alarmes avec une action personnalisée, le privilège d'exécuter l'action est vérifié quand l'utilisateur crée l'alarme.	Objet sur lequel une alarme est définie
Alarmes.Désactiver une action d'alarme	Permet d'empêcher une action d'alarme après le déclenchement d'une alarme. Cette intervention ne désactive pas l'alarme.	Objet sur lequel une alarme est définie
Alarmes.Modifier une alarme	Permet le changement des propriétés d'une alarme.	Objet sur lequel une alarme est définie
Alarmes.Supprimer une alarme	Permet la suppression d'une alarme.	Objet sur lequel une alarme est définie
Alarmes.Définir l'état d'une alarme	Permet de changer l'état de l'alarme d'événement configurée. L'état peut changer en Normal , Avertissement ou Alerte .	Objet sur lequel une alarme est définie

Privilèges Auto Deploy et privilèges de profil d'image

Les privilèges Auto Deploy contrôlent qui peut effectuer différentes tâches sur les règles Auto Deploy et qui peut associer un hôte. Ils permettent également de contrôler qui peut créer ou modifier un profil d'image.

Le tableau suivant décrit les privilèges qui déterminent les personnes pouvant gérer les règles et les ensembles de règles Auto Deploy et celles qui peuvent créer et modifier des profils d'image. Reportez-vous à *Installation et configuration de vSphere*.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-2. Privilèges Auto Deploy

Nom de privilège	Description	Requis sur
Auto Deploy.Hôte.Associer une machine	Permet aux utilisateurs d'associer un hôte à une machine.	vCenter Server
Auto Deploy.Profil d'image .Créer	Permet de créer des profils d'image.	vCenter Server
Auto Deploy.Profil d'image .Modifier	Permet de modifier des profils d'image.	vCenter Server
Auto Deploy.Règle .Créer	Permet de créer des règles Auto Deploy.	vCenter Server
Auto Deploy.Règle .Supprimer	Permet de supprimer des règles Auto Deploy.	vCenter Server
Auto Deploy.Règle.Modifier	Permet de modifier des règles Auto Deploy.	vCenter Server

Tableau 11-2. Privilèges Auto Deploy (suite)

Nom de privilège	Description	Requis sur
Auto Deploy.Ensemble de règles .Activer	Permet d'activer des ensembles de règles Auto Deploy.	vCenter Server
Auto Deploy.Ensemble de règles .Modifier	Permet de modifier des ensembles de règles Auto Deploy.	vCenter Server

Privilèges de certificats

Les privilèges de certificats déterminent les utilisateurs pouvant gérer les certificats d'ESXi.

Ce privilège détermine qui peut effectuer la gestion de certificats pour les hôtes ESXi. Reportez-vous à [Privilèges requis pour les opérations de gestion de certificats](#) pour plus d'informations sur la gestion de certificats vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-3. Privilèges de certificats d'hôte

Nom de privilège	Description	Requis sur
Certificates. Gérer les certificats	Permet la gestion de certificats pour les hôtes ESXi.	vCenter Server

Privilèges de bibliothèque de contenu

Les bibliothèques de contenu offrent une méthode simple et efficace pour gérer les modèles de machines virtuelles et les vApp. Les privilèges de bibliothèque de contenu contrôlent qui peut afficher ou gérer les différents aspects des bibliothèques de contenu.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-4. Privilèges de bibliothèque de contenu

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Ajouter un élément de bibliothèque	Autorise l'ajout d'éléments à une bibliothèque.	Bibliothèque
Bibliothèque de contenu.Créer une bibliothèque locale	Autorise la création de bibliothèques locales sur le système vCenter Server spécifié.	vCenter Server
Bibliothèque de contenu.Créer la bibliothèque abonnée	Autorise la création de bibliothèques abonnées.	vCenter Server
Bibliothèque de contenu.Supprimer l'élément de la bibliothèque	Autorise la suppression d'éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Supprimer la bibliothèque locale	Autorise la suppression d'une bibliothèque locale.	Bibliothèque
Bibliothèque de contenu.Supprimer la bibliothèque abonnée	Autorise la suppression d'une bibliothèque abonnée.	Bibliothèque
Bibliothèque de contenu.Télécharger des fichiers	Autorise le téléchargement de fichiers de la bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Expulser l'élément de bibliothèque	Autorise l'éviction d'éléments. Le contenu d'une bibliothèque abonnée peut être mis en cache ou non. S'il est mis en cache, vous pouvez libérer un élément de la bibliothèque en l'expulsant (si vous disposez de ce privilège).	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Expulser la bibliothèque abonnée	Autorise l'éviction d'une bibliothèque abonnée. Le contenu d'une bibliothèque abonnée peut être mis en cache ou non. S'il est mis en cache, vous pouvez libérer une bibliothèque en l'expulsant (si vous disposez de ce privilège).	Bibliothèque
Bibliothèque de contenu.Importer le stockage	Autorise un utilisateur à importer un élément de bibliothèque si l'URL du fichier source commence par ds:// ou file://. Ce privilège est désactivé pour l'administrateur de bibliothèque de contenu par défaut. Comme une importation à partir d'une URL de stockage implique une importation de contenu, n'activez ce privilège qu'en cas de besoin et s'il n'existe aucun problème de sécurité concernant l'utilisateur qui va effectuer l'importation.	Bibliothèque

Tableau 11-4. Privilèges de bibliothèque de contenu (suite)

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Contrôler les informations sur l'abonnement	Ce privilège autorise les utilisateurs de solution et les API à contrôler les informations d'abonnement d'une bibliothèque distante (URL, certificat SSL et mot de passe, notamment). La structure obtenue indique si la configuration de l'abonnement s'est bien déroulée ou si des problèmes se sont produits (des erreurs SSL, par exemple).	Bibliothèque
Bibliothèque de contenu.Stockage de lecture	Autorise la lecture du stockage d'une bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Synchroniser l'élément de la bibliothèque	Autorise la synchronisation des éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Synchroniser la bibliothèque abonnée	Autorise la synchronisation des bibliothèques abonnées.	Bibliothèque
Bibliothèque de contenu.Introspection de type	Autorise un utilisateur de solution ou un API à examiner les plug-ins de support de type pour Content Library Service.	Bibliothèque
Bibliothèque de contenu.Mettre à jour les paramètres de configuration	Vous autorise à mettre à jour les paramètres de configuration. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Bibliothèque
Bibliothèque de contenu.Mettre à jour des fichiers	Vous autorise à télécharger le contenu dans la bibliothèque de contenu. Vous permet également de supprimer les fichiers d'un élément de bibliothèque.	Bibliothèque
Bibliothèque de contenu.Mettre à jour la bibliothèque	Permet de mettre à jour la bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Mettre à jour l'élément de bibliothèque	Permet de mettre à jour les éléments de bibliothèque.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Mettre à jour la bibliothèque locale	Permet de mettre à jour les bibliothèques locales.	Bibliothèque

Tableau 11-4. Privilèges de bibliothèque de contenu (suite)

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Mettre à jour la bibliothèque abonnée	Vous autorise à mettre à jour les propriétés d'une bibliothèque abonnée.	Bibliothèque
Bibliothèque de contenu.Afficher les paramètres de configuration	Vous autorise à afficher les paramètres de configuration. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Bibliothèque

Privilèges de centre de données

Les privilèges de centre de données contrôlent la capacité à créer et modifier des centres de données dans l'inventaire vSphere Web Client.

Tous les privilèges de centre de données ne sont utilisés que dans vCenter Server. Le privilège **Créer un centre de données** est défini sur les dossiers du centre de données ou l'objet racine. Tous les autres privilèges de centre de données sont associés à des centres de données, des dossiers de centres de données ou à l'objet racine.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-5. Privilèges de centre de données

Nom de privilège	Description	Requis sur
Centre de données.Créer un centre de données	Permet de créer un centre de données.	Objet de dossier de centre de données ou objet racine
Centre de données.Déplacer un centre de données	Permet de déplacer un centre de données. Le privilège doit être présent à la fois à la source et à la destination.	Centre de données, source et destination
Centre de données.Configuration du profil de protocole réseau	Permet de configurer le profil réseau d'un centre de données.	Centre de données
Centre de données.Allocation de requête de pool d'adresses IP	Permet la configuration d'un pool d'adresses IP.	Centre de données
Centre de données.Reconfigurer un centre de données	Permet de reconfigurer un centre de données.	Centre de données
Centre de données.Libérer une allocation IP	Permet de libérer l'allocation IP attribuée à un centre de données.	Centre de données

Tableau 11-5. Privilèges de centre de données (suite)

Nom de privilège	Description	Requis sur
Centre de données.Supprimer un centre de données	Permet de supprimer un centre de données. Pour pouvoir exécuter cette opération, ce privilège doit être assigné à la fois à l'objet et à son objet parent.	Centre de données et objet parent
Centre de données.Renommer un centre de données	Permet de modifier le nom d'un centre de données.	Centre de données

Privilèges de banque de données

Les privilèges de banque de données contrôlent la capacité à parcourir, gérer, et allouer l'espace sur les banques de données.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-6. Privilèges de banque de données

Nom de privilège	Description	Requis sur
Banque de données.Allouer de l'espace	Permet l'allocation d'espace sur une banque de données pour une machine virtuelle, un snapshot, un clone ou un disque virtuel.	Centres de données
Banque de données.Parcourir une banque de données	Permet la recherche de fichiers sur une banque de données.	Centres de données
Banque de données.Configurer une banque de données	Permet la configuration d'une banque de données.	Centres de données
Banque de données.Opérations de fichier de niveau inférieur	Permet l'exécution d'opérations de lecture, d'écriture, de suppression et de changement de nom dans le navigateur de la banque de données.	Centres de données
Banque de données.Déplacer une banque de données	Permet le déplacement d'une banque de données entre dossiers. Les privilèges doivent être présents à la fois à la source et à la destination.	La banque de données, source et destination
Banque de données.Supprimer une banque de données	Permet la suppression d'une banque de données. Ce privilège est à éviter. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Centres de données
Banque de données.Supprimer un fichier	Permet la suppression de fichiers dans la banque de données. Ce privilège est à éviter. Attribue le privilège Opérations de fichier de niveau inférieur .	Centres de données

Tableau 11-6. Privilèges de banque de données (suite)

Nom de privilège	Description	Requis sur
Banque de données.Renommer une banque de données	Permet de renommer une banque de données.	Centres de données
Banque de données.Mettre à jour les fichiers de machine virtuelle	Permet de mettre à niveau les chemins d'accès aux fichiers de machine virtuelle sur une banque de données après que la banque de données a été resignée.	Centres de données
Banque de données.Mettre à jour les métadonnées de la machine virtuelle	Permet de mettre à jour les métadonnées de la machine virtuelle associées à une banque de données.	Centres de données

Privilèges de cluster de banques de données

Les privilèges de cluster de banques de données contrôlent la configuration des clusters de banques de données du DRS de stockage.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-7. Privilèges de cluster de banques de données

Nom de privilège	Description	Requis sur
Cluster de banques de données.Configurer un cluster de banques de données	Permet la création et la configuration de paramètres pour les clusters de banques de données de Storage DRS.	Clusters de banques de données

Privilèges de Distributed Switch

Les privilèges de Distributed Switch contrôlent la capacité à effectuer des tâches associées à la gestion des instances de Distributed Switch.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-8. Privilèges de vSphere Distributed Switch

Nom de privilège	Description	Requis sur
Commutateur distribué.Créer	Autorise la création d'une instance de Distributed Switch.	Centres de données, dossiers réseau
Commutateur distribué.Supprimer	Autorise la suppression d'une instance de Distributed Switch. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Distributed switches
Commutateur distribué.Opération de l'hôte	Autorise le changement des membres hôtes d'une instance de Distributed Switch.	Distributed switches
Commutateur distribué.Modifier	Autorise la modification de la configuration d'une instance de Distributed Switch.	Distributed switches
Commutateur distribué.Déplacer	Autorise le déplacement d'un vSphere Distributed Switch vers un autre dossier.	Distributed switches
Distributed Switch.Opération de Network I/O control	Autorise la modification des paramètres de ressources d'un vSphere Distributed Switch.	Distributed switches
Commutateur distribué.Opération de stratégie	Autorise la modification de la règle d'un vSphere Distributed Switch.	Distributed switches
Commutateur distribué.Opération de configuration de port	Autorise la modification de la configuration d'un port dans un vSphere Distributed Switch.	Distributed switches
Commutateur distribué.Opération de définition de port	Autorise la modification des paramètres d'un port dans un vSphere Distributed Switch.	Distributed switches
Commutateur distribué.Opération VSPAN	Autorise la modification de la configuration VSPAN d'un vSphere Distributed Switch.	Distributed switches

Privilèges de gestionnaire d'agent ESX

Les privilèges de gestionnaire d'agent ESX contrôlent les opérations liées au Gestionnaire d'agent ESX et aux machines virtuelles d'agent. Le gestionnaire d'agent ESX est un service qui vous permet d'installer des machines virtuelles de gestion liées à un hôte et non affectées par VMware DRS ou d'autres services qui migrent des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-9. Gestionnaire d'agent ESX

Nom de privilège	Description	Requis sur
Gestionnaire d'agent ESX.Config	Permet de déployer une machine virtuelle d'agent sur un hôte ou un cluster.	Machines virtuelles
Gestionnaire d'agent ESX.Modifier	Permet d'apporter des modifications à une machine virtuelle d'agent telles que la mise hors tension ou la suppression de la machine virtuelle.	Machines virtuelles
Affichage d'agent ESX.Affichage	Permet d'afficher une machine virtuelle d'agent.	Machines virtuelles

Privilèges d'extension

Les privilèges d'extension contrôlent la capacité à installer et gérer des extensions.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-10. Privilèges d'extension

Nom de privilège	Description	Requis sur
Extension.Enregistrer une étendue	Permet d'enregistrer une extension (plug-in).	Racine vCenter Server
Extension.Annuler l'enregistrement d'une étendue	Permet d'annuler l'enregistrement d'une extension (plug-in).	Racine vCenter Server
Extension.Mettre à jour une étendue	Permet de mettre à jour une extension (plug-in).	Racine vCenter Server

Privilèges de dossier

Les privilèges de dossier contrôlent la capacité à créer et gérer des dossiers.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-11. Privilèges de dossier

Nom de privilège	Description	Requis sur
Dossier.Créer un dossier	Permet de créer un dossier.	Dossiers
Dossier.Supprimer un dossier	Permet de supprimer un dossier. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Dossiers
Dossier.Déplacer un dossier	Permet de déplacer un dossier. Le privilège doit être présent à la fois à la source et à la destination.	Dossiers
Dossier.Renommer un dossier	Permet de modifier le nom d'un dossier.	Dossiers

Privilèges globaux

Les privilèges globaux contrôlent un certain nombre de tâches globales associées aux tâches, aux scripts et aux extensions.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-12. Privilèges globaux

Nom de privilège	Description	Requis sur
Global.Agir en tant que vCenter Server	Permet la préparation ou le lancement d'une opération d'envoi vMotion ou d'une opération de réception vMotion.	Racine vCenter Server
Global.Annuler une tâche	Permet l'annulation d'une tâche en cours d'exécution ou en file d'attente.	Objet d'inventaire associé à la tâche
Global.Planification de capacité	Permet l'activation de l'utilisation de la planification de capacité pour prévoir la consolidation de machines physiques en machines virtuelles.	Racine vCenter Server
Global.Diagnostics	Permet la récupération d'une liste de fichiers de diagnostic, d'un en-tête de journal, de fichiers binaires ou d'un groupe de diagnostic. Pour éviter d'éventuelles failles de sécurité, limitez ce privilège au rôle d'administrateur vCenter Server.	Racine vCenter Server
Global.Désactiver méthodes	Permet à des serveurs d'extensions de vCenter Server de désactiver des opérations sur des objets gérés par vCenter Server.	Racine vCenter Server
Global.Activer des méthodes	Permet aux serveurs d'extensions vCenter Server d'activer certaines opérations sur des objets gérés par vCenter Server.	Racine vCenter Server
Global.Balise globale	Permet l'ajout ou la suppression de balises globales.	Hôte racine ou vCenter Server

Tableau 11-12. Privilèges globaux (suite)

Nom de privilège	Description	Requis sur
Global.Intégrité	Permet l'affichage de l'état de fonctionnement de composants de vCenter Server.	Racine vCenter Server
Global.Licences	Permet l'affichage de licences installées, ainsi que l'ajout ou la suppression de licences.	Hôte racine ou vCenter Server
Global.Événement de journal	Permet la consignation d'un événement défini par l'utilisateur par rapport à une entité gérée.	Tout objet
Global.Gérer des attributs personnalisés	Permet d'ajouter, de supprimer ou de renommer des définitions de champs personnalisés.	Racine vCenter Server
Global.Proxy	Permet l'accès à une interface interne pour ajouter ou supprimer des points finaux à ou depuis un proxy.	Racine vCenter Server
Global.Action de script	Permet de planifier une action de script en relation avec une alarme.	Tout objet
Global.Gestionnaires de services	Permet l'utilisation de la commande <code>resxtop</code> dans l'interface de ligne de commande vSphere.	Hôte racine ou vCenter Server
Global.Définir un attribut personnalisé	Permet de visualiser, créer ou supprimer des attributs personnalisés pour un objet géré.	Tout objet
Global.Paramètres	Permet la lecture ou la modification de paramètres de configuration d'exécution de vCenter Server.	Racine vCenter Server
Global.Balise système	Permet l'ajout ou la suppression de balises système.	Racine vCenter Server

Privilèges CIM d'hôte

Les privilèges d'hôte CIM contrôlent l'utilisation du CIM pour la surveillance de la santé de l'hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-13. Privilèges CIM d'hôte

Nom de privilège	Description	Requis sur
Hôte.CIM.Interaction CIM	Permettre à un client d'obtenir un billet pour l'utilisation de services CIM.	Hôtes

Privilèges de configuration d'hôte

Les privilèges de configuration d'hôte contrôlent la capacité à configurer des hôtes.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-14. Privilèges de configuration d'hôte

Nom de privilège	Description	Requis sur
Hôte.Configuration.Paramètres avancés	Permet de définir des options avancées de configuration d'hôte.	Hôtes
Hôte.Configuration.Banque d'authentification	Permet de configurer les banques d'authentification d'Active Directory.	Hôtes
Hôte.Configuration.Modifier les paramètres PciPassthru	Permet de modifier les paramètres PciPassthru pour un hôte.	Hôtes
Hôte.Configuration.Modifier les paramètres SNMP	Permet de modifier les paramètres SNMP d'un hôte.	Hôtes
Hôte.Configuration.Modifier les paramètres de date et d'heure	Permet de modifier les paramètres de date et d'heure sur l'hôte.	Hôtes
Hôte.Configuration.Modifier les paramètres	Permet de paramétrer le mode verrouillage sur des hôtes ESXi.	Hôtes
Hôte.Configuration.Connexion	Permet de modifier l'état de la connexion d'un hôte (connecté ou déconnecté).	Hôtes
Hôte.Configuration.Micrologiciel	Permet de mettre à jour le microprogramme des hôtes ESXi.	Hôtes
Hôte.Configuration.Hyperthreading	Permet de mettre sous et hors tension la technologie Hyperthread dans un planificateur CPU d'hôte.	Hôtes
Hôte.Configuration.Configuration d'image	Permet de modifier l'image associée à un hôte.	
Hôte.Configuration.Maintenance	Permet de mettre l'hôte en mode maintenance et hors de ce mode, ainsi que d'arrêter et de redémarrer l'hôte.	Hôtes
Hôte.Configuration.Configuration de la mémoire	Permet de modifier la configuration de l'hôte.	Hôtes
Hôte.Configuration.Configuration du réseau	Permet de configurer le réseau, le pare-feu et le réseau de vMotion.	Hôtes
Hôte.Configuration.Alimentation	Permet de configurer les paramètres de gestion de l'alimentation de l'hôte.	Hôtes
Hôte.Configuration.Interroger un correctif	Permet de demander les correctifs installables et de les installer sur l'hôte.	Hôtes
Hôte.Configuration.Profil de sécurité et pare-feu	Permet de configurer les services Internet, tels que le protocole SSH, Telnet, SNMP et le pare-feu de l'hôte.	Hôtes
Hôte.Configuration.Configuration de la partition de stockage	Permet de gérer des partitions de la banque de données et de diagnostic de VMFS. Les utilisateurs disposant de ce privilège peuvent rechercher de nouveaux périphériques de stockage et gérer l'iSCSI.	Hôtes

Tableau 11-14. Privilèges de configuration d'hôte (suite)

Nom de privilège	Description	Requis sur
Hôte.Configuration.Gestion du système	Permet à des extensions de manier le système de fichiers sur l'hôte.	Hôtes
Hôte.Configuration.Ressources système	Permet de mettre à jour la configuration de la hiérarchie des ressources système.	Hôtes
Hôte.Configuration.Configuration du démarrage automatique de machine virtuelle	Permet de modifier la commande de démarrage et d'arrêt automatique des machines virtuelles sur un hôte unique.	Hôtes

Inventaire d'hôte

Les privilèges d'inventaire d'hôte contrôlent l'ajout des hôtes à l'inventaire, l'ajout des hôtes aux clusters et le déplacement des hôtes dans l'inventaire.

Le tableau décrit les privilèges requis pour ajouter et déplacer des hôtes et des clusters dans l'inventaire.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-15. Privilèges d'inventaire d'hôte

Nom de privilège	Description	Requis sur
Hôte.Inventaire.Ajouter un hôte au cluster	Permet d'ajouter un hôte à un cluster existant.	Clusters
Hôte.Inventaire .Ajouter un hôte autonome	Permet d'ajouter un hôte autonome.	Dossiers d'hôte
Hôte.Inventaire.Créer un cluster	Permet de créer un cluster.	Dossiers d'hôte
Hôte.Inventaire.Modifier un cluster	Permet de changer les propriétés d'un cluster.	Clusters
Hôte.Inventaire.Déplacer un cluster ou un hôte autonome	Permet de déplacer un cluster ou un hôte autonome d'un dossier à l'autre. Le privilège doit être présent à la fois à la source et à la destination.	Clusters
Hôte.Inventaire.Déplacer un hôte	Permet de déplacer un ensemble d'hôtes existants au sein d'un cluster ou en dehors. Le privilège doit être présent à la fois à la source et à la destination.	Clusters
Hôte.Inventaire.Supprimer un cluster	Permet de supprimer un cluster ou un hôte autonome. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Clusters, hôtes

Tableau 11-15. Privilèges d'inventaire d'hôte (suite)

Nom de privilège	Description	Requis sur
Hôte.Inventaire.Supprimer un hôte	Permet de supprimer un hôte. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Objet d'hôtes plus objet parent
Hôte.Inventaire.Renommer un cluster	Permet de renommer un cluster.	Clusters

Privilèges d'opérations locales d'hôte

Les privilèges d'opérations locales d'hôtes contrôlent les actions effectuées lorsque vSphere Client est connecté directement à un hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-16. Privilèges d'opérations locales d'hôte

Nom de privilège	Description	Requis sur
Hôte.Opérations locales.Ajouter un hôte à vCenter	Permet d'installer et de supprimer des agents vCenter, tels que vpxa et aam, sur un hôte.	Hôte racine
Hôte.Opérations locales.Créer une machine virtuelle	Permet de créer une machine virtuelle entièrement nouvelle sur un disque sans l'enregistrer sur l'hôte.	Hôte racine
Hôte.Opérations locales.Supprimer une machine virtuelle	Permet de supprimer une machine virtuelle sur le disque. Cette opération est autorisée pour les machines virtuelles enregistrées comme pour celles dont l'enregistrement a été annulé.	Hôte racine
Hôte.Opérations locales.Extraire du contenu NVRAM	Permet d'extraire le contenu NVRAM d'un hôte.	
Hôte.Opérations locales.Gérer des groupes d'utilisateurs	Permet de gérer des comptes locaux sur un hôte.	Hôte racine
Hôte.Opérations locales.Reconfigurer une machine virtuelle	Permet de reconfigurer une machine virtuelle.	Hôte racine
Hôte.Opérations locales.Réorganisation de snapshots	Permet de modifier la disposition des snapshots d'une machine virtuelle.	Hôte racine

Privilèges de réplication d'hôte vSphere

Les privilèges de vSphere Replication d'hôte contrôlent l'utilisation de la réplication de machine virtuelle par VMware vCenter Site Recovery Manager™ pour un hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-17. Privilèges de réplication d'hôte vSphere

Nom de privilège	Description	Requis sur
Hôte.vSphere Replication.Gérer la réplication	Autorise la gestion de la réplication de machine virtuelle sur cet hôte.	Hôtes

Privilèges de profil d'hôte

Les privilèges de profil d'hôte contrôlent les opérations liées à la création et à la modification des profils d'hôte.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-18. Privilèges de profil d'hôte

Nom de privilège	Description	Requis sur
Profil d'hôte.Effacer	Permet d'effacer les informations liées au profil.	Racine vCenter Server
Profil d'hôte.Créer	Permet la création d'un profil d'hôte.	Racine vCenter Server
Profil d'hôte.Supprimer	Permet la suppression d'un profil d'hôte.	Racine vCenter Server
Profil d'hôte.Modifier	Permet la modification d'un profil d'hôte.	Racine vCenter Server
Profil d'hôte.Exportation	Permet l'exportation d'un profil d'hôte	Racine vCenter Server
Profil d'hôte.Afficher	Permet l'affichage d'un profil d'hôte.	Racine vCenter Server

Privilèges du fournisseur Inventory Service

Les privilèges Fournisseur d'Inventory Service sont à usage interne uniquement. Ne l'utilisez pas.

Privilèges de balisage Inventory Service

Les privilèges de balisage Inventory Service contrôlent la capacité à créer et supprimer des balises et des catégories de balises, ainsi qu'à attribuer et supprimer des balises sur les objets d'inventaire vSphere.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-19. Privilèges vCenter Inventory Service

Nom du privilège	Description	Requis sur
Inventory Service.Balisage vSphere.Affecter ou désaffecter une balise vSphere	Permet d'attribuer ou non une balise pour un objet dans l'inventaire vCenter Server.	Tout objet
Inventory Service.Balisage vSphere.Créer une balise vSphere	Permet de créer une balise.	Tout objet
Inventory Service.Balisage vSphere.Créer une catégorie de balises vSphere	Permet de créer une catégorie de balise.	Tout objet
Inventory Service.Balisage vSphere.Créer une étendue de balise vSphere	Permet la création d'une étendue de balise.	Tout objet
Inventory Service.Balisage vSphere.Supprimer une balise vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Inventory Service.Balisage vSphere.Supprimer une catégorie de balises vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Inventory Service.Balisage vSphere.Supprimer une étendue de balise vSphere	Permet la suppression d'une étendue de balise.	Tout objet
Inventory Service.Balisage vSphere.Modifier une balise vSphere	Permet de modifier une balise.	Tout objet
Inventory Service.Balisage vSphere.Modifier une catégorie de balises vSphere	Permet la modification d'une catégorie de balise.	Tout objet
Inventory Service.Balisage vSphere.Modifier une étendue de balise vSphere	Permet la modification d'une étendue de balise.	Tout objet

Tableau 11-19. Privilèges vCenter Inventory Service (suite)

Nom du privilège	Description	Requis sur
Inventory Service.Balisage vSphere.Modifier le champ UsedBy d'une catégorie	Permet la modification du champ UsedBy pour une catégorie de balise.	Tout objet
Inventory Service.Balisage vSphere.Modifier le champ UsedBy d'une balise	Permet la modification du champ UsedBy pour une balise.	Tout objet

Privilèges de réseau

Les privilèges de réseau contrôlent les tâches associées à la gestion du réseau.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-20. Privilèges de réseau

Nom de privilège	Description	Requis sur
Réseau.Assigner un réseau	Permet l'attribution d'un réseau à une machine virtuelle.	Réseaux, machines virtuelles
Réseau.Configurer	Permet la configuration d'un réseau.	Réseaux, machines virtuelles
Réseau.Déplacer un réseau	Permet de déplacer un réseau entre des dossiers. Le privilège doit être présent à la fois à la source et à la destination.	Réseaux
Réseau.Supprimer	Permet la suppression d'un réseau. Ce privilège est à éviter. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Réseaux

Privilèges de performances

Les privilèges de performances contrôlent la modification de paramètres statistiques de performances.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-21. Privilèges de performances

Nom de privilège	Description	Requis sur
Performances.Modifier des intervalles	Permet la création, la suppression et la mise à jour d'intervalles de collecte de données de performance.	Racine vCenter Server

Privilèges d'autorisations

Les privilèges d'autorisations contrôlent l'attribution des rôles et des autorisations.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-22. Privilèges d'autorisations

Nom de privilège	Description	Requis sur
Autorisations.Modifier une autorisation	Permet de définir une ou plusieurs règles d'autorisation sur une entité, ou met à jour des règles éventuellement déjà présentes, pour l'utilisateur ou le groupe donné de l'entité. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Tout objet plus objet parent
Autorisations.Modifier un privilège	Permet de modifier le groupe d'un privilège ou sa description. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	
Autorisations.Modifier un rôle	Permet de mettre à jour du nom d'un rôle et des privilèges associés à ce rôle.	Tout objet
Autorisations.Réassigner des autorisations de rôle	Permet la réattribution de toutes les autorisations d'un rôle à un autre rôle.	Tout objet

Privilèges de stockage basé sur le profil

Les privilèges de stockage basé sur le profil contrôlent les opérations liées aux profils de stockage.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-23. Privilèges de stockage basé sur le profil

Nom de privilège	Description	Requis sur
Stockage basé sur le profil.Mise à jour du stockage basée sur le profil	Permet d'apporter des modifications aux profils de stockage, telles que la création et la mise à jour de capacités de stockage et de profils de stockage de machine virtuelle.	Racine vCenter Server
Stockage basé sur le profil.Vue du stockage basée sur le profil	Permet d'afficher les capacités de stockage et les profils de stockage définis.	Racine vCenter Server

Privilèges de ressources

Les privilèges de ressource contrôlent la création et la gestion des pools de ressources, ainsi que la migration des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-24. Privilèges de ressources

Nom de privilège	Description	Requis sur
Ressource.Appliquer une recommandation	Permet d'accepter une suggestion du serveur pour effectuer une migration vers vMotion.	Clusters
Ressource.Attribuer un vApp au pool de ressources	Permet d'attribuer un vApp à un pool de ressources.	Pools de ressources
Ressource.Attribuer une machine virtuelle au pool de ressources	Permet d'attribuer une machine virtuelle à un pool de ressources.	Pools de ressources
Ressource.Créer un pool de ressources	Permet de créer un pool de ressources.	Pools de ressources, clusters
Ressource.Migrer une machine virtuelle hors tension	Permet de migrer une machine virtuelle hors tension vers un autre pool de ressources ou un autre hôte.	Machines virtuelles
Ressource.Migrer une machine virtuelle sous tension	Permet de migrer une machine virtuelle hors tension vers un autre pool de ressources ou un autre hôte à l'aide de vMotion.	
Ressource.Modifier un pool de ressources	Permet de changer les allocations d'un pool de ressources.	Pools de ressources
Ressource.Déplacer un pool de ressources	Permet de déplacer un pool de ressources. Le privilège doit être présent à la fois à la source et à la destination.	Pools de ressources
Ressource.Interroger vMotion	Permet d'interroger la compatibilité générale de la fonction vMotion d'une machine virtuelle avec un ensemble d'hôtes.	Racine vCenter Server

Tableau 11-24. Privilèges de ressources (suite)

Nom de privilège	Description	Requis sur
Ressource.Supprimer un pool de ressources	Permet de supprimer un pool de ressources. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Pools de ressources
Ressource.Renommer un pool de ressources	Permet de renommer un pool de ressources.	Pools de ressources

Privilèges de tâche planifiée

Les privilèges de tâche planifiée contrôlent la création, l'édition et la suppression de tâches planifiées.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-25. Privilèges de tâche planifiée

Nom de privilège	Description	Requis sur
Tâche planifiée.Créer des tâches	Permet de planifier une tâche. Requis en plus des privilèges pour exécuter l'action programmée au moment de l'établissement de la planification.	Tout objet
Tâche planifiée.Modifier la tâche	Permet de reconfigurer les propriétés de tâche planifiée.	Tout objet
Tâche planifiée.Supprimer la tâche	Permet de supprimer une tâche planifiée de la file d'attente.	Tout objet
Tâche planifiée.Exécuter une tâche	Permet d'exécuter la tâche planifiée immédiatement. La création et l'exécution d'une tâche planifiée exigent également l'autorisation d'exécuter l'action associée.	Tout objet

Privilèges de sessions

Les privilèges de sessions contrôlent la capacité des extensions à ouvrir des sessions sur le système vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-26. Privilèges de session

Nom de privilège	Description	Requis sur
Sessions.Emprunter l'identité de l'utilisateur	Permet d'emprunter l'identité d'un autre utilisateur. Cette capacité est utilisée par des extensions.	Racine vCenter Server
Sessions.Message	Permet de définir le message global de procédure de connexion.	Racine vCenter Server
Sessions.Valider une session	Permet de vérifier la validité de la session.	Racine vCenter Server
Sessions.Afficher et arrêter des sessions	Permet d'afficher les sessions et de forcer un ou plusieurs utilisateurs connectés à fermer leurs sessions.	Racine vCenter Server

Privilèges de vues de stockage

Les privilèges pour les vues de stockage contrôlent les privilèges pour les API du service de surveillance du stockage.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-27. Privilèges de vues de stockage

Nom de privilège	Description	Requis sur
Vues de stockage.Configurer le service	Permet aux utilisateurs privilégiés d'utiliser toutes les API du service de surveillance du stockage. Utilisez Vues de stockage.Affichage pour les privilèges des API en lecture seule du service de surveillance du stockage.	Racine vCenter Server
Vues de stockage.Affichage	Permet aux utilisateurs ayant des privilèges d'utiliser les API en lecture seule du service de surveillance du stockage.	Racine vCenter Server

Privilèges de tâches

Les privilèges de tâches contrôlent la capacité des extensions à créer et mettre à jour des tâches sur vCenter Server.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-28. Privilèges de tâches

Nom de privilège	Description	Requis sur
Tâches.Créer une tâche	Permet à une extension de créer une tâche définie par l'utilisateur. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Racine vCenter Server
Tâches.Mettre à jour une tâche	Permet à une extension de mettre à niveau une tâche définie par l'utilisateur. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Racine vCenter Server

Privilèges Transfer Service

Les privilèges Transfer Service sont internes à VMware. N'utilisez pas ces privilèges.

Privilèges de règle de VRM

Les privilèges de stratégie VRM sont internes à VMware. N'utilisez pas ces privilèges.

Privilèges de configuration de machine virtuelle

Les privilèges de configuration de la machine virtuelle contrôlent la capacité de configuration des options et des périphériques de machine virtuelle.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-29. Privilèges de configuration de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Ajouter un disque existant	Permet l'ajout d'un disque virtuel existant à une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Ajouter un nouveau disque	Permet la création d'un disque virtuel à ajouter à une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Ajouter ou supprimer un périphérique	Permet l'ajout ou la suppression de n'importe quel périphérique non-disque.	Machines virtuelles
Machine virtuelle.Configuration.Advancée	Permet l'ajout ou la modification de paramètres avancés dans le fichier de configuration de la machine virtuelle.	Machines virtuelles

Tableau 11-29. Privilèges de configuration de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Modifier le nombre de CPU	Permet de changer le nombre de CPU virtuelles.	Machines virtuelles
Machine virtuelle.Configuration.Modifier une ressource	Permet la modification de la configuration des ressources d'un ensemble de nœuds de machine virtuelle dans un pool de ressources donné.	Machines virtuelles
Machine virtuelle.Configuration.Configurer managedBy	Permet à une extension ou à une solution de marquer une machine virtuelle comme étant gérée par cette extension ou solution.	Machines virtuelles
Machine virtuelle.Configuration.Suivi des changements de disques	Permet l'activation ou la désactivation du suivi des modifications des disques de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Bail de disque	Permet des opérations de bail de disque pour une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Ajouter les paramètres de connexion	Permet de configurer les options de la console distante d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Développer un disque virtuel	Permet d'étendre la taille d'un disque virtuel.	Machines virtuelles
Machine virtuelle.Configuration.Périphérique USB hôte	Permet d'attacher à une machine virtuelle un périphérique USB hébergé sur hôte.	Machines virtuelles
Machine virtuelle.Configuration.Modifier la mémoire	Permet de changer la quantité de mémoire allouée à la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Modifier les paramètres de périphérique	Permet de changer les propriétés d'un périphérique existant.	Machines virtuelles
Machine virtuelle.Configuration.Interroger la compatibilité avec Fault Tolerance	Permet de contrôler si une machine virtuelle est compatible avec Fault Tolerance.	Machines virtuelles
Machine virtuelle.Configuration.Interroger les fichiers sans propriétaire	Permet d'interroger des fichiers sans propriétaire.	Machines virtuelles

Tableau 11-29. Privilèges de configuration de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Périphérique brut	Permet d'ajouter ou de retirer un mappage de disque brut ou un périphérique de relais SCSI. La définition de ce paramètre ne tient compte d'aucun autre privilège pour modifier les périphériques bruts, y compris des états de connexion.	Machines virtuelles
Machine virtuelle.Configuration.Recharger à partir du chemin	Permet de changer un chemin de configuration de machine virtuelle tout en préservant l'identité de la machine virtuelle. Les solutions telles que VMware vCenter Site Recovery Manager utilisent cette opération pour préserver l'identité de la machine virtuelle pendant le basculement et la restauration automatique.	Machines virtuelles
Machine virtuelle.Configuration.Supprimer un disque	Permet la suppression d'un périphérique de disque virtuel.	Machines virtuelles
Machine virtuelle.Configuration.Renommer	Permet de renommer une machine virtuelle ou de modifier les notes associées d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Réinitialiser les informations de l'invité	Permet de modifier les informations du système d'exploitation invité d'une machine virtuelle	Machines virtuelles
Machine virtuelle.Configuration.Définir des annotations	Permet d'ajouter ou de modifier une annotation de machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Paramètres	Permet de modifier les paramètres généraux d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Emplacement du fichier d'échange	Permet de changer la règle de placement du fichier d'échange d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Déverrouiller machine virtuelle	Permet d'autoriser le déchiffrement d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Mettre à niveau la compatibilité de machine virtuelle	Permet la mise à niveau de la version de compatibilité des machines virtuelles.	Machines virtuelles

Privilèges d'opérations d'invité de machine virtuelle

Les privilèges d'opérations d'invité de machine virtuelle contrôlent la capacité à interagir avec les fichiers et les programmes au sein du système d'exploitation invité d'une machine virtuelle avec l'API.

Pour obtenir plus d'informations sur ces opérations, consultez la documentation *Référence API de VMware vSphere*.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-30. Opérations de système invité d'une machine virtuelle

Nom de privilège	Description	Pertinent sur l'objet
Machine virtuelle.Opérations invité.Modifications de l'alias d'opération invité	Autorise les opérations d'invité d'une machine virtuelle impliquant la modification de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Opérations invité.Requête d'alias d'opération invité	Autorise les opérations d'invité d'une machine virtuelle impliquant l'interrogation de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Opérations invité.Modifications d'opération invité	Autorise les opérations de système invité d'une machine virtuelle impliquant des modifications apportées au système d'exploitation invité d'une machine virtuelle, telles que le transfert d'un fichier vers la machine virtuelle. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles
Machine virtuelle.Opérations invité.Exécution d'un programme d'opération invité	Autorise les opérations de système invité d'une machine virtuelle impliquant l'exécution d'un programme dans la machine virtuelle. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles
Machine virtuelle.Opérations invité.Requêtes opération invité	Autorise les opérations de système invité d'une machine virtuelle impliquant l'interrogation du système d'exploitation invité, telles que l'énumération des fichiers du système d'exploitation invité. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	Machines virtuelles

Privilèges d'interaction de machine virtuelle

Les privilèges d'interaction de machine virtuelle contrôlent la capacité à interagir avec une console de machine virtuelle, à configurer des médias, à exécuter des opérations d'alimentation et à installer VMware Tools.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-31. Interaction de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Répondre à une question	Permet de résoudre les problèmes de transitions d'état ou d'erreurs d'exécution de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Opération de sauvegarde sur une machine virtuelle	Permet d'exécuter des opérations de sauvegarde sur des machines virtuelles.	Machines virtuelles
Machine virtuelle.Interaction.Configurer un support CD	Permet de configurer un DVD virtuel ou un lecteur de CD-ROM.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Configurer un support de disquette	Permet de configurer un périphérique de disquette virtuel.	Machines virtuelles
Machine virtuelle.Interaction.Interaction avec une console	Permet d'interagir avec la souris virtuelle, le clavier et l'écran de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Créer une capture d'écran	Permet de créer une capture d'écran de machine virtuelle.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Défragmenter tous les disques	Permet de défragmenter des opérations sur tous les disques sur la machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Connexion de périphérique	Permet de modifier l'état connecté des périphériques virtuels deconectables d'une machine virtuelle.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Désactiver Fault Tolerance	Permet de désactiver la machine virtuelle secon daire pour une machine virtuelle utilisant Fault Tolerance.	Machines virtuelles
Machine virtuelle.Interaction.Glisser-déplacer	Permet le glisser-déplacer de fichiers entre une machine virtuelle et un client distant .	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Activer Fault Tolerance	Permet d'activer la machine virtuelle seconde pour une machine virtuelle utilisant Fault Tolerance.	Machines virtuelles
Machine virtuelle.Interaction.Gestion par VIX API du système d'exploitation invité	Permet de gérer le système d'exploitation de la machine virtuelle via VIX API.	Machines virtuelles
Machine virtuelle.Interaction.Injecter des codes de balayage HID USB	Permet l'injection de codes de balayage HID USB.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Interruption/reprise	Permet l'interruption ou la reprise de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Exécuter des opérations d'effacement ou de réduction	Permet d'effectuer des opérations d'effacement ou de réduction sur la machine virtuelle.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Mettre hors tension	Permet de mettre hors tension une machine virtuelle sous tension. Cette opération met hors tension le système d'exploitation invité.	Machines virtuelles
Machine virtuelle.Interaction.Mettre sous tension	Permet de mettre sous tension une machine virtuelle hors tension et de redémarrer une machine virtuelle interrompue.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Session d'enregistrement sur une machine virtuelle	Permet d'enregistrer une session sur une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Session de lecture sur une machine virtuelle	Permet de réinsérer une session enregistrée sur une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Réinitialiser	Permet de réinitialiser une machine virtuelle et redémarrer le système d'exploitation invité.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
avec une machine virtuelle...Relancer Fault Tolerance	Permet la reprise de Fault Tolerance pour une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Interrompre	Permet d'interrompre une machine virtuelle sous tension. Cette opération met l'invité en mode veille.	Machines virtuelles
Interaction.avec une machine virtuelle.Interrompre Fault Tolerance	Permet la suspension de Fault Tolerance pour une machine virtuelle.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Tester le basculement	Permet de tester le basculement de Fault Tolerance en faisant de la machine virtuelle secondaire la machine virtuelle principale.	Machines virtuelles
Machine virtuelle.Interaction.Tester le redémarrage de la VM secondaire	Permet de terminer une machine virtuelle secondaire pour une machine virtuelle utilisant Fault Tolerance.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Désactiver la Fault Tolerance	Permet de mettre hors tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles

Tableau 11-31. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Activer la Fault Tolerance	Permet de mettre sous tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Installer VMware Tools	Permet de monter et démonter le programme d'installation CD de VMware Tools comme un CD-ROM pour le système d'exploitation invité.	Machines virtuelles

Privilèges d'inventaire de machine virtuelle

Les privilèges d'inventaire de machine virtuelle contrôlent l'ajout, le déplacement et la suppression des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-32. Privilèges d'inventaire de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle .Inventaire .Créer à partir d'un modèle/ d'une machine virtuelle existante	Permet la création d'une machine virtuelle basée sur une machine virtuelle existante ou un modèle existant, par clonage ou déploiement à partir d'un modèle.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire .Créer nouveau	Permet la création d'une machine virtuelle et l'allocation de ressources pour son exécution.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire .Déplacer	Permet le déplacement d'une machine virtuelle dans la hiérarchie. Le privilège doit être présent à la fois à la source et à la destination.	Machines virtuelles
Machine virtuelle .Inventaire .Registre	Permet d'ajouter une machine virtuelle existante à vCenter Server ou à un inventaire d'hôtes.	Clusters, hôtes, dossiers de machine virtuelle
Machine virtuelle .Inventaire .Supprimer	Permet la suppression d'une machine virtuelle. L'opération supprime du disque les fichiers sous-jacents de la machine virtuelle. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Machines virtuelles
Machine virtuelle .Inventaire .Annuler l'enregistrement	Permet l'annulation de l'enregistrement d'une machine virtuelle d'une instance de vCenter Server ou d'un inventaire d'hôte. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Machines virtuelles

Privilèges de provisionnement de machine virtuelle

Les privilèges de provisionnement de machine virtuelle contrôlent les activités associées au déploiement et à la personnalisation des machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-33. Privilèges de provisionnement de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Provisionnement.Autoriser l'accès au disque	Permet d'ouvrir un disque sur une machine virtuelle pour l'accès aléatoire en lecture et en écriture. Utilisé en majeure partie pour le montage distant de disque.	Machines virtuelles
Machine virtuelle.Provisionnement.Autoriser l'accès au disque en lecture seule	Permet d'ouvrir un disque sur une machine virtuelle pour l'accès aléatoire en lecture. Utilisé en majeure partie pour le montage distant de disque.	Machines virtuelles
Machine virtuelle.Provisionnement.Autoriser le téléchargement de machines virtuelles	Permet de lire des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	Hôte racine ou vCenter Server
Machine virtuelle.Provisionnement.Autoriser le chargement de fichiers de machines virtuelles	Permet d'écrire sur des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	Hôte racine ou vCenter Server
Machine virtuelle.Provisionnement.Cloner un modèle	Permet de cloner un modèle.	Modèles
Machine virtuelle.Provisionnement.Cloner une machine virtuelle	Permet de cloner une machine virtuelle existante et d'allouer des ressources.	Machines virtuelles
Machine virtuelle.Provisionnement.Créer un modèle à partir d'une machine virtuelle	Permet de créer un nouveau modèle à partir d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Provisionnement.Personnaliser	Permet de personnaliser le système d'exploitation invité d'une machine virtuelle sans déplacer cette dernière.	Machines virtuelles
Machine virtuelle.Provisionnement.Déploier un modèle	Permet de déployer une machine virtuelle à partir d'un modèle.	Modèles
Machine virtuelle.Provisionnement.Marquer comme modèle	Permet de marquer une machine virtuelle existante hors tension comme modèle.	Machines virtuelles
Machine virtuelle.Provisionnement.Marquer comme machine virtuelle	Permet de marquer un modèle existant comme machine virtuelle.	Modèles
Machine virtuelle.Provisionnement.Modifier la spécification de personnalisation	Permet de créer, modifier ou supprimer des spécifications de personnalisation.	Racine vCenter Server

Tableau 11-33. Privilèges de provisionnement de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Provisionnement.Promouvoir des disques	Permet de promouvoir des opérations sur les disques d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Provisionnement.Lire les spécifications de personnalisation	Permet de lire une spécification de personnalisation.	Machines virtuelles

Privilèges de configuration de services de machine virtuelle

Les privilèges de configuration de services de machine virtuelle contrôlent qui peut exécuter une tâche de surveillance de gestion sur la configuration des services.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Note Dans vSphere 6.0, n'attribuez pas et ne supprimez pas ce privilège à l'aide de vSphere Web Client.

Tableau 11-34. Privilèges de configuration de services de machine virtuelle

Nom de privilège	Description
Machine virtuelle.Configuration des services. Autoriser les notifications	Permet la génération et la consommation de notifications sur l'état des services.
Machine virtuelle.Configuration des services. Autoriser l'interrogation de notifications d'événements globales	Permet de déterminer la présence éventuelle de notifications.
Machine virtuelle.Configuration de service. Gérer les configurations de service	Permet la création, la modification et la suppression de services de machine virtuelle.
Machine virtuelle.Configuration de service.Modifier une configuration de service	Permet la modification d'une configuration de services d'une machine virtuelle existante.
Machine virtuelle.Configuration de service. Interroger les configurations de service	Permet la récupération d'une liste de services de machine virtuelle.
Machine virtuelle.Configuration de service. Lire une configuration de service	Permet la récupération d'une configuration de services d'une machine virtuelle existante.

Privilèges de gestion des snapshots d'une machine virtuelle

Les privilèges de gestion des snapshots d'une machine virtuelle contrôlent la capacité à prendre, supprimer, renommer et restaurer des snapshots.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-35. Privilèges d'état de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Gestion des snapshots.Créer un snapshot	Permet de créer un nouveau snapshot de l'état actuel de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Gestion des snapshots.Supprimer un snapshot	Permet de supprimer un snapshot de l'historique de snapshots.	Machines virtuelles
Machine virtuelle.Gestion des snapshots.Renommer un snapshot	Permet de renommer un snapshot avec un nouveau nom, une nouvelle description, ou les deux.	Machines virtuelles
Machine virtuelle.Gestion des snapshots.Rétablir le snapshot	Permet de paramétrer la machine virtuelle à l'état où elle était à un snapshot donné.	Machines virtuelles

Privilèges vSphere Replication de machine virtuelle

Les privilèges vSphere Replication de machine virtuelle contrôlent l'utilisation de la réplication par VMware vCenter Site Recovery Manager™ pour les machines virtuelles.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-36. Réplication de machine virtuelle vSphere

Nom de privilège	Description	Requis sur
Machine virtuelle.vSphere Replication.Configurer la réplication	Permet de configurer la réplication de la machine virtuelle.	Machines virtuelles
Machine virtuelle.vSphere Replication.Gérer la réplication	Permet de déclencher la synchronisation complète, la synchronisation en ligne ou la synchronisation hors ligne d'une réplication.	Machines virtuelles
Machine virtuelle.vSphere Replication.Surveiller la réplication	Permet de contrôler la réplication.	Machines virtuelles

Privilèges du groupe dvPort

Les privilèges de groupes de ports virtuels distribués contrôlent la capacité à créer, supprimer et modifier les groupes de ports virtuels distribués.

Le tableau décrit les privilèges requis pour créer et configurer des groupes de ports virtuels distribués.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-37. Privilèges de groupes de ports virtuels distribués

Nom de privilège	Description	Requis sur
Groupe dvPort.Créer	Permet de créer un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Supprimer	Permet de supprimer un groupe de ports virtuels distribués. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	Groupes de ports virtuels
Groupe dvPort.Modifier	Permet de modifier la configuration d'un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Opération de stratégie	Permet de définir la règle d'un groupe de ports virtuels distribués.	Groupes de ports virtuels
Groupe dvPort.Opération d'étendue	Permet de définir la portée d'un groupe de ports virtuels distribués.	Groupes de ports virtuels

Privilèges de vApp

Les privilèges vApp contrôlent des opérations associées au déploiement et à la configuration d'un vApp.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-38. Privilèges de vApp

Nom de privilège	Description	Requis sur
vApp.Ajouter une machine virtuelle	Permet d'ajouter une machine virtuelle à un vApp.	vApp
vApp.Assigner un pool de ressources	Permet d'attribuer un pool de ressources à un vApp.	vApp
vApp.Assigner un vApp	Permet d'attribuer un vApp à un autre vApp.	vApp
vApp.Cloner	Permet de cloner un vApp.	vApp
vApp.Créer	Permet de créer un vApp.	vApp
vApp.Supprimer	Permet de supprimer un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApp
vApp.Exportation	Permet d'exporter un vApp à partir de vSphere.	vApp
vApp.Importation	Permet d'importer un vApp dans vSphere.	vApp
vApp.Déplacer	Permet de déplacer un vApp vers un nouvel emplacement d'inventaire.	vApp
vApp.Mettre hors tension	Permet de désactiver des opérations sur un vApp.	vApp
vApp.Mettre sous tension	Permet d'activer des opérations sur un vApp.	vApp
vApp.Renommer	Permet de renommer un vApp.	vApp
vApp.Interrompre	Permet d'interrompre un vApp.	vApp
vApp.Annuler l'enregistrement	Permet d'annuler l'enregistrement d'un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApp
vApp.Afficher l'environnement OVF	Permet de consulter l'environnement OVF d'une machine virtuelle sous tension au sein d'un vApp.	vApp

Tableau 11-38. Privilèges de vApp (suite)

Nom de privilège	Description	Requis sur
vApp.Configuration d'application vApp	Permet de modifier la structure interne d'un vApp, telle que l'information produit et les propriétés.	vApp
vApp.Configuration d'instance vApp	Permet de modifier la configuration d'une instance de vApp, telle que les stratégies.	vApp
vApp.Configuration de vApp managedBy	Permet à une extension ou à une solution de marquer un vApp comme étant géré par cette extension ou solution. Aucun élément d'interface utilisateur de vSphere Web Client n'est associé à ce privilège.	vApp
vApp.Configuration des ressources vApp	Permet de modifier la configuration des ressources d'un vApp. Pour pouvoir exécuter cette opération, un utilisateur ou un groupe d'utilisateurs doit disposer de ce privilège attribué à la fois à l'objet et à son objet parent.	vApp

Privilèges vServices

Les privilèges vServices contrôlent la capacité à créer, configurer et mettre à niveau les dépendances vService des machines virtuelles et des vApp.

Vous pouvez définir ce privilège à différents niveaux dans la hiérarchie. Par exemple, si vous définissez un privilège au niveau du dossier, vous pouvez propager le privilège à un ou plusieurs objets dans le dossier. Le privilège doit être défini pour l'objet répertorié dans la colonne Requis, soit directement soit de manière héritée.

Tableau 11-39. vServices

Nom de privilège	Description	Requis sur
vService.Créer une dépendance	Permet de créer une dépendance vService pour une machine virtuelle ou un vApp.	vApp et machines virtuelles
vService.Détruire la dépendance	Permet de supprimer une dépendance vService d'une machine virtuelle ou d'un vApp.	vApp et machines virtuelles
vService.Reconfigurer la configuration de dépendance	Permet la reconfiguration d'une dépendance pour mettre à jour le fournisseur ou la liaison.	vApp et machines virtuelles
vService.mettre à niveau la dépendance	Permet des mises à jour d'une dépendance pour configurer le nom ou la description.	vApp et machines virtuelles