Sécurité vSphere

Update 2
Modifié le 13 mai 2021
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

vmware®

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

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

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

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

Table des matières

À propos de la sécurité de vSphere 14

Informations mises à jour 17

1 Sécurité dans l'environnement vSphere 18

- Sécurisation de l'hyperviseur ESXi 18
- Sécurisation des systèmes vCenter Server et services associés 21
- Sécurisation des machines virtuelles 22
- Sécurisation de la couche de mise en réseau virtuelle 23
- Mots de passe dans votre environnement vSphere 25
- Meilleures pratiques en matière de sécurité et ressources de sécurité 27

2 Tâches de gestion des utilisateurs et des autorisations de vSphere 29

- Présentation des autorisations dans vSphere 30
  - Héritage hiérarchique des autorisations 34
  - Paramètres d'autorisation multiples 37
    - Exemple 1 : Héritage d'autorisations de plusieurs groupes 37
    - Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent 38
    - Exemple 3 : Rôle d'utilisateur supprimant un rôle de groupe 39
- Gestion des autorisations des composants vCenter 39
  - Ajouter une autorisation à un objet d'inventaire 40
  - Modifier ou supprimer des autorisations 41
  - Changer les paramètres de validation d'utilisateur 41
- Autorisations globales 42
  - Ajouter une autorisation globale 43
  - Autorisations sur les objets de balise 44
- Utilisation des rôles pour assigner des privilèges 46
  - Créer un rôle personnalisé 48
  - Rôles système de vCenter Server 48
- Meilleures pratiques pour les rôles et les autorisations 50
- Privilèges requis pour les tâches courantes 50

3 Sécurisation des hôtes ESXi 55

- Recommandations générales de sécurité pour ESXi 56
  - Configurer des hôtes ESXi avec des profils d'hôte 58
  - Utiliser des scripts pour gérer des paramètres de configuration d'hôte 58
  - Verrouillage des mots de passe et des comptes ESXi 60
  - Sécurité SSH 62

Clés SSH ESXi 63
Périphériques PCI et PCIe et ESXi 65
Désactiver Managed Object Browser 65
Recommandations de sécurité pour la mise en réseau d'ESXi 66
Modifier les paramètres proxy Web ESXi 67
Considérations relatives à la sécurité dans vSphere Auto Deploy 67
Contrôler l'accès aux outils de surveillance du matériel basée sur CIM 68
Gestion de certificats pour les hôtes ESXi 70
Mises à niveau d'hôtes et certificats 72
Workflows de changement mode de certificat 73
Paramètres par défaut des certificats ESXi 76
Modifier les paramètres par défaut de certificat 77
Afficher les informations d'expiration de certificat pour plusieurs hôtes ESXi 78
Afficher les détails de certificat pour un hôte ESXi spécifique 78
Renouveler ou actualiser des certificats ESXi 79
Changer le mode de certificat 80
Remplacement de certificats et de clés SSL pour ESXi 81
Configuration requise pour les demandes de signature de certificat ESXi 82
Remplacer le certificat et la clé par défaut dans ESXi Shell 82
Remplacer un certificat et une clé par défaut à l'aide de la commande vifs 83
Remplacer un certificat par défaut à l'aide de HTTPS PUT 84
Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés) 85
Utiliser des certificats personnalisés avec Auto Deploy 86
Restaurer les fichiers de certificat et de clé ESXi 87
Personnalisation des hôtes avec le profil de sécurité 88
Configuration du pare-feu ESXi 89
Gérer les paramètres du pare-feu ESXi 89
Ajouter des adresses IP autorisées pour un hôte ESXi 90
Ports de pare-feu entrants et sortants pour les hôtes ESXi 91
Comportement du pare-feu client NFS 91
Commandes de pare-feu ESXCLI d'ESXi 92
Personnalisation des services ESXi à partir du profil de sécurité 93
Activer ou désactiver un service 95
Mode verrouillage 96
Comportement du mode de verrouillage 96
Activer le mode verrouillage 98
Désactiver le mode de verrouillage 98
Activer ou désactiver le mode de verrouillage normal à partir de l'interface utilisateur de la console directe 99
Spécification des comptes disposant de privilèges d'accès en mode de verrouillage 100
Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB 102

Attribution de privilèges pour les hôtes ESXi 104
Utilisation d'Active Directory pour gérer des utilisateurs ESXi 107
Configurer un hôte pour utiliser Active Directory 107
Ajouter un hôte à un domaine de service d'annuaire 109
Afficher les paramètres du service d'annuaire 110
Utiliser vSphere Authentication Proxy 110
Activer vSphere Authentication Proxy 111
Ajouter un domaine à vSphere Authentication Proxy avec vSphere Client 112
Ajouter un domaine à vSphere Authentication Proxy avec la commande camconfig 113
Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine 114
Activer l'authentification du client pour vSphere Authentication Proxy 114
Importer le certificat vSphere Authentication Proxy sur l'hôte ESXi 115
Générer un nouveau certificat pour vSphere Authentication Proxy 116
Configurer vSphere Authentication Proxy pour utiliser des certificats personnalisés 117
Configuration de l'authentification par carte à puce pour ESXi 119
Activer l'authentification par carte à puce 120
Désactiver l'authentification par carte à puce 121
S'authentifier avec le nom d'utilisateur et le mot de passe en cas de problèmes de connectivité 121
Utilisation de l'authentification par carte à puce en mode de verrouillage 121
Utilisation du ESXi Shell 122
Activer l'accès à ESXi Shell 123
Créer un délai d'attente de disponibilité pour ESXi Shell 123
Créer un délai d'expiration pour des sessions ESXi Shell inactives 124
Utiliser l'interface utilisateur de la console directe pour activer l'accès au service ESXi Shell 125
Définir le délai d'expiration de disponibilité ou le délai d'inactivité de ESXi Shell 125
Connexion au service ESXi Shell pour une opération de dépannage 126
Démarrage sécurisé UEFI des hôtes ESXi 127
Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau 128
Sécurisation des hôtes ESXi avec un module de plate-forme sécurisée 130
Afficher l'état de l'attestation de l'hôte ESXi 131
Résoudre les problèmes d'attestation de l'hôte ESXi 132
Fichiers journaux ESXi 132
Configurer Syslog sur des hôtes ESXi 133
Emplacements des fichiers journaux ESXi 134
Trafic de la journalisation de la tolérance aux pannes 135
Sécurisation de la configuration ESXi 136
Présentation de la sécurisation de la configuration ESXi 136
Présentation des stratégies de scellement TPM 138
Gestion d'une configuration ESXi sécurisée 139
Répertorier le contenu de la clé de récupération de la configuration ESXi sécurisée 139

Effectuer une rotation de la clé de récupération de la configuration ESXi sécurisée 140
Dépannage et récupération de la configuration ESXi sécurisée 141
Récupérer la configuration ESXi sécurisée 141
Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée 142
Activer ou désactiver l'application d'execInstalledOnly pour une configuration ESXi sécurisée 145

4 Sécurisation des systèmes vCenter Server 149
Meilleures pratiques de sécurité de vCenter Server 149
Meilleures pratiques pour le contrôle d'accès à vCenter Server 149
Configurer la stratégie de mot de passe de vCenter Server 151
Suppression de certificats expirés ou révoqués et de journaux d'installations ayant échoué 152
Limitation de la connectivité réseau vCenter Server 152
Évaluer l'utilisation de clients Linux avec des interfaces de lignes de commande et des SDK 153
Examiner les plug-ins des clients 153
Meilleures pratiques de sécurité de vCenter Server 154
Exigences de mots de passe et comportement de verrouillage de vCenter 154
Vérifier les empreintes des hôtes ESXi hérités 156
Ports requis pour vCenter Server 156

5 Sécurisation des machines virtuelles 158
Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle 158
Limiter les messages d'information entre les machines virtuelles et les fichiers VMX 160
Empêcher la réduction de disque virtuel 161
Recommandations en matière de sécurité des machines virtuelles 162
Protection générale d'une machine virtuelle 162
Utiliser des modèles pour déployer des machines virtuelles 163
Minimiser l'utilisation de la console de machine virtuelle 164
Empêcher les machines virtuelles de récupérer les ressources 164
Désactiver les fonctions inutiles à l'intérieur des machines virtuelles 165
Supprimer les périphériques matériels inutiles 166
Désactiver les fonctionnalités d'affichage inutilisées 167
Désactiver les fonctions non exposées 167
Désactiver la fonctionnalité de dossiers partagés VMware pour le partage des fichiers de l'hôte sur la machine virtuelle 168
Désactiver les opérations Copier et Coller entre le système d'exploitation client et la console distante 169
Limitation de l'exposition des données sensibles copiées dans le presse-papiers 169
Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle 170
Interdiction pour les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques 171

Empêcher les processus du système d'exploitation invité d'envoyer des messages de configuration à l'hôte 171
Éviter d'utiliser des disques indépendants non persistants 172
Sécurisation des machines virtuelles avec Intel Software Guard Extensions 173
Présentation de vSGX 173
Activer vSGX sur une machine virtuelle 174
Activer vSGX sur une machine virtuelle existante 175
Supprimer vSGX d'une machine virtuelle 176
Sécurisation des machines virtuelles avec SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD 176
Présentation de l'état chiffré sécurisé SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD 177
Ajouter un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD à une machine virtuelle avec vSphere Client 178
Ajouter un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD à une machine virtuelle 179
Activer un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle existante avec vSphere Client 181
Activer SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle existante 182
Désactiver l'état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle avec vSphere Client 183
Désactiver l'état SEV-ES AMD (Secure Encrypted Virtualization-Encrypted State) sur une machine virtuelle 184

6 Chiffrement des machines virtuelles 185
Comparaison des fournisseurs de clés vSphere 186
Méthodologie utilisée par le chiffrement de machine virtuelle vSphere pour protéger votre environnement 188
Composants du chiffrement des machines virtuelles vSphere 193
Flux de chiffrement 195
Chiffrement des disques virtuels 199
Erreurs de chiffrement des machines virtuelles 200
Conditions préalables et privilèges requis pour les tâches de chiffrement 201
vSphere vMotion chiffré 203
Meilleures pratiques de chiffrement, mises en garde et interopérabilité 206
Meilleures pratiques de chiffrement des machines virtuelles 206
Mises en garde concernant le chiffrement des machines virtuelles 210
Interopérabilité du chiffrement des machines virtuelles 211
Présentation de la persistance des clés 213

7 Configuration et gestion d'un fournisseur de clés standard 215
Présentation du fournisseur de clés standard 215
Configurer le fournisseur de clés standard 216
Ajouter un fournisseur de clés standard à l'aide de vSphere Client 216

Établissement d'une connexion approuvée de fournisseur de clés standard en échangeant des certificats 218
Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance avec le fournisseur de clés standard 219
Utiliser l'option de certificat pour établir une connexion de confiance avec le fournisseur de clés standard 220
Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance avec le fournisseur de clés standard 221
Utiliser l'option Nouvelle demande de signature de certificat pour établir une connexion de confiance avec un fournisseur de clés standard 221
Définir le fournisseur de clés par défaut 222
Terminer la configuration de l'approbation pour un fournisseur de clés standard 223
Configurer des fournisseurs de clés distincts pour différents utilisateurs 224

8 Configuration et gestion de vSphere Native Key Provider 225
Présentation de vSphere Native Key Provider 225
Flux de processus vSphere Native Key Provider 228
Configurer un fournisseur vSphere Native Key Provider 229
Sauvegarder un vSphere Native Key Provider 230
Récupération d'un vSphere Native Key Provider 232
Restaurer un vSphere Native Key Provider à l'aide de vSphere Client 232
Configurer une instance de vSphere Native Key Provider 233
Supprimer un vSphere Native Key Provider 234

9 Autorité d'approbation vSphere 235
Concepts et fonctionnalités de Autorité d'approbation vSphere 235
Protection de votre environnement par l'autorité d'approbation vSphere 235
Présentation de l'infrastructure approuvée 240
Flux de processus de l'autorité d'approbation vSphere 243
Topologie de Autorité d'approbation vSphere 246
Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere 247
Meilleures pratiques de Autorité d'approbation vSphere , mises en garde et interopérabilité 251
Cycle de vie de l'autorité d'approbation vSphere 252
Configuration de Autorité d'approbation vSphere 254
Activer l'administrateur de l'autorité d'approbation 257
Activer l'état de l'autorité d'approbation 258
Collecter des informations sur les hôtes ESXi et vCenter Server à approuver 260
Exportation et importation d'un certificat de paire de clés de type EK (Endorsement Key) du TPM 265
Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation 270
Créer le fournisseur de clés sur le cluster d'autorité d'approbation 273
Téléchargement du certificat client pour établir une connexion fiable avec le fournisseur de clés approuvé 279

Téléchargez le certificat et la clé privée pour établir une connexion fiable avec le fournisseur de clés approuvé 281
Création d'une demande de signature de certificat pour établir une connexion fiable avec un fournisseur de clé approuvé 283
Exporter les informations du cluster d'autorité d'approbation 285
Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés 286
Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de vSphere Client 291
Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de la ligne de commande 292
Gestion de Autorité d'approbation vSphere dans votre environnement vSphere 293
Démarrer, arrêter et redémarrer les services Autorité d'approbation vSphere 294
Afficher les hôtes de l'autorité d'approbation 294
Afficher l'état du cluster Autorité d'approbation vSphere 294
Redémarrer le service d'hôte approuvé 295
Ajout et suppression d'hôtes Autorité d'approbation vSphere 295
Ajouter un hôte à un cluster approuvé avec vSphere Client 295
Ajouter un hôte à un cluster approuvé avec l'interface de ligne de commande 296
Désaffectation d'hôtes approuvés d'un cluster approuvé 298
Sauvegarde de la configuration de Autorité d'approbation vSphere 299
Modifier la clé principale d'un fournisseur de clés 300
Présentation des rapports d'attestation de l'hôte approuvé 301
Afficher l'état d'attestation du cluster approuvé 302
Résoudre les problèmes d'attestation d'hôte approuvé 303
Vérification et correction de la santé d'un cluster approuvé 304
Présentation de la santé et de la correction du cluster approuvé 304
Vérifier la santé du cluster approuvé 305
Corriger un cluster approuvé 306

10 Utiliser le chiffrement dans votre environnement vSphere 308
Créer une stratégie de stockage de chiffrement 308
Activer explicitement le mode de chiffrement de l'hôte 309
Désactiver le mode de chiffrement de l'hôte 310
Créer une machine virtuelle chiffrée 310
Cloner une machine virtuelle chiffrée 312
Chiffrer une machine virtuelle ou un disque virtuel existant 313
Déchiffrer une machine ou un disque virtuel 315
Modifier la stratégie de chiffrement des disques virtuels 316
Résoudre les problèmes de clés manquantes 317
Déverrouiller les machines virtuelles verrouillées 319
Résoudre les problèmes du mode de chiffrement de l'hôte ESXi 320
Réactiver le mode de chiffrement de l'hôte ESXi 321
Définir le seuil d'expiration du certificat du serveur KMS 321

Chiffrement de machines virtuelles vSphere et vidages mémoire 322
Collecter un module vm-support pour un hôte ESXi qui utilise le chiffrement 323
Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré 325
Activer ou désactiver la persistance de clé sur un hôte ESXi 326

11 Sécurisation des machines virtuelles avec le TPM 328
Présentation du vTPM (Virtual Trusted Platform Module) 328
Créer une machine virtuelle avec un vTPM (Virtual Trusted Platform Module) 330
Activer le module de plate-forme sécurisée virtuel pour une machine virtuelle existante 331
Supprimer le module de plate-forme sécurisée virtuel d'une machine virtuelle 332
Identifier les machines virtuelles compatibles vTPM (Virtual Trusted Platform Module) 333
Afficher les certificats des périphériques Virtual Trusted Platform Module 334
Exporter et remplacer les certificats des périphériques Virtual Trusted Platform Module 334

12 Sécurisation des systèmes d'exploitation invités Windows avec la sécurité basée sur la virtualisation 336
Recommandations sur la sécurité basée sur la virtualisation 337
Activer la sécurité basée sur la virtualisation sur une machine virtuelle 338
Activer la sécurité basée sur la virtualisation sur une machine virtuelle existante 340
Activer la sécurité basée sur la virtualisation sur le système d'exploitation invité 341
Désactiver la sécurité basée sur la virtualisation 341
Identifier les machines virtuelles sur lesquelles la sécurité basée sur la virtualisation est activée 342

13 Sécurisation de la mise en réseau vSphere 343
Introduction à la sécurité du réseau vSphere 343
Sécurisation du réseau avec des pare-feu 345
Pare-feux pour configurations avec vCenter Server 346
Connexion à vCenter Server via un pare-feu 347
Connexion des hôtes ESXi via des pare-feu 347
Pare-feu pour les configurations sans vCenter Server 347
Connexion à la console de machine virtuelle via un pare-feu 348
Sécuriser le commutateur physique 349
Sécurisation des ports du commutateur standard à l'aide de stratégies de sécurité 350
Sécuriser les commutateurs vSphere standard 350
Modifications d'adresse MAC 351
Transmissions forgées 352
Fonctionnement en mode promiscuité 352
Protection des commutateurs standard et VLAN 353
Sécuriser les vSphere Distributed Switches et les groupes de ports distribués 354
Sécurisation des machines virtuelles avec des VLAN 356
Considérations relatives à la sécurité pour les VLAN 357

Sécuriser les VLAN 358
Création de plusieurs réseaux sur un hôte ESXi 358
Sécurité du protocole Internet 361
Liste des associations de sécurité disponibles 361
Ajouter une association de sécurité IPsec 362
Supprimer une association de sécurité IPsec 363
Répertorier les stratégies de sécurité IPsec disponibles 363
Créer une stratégie de sécurité IPSec 363
Supprimer une stratégie de sécurité IPsec 364
Garantir une configuration SNMP appropriée 365
Meilleures pratiques en matière de sécurité de la mise en réseau vSphere 365
Recommandations générales de sécurité pour la mise en réseau 365
Étiquetage de composants de mise en réseau 367
Documenter et vérifier l'environnement VLAN vSphere 368
Adoption de pratiques d'isolation réseau 369
Utiliser des commutateurs virtuels avec vSphere Network Appliance API, uniquement si nécessaire 370

14 Meilleures pratiques concernant plusieurs composants vSphere 372
Synchronisation des horloges sur le réseau vSphere 372
Synchroniser les horloges ESXi avec un serveur de temps réseau 373
Configuration des paramètres de synchronisation horaire dans vCenter Server 374
Utiliser la synchronisation de l'heure de VMware Tools 374
Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server 375
Synchroniser l'heure dans vCenter Server avec un serveur NTP 376
Meilleures pratiques en matière de sécurité du stockage 376
Sécurisation du stockage iSCSI 377
Sécurisation des périphériques iSCSI 377
Protection d'un SAN iSCSI 378
Masquage et zonage des ressources SAN 379
Utilisation de Kerberos pour NFS 4.1 379
Vérifier que l'envoi des données de performances de l'hôte aux invités est désactivé 380
Configuration de délais d'expiration pour ESXi Shell et vSphere Client 381

15 Gestion de la configuration du protocole TLS avec l'utilitaire de configuration de TLS 383
Ports prenant en charge la désactivation des versions TLS 383
Activation ou désactivation des versions de TLS dans vSphere 384
Effectuer une sauvegarde manuelle facultative 385
Activer ou désactiver les versions TLS sur les systèmes vCenter Server 386
Activer ou désactiver les versions de TLS sur les hôtes ESXi 387
Analyser vCenter Server pour les protocoles TLS activés 388

Restaurer les modifications de l'utilitaire de configuration TLS 389

16 Privilèges définis 390

Privilèges d'alarmes 392
Privilèges Auto Deploy et privilèges de profil d'image 393
Privilèges de certificats 394
Privilèges de bibliothèque de contenu 394
Privilèges d'opérations de chiffrement 397
Privilèges du groupe dvPort 399
Privilèges de Distributed Switch 400
Privilèges de centre de données 400
Privilèges de banque de données 401
Privilèges de cluster de banques de données 402
Privilèges de gestionnaire d'agent ESX 403
Privilèges d'extension 403
Privilèges de fournisseur de statistiques externes 404
Privilèges de dossier 404
Privilèges globaux 404
Privilèges de fournisseur de mises à jour de santé 406
Privilèges CIM d'hôte 406
Privilèges de configuration d'hôte 406
Inventaire d'hôte 408
Privilèges d'opérations locales d'hôte 408
Privilèges de réplication d'hôte vSphere 409
Privilèges de profil d'hôte 409
Privilèges de vSphere with Tanzu 410
Privilèges de réseau 410
Privilèges de performances 411
Privilèges d'autorisations 411
Privilèges de stockage basé sur le profil 412
Privilèges de ressources 412
Privilèges de tâche planifiée 413
Privilèges de sessions 414
Privilèges de vues de stockage 414
Privilèges de tâches 415
Privilèges Transfer Service 415
Privilèges VcTrusts/VcIdentity 415
Privilèges d'administrateur d'infrastructure approuvée 416
Privilèges de vApp 417
Privilèges VcIdentityProviders 419
Privilèges de configuration de VMware vSphere Lifecycle Manager 419

Privilèges de perspectives de santé ESXi de VMware vSphere Lifecycle Manager 420
Privilèges généraux de VMware vSphere Lifecycle Manager 420
Privilèges de compatibilité matérielle de VMware vSphere Lifecycle Manager 421
Privilèges d'images de VMware vSphere Lifecycle Manager 421
Privilèges de correction d'image de VMware vSphere Lifecycle Manager 422
Privilèges de paramètres de VMware vSphere Lifecycle Manager 423
Privilèges de gestion des lignes de base de VMware vSphere Lifecycle Manager 423
Privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager 424
Privilèges Télécharger les fichiers de VMware vSphere Lifecycle Manager 425
Privilèges de configuration de machine virtuelle 425
Privilèges d'opérations d'invité de machine virtuelle 428
Privilèges d'interaction de machine virtuelle 429
Privilèges d'inventaire de machine virtuelle 432
Privilèges de provisionnement de machine virtuelle 433
Privilèges de configuration de services de machine virtuelle 434
Privilèges de gestion des snapshots d'une machine virtuelle 435
Privilèges vSphere Replication de machine virtuelle 436
Privilèges vServices 436
Privilèges de balisage vSphere 437

17 Présentation de la sécurisation renforcée et de la conformité dans vSphere 439
Sécurité ou conformité dans l'environnement vSphere 439
Présentation du guide de configuration de sécurité vSphere 442
À propos de l'Institut national des normes et de la technologie (NIST, National Institute of Standards and Technology) 445
À propos des directives STIG DISA 446
À propos du cycle de développement de sécurité de VMware 446
Journalisation d'audit 447
Événements d'audit Single Sign-On 447
Présentation des prochaines étapes de sécurité de conformité 448
vCenter Server et FIPS 449
Activer et désactiver FIPS sur le vCenter Server Appliance 450
Considérations lors de l'utilisation de FIPS 451

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.

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

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
Gestion des autorisations et des utilisateurs	■ Modèle d'autorisations (rôles, groupes et objets). ■ Création de rôles personnalisés. ■ Définition des autorisations. ■ Gestion des autorisations globales.
Fonctionnalités relatives à la sécurité de l'hôte	■ Mode de verrouillage et autres fonctionnalités de profil de sécurité. ■ Authentification des hôtes par carte à puce. ■ vSphere Authentication Proxy. ■ Démarrage sécurisé UEFI. ■ TPM (Trusted Platform Module). ■ Autorité d'approbation vSphere ™ VMware® ■ Sécurisation de la configuration ESXi et scellement de la configuration
Chiffrement des machines virtuelles	■ VMware vSphere® Native Key Provider™. ■ Comment fonctionne le chiffrement des machines virtuelles ? ■ Configuration de KMS. ■ Chiffrement et déchiffrement des machines virtuelles. ■ Dépannage et meilleures pratiques.
Sécurité du système d'exploitation invité	■ vTPM (Virtual Trusted Platform Module) ■ Sécurité basée sur la virtualisation (VBS).
Gestion de la configuration du protocole TLS	Modification de la configuration du protocole TLS à l'aide d'un utilitaire de ligne de commande.

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

Rubriques	Points forts du contenu
Meilleures pratiques en matière de sécurité et de sécurisation renforcée	Meilleures pratiques et avis des experts en sécurité VMware. ■ 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

Un document complément, *Authentification vSphere*, explique comment utiliser les services d'authentification, par exemple pour gérer l'authentification avec vCenter Single Sign-On et pour gérer les certificats dans l'environnement vSphere.

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

Qu'est-il arrivé à Platform Services Controller ?

À partir de vSphere 7.0, le déploiement d'une nouvelle instance de vCenter Server ou la mise à niveau vers vCenter Server 7.0 nécessite l'utilisation de vCenter Server Appliance, une machine virtuelle préconfigurée optimisée pour l'exécution de vCenter Server. La nouvelle instance de vCenter Server contient tous les services Platform Services Controller, en préservant les fonctionnalités et les workflows, notamment l'authentification, la gestion des certificats, les balises et la gestion des licences. Il n'est plus nécessaire ni possible de déployer et d'utiliser une instance externe de Platform Services Controller. Tous les services Platform Services Controller sont consolidés dans vCenter Server, et le déploiement et l'administration sont simplifiés.

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

Public cible

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

Certifications

VMware publie une liste publique des produits VMware ayant passé les certifications Critères communs. Pour vérifier si la version particulière d'un produit VMware est certifiée, reportez-vous à la page Web Évaluation et validation des critères communs (https://www.vmware.com/security/certifications/common-criteria.html).

Informations mises à jour

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

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

Révision	Description
13 mai 2021	■ Ajout d'informations sur les privilèges dans Rôles système de vCenter Server. ■ Mise à jour mineure dans Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine. ■ Mise à jour des informations de version dans Présentation de vSphere Native Key Provider. ■ Correction des étapes d'ajout de serveurs NTP dans Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server.
14 avril 2021	■ Mise à jour de Verrouillage des mots de passe et des comptes ESXi pour inclure plus d'informations sur les options de mot de passe. ■ Mise à jour de la section Configuration requise pour les demandes de signature de certificat ESXi avec un lien vers un article de la base de connaissances VMware pour plus d'informations sur la génération de demandes de signature de certificat. ■ Correction des commandes `dir-cli` dans Mettre à jour le magasin TRUSTED_ROOTS de vCenter Server (Certificats personnalisés). ■ Mise à jour mineure dans Comportement du mode de verrouillage. ■ Mise à jour de Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB pour corriger la syntaxe de la commande de l'interface de ligne de commande et pour clarifier l'emplacement de la prise en charge des VIB VMwareAccepted et PartnerSupported. ■ Mise à jour mineure dans Présentation de la sécurisation de la configuration ESXi. ■ Mise à jour des sections Présentation des stratégies de scellement TPM et Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée pour inclure plus d'informations sur le mode TPM. ■ Mise à jour mineure dans Meilleures pratiques de sécurité de vCenter Server. ■ Mise à jour mineure dans Supprimer les périphériques matériels inutiles. ■ Ajout de Configurer une instance de vSphere Native Key Provider. ■ Mise à jour des sections Recommandations sur la sécurité basée sur la virtualisation, Activer la sécurité basée sur la virtualisation sur une machine virtuelle et Activer la sécurité basée sur la virtualisation sur une machine virtuelle existante pour les CPU AMD. ■ Mise à jour mineure dans À propos des directives STIG DISA.
09 mars 2021	Version initiale.

Sécurité dans l'environnement vSphere

1

Les composants d'un environnement vSphere sont sécurisés d'origine par plusieurs fonctionnalités telles que l'authentification, l'autorisation, un pare-feu sur chaque hôte ESXi, 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. Vous pouvez prendre des mesures de sécurité sur différents objets dans la hiérarchie d'objets vCenter, comme les systèmes vCenter Server, les hôtes ESXi, les machines virtuelles et les objets du réseau et de stockage.

Une présentation globale des différentes parties de vSphere à surveiller 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 défaut. Vous pouvez renforcer la protection des hôtes ESXi en utilisant le mode de verrouillage et d'autres fonctionnalités intégrées. À des fins d'uniformité, vous pouvez définir un hôte de référence et laisser tous les hôtes en synchronisation avec le profil de l'hôte de référence. Vous pouvez également protéger votre environnement en effectuant une gestion chiffrée, qui garantit que les modifications sont appliquées à tous les hôtes.

Vous pouvez renforcer la protection des hôtes ESXi qui sont gérés par vCenter Server en effectuant les actions suivantes. Consultez le livre blanc *Sécurité de VMware vSphere Hypervisor* pour accéder à des informations de fond et des détails.

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 du système vCenter Server qui gère l'hôte.

Utiliser des utilisateurs nommés et le moindre privilège

Par défaut, l'utilisateur racine peut effectuer de nombreuses tâches. N'autorisez pas les administrateurs à se connecter à l'hôte ESXi en utilisant le compte d'utilisateur racine. Au lieu de cela, créez des utilisateurs Administrateur nommés à partir de vCenter Server et attribuez-leur le rôle d'administrateur. Vous pouvez également attribuer à ces utilisateurs un rôle personnalisé. Reportez-vous à la section Créer un rôle personnalisé.

Si vous gérez les utilisateurs directement sur l'hôte, les options de gestion des rôles sont limitées. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host 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 Client, ESXCLI ou PowerCLI pour vérifier et gérer l'état des ports du pare-feu.

Reportez-vous à la section Configuration du pare-feu ESXi.

Automatiser la gestion des hôtes 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'hôte sont une alternative à la gestion chiffrée. Vous définissez un hôte de référence, exportez le profil d'hôte et appliquez celui-ci à tous les hôtes. 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 vCenter Server* 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. Vous pouvez sélectionner le mode de verrouillage strict ou le mode de

verrouillage normal. Vous pouvez définir des utilisateurs exceptionnels pour autoriser l'accès direct aux comptes de service, tels que les agents de sauvegarde.

Reportez-vous à la section 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 la section Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB.

Gérer les certificats ESXi

VMware Certificate Authority (VMCA) fournit à chaque hôte ESXi un certificat signé dont VMCA est l'autorité de certification racine par défaut. Si la stratégie de votre entreprise l'exige, vous pouvez remplacer les certificats existants par des certificats signés par une autorité de certification d'entreprise ou tierce.

Reportez-vous à la section Gestion de certificats pour les hôtes ESXi.

Envisager l'authentification par carte à puce

ESXi prend en charge l'utilisation de l'authentification par carte à puce plutôt que l'authentification par nom d'utilisateur et mot de passe. Pour une sécurité renforcée, vous pouvez configurer l'authentification par carte à puce. L'authentification à deux facteurs est également prise en charge pour vCenter Server. Vous pouvez configurer l'authentification par nom d'utilisateur et mot de passe, et l'authentification par carte à puce en même temps.

Reportez-vous à la section Configuration de l'authentification par carte à puce pour ESXi.

Envisager le verrouillage des comptes ESXi

Le verrouillage des comptes est pris en charge pour l'accès via SSH et vSphere Web Services SDK. Par défaut, un nombre maximal de 10 tentatives de connexion échouées est autorisé avant le verrouillage du compte. Par défaut, le compte est déverrouillé au bout de deux minutes.

Note L'interface de console directe (DCUI) et ESXi Shell ne prennent pas en charge le verrouillage de compte.

Reportez-vous à la section 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 *Gestion individuelle des hôtes vSphere - VMware Host 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 et prendre des mesures supplémentaires pour limiter 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.

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.

En savoir plus sur le modèle de certificat vCenter

Par défaut, l'autorité de certification VMware provisionne chaque hôte ESXi et chaque machine de l'environnement avec un certificat signé par VMCA (VMware Certificate Authority). Si la stratégie de votre entreprise l'exige, vous pouvez modifier le comportement par défaut. Pour plus d'informations, reportez-vous à la documentation *Authentification 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. Lors de la première installation des logiciels, vous devez spécifier un mot de passe pour l'administrateur du domaine vCenter Single Sign-On (par défaut, administrator@vsphere.local). Seul ce domaine est disponible initialement comme source d'identité. Vous pouvez ajouter un fournisseur d'identité, tel que Microsoft Active Directory Federation Services (AD FS). Vous pouvez ajouter d'autres sources d'identité (Active Directory ou LDAP) et définir une source d'identité par défaut. Les utilisateurs qui peuvent s'authentifier auprès d'une de ces sources d'identité ont la possibilité d'afficher des objets et d'effectuer des tâches, dans la mesure où ils y ont été autorisés. Pour plus d'informations, reportez-vous à la documentation *Authentification vSphere*.

Attribuer des rôles à des utilisateurs ou groupes nommés

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 procure une grande flexibilité en offrant la possibilité

d'autoriser les utilisateurs et les groupes de diverses façons. Reportez-vous aux sections Présentation des autorisations dans vSphere et Privilèges requis pour les tâches courantes.

Limitez les privilèges d'administrateur et l'utilisation du rôle d'administrateur. Dans la mesure du possible, évitez d'utiliser l'utilisateur Administrateur anonyme.

Configurer PTP ou NTP

Configurez PTP ou 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 la section 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 HGFS (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 (par exemple, PowerCLI). 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, voir Utiliser des modèles pour déployer des machines virtuelles et la documentation *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 qu'un 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.

Activer le démarrage sécurisé UEFI

Vous pouvez configurer votre machine virtuelle pour qu'elle utilise le démarrage UEFI. Si le système d'exploitation prend en charge le démarrage UEFI sécurisé, vous pouvez sélectionner cette option pour vos machines virtuelles pour plus de sécurité. Reportez-vous à la section Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle.

Prendre en compte Carbon Black Cloud Workload

Vous pouvez installer et utiliser Carbon Black Cloud Workload pour identifier les risques, éviter les attaques et détecter des activités inhabituelles. Avec la fonctionnalité AppDefense intégrée à la plate-forme Carbon Black Cloud, Carbon Black Cloud Workload est le produit qui succède à AppDefense.

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 de mise en réseau 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 le Chapitre 13 Sécurisation de la mise en réseau vSphere.

Isoler le trafic réseau

L'isolation du trafic réseau est essentielle pour un environnement ESXi sécurisé. 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. Assurez-vous que seuls les administrateurs système, réseau et de la sécurité peuvent accéder au réseau de gestion.

Reportez-vous à la section 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. Pour les hôtes ESXi, les règles de pare-feu associent les services avec les pare-feu correspondants et peuvent ouvrir et fermer le pare-feu en fonction de l'état du service.

Vous pouvez également ouvrir explicitement des ports sur les instances de vCenter Server.

Pour obtenir la liste de tous les ports et protocoles pris en charge dans les produits VMware, y compris vSphere et vSAN, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/. Vous pouvez rechercher des ports selon le produit VMware, créer une liste personnalisée de ports et imprimer ou enregistrer des listes de ports.

Envisager des stratégies de sécurité du réseau

Les stratégies de sécurité du réseau assurent 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 Proximité, 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 de machines virtuelles

Les méthodes qui vous permettent de sécuriser la mise en réseau de machines virtuelles dépendent de plusieurs facteurs, notamment :

- Le système d'exploitation invité qui est installé
- de l'utilisation d'un environnement approuvé pour les machines virtuelles.

Les commutateurs virtuels et les commutateurs virtuels distribués offrent un niveau de protection élevé lorsqu'ils sont utilisés avec d'autres mesures de sécurité courantes (installation de pare-feu, notamment).

Reportez-vous à la section Chapitre 13 Sécurisation de la mise en réseau vSphere.

Envisager les VLAN pour protéger votre environnement

ESXi prend en charge les VLAN IEEE 802.1q. Les VLAN vous permettent de segmenter un réseau physique. Vous pouvez les utiliser pour renforcer la protection de la configuration du stockage ou du réseau de machines virtuelles. Lorsque des VLAN sont utilisés, deux machines sur le même réseau physique ne peuvent pas s'envoyer mutuellement des paquets ni en recevoir, sauf s'ils se trouvent sur le même réseau VLAN.

Reportez-vous à la section 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 d'applications 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.

Le système 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 utiliser le protocole CHAP. Si la stratégie de l'entreprise l'exige, vous pouvez configurer une authentification CHAP mutuelle. Utilisez vSphere Client ou les interfaces de ligne de commande pour configurer CHAP.

Reportez-vous à la section 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 la section Sécurité du protocole Internet.

De plus, déterminez si VMware NSX for 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, l'expiration du mot de passe et le verrouillage du compte dans votre environnement vSphere dépendent de plusieurs facteurs : système visé par l'utilisateur, identité de l'utilisateur et mode de définition des stratégies.

Mots de passe d'ESXi

Les restrictions de mot de passe ESXi sont déterminées par certaines exigences. Reportez-vous à la section 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, l'expiration du mot de passe et le verrouillage du compte dépendent du domaine de l'utilisateur et de l'identité de l'utilisateur.

Administrateur de vCenter Single Sign-On

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 *Authentification vSphere* pour plus de détails.

Si vous oubliez le mot de passe de cet utilisateur, recherchez dans le système de la base de connaissances VMware des informations sur la réinitialisation de ce mot de passe. Pour réinitialiser le mot de passe, des privilèges supplémentaires comme un accès racine sont nécessaires pour accéder au système vCenter Server.

Autres utilisateurs du domaine Single Sign-On vCenter

Les mots de passe des autres utilisateurs vsphere.local ou des utilisateurs du domaine que vous avez spécifiés au cours de l'installation doivent respecter les restrictions qui sont définies par la stratégie de mot de passe et de verrouillage de vCenter Single Sign-On. Consultez *Authentification vSphere* pour plus d'informations. Ces mots de passe expirent après 90 jours par défaut. Les administrateurs peuvent modifier l'expiration dans le cadre de la stratégie de mot de passe.

Si vous oubliez votre 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, l'expiration du mot de passe et le verrouillage du compte 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. Les utilisateurs peuvent se connecter au domaine correspondant de vSphere Client avec leur nom d'utilisateur. Si des utilisateurs veulent se connecter à 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 d'accès au domaine s'appliquent à chaque domaine.

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

L'instance de vCenter Server Appliance est une machine virtuelle préconfigurée et optimisée pour l'exécution de vCenter Server et des services associés.

Lorsque vous déployez le dispositif vCenter Server, vous devez spécifier ces mots de passe.

- Mot de passe de l'utilisateur racine.
- Mot de passe de l'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut.

Vous pouvez modifier le mot de passe de l'utilisateur racine et effectuer d'autres tâches de gestion d'utilisateur local de vCenter Server depuis l'interface de gestion de vCenter Server. Reportez-vous à la section *Configuration de vCenter Server*.

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	Chapitre 3 Sécurisation des hôtes 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 que vous devez utiliser 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
Informations sur la sécurité et les opérations d'ESXi et de vCenter Server, y compris la configuration sécurisée et la sécurité de l'hyperviseur.	https://core.vmware.com/security
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.

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

Rubrique	Ressource
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	https://core.vmware.com/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 configuration de la sécurité (nommés auparavant Guides de sécurisation renforcée) pour différentes versions de vSphere et d'autres produits VMware.	https://core.vmware.com/security
Livre blanc *Sécurité de VMware vSphere Hypervisor*	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

Tâches de gestion des utilisateurs et des autorisations de vSphere

2

L'authentification et l'autorisation gouvernent l'accès. vCenter Single Sign-On prend en charge l'authentification, ce qui signifie qu'il détermine si un utilisateur peut se connecter aux composants vSphere ou pas. Chaque utilisateur doit également être autorisé à afficher ou à manipuler des objets vSphere.

vSphere prend en charge différents mécanismes d'autorisation abordés dans Présentation des autorisations dans vSphere. Cette section est axée sur le fonctionnement du modèle d'autorisation de vCenter Serveret sur la manière d'effectuer 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.

À l'origine, seul l'utilisateur administrateur du domaine vCenter Single Sign-On est autorisé à se connecter au système vCenter Server. Le domaine par défaut est vsphere.local et l'administrateur par défaut administrator@vsphere.local. Vous pouvez modifier le domaine par défaut lors de l'installation vSphere.

L'utilisateur administrateur peut procéder comme suit :

1. Ajouter une source d'identité dans laquelle les utilisateurs et les groupes sont définis sur vCenter Single Sign-On. Consultez la documentation de *Authentification vSphere*.
2. Accordez 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.

Attribution des rôles et des autorisations à l'aide de vSphere Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_roles)

Ce chapitre contient les rubriques suivantes :

- Présentation des autorisations dans vSphere
- 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

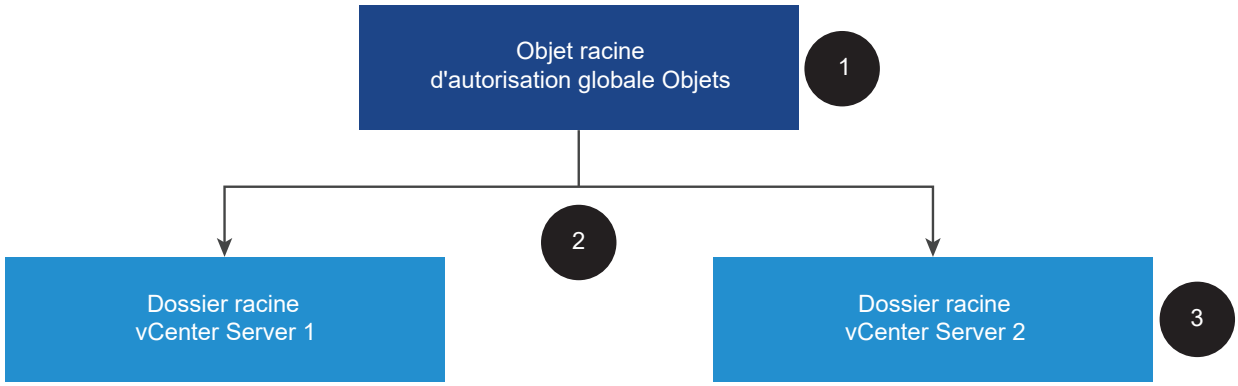
vSphere prend en charge plusieurs modèles pour déterminer si un utilisateur est autorisé à effectuer une tâche. L'appartenance à un groupe vCenter Single Sign-On détermine ce que vous êtes autorisé à faire. Votre rôle sur un objet ou votre autorisation globale détermine si vous êtes autorisé à effectuer d'autres tâches.

Présentation des autorisations

vSphere permet aux utilisateurs privilégiés d'accorder à d'autres utilisateurs des autorisations d'exécution de tâches. Vous pouvez exploiter les autorisations globales ou les autorisations vCenter Server locales pour permettre à d'autres utilisateurs d'utiliser des instances vCenter Server individuelles.

La figure suivante illustre le fonctionnement des autorisations globales et locales.

Figure 2-1. Autorisations globales et autorisations locales



Dans cette figure :

1 Vous attribuez une autorisation globale au niveau de l'objet racine en sélectionnant l'option « Propager vers les enfants ».

2 vCenter Server propage les autorisations aux hiérarchies d'objets vCenter Server 1 et vCenter Server 2 dans l'environnement.

3 Une autorisation locale sur le dossier racine sur vCenter Server 2 remplace l'autorisation globale.

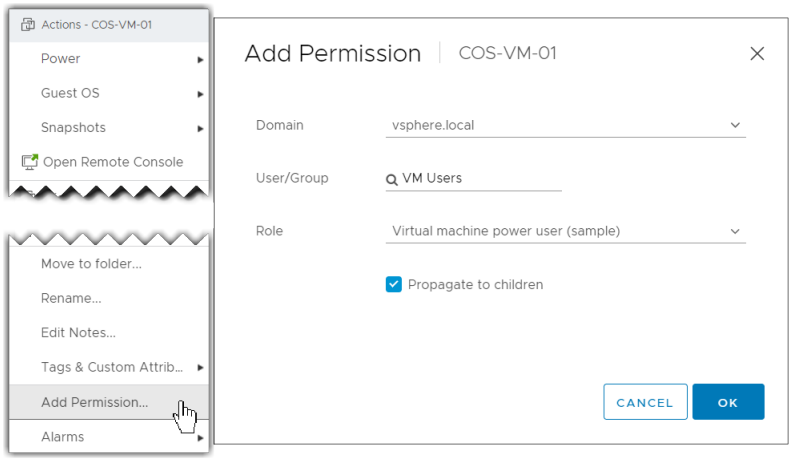
Autorisations vCenter Server

Le modèle d'autorisation des systèmes vCenter Server repose sur l'attribution d'autorisations à des objets dans la hiérarchie d'objets. Les utilisateurs obtiennent des autorisations de l'une des manières suivantes.

- À partir d'une autorisation spécifique pour l'utilisateur ou à partir des groupes dont l'utilisateur est membre.
- À partir d'une autorisation sur l'objet ou via l'héritage d'autorisations depuis un objet parent.

Chaque autorisation accorde à un utilisateur ou à un groupe un ensemble de privilèges, c'est-à-dire un rôle sur l'objet sélectionné. Vous pouvez utiliser vSphere Client pour ajouter des autorisations. Par exemple, vous pouvez cliquer avec le bouton droit sur une machine virtuelle, sélectionner **Ajouter une autorisation** et remplir la boîte de dialogue pour attribuer un rôle à un groupe d'utilisateurs. Ce rôle accorde à ces utilisateurs les privilèges correspondants sur la machine virtuelle.

Figure 2-2. Ajout d'autorisations à une machine virtuelle à l'aide de vSphere Client



Autorisations globales

Les autorisations globales donnent à un utilisateur ou à un groupe des privilèges pour afficher ou gérer tous les objets dans chacune des hiérarchies d'inventaire des solutions du déploiement. Autrement dit, les autorisations globales sont appliquées à un objet racine global qui couvre les hiérarchies d'inventaire de solutions. (Les solutions incluent vCenter Server, vRealize Orchestrator, etc.) Les autorisations globales s'appliquent également aux objets globaux tels que les balises et les bibliothèques de contenu. Par exemple, envisagez un déploiement qui se compose de deux solutions : vCenter Server et vRealize Orchestrator. Vous pouvez utiliser des autorisations globales pour attribuer un rôle à un groupe d'utilisateurs qui dispose de privilèges en lecture seule sur tous les objets dans les hiérarchies d'objets vCenter Server et vRealize Orchestrator.

Les autorisations globales sont répliquées dans le domaine vCenter Single Sign-On (par défaut, vsphere.local). Les autorisations globales ne fournissent pas d'autorisations pour les services gérés via des groupes du domaine vCenter Single Sign-On. Reportez-vous à la section Autorisations globales.

Appartenance à un groupe dans des groupes vCenter Single Sign-On

Les membres d'un groupe du domaine vCenter Single Sign-On peuvent effectuer certaines tâches. Par exemple, vous pouvez effectuer la gestion de licences si vous êtes membre du groupe LicenseService.Administrators. Consultez la documentation de *Authentification vSphere*.

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 *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Pour les hôtes gérés, attribuez des rôles à l'objet hôte ESXi dans l'inventaire vCenter Server.

Présentation du modèle d'autorisation de niveau objet

Vous autorisez un utilisateur ou un groupe d'utilisateurs à effectuer des tâches sur les objets vCenter Server en utilisant des autorisations sur l'objet. D'un point de vue programmatique, lorsqu'un utilisateur tente d'effectuer une opération, une méthode API est exécutée. vCenter Server vérifie les autorisations de cette méthode pour voir si l'utilisateur est autorisé à effectuer l'opération. Par exemple, lorsqu'un utilisateur tente d'ajouter un hôte, la méthode `AddStandaloneHost_Task(addStandaloneHost)` est invoquée. Cette méthode nécessite que le rôle de l'utilisateur dispose du privilège **Hôte.Inventaire.Ajouter un hôte autonome**. Si la vérification ne trouve pas ce privilège, l'autorisation d'ajout de l'hôte est refusée à l'utilisateur.

Les concepts suivants sont importants.

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. Les autorisations peuvent se propager aux objets enfants.

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.

Privilèges

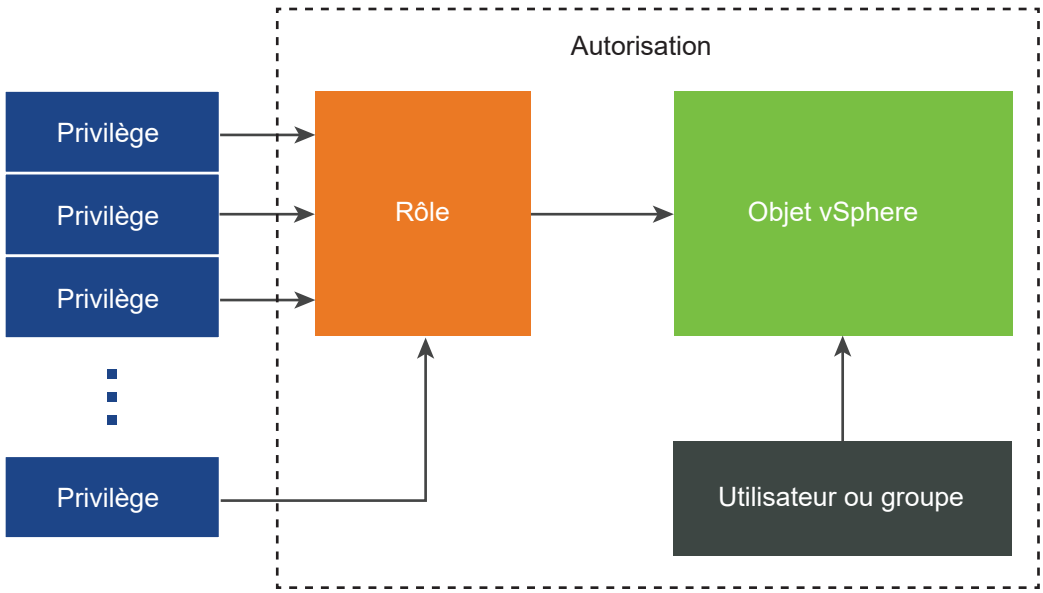
Les privilèges sont des contrôles d'accès précis. Vous pouvez regrouper ces privilèges dans des rôles, que vous pouvez ensuite mapper à des utilisateurs ou à des groupes.

Rôles

Les rôles sont des ensembles de privilèges. 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 système, par exemple Administrateur, sont prédéfinis sur vCenter Server et ne peuvent pas être modifiés. vCenter Server fournit également des exemples de rôles par défaut, tels que l'administrateur de pool de ressources, que vous pouvez modifier. Vous pouvez créer des rôles personnalisés totalement nouveaux, ou cloner et modifier des exemples de rôles. Reportez-vous à la section Créer un rôle personnalisé.

La figure suivante illustre comment une autorisation est construite à partir de privilèges et de rôles, puis attribuée à un utilisateur ou à un groupe pour un objet vSphere.

Figure 2-3. Autorisations de vSphere



Pour attribuer des autorisations à un objet, suivez les étapes suivantes :

1 Sélectionnez l'objet auquel vous souhaitez appliquer l'autorisation dans la hiérarchie d'objets vCenter Server.

2 Sélectionnez le groupe ou l'utilisateur qui doit avoir des privilèges sur l'objet.

3 Sélectionnez des privilèges individuels ou un rôle, c'est-à-dire un ensemble de privilèges, que le groupe ou l'utilisateur doit avoir sur l'objet.

   Par défaut, l'option Propager vers les enfants n'est pas sélectionnée. Vous devez cocher la case pour le groupe ou l'utilisateur afin d'obtenir le rôle sélectionné sur l'objet sélectionné et ses objets enfants.

vCenter Server offre des exemples de rôles qui combinent les ensembles de privilèges fréquemment utilisés. Vous pouvez également créer des rôles personnalisés en combinant un ensemble de rôles.

Les autorisations doivent souvent 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 privilèges sur cette machine virtuelle ainsi que sur le centre de données de destination.

Consultez les informations suivantes.

Pour savoir comment...	Reportez-vous à...
Création de rôles personnalisés.	Créer un rôle personnalisé
Tous les privilèges et objets auxquels vous pouvez appliquer les privilèges	Chapitre 16 Privilèges définis
Ensembles de privilèges requis sur des objets différents pour des tâches différentes.	Privilèges requis pour les tâches courantes

Le modèle d'autorisations des hôtes ESXi autonomes est plus simple. Reportez-vous à la section Attribution de privilèges pour les hôtes 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, supposez qu'un rôle soit attribué à l'utilisateur Smith sur plusieurs objets. L'administrateur de domaine modifie le nom en Smith2. L'hôte conclut que Smith n'existe plus et supprime les autorisations associées à cet utilisateur à partir des objets vSphere lors de la prochaine validation.

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.

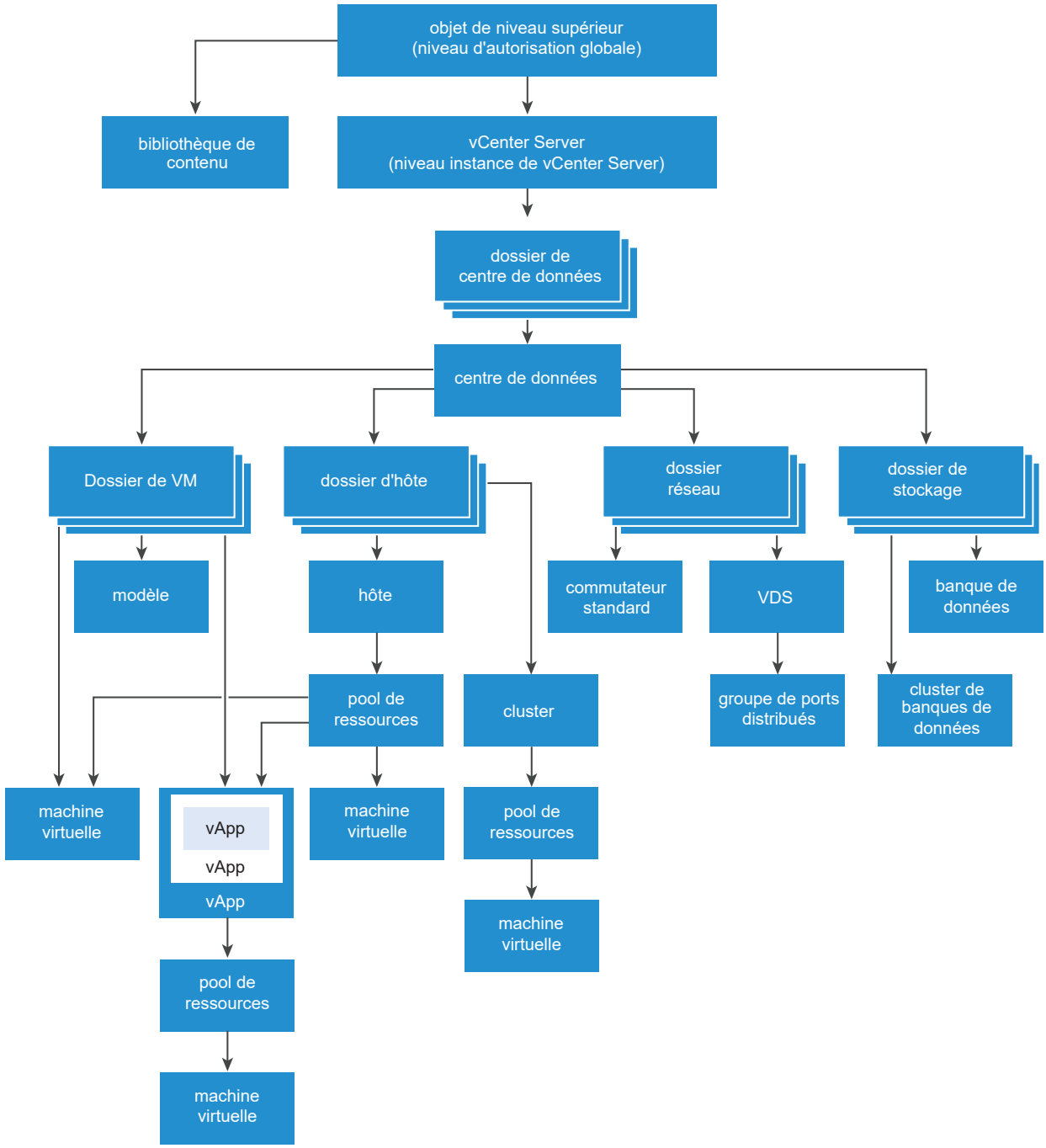
Héritage hiérarchique des autorisations

Lorsque vous attribuez une autorisation à un objet, vous pouvez choisir si l'autorisation propage la hiérarchie d'objets. Vous définissez la propagation pour chaque autorisation. La propagation n'est pas appliquée universellement. Les autorisations définies pour un objet enfant ignorent toujours les autorisations qui sont propagées à partir des objets parent.

La figure suivante illustre la hiérarchie d'inventaire et les chemins par lesquels les autorisations peuvent se propager.

Note Les autorisations globales prennent en charge l'attribution de privilèges entre les solutions à partir d'un objet racine global. Reportez-vous à la section Autorisations globales.

Figure 2-4. Hiérarchie d'inventaire de vSphere



À propos de cette figure :

- Vous ne pouvez pas définir d'autorisations directes sur les dossiers de VM, d'hôte, de réseau et de stockage. Autrement dit, ces dossiers agissent comme des conteneurs et ne sont donc pas visibles par les utilisateurs.
- Vous ne pouvez pas définir d'autorisations sur des commutateurs standard.

La plupart des objets d'inventaire héritent des autorisations d'un objet parent unique dans la hiérarchie. Par exemple, une banque de données hérite des autorisations de son dossier de la banque de données parente ou du centre de données 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, vous pouvez définir des autorisations pour un commutateur distribué et ses groupes de ports distribués associés, en réglant des 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 entités gérées font référence aux objets vSphere suivants. Les entités gérées offrent des opérations spécifiques qui varient selon le type d'entité. Les utilisateurs privilégiés peuvent définir des autorisations sur des entités gérées. Consultez la documentation de vSphere API pour plus d'informations sur les objets, les propriétés et les méthodes de vSphere.

- 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 GroupAdmin dispose du rôle Administrateur sur un objet. Une autre autorisation peut spécifier que GroupVMAdmin possède le rôle d'administrateur de machines virtuelles sur le même objet. Toutefois, le groupe GroupVMAdmin ne peut pas avoir une autre autorisation pour le même GroupVMAdmin sur cet objet.

Un objet enfant hérite des autorisations de son parent si la propriété de propagation du parent est définie sur true. Une autorisation qui est définie directement sur un objet enfant remplace l'autorisation dans l'objet parent. Reportez-vous à la section Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent.

Si plusieurs rôles de groupe sont définis sur le même objet et qu'un utilisateur appartient à deux de ces groupes ou plus, deux situations sont possibles :

- Aucune autorisation n'est définie directement sur l'objet pour l'utilisateur. Dans ce cas, l'utilisateur obtient l'union des autorisations dont les groupes ont sur l'objet.
- Une autorisation est définie directement sur l'objet pour l'utilisateur. Dans ce cas, les autorisations de l'utilisateur sont prioritaires sur toutes les autorisations de groupe.

Exemple 1 : Héritage d'autorisations de plusieurs groupes

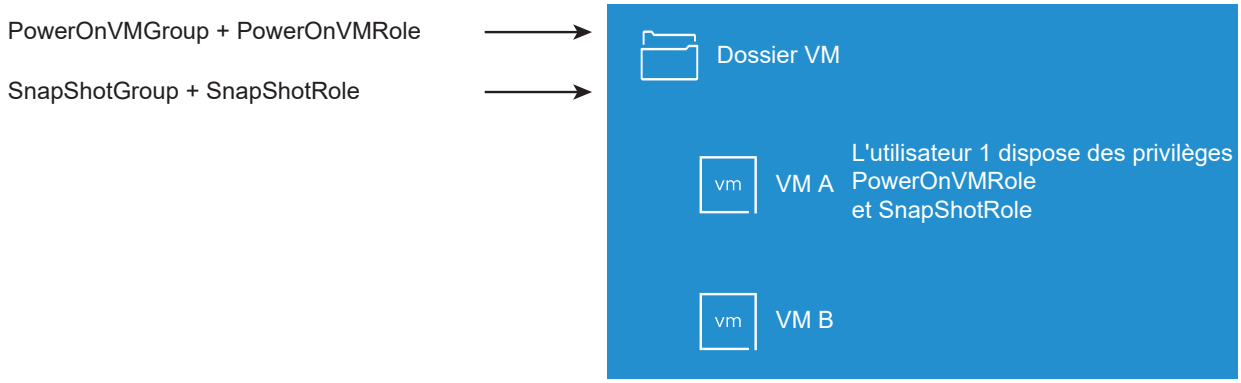
Cet exemple illustre comment un objet peut hériter d'autorisations multiples de groupes auxquels ont été accordés l'autorisation sur un objet parent.

Dans cet exemple, deux autorisations sont assignées sur le même objet pour deux groupes différents.

- PowerOnVMRole peut mettre des machines virtuelles sous tension.
- SnapShotRole peut prendre des snapshots de machines virtuelles.
- PowerOnVMRole est accordé à PowerOnVMGroup sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- SnapShotRole est accordé à SnapShotGroup 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 à la fois à PowerOnVMGroup et SnapShotGroup, se connecte. L'utilisateur 1 peut mettre sous tension et prendre des snapshots des VM A et B.

Figure 2-5. Exemple 1 : Héritage d'autorisations de plusieurs groupes



Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent

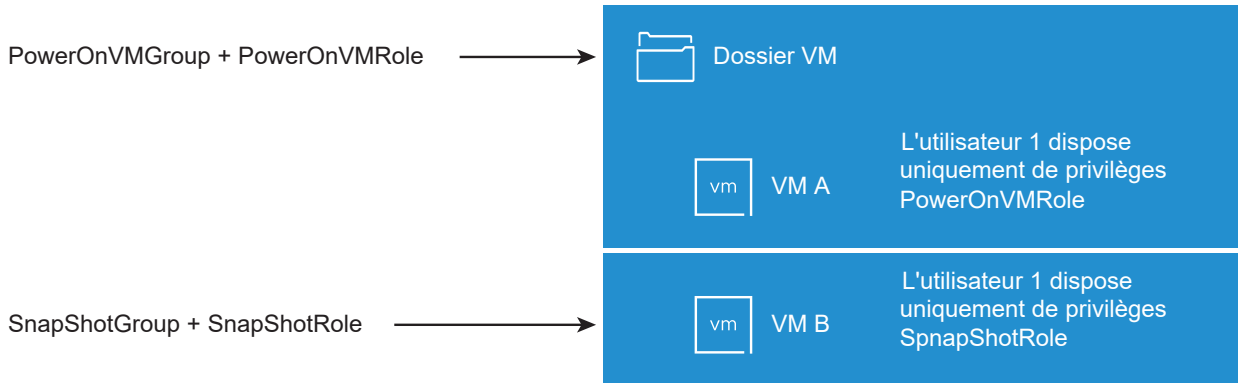
Cet exemple illustre comment les autorisations attribuées sur un objet enfant peuvent remplacer les autorisations attribuées sur un objet parent. Vous pouvez utiliser ce comportement de non prise en compte pour limiter l'accès client à des zones spécifiques de l'inventaire.

Dans cet exemple, des autorisations sont définies sur deux objets différents pour deux groupes différents.

- PowerOnVMRole peut mettre des machines virtuelles sous tension.
- SnapShotRole peut prendre des snapshots de machines virtuelles.
- PowerOnVMRole est accordé à PowerOnVMGroup sur le dossier de VM, avec l'autorisation définie pour propager aux objets enfant.
- SnapShotRole est accordé à SnapShotGroup sur VM B.

L'utilisateur 1, qui appartient à la fois à PowerOnVMGroup et SnapShotGroup, se connecte. Puisque SnapShotRole est assigné à un point inférieur dans la hiérarchie que PowerOnVMRole, il ignore le PowerOnVMRole 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 2-6. Exemple 2 : Autorisations d'enfant ignorant des autorisations de parent



Exemple 3 : Rôle d'utilisateur supprimant un rôle de groupe

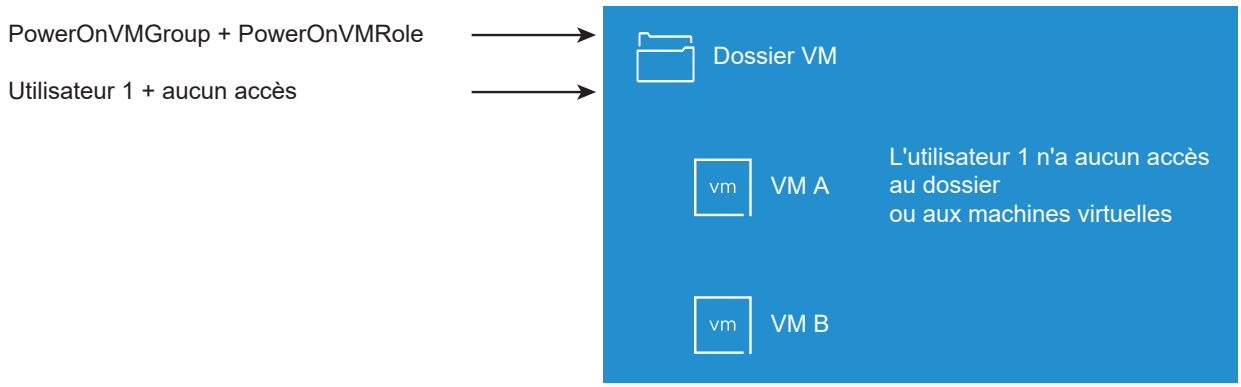
Cet exemple illustre comment le rôle attribué directement à un utilisateur individuel remplace les privilèges associés à un rôle attribué à un groupe.

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.

- PowerOnVMRole peut mettre des machines virtuelles sous tension.
- PowerOnVMRole est accordé à PowerOnVMGroup sur le dossier de VM.
- On accorde à l'utilisateur 1 un rôle NoAccess sur le dossier de VM.

L'utilisateur 1, qui appartient à PowerOnVMGroup, se connecte. Le rôle NoAccess accordé à l'utilisateur 1 sur le dossier de VM remplace le rôle attribué au groupe. L'utilisateur 1 n'a pas accès au dossier de VM ou aux VM A et B. Les VM A et B ne sont pas visibles dans la hiérarchie de l'utilisateur 1.

Figure 2-7. 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 au rôle d'accès correspondant. 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 obtenir des informations conceptuelles sur les autorisations, consultez les explications dans Présentation du modèle d'autorisation de niveau objet.

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 la section Héritage hiérarchique des autorisations.Vous pouvez également attribuer des autorisations de propagation à un objet racine global pour appliquer les autorisations à l'ensemble des objets dans toutes les solutions. Reportez-vous à la section 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 simultanément les mêmes autorisations de propagation à plusieurs objets en déplaçant les objets dans un dossier et en en classant les autorisations sur le dossier.

Lorsque vous attribuez des autorisations, 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

Le rôle qui vous est attribué sur l'objet dont vous souhaitez modifier les autorisations doit inclure le privilège **Autorisations.Modifier autorisation**.

Procédure

1. Accédez à l'objet auquel vous souhaitez attribuer des autorisations dans le navigateur d'objets de vSphere Client.
2. Cliquez sur l'onglet **Autorisations**.
3. Cliquez sur l'icône **Ajouter autorisation**.
4. (Facultatif) Si vous avez configuré un fournisseur d'identité externe tel qu'AD FS pour l'authentification fédérée, ce fournisseur d'identité peut être sélectionné dans le menu déroulant **Domaine**.
5. Sélectionnez 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 groupe.
   b. Entrez un nom dans la zone de recherche.

      Le système recherche des noms d'utilisateur et des noms de groupe.
   c. Sélectionnez l'utilisateur ou le groupe.
6. Sélectionnez un rôle dans le menu déroulant **Rôle**.

7 (Facultatif) Pour propager les autorisations, sélectionnez la case à cocher **Propager vers les enfants** .

Le rôle est appliqué à l'objet sélectionné et se propage aux objets enfant.

8 Cliquez sur **OK**.

Modifier ou supprimer 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 groupe ou changer le paramètre de la case à cocher **Propager vers les enfants**. Vous pouvez également supprimer le paramètre d'autorisation.

Procédure

1 Accédez à l'objet dans le navigateur d'objets de vSphere Client.

2 Cliquez sur l'onglet **Autorisations**.

3 Cliquez sur une ligne pour sélectionner une autorisation.

Tâche	Étapes
Modifier des autorisations	a Cliquez sur l'icône **Modifier un rôle**. b Sélectionnez un rôle pour l'utilisateur ou le groupe dans le menu déroulant **Rôle**. c Cochez/décochez la case **Propager vers les enfants** pour modifier l'héritage des autorisations. d Cliquez sur **OK**.
Supprimer des autorisations	Cliquez sur l'icône **Supprimer autorisation**.

Changer les paramètres de validation d'utilisateur

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. Vous ne pouvez pas faire des recherches dans les listes d'utilisateurs de ESXi de la même façon.

Procédure

1 Accédez au système vCenter Server dans le navigateur d'objets de vSphere Client.

2 Sélectionnez **Configurer** et cliquez sur **Paramètres > Général**.

3 Cliquez sur **Modifier** et sélectionnez **Répertoire de l'utilisateur**.

4 Modifiez les valeurs si nécessaire, puis cliquez sur **Enregistrer**.

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	Activez pour définir le nombre maximal d'utilisateurs et de groupes qui s'affichent dans vCenter Server.
Taille limite de requête	Nombre maximal d'utilisateurs et de groupes du domaine sélectionné que vCenter Server affiche dans la boîte de dialogue **Choisir les utilisateurs ou les groupes**. Si vous entrez 0 (zéro), tous les utilisateurs et groupes apparaissent.
Validation	Désactivez pour désactiver la validation.
Période de validation	Spécifie combien de fois vCenter Server valide les autorisations, en minutes.

Autorisations globales

Les autorisations globales sont appliquées à un objet racine global qui peut couvrir plusieurs solutions à la fois. Dans un SDDC sur site, les autorisations globales peuvent s'étendre à la fois à vCenter Server et vRealize Orchestrator. Toutefois, pour un SDDC vSphere, les autorisations globales s'appliquent aux objets globaux tels que les balises et les bibliothèques de contenu.

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 attribués à l'utilisateur ou au groupe pour tous les objets de la hiérarchie. Vous pouvez attribuer un rôle prédéfini ou créer des rôles personnalisés. Reportez-vous à la section 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'une machine virtuelle. Dans ce cas, vous spécifiez qu'un utilisateur ou un groupe dispose d'un rôle (ensemble de privilèges) sur l'objet.

Autorisations globales

Les autorisations globales donnent à un utilisateur ou à un groupe des privilèges pour afficher ou gérer tous les objets dans chacune des hiérarchies d'inventaire de votre déploiement. Les autorisations globales s'appliquent également aux objets globaux tels que les balises et les bibliothèques de contenu. Reportez-vous à la section Autorisations sur les objets de balise.

Si vous attribuez une autorisation globale sans sélectionner l'option 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.

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.

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. Connectez-vous à vCenter Server en utilisant vSphere Client.
2. Sélectionnez **Administration** et cliquez sur **Autorisations globales** dans la zone Contrôle d'accès.
3. Cliquez sur l'icône **Ajouter autorisation**.
4. (Facultatif) Si vous avez configuré un fournisseur d'identité externe tel qu'AD FS pour l'authentification fédérée, ce fournisseur d'identité peut être sélectionné dans le menu déroulant **Domaine**.
5. Sélectionnez 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 groupe.
   b. Entrez un nom dans la zone de recherche.

      Le système recherche des noms d'utilisateur et des noms de groupe.
   c. Sélectionnez l'utilisateur ou le groupe.
6. Sélectionnez un rôle dans le menu déroulant **Rôle**.

7 Décidez si vous souhaitez répercuter les autorisations en sélectionnant la case à cocher **Propager vers les enfants**.

   Si vous attribuez une autorisation globale sans sélectionner l'option **Propager vers les enfants**, 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.

8 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 supérieur 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, tel qu'une machine virtuelle, cet utilisateur peut effectuer les tâches associées à l'autorisation. Toutefois, l'utilisateur ne peut pas effectuer d'opérations liées aux balises sur l'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 supérieur (c'est-à-dire une autorisation globale) ou du privilège pour l'objet de balise.

Tableau 2-1. 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 n'est 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 n'est 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 de niveau supérieur, 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 supérieur, 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 pour la production de balises, car il a l'autorisation globale, qui se propage depuis le niveau supérieur. Si vous ne modifiez pas l'autorisation globale, vous ne pouvez pas restreindre les privilèges.

Tableau 2-2. 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.

Note Ce comportement est différent de la manière dont les privilèges vCenter Server sont hérités. Dans vCenter Server, les autorisations définies pour un objet enfant ignorent toujours les autorisations qui sont propagées à partir des objets parent.

Tableau 2-3. 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 machines virtuelles permet à un utilisateur de lire et de modifier les attributs de machines virtuelles.

Lorsque vous attribuez des autorisations, vous couplez 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, supposez que votre inventaire comprend deux pools de ressources, le pool A et le pool B ; vous pouvez attribuer au groupe Ventes le rôle Utilisateur de machine virtuelle sur le pool A et le rôle Lecture seule sur le pool B. Ainsi, les utilisateurs du groupe Ventes peuvent 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 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 interface de ligne de commande ou VMware Host Client. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*. Les rôles d'hôtes personnalisés ne sont pas accessibles à partir de vCenter Server.

Si vous gérez des hôtes ESXi via vCenter Server, ne conservez pas de rôles personnalisés dans l'hôte et dans vCenter Server. Définissez les rôles au niveau de vCenter Server.

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 Lorsque vous ajoutez un rôle personnalisé auquel vous n'attribuez aucun privilège, le rôle est créé comme un rôle Lecture seule avec trois privilèges définis par le système : **Système.Anonyme**, **Système.Affichage** et **Système.Lecture**. Ces privilèges ne sont pas visibles dans l'instance de vSphere Client, mais sont utilisés pour lire certaines propriétés de certains objets gérés. Tous les rôles prédéfinis dans vCenter Server contiennent ces trois privilèges définis par le système. Pour plus d'informations, reportez-vous à la documentation de l'*API vSphere Web Services*.

Créer un rôle personnalisé

Vous pouvez créer des rôles personnalisés vCenter Server correspondant aux besoins de contrôle d'accès de votre environnement. Vous pouvez créer un rôle ou cloner un rôle existant.

Vous pouvez créer ou modifier un rôle sur un système vCenter Server qui fait partie du même domaine vCenter Single Sign-On que les autres systèmes vCenter Server. VMware Directory Service (vmdir) propage les modifications de rôle que vous apportez à tous les autres systèmes vCenter Server dans le 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 en utilisant vSphere Client.
2. Sélectionnez **Administration** et cliquez sur **Rôles** dans la zone **Contrôle d'accès**.
3. Créez le rôle :

Option	Description
Pour créer un rôle	Cliquez sur l'icône **Créer une action de rôle**.
Pour créer un rôle par clonage :	Sélectionnez un rôle et cliquez sur l'icône **Cloner une action de rôle**.

   Consultez Rôles système de vCenter Server pour plus d'informations.
4. Sélectionnez et désélectionnez les privilèges du rôle.

   Consultez Chapitre 16 Privilèges définis pour plus d'informations.

   Note Lors de la création d'un rôle cloné, vous ne pouvez pas modifier les privilèges. Pour modifier les privilèges, sélectionnez le rôle cloné après sa création et cliquez sur l'icône **Modifier une action de rôle**.
5. Entrez le nom du nouveau rôle.
6. Cliquez sur **Terminer**.

Étape suivante

Vous pouvez créer des autorisations en sélectionnant un objet et en attribuant le rôle à un utilisateur ou à un groupe pour cet objet.

Rôles système de vCenter Server

Un rôle est un ensemble prédéfini de privilèges. Lorsque vous ajoutez des autorisations à un objet, vous couplez un utilisateur ou un groupe avec un rôle. vCenter Server inclut certains rôles système par défaut, que vous ne pouvez pas modifier.

vCenter Server fournit des 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.

Pour afficher les privilèges associés à un rôle par défaut, accédez au rôle dans l'instance de vSphere Client (**Menu > Administration > Rôles**) et cliquez sur l'onglet **Privilèges**.

La hiérarchie de rôle vCenter Server inclut également plusieurs exemples de rôles. Vous pouvez cloner un exemple de rôle pour créer un rôle similaire.

Si vous créez un rôle, il n'hérite des privilèges d'aucun rôle système.

Rôle d'administrateur

Les utilisateurs qui ont le 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 du rôle Lecture seule. Si vous disposez du rôle Administrateur sur un objet, vous pouvez attribuer des privilèges à des utilisateurs individuels ou à 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. Reportez-vous à la documentation *Authentification vSphere* pour les services d'identité pris en charge.

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 Lecture seule

Les utilisateurs qui ont le rôle Lecture seule pour un objet sont autorisés à afficher l'état et les détails de l'objet. Par exemple, les utilisateurs ayant ce rôle peuvent afficher la machine virtuelle, l'hôte et les attributs du pool de ressources, mais ne peuvent pas afficher la console distante d'un hôte. Toutes les actions via les menus et barres d'outils ne sont pas autorisées.

Rôle Aucun accès

Les utilisateurs qui ont le 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.

Le rôle Administrateur est attribué par défaut à l'administrateur du domaine vCenter Single Sign-On (par défaut administrator@vsphere.local) ainsi qu'aux utilisateurs racine et vpxuser. Le rôle Aucun accès est attribué par défaut aux autres utilisateurs.

La meilleure pratique consiste à créer un utilisateur au niveau racine et à lui attribuer le rôle Administrateur. Après avoir créé un utilisateur nommé ayant les privilèges Administrateur, vous ne pouvez pas supprimer l'utilisateur racine des autorisations ni remplacer son rôle par le rôle Aucun accès.

Meilleures pratiques pour les rôles et les autorisations

Suivez les meilleures pratiques pour les rôles et les autorisations afin d'optimiser la sécurité et la facilité de gestion de votre environnement vCenter Server.

Suivez ces meilleures pratiques lorsque vous configurez les rôles et les autorisations dans votre environnement vCenter Server :

- Si possible, attribuez un rôle à un groupe plutôt qu'à des utilisateurs individuels.
- 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. Utilisez un nombre minimal d'autorisations pour faciliter 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 groupe le rôle restrictif.
- Utilisez des dossiers pour grouper des objets. Par exemple, pour 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.
- Pensez à activer la propagation lorsque vous attribuez des autorisations à un objet. La propagation garantit que les nouveaux objets de la hiérarchie d'objets héritent des autorisations. Par exemple, vous pouvez attribuer une autorisation à un dossier de machine virtuelle et activer la propagation pour vous assurer que l'autorisation s'applique à toutes les machines virtuelles du dossier.
- Utilisez le rôle Aucun accès pour masquer des zones spécifiques de la hiérarchie. Le rôle Aucun accès restreint l'accès aux utilisateurs ou groupes avec ce rôle.
- Les modifications apportées aux licences se propagent à tous les systèmes vCenter Server du même domaine vCenter Single Sign-On.
- La propagation de licence s'effectue même si l'utilisateur ne dispose pas de privilèges sur tous les systèmes vCenter Server .

Privilèges requis pour les tâches courantes

De nombreuses tâches requièrent des autorisations sur plusieurs objets d'inventaire. Si l'utilisateur qui tente d'effectuer la tâche dispose de privilèges sur un objet uniquement, il est possible que la tâche ne se termine pas correctement.

Le tableau suivant répertorie les tâches courantes qui exigent plusieurs privilèges. Vous pouvez ajouter des autorisations aux objets d'inventaire en associant un utilisateur à l'un des rôles prédéfinis ou à plusieurs privilèges. Si vous envisagez d'attribuer plusieurs fois un ensemble de privilèges, créez des rôles personnalisés.

Reportez-vous à la documentation *Référence de l'API vSphere Web Services* pour découvrir comment les opérations de l'interface utilisateur de vSphere Client sont mappées aux appels d'API et les privilèges requis pour effectuer des opérations. Par exemple, la documentation de l'API pour la méthode `AddHost_Task(addHost)` spécifie que le privilège **Hôte.Inventaire.AddHostToCluster** est requis pour ajouter un hôte à un cluster.

Si la tâche que vous souhaitez exécuter ne se trouve pas dans ce tableau, suivez les règles suivantes afin d'attribuer les autorisations requises pour certaines opérations :

- Toute opération qui consomme de l'espace de stockage requiert le privilège **Banque de données.Allouer de l'espace**pour la banque de données cible et le privilège d'exécuter l'opération proprement dite. Vous devez disposer de ces privilèges, par exemple, lorsque vous créez un disque virtuel ou que vous réalisez un snapshot.
- 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 2-4. 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 : ■ **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.Configurer le 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 de destination ou le dossier qui contient la 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.Attribuer un réseau**	Utilisateur réseau ou Administrateur

Tableau 2-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
Mettre sous tension une machine virtuelle	Sur le centre de données dans lequel la machine virtuelle est déployée : **Machine virtuelle.Interaction.Mettre sous tension**	Utilisateur avancé de machines virtuelles ou Administrateur
	Sur la machine virtuelle ou le dossier des machines virtuelles : **Machine virtuelle.Interaction.Mettre sous tension**	
Déployer une machine virtuelle à partir d'un modèle	Dans le dossier ou le centre de données de destination : ■ **Machine virtuelle .Inventaire.Créer à partir d'un modèle existant** ■ **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.Attribuer 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 : ■ **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
Installer un système d'exploitation invité sur une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **Machine virtuelle.Interaction.Répondre à une question** ■ **Machine virtuelle.Interaction.Interaction avec une console** ■ **Machine virtuelle.Interaction.Connexion à un périphérique** ■ **Machine virtuelle.Interaction.Mettre hors tension** ■ **Machine virtuelle.Interaction.Mettre sous tension** ■ **Machine virtuelle.Interaction.Réinitialiser** ■ **Machine virtuelle.Interaction.Configurer un support sur CD** (en cas d'installation à partir d'un CD) ■ **Machine virtuelle.Interaction.Configurer un support sur disquette** (en cas d'installation à partir d'une disquette) ■ **Machine virtuelle.Interaction.Installation de VMware Tools**	Utilisateur avancé de machines virtuelles ou Administrateur

Tableau 2-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
	Sur une banque de données qui contient l'image ISO de support d'installation : **Banque de données.Parcourir une banque de données** (en cas d'installation à partir d'une image ISO sur une banque de données) Sur la banque de données sur laquelle vous chargez l'image ISO de support d'installation : ■ **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	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **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
	Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de pool de ressources ou Administrateur
Migrer à froid (relocaliser) une machine virtuelle	Sur la machine virtuelle ou le dossier des machines virtuelles : ■ **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
	Sur l'hôte, le cluster ou le pool de ressources de destination (si différent de la source) : **Ressource.Attribuer une machine virtuelle au pool de ressources**	Administrateur de pool de ressources ou Administrateur
	Sur la banque de données de destination (si différent de la source) : **Banque de données.Allouer de l'espace**	Utilisateur de banque de données ou Administrateur
Migration d'une machine virtuelle avec Storage vMotion	Sur la machine virtuelle ou le dossier des machines virtuelles : **Ressource.Migrer une machine virtuelle sous tension**	Administrateur de pool de ressources ou Administrateur
	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** ■ **Hôte.Inventaire.Modifier cluster**	Administrateur
Ajouter un hôte unique à un centre de données à l'aide de vSphere Client ou	Sur l'hôte : **Hôte.Inventaire.Ajouter un hôte au cluster**	Administrateur

Tableau 2-4. Privilèges requis pour les tâches courantes (suite)

Tâche	Privilèges requis	Rôle applicable
ajouter un hôte unique à un cluster à l'aide de PowerCLI ou d'une API (utilisant l'API addHost)	Sur le cluster : ■ **Hôte.Inventaire.Modifier cluster** ■ **Hôte.Inventaire.Ajouter un hôte au cluster**	Administrateur
	Sur le centre de données : **Hôte.Inventaire.Ajouter un hôte autonome**	Administrateur
Ajouter plusieurs hôtes au cluster	Sur le cluster : ■ **Hôte.Inventaire.Modifier cluster** ■ **Hôte.Inventaire.Ajouter un hôte au cluster**	Administrateur
	Sur le centre de données parent du cluster (avec propagation) : ■ **Hôte.Inventaire.Ajouter un hôte autonome** ■ **Hôte.Inventaire.Déplacer un hôte** ■ **Hôte.Inventaire.Modifier cluster** ■ **Hôte.Configuration.Maintenance**	Administrateur
Chiffrer une machine virtuelle	Les tâches de chiffrement sont possibles uniquement dans les environnements qui incluent vCenter Server. De plus, le mode de chiffrement doit être activé sur l'hôte ESXi pour la plupart des tâches de chiffrement. L'utilisateur qui exécute la tâche doit disposer des privilèges appropriés. Un ensemble de privilèges **Opérations de chiffrement** permet d'effectuer un contrôle plus précis. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.	Administrateur

Sécurisation des hôtes ESXi 3

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 configure 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. Les hôtes ESXi participent à l'infrastructure des certificats. Les hôtes sont provisionnés à l'aide de certificats signés par VMware Certificate Authority (VMCA) par défaut.

Pour plus d'informations sur la sécurité d'ESXi, reportez-vous au livre blanc VMware *Sécurité de VMware vSphere Hypervisor*.

Note ESXi n'est pas basé sur le noyau Linux ou sur une distribution Linux de base. Il utilise ses propres outils logiciels et de noyau spécialisés et propriétaires VMware, fournis en tant qu'unité autonome, et ne contient pas d'applications et de composants provenant de distributions Linux.

Ce chapitre contient les rubriques suivantes :

- Recommandations générales de sécurité pour ESXi
- Gestion de certificats pour les hôtes ESXi
- Personnalisation des hôtes avec le profil de sécurité
- Attribution de privilèges pour les hôtes ESXi
- Utilisation d'Active Directory pour gérer des utilisateurs ESXi
- Utiliser vSphere Authentication Proxy
- Configuration de l'authentification par carte à puce pour ESXi
- Utilisation du ESXi Shell
- Démarrage sécurisé UEFI des hôtes ESXi
- Sécurisation des hôtes ESXi avec un module de plate-forme sécurisée

- Fichiers journaux ESXi
- Sécurisation de la configuration ESXi

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. Dans ce cas, assurez-vous de travailler dans un environnement de confiance et prenez d'autres mesures de sécurité.

Fonctionnalités de sécurité intégrées

Les risques pour les hôtes sont atténués comme suit :

- Les interfaces ESXi Shell et SSH sont désactivées par défaut. Maintenez ces interfaces désactivées, sauf si vous effectuez des activités de dépannage ou de prise en charge. Pour les activités quotidiennes, utilisez vSphere Client, où l'activité est soumise à des méthodes de contrôle d'accès basé sur les rôles et modernes.
- 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 l'accès de gestion à l'hôte sont fermés. Ouvrez les ports si vous avez besoin de services supplémentaires.
- 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 comme algorithme de signature.
- Un service Web interne est utilisé par ESXi pour prendre en charge l'accès par les clients Web. Le service a été modifié pour exécuter uniquement les fonctions dont un client Web a besoin pour l'administration et la surveillance. Par conséquent, ESXi n'est pas exposé aux problèmes de sécurité du service Web signalés pour une utilisation plus large.
- 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. Vous pouvez vous abonner à la liste de diffusion d'avis et d'alertes de sécurité VMware pour recevoir des alertes de sécurité. Consultez la page Web à l'adresse http://lists.vmware.com/mailman/listinfo/security-announce.
- Les services non sécurisés (tels que FTP et Telnet) ne sont pas installés, et les ports associés à ces services sont fermés par défaut.

- Pour protéger les hôtes contre le chargement de pilotes et d'applications qui ne sont pas signés avec chiffrement, utilisez le démarrage sécurisé UEFI. L'activation du démarrage sécurisé s'effectue au niveau du BIOS du système. Aucune modification de configuration supplémentaire n'est requise sur l'hôte ESXi, par exemple, sur des partitions de disque. Reportez-vous à la section Démarrage sécurisé UEFI des hôtes ESXi.
- Si votre hôte ESXi dispose d'une puce TPM 2.0, activez et configurez la puce dans le BIOS du système. En collaboration avec le démarrage sécurisé, TPM 2.0 fournit une sécurité améliorée et une assurance d'approbation intégrée dans le matériel. Reportez-vous à la section Sécurisation des hôtes ESXi avec un module de plate-forme sécurisée.

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 activez l'accès à l'interface DCUI (Direct Console User Interface), ESXi Shell ou SSH, appliquez 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 Client pour administrer les hôtes ESXi qui sont gérés par vCenter Server. N'accédez pas aux hôtes gérés directement avec VMware Host Client et ne modifiez pas les hôtes gérés à partir de l'interface DCUI.

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.

Utiliser l'interface DCUI pour le dépannage

Accédez à l'hôte via l'interface DCUI ou ESXi Shell en tant qu'utilisateur racine uniquement pour le dépannage. Pour administrer vos hôtes ESXi, utilisez l'un des clients d'interface utilisateur graphique ou l'une des API VMware. Reportez-vous à *Concepts et exemples d'ESXCLI* à l'adresse https://code.vmware.com/. Si vous utilisez ESXi Shell ou SSH, limitez les comptes qui disposent d'un accès et définissez des délais d'expiration.

N'utilisez que des sources VMware pour mettre à niveau les composants ESXi.

L'hôte exécute plusieurs modules tiers pour prendre en charge les interfaces de gestion ou les tâches que vous devez effectuer. VMware prend en charge uniquement les mises à niveau vers les modules provenant 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. Consultez les sites Web des fournisseurs tiers et la base de connaissances VMware pour connaître les alertes de sécurité.

Note Suivez les instructions de sécurité fournies par VMware, disponible sur le site http://www.vmware.com/security/.

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 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. Reportez-vous à la documentation *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.

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 Client.

vSphere inclut plusieurs langages de script pour la gestion des hôtes. Pour obtenir des informations de référence et des conseils de programmation, et accéder aux communautés VMware pour des astuces supplémentaires sur la gestion chiffrée, consultez la *Documentation ESXCLI* et la *Documentation vSphere API/SDK*. La documentation de l'administrateur de vSphere est principalement axée sur l'utilisation de vSphere Client pour la gestion.

VMware PowerCLI

VMware PowerCLI est une interface Windows PowerShell avec vSphere API. VMware PowerCLI inclut des applets de commande PowerShell pour administrer les composants vSphere.

VMware PowerCLI inclut des centaines d'applets de commande, un ensemble d'exemples de scripts et une bibliothèque de fonctions pour la gestion et l'automatisation. Reportez-vous à la section https://developer.vmware.com/powercli.

ESXCLI

ESXCLI inclut un ensemble de commandes pour la gestion des hôtes ESXi et des machines virtuelles. Consultez la *documentation d'ESXCLI*.

Vous pouvez également utiliser l'une des interfaces de script au vSphere Automation SDK, comme le vSphere Automation SDK pour 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 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

ESXCLI	`esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeOut`
	
	`esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list | grep /UserVars/ESXiShellTimeOut`

PowerCLI	`#List UserVars.ESXiShellInteractiveTimeOut for each host`
	`Get-VMHost | Select Name,`
	`@{N="UserVars.ESXiShellInteractiveTimeOut";E={$_`
	`| Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut`
	`| Select -ExpandProperty Value}}`
	
	`# Set UserVars.ESXiShellTimeOut to 900 on all hosts`
	`Get-VMHost`
	`| Foreach { Get-AdvancedSetting -Entity $_ -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900 }`

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.

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`. Vous pouvez également définir le nombre de mots de passe à mémoriser pour chaque utilisateur à l'aide de l'option avancée `Security.PasswordHistory`.

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 VMware Host 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.
- Par défaut, la longueur du mot de passe est supérieure à 7 et inférieure à 40.
- Les mots de passe ne doivent pas contenir un mot du dictionnaire ou une partie d'un mot du dictionnaire.

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.

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, un utilisateur est invité jusqu'à trois fois (retry=3) à entrer un nouveau mot de passe si celui-ci n'est pas suffisamment sécurisé ou si le mot de passe n'a pas été entré correctement deux fois. Les mots de passe avec une ou deux classes de caractères et des phrases de passe 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. Consultez la page du manuel `pam_passwdqc` pour plus d'informations sur les autres options, telles que `max`, `passphrase`, etc.

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 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 trois 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 (`passphrase=4`), comme suit :

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

Pour plus de détails, reportez-vous aux pages du manuel concernant `pam_passwdqc`.

Note Les combinaisons possibles des options de mot de passe 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

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 5 échecs de tentative de connexion est autorisé avant le verrouillage du compte. Le compte est déverrouillé au bout de 15 minutes par défaut.

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.
- `Security.PasswordHistory`. Nombre de mots de passe à mémoriser pour chaque utilisateur. La valeur zéro désactive l'historique du mot de passe.

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.

Sécurité SSH

Les interfaces ESXi Shell et SSH sont désactivées par défaut. Maintenez ces interfaces désactivées, sauf si vous effectuez des activités de dépannage ou de prise en charge. Pour les activités quotidiennes, utilisez vSphere Client, où l'activité est soumise à des méthodes de contrôle d'accès basé sur les rôles et modernes.

La configuration SSH d'ESXi utilise les paramètres suivants :

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.

Clés SSH ESXi

Les clés SSH peuvent restreindre, contrôler et sécuriser l'accès à un hôte ESXi. Une clé SSH peut autoriser un utilisateur approuvé ou un script à se connecter à un hôte sans entrer un mot de passe.

Vous pouvez copier la clé SSH sur l'hôte en utilisant la commande `vifs`. Il est également possible d'utiliser HTTPS PUT pour copier la clé SSK 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. Consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/1002866.

Activer SSH et ajouter des clés SSH à l'hôte présente des risques inhérents. Évaluez le risque potentiel d'exposer un nom d'utilisateur et un mot de passe par rapport au risque d'intrusion par un utilisateur qui dispose d'une clé approuvée.

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.

- Fichiers 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`. Si vous le faites, vous apportez une modification dont le démon de l'hôte (`hostd`) ne sait rien.

Procédure

- Sur la ligne de commande ou un serveur d'administration, utilisez la commande `vifs` pour télécharger la clé SSH dans un 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	`https://`*`hostname_or_IP_address`*`/host/ssh_root_authorized_keys` Vous devez disposer de tous les privilèges Administrateur sur l'hôte pour télécharger ce fichier.
Clés DSA	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key`
Clés DSA publiques	`https://`*`hostname_or_IP_address`*`/host/ssh_host_dsa_key_pub`

Type de clés :	Emplacement
Clés RSA	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
Clés RSA publiques	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

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 si un code bogué ou malveillant, tel qu'un pilote de périphérique, s'exécute en mode privilégié dans le système d'exploitation invité. Les standards matériels et micrologiciels n'ont pour le moment pas la prise en charge nécessaire des conteneurs d'erreur pour protéger les hôtes ESXi de la vulnérabilité.

N'utilisez un relais PCI ou PCIe sur une machine virtuelle que si une entité approuvée possède et administre la machine virtuelle. 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 ou d'incompatibilités dans les périphériques matériels et qui sont ensuite transmises. Des problèmes de pilotes dans le système d'exploitation invité peuvent également être une source possible d'erreurs.
- Le système d'exploitation invité peut générer une opération DMA (Direct Memory Access) et provoquer une erreur de page IOMMU sur l'hôte ESXi. Cette opération peut être le résultat d'une opération DMA visant une adresse en dehors de la mémoire de la machine virtuelle. Sur certaines machines, le microprogramme de l'hôte configure les pannes IOMMU pour signaler une erreur fatale via une interruption non masquable (NMI). Cette erreur fatale 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 fausse interruption peut entraîner un blocage de l'hôte ESXi. Il existe en théorie d'autres façons d'exploiter ces fausses interruptions.

Désactiver Managed Object Browser

Le navigateur d'objets gérés (Managed Object Browser, MOB) permet 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 il est possible de modifier la

configuration de l'hôte à l'aide du MOB. Utilisez le MOB uniquement à des fins de débogage et assurez-vous qu'il est désactivé dans les systèmes de production.

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. Vous pouvez activer ou désactiver le MOB de la manière suivante.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, cliquez sur **Paramètres système avancés**.
4. Vérifiez la valeur de **Config.HostAgent.plugins.solo.enableMob** et cliquez sur **Modifier** pour la modifier si nécessaire.

   N'utilisez pas la commande `vim-cmd` depuis ESXi Shell.

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 VMware 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 vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN et le stockage. Isolez ces réseaux pour leurs fonctions spécifiques. Il n'est souvent pas nécessaire de router ces réseaux à l'extérieur d'un rack de serveur physique spécifique.
- 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 de tout autre trafic. 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. Contrôlez strictement l'accès à ce réseau.
- 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.

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

Lorsque vous utilisez vSphere Auto Deploy, soyez très vigilants à la sécurité du réseau, la sécurité de l'image de démarrage et l'éventuelle exposition des mots de passe dans les profils d'hôtes afin de protéger votre environnement.

Sécurité de la mise en réseau

Sécurisez votre réseau exactement comme si vous sécurisiez le réseau pour n'importe quelle autre méthode déploiement basée sur 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 une 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 hachés avec SHA-512.
  - 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 Proxy afin d'éviter d'exposer les mots de passe d'Active Directory. 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.

Contrôler l'accès aux outils de surveillance du matériel basée sur 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 garantir que l'interface CIM est sécurisée, ne fournissez que le niveau d'accès minimal nécessaire à ces applications distantes. Si vous provisionnez une application distante avec un compte racine ou d'administrateur, et si l'application est compromise, l'environnement virtuel peut l'être également.

Le modèle CIM est une norme ouverte qui définit une architecture pour la surveillance des ressources matérielles sans agent et basée sur des normes pour les hôtes 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 prennent en charge l'accès de gestion aux pilotes des périphériques et au matériel sous-jacent. Les fournisseurs de matériel, y compris les fabricants de serveurs et les fournisseurs de périphériques matériel, peuvent inscrire les fournisseurs qui surveillent et gèrent leurs périphériques. VMware inscrit les fournisseurs qui surveillent le matériel de serveur, l'infrastructure de stockage ESXi et les ressources spécifiques à la virtualisation. Ces fournisseurs sont exécutés au sein de l'hôte ESXi. Ils sont légers et axés sur des tâches de gestion spécifiques. Le courtier CIM recueille les informations de tous les fournisseurs CIM et les présente à l'extérieur à l'aide d'API standard. L'API la plus standard est WS-MAN.

Ne fournissez pas aux applications distantes des informations d'identification racine permettant d'accéder à l'interface CIM. Créez plutôt un compte d'utilisateur vSphere de moindre privilège pour ces applications et utilisez la fonction de ticket de l'API VIM pour émettre un sessionId (appelé « ticket ») pour ce compte d'utilisateur de moindre privilège à des fins d'authentification auprès du modèle de données unifié (Common Information Model, CIM). Si le compte a été autorisé à obtenir des tickets de modèle de données unifié, l'API VIM peut ensuite fournir le ticket au modèle de données unifié. Ces tickets sont ensuite fournis sous la forme de l'ID et du mot de passe d'utilisateur à un appel d'API CIM-XML. Reportez-vous à la méthode `AcquireCimServicesTicket()` pour plus d'informations.

Le service CIM démarre lorsque vous installez un VIB CIM tiers, par exemple, lorsque vous exécutez la commande `esxcli software vib install –n` *`VIBname`*.

Si vous devez activer le service CIM manuellement, exécutez la commande suivante :

```
esxcli system wbem set –e true
```

Si nécessaire, vous pouvez désactiver wsman (WSManagement Service) afin que seul le service CIM soit en cours d'exécution :

```
esxcli system wbem set –W false
```

Pour confirmer que wsman est désactivé, exécutez la commande suivante :

```
esxcli system wbem get
…
WSManagement PID: 0
WSManagement Service: false
```

Pour plus d'informations sur les commandes ESXCLI, consultez la *Documentation ESXCLI*. Pour plus d'informations sur l'activation du service CIM, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/1025757.

Procédure

1. Créez un compte d'utilisateur vSphere non racine pour les applications CIM.

   Reportez-vous à la rubrique concernant l'ajout d'utilisateurs vCenter Single Sign-On dans *Authentification vSphere*. Le privilège vSphere requis pour le compte d'utilisateur est **Host.CIM.Interaction**.

2. Utilisez le SDK vSphere API de votre choix pour authentifier le compte d'utilisateur au niveau de vCenter Server. Appelez ensuite `AcquireCimServicesTicket()` pour renvoyer un ticket à des fins d'authentification auprès de ESXi en tant que compte de niveau administrateur, à l'aide des API de port 5989 CIM-XML ou de port 433 WS-Management.

   Pour plus d'informations, consultez *Référence de l'API vSphere Web Services*.

3. Renouvelez le ticket toutes les deux minutes si nécessaire.

Gestion de certificats pour les hôtes ESXi

VMware Certificate Authority (VMCA) fournit à chaque nouvel hôte ESXi 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 ESXi depuis vSphere 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 6.0 et version ultérieure

Lorsque ESXi et vCenter Server communiquent, ils utilisent TLS pour presque tout le trafic de gestion.

Dans vSphere 6.0 et versions ultérieures, vCenter Server prend en charge les modes de certificat suivants pour les hôtes ESXi.

Tableau 3-1. Modes de certificat des hôtes ESXi

Mode de certificat	Description
VMware Certificate Authority (par défaut)	Utilisez ce mode si VMCA provisionne tous les hôtes ESXi, comme autorité de certification de niveau supérieur ou comme autorité de certification intermédiaire. Par défaut, VMCA provisionne les hôtes ESXi avec des certificats. Dans ce mode, vous pouvez actualiser et renouveler les certificats dans vSphere Client.
Autorité de certification personnalisée	Utilisez ce mode si vous souhaitez uniquement utiliser des certificats personnalisés qui sont signés par une autorité de certification tierce ou de l'entreprise. Dans ce mode, vous êtes responsable de la gestion des certificats. Vous ne pouvez pas actualiser et renouveler des certificats dans vSphere Client. **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 Client.
Mode d'empreinte	vSphere 5.5 utilisait le mode empreinte numérique. Ce mode reste disponible en tant qu'option de repli pour vSphere 6.x. 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. 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.x et versions ultérieures ne fonctionnent pas correctement en mode d'empreinte.

Expiration du certificat

Vous pouvez afficher des informations sur l'expiration des certificats qui sont signés par VMCA ou par une autorité de certification tierce dans vSphere 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 huit mois). Une alarme rouge se déclenche si le certificat est dans l'état **Expiration imminente** (inférieure à deux 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 système vCenter Server.

Si VMCA n'est pas disponible lorsqu'un hôte Auto Deploy démarre pour la première fois, l'hôte tente de se connecter en premier lieu. Si cet hôte ne peut pas se connecter, il alterne les arrêts et les redémarrages jusqu'à ce que VMCA devienne disponible et que l'hôte soit provisionné avec un certificat signé.

Privilèges requis pour la gestion des certificats de ESXi

Pour la gestion des certificats des hôtes ESXi, vous devez disposer du privilège**Certificats.Gérer des certificats**. Vous pouvez définir ce privilège à partir de vSphere Client.

Modifications de nom d'hôte et d'adresse IP

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 3-2. 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.

Mises à niveau d'hôtes et certificats

Si vous mettez à niveau un hôte ESXi vers ESXi 6.5 ou version ultérieure, le processus de mise à niveau remplace les certificats auto-signés (empreinte) par des certificats signés par VMCA. Si l'hôte ESXi utilise des certificats personnalisés, le processus de mise à niveau conserve ces certificats même s'ils sont expirés ou non valides.

Si vous décidez de ne pas mettre à niveau vos hôtes vers ESXi 6.5 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.

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 devrez plus tard mettre à niveau ces hôtes vers ESXi 6.5.

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 pendant la mise à niveau. Optez pour le mode de certificat **Personnalisé** pour garantir que les certificats ne sont pas remplacés accidentellement lors d'une actualisation de certificats ultérieure.

Note Si votre environnement est en mode VMCA et que vous actualisez les certificats dans vSphere 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 Client.

Hôtes provisionnés avec Auto Deploy

Les hôtes qui sont provisionnés par Auto Deploy obtiennent toujours de nouveaux certificats lors de leur premier démarrage avec le logiciel ESXi 6.5 ou version ultérieure. 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.

Reportez-vous à la section Utiliser des certificats personnalisés avec Auto Deploy.

Workflows de changement mode de certificat

À partir de vSphere 6.0, les hôtes ESXi sont provisionnés avec des certificats par VMCA par défaut. Vous devez plutôt utiliser le mode de certification personnalisée ou, à des fins de débogage, le mode d'empreinte hérité. 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.

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 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 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 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 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 validitié. 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 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 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.

Paramètres par défaut des certificats ESXi

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. La plupart des valeurs par défaut conviennent à de nombreuses situations, mais les informations spécifiques à l'entreprise peuvent être modifiées.

Vous pouvez modifier un grand nombre des paramètres par défaut à l'aide de vSphere Client. Envisagez de changer les informations sur l'entreprise et l'emplacement. Reportez-vous à la section Modifier les paramètres par défaut de certificat.

Tableau 3-3. Paramètres CSR ESXi

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.daysValid
Seuil fixe d'expiration des certificats. vCenter Server déclenche 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 3-3. Paramètres CSR ESXi (suite)

Paramètre	Valeur par défaut	Option avancée
Seuil dynamique d'expiration des certificats. vCenter Server déclenche 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 la section Mises à niveau d'hôtes et certificats.	vmca Vous pouvez également spécifier Empreinte ou Personnalisé. Reportez-vous à la section Changer le mode de certificat.	vpxd.certmgmt.mode

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 Client.

Pour obtenir la liste des paramètres par défaut, reportez-vous à Paramètres par défaut des certificats ESXi. Certaines valeurs par défaut ne peuvent pas être modifiées.

Procédure

1. Dans vSphere Client, sélectionnez le système vCenter Server qui gère les hôtes.
2. Cliquez sur **Configurer**, puis sur **Paramètres avancés**.
3. Cliquez sur **Modifier les paramètres**.
4. Cliquez sur l'icône **Filtre** dans la colonne Nom, et dans la zone Filtre, entrez **`vpxd.certmgmt`** pour afficher uniquement les paramètres de gestion de certificat.
5. Modifiez la valeur des paramètres existants pour appliquer la stratégie de l'entreprise, puis cliquez sur **Enregistrer**.

   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 certificate 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, ou renouveler les certificats.

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 Client. Il n'est pas possible d'afficher des informations sur l'état du certificat pour les hôtes en mode Empreinte.

Procédure

1. Connectez-vous à vCenter Server en utilisant vSphere Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Sélectionnez **Hôtes et clusters > Hôtes**.

   Par défaut, l'affichage des hôtes n'inclut pas l'état du certificat.
4. Cliquez sur la flèche vers le bas dans un en-tête de colonne pour afficher/masquer les colonnes.
5. Cochez la case **Certificat valide pour** 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.
6. (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 la section 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 Client. Les informations sur le certificat peuvent être utiles lors d'un débogage.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.

3 Sous **Système**, 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. **Bon** Fonctionnement normal. **Expiration** Le certificat va bientôt expirer. **Expiration imminente** La date d'expiration du certificat se situe dans huit mois ou moins (par défaut). **Expiration imminente** La date d'expiration du certificat se situe dans deux mois ou moins (par défaut). **Expiré** Le certificat n'est pas valide, car il a expiré.

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 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.

Conditions préalables

Vérifiez les éléments suivants :

- Les hôtes ESXi sont connectés au système vCenter Server.

- La synchronisation de l'heure est effectuée entre le système vCenter Server et les hôtes ESXi.
- La résolution DNS fonctionne entre le système vCenter Server et les hôtes ESXi.
- Les certificats MACHINE_SSL_CERT et Trusted_Root du système vCenter Server sont valides et n'ont pas expiré. Consultez l'article de la base de connaissances de VMware à l'adresse https://kb.vmware.com/s/article/2111411.
- Les hôtes ESXi ne sont pas en mode de maintenance.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Sous **Système**, 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.

Changer le mode de certificat

Utilisez VMCA pour provisionner les hôtes ESXi dans votre environnement, sauf si la stratégie d'entreprise exige que vous utilisiez des certificats personnalisés. Pour utiliser des certificats personnalisés avec une autorité de certification racine différente, vous pouvez modifier l'option avancée vCenter Server `vpxd.certmgmt.mode`. Après la modification, les hôtes ne sont plus provisionnés automatiquement avec des certificats VMCA lorsque vous actualisez les certificats. Vous êtes 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. Dans vSphere Client, sélectionnez le système vCenter Server qui gère les hôtes.
2. Cliquez sur **Configurer**, puis sous Paramètres, cliquez sur **Paramètres avancés**.
3. Cliquez sur **Modifier les paramètres**.
4. Cliquez sur l'icône **Filtre** dans la colonne Nom, et dans la zone Filtre entrez **`vpxd.certmgmt`** pour afficher uniquement les paramètres de gestion de certificat.

5 Définissez la valeur de `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 **Enregistrer**.

6 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 votre 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 les certificats par défaut par des certificats approuvés de plusieurs manières.

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.

Pour obtenir des instructions détaillées sur l'utilisation des certificats signés par une autorité de certification pour les hôtes ESXi, consultez la section Workflows de changement mode de certificat.

Note Si vous remplacez les certificats SSL sur un hôte ESXi faisant partie d'un cluster vSAN, suivez les étapes figurant dans l'article de la base de connaissances VMware https://kb.vmware.com/s/article/56441.

- Configuration requise pour les demandes de signature de certificat ESXi

  Si vous souhaitez utiliser un certificat d'entreprise ou signé par une autorité de certification tierce, vous devez envoyer une demande de signature de certificat (CRS) 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 VMware Certificate Authority (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 d'entreprise ou signé par une autorité de certification tierce, vous devez envoyer une demande de signature de certificat (CRS) à l'autorité de certification.

Utilisez une demande de signature de certificat présentant les caractéristiques suivantes :

- Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
- Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8.
- x509 version 3
- 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.

Pour d'informations sur la génération de la demande de signature de certificat, consultez l'article de la base de connaissances VMware https://kb.vmware.com/s/article/2113926.

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 Client.
- 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.

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 vCenter Server TRUSTED_ROOTS. Reportez-vous à la section 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 VMware Certificate Authority (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 Client.

- 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.

Procédure

1. Sauvegardez les certificats existants.
2. Générez une demande de certificat en suivant les instructions de l'autorité de certification.

   Reportez-vous à la section Configuration requise pour les demandes de signature de certificat ESXi.
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 nom_hôte --username nom_utilisateur --put rui.crt /host/ssl_cert
   vifs --server nom_hôte --username nom_utilisateur --put rui.key /host/ssl_key
   ```
4. Redémarrez l'hôte.

Étape suivante

Mettez à jour le magasin vCenter Server TRUSTED_ROOTS. Reportez-vous à la section 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 Client.
- 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.

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	`https://hostname/host/ssl_cert`
Clés	`https://hostname/host/ssl_key`

   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 vCenter Server TRUSTED_ROOTS. Reportez-vous à la section 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.

Note Cette étape n'est pas requise si le système vCenter Server s'exécute également avec des certificats personnalisés émis par la même autorité de certification que celle de ceux installés sur les hôtes ESXi.

Procédure

1 Connectez-vous à l'interpréteur de commandes vCenter Server du système vCenter Server qui gère les hôtes ESXi.

2 Pour ajouter les nouveaux certificats au magasin `TRUSTED_ROOTS`, exécutez `dir-cli`, par exemple :

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
```

3 Lorsque vous y êtes invité, fournissez les informations d'identification d'administrateur Single Sign-On.

4 Si vos certificats personnalisés sont émis par une autorité de certification intermédiaire, vous devez également ajouter l'autorité de certification intermédiaire au magasin TRUSTED_ROOTS sur vCenter Server, par exemple :

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
```

Étape suivante

Définissez le mode de certificat sur Personnalisé. Si le mode de certificat est VMCA (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 la section 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 à votre autorité de certification. Le certificat doit répondre aux conditions suivantes.
  - Taille de clé : de 2 048 bits (minimum) à 16 384 bits (maximum) (codée au format PEM)
  - Format PEM. VMware prend en charge PKCS8 et PKCS1 (clés RSA). Lorsque des clés sont ajoutées à VECS, elles sont converties en PKCS8.
  - x509 version 3
  - 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 trouvent dans le répertoire `/etc/vmware-rbd/ssl/`.

2 Arrêtez le service vSphere Authentication Proxy.

Outil	Étapes
Interface de gestion de vCenter Server	a Dans un navigateur Web, accédez à l'interface de gestion de vCenter Server, https://*appliance-IP-address-or-FQDN*:5480. b Connectez-vous en tant qu'utilisateur racine. Le mot de passe racine par défaut est le mot de passe que vous définissez lors du déploiement de vCenter Server. c Cliquez sur **Services**, puis sur le **service VMware vSphere Authentication Proxy**. d Cliquez sur **Arrêter**.
CLI	`service-control --stop vmcam`

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 vos fichiers de clés.

4 Sur le système sur lequel s'exécute le service Auto Deploy, exécutez la commande suivante pour mettre à jour le magasin TRUSTED_ROOTS dans VECS afin d'utiliser vos nouveaux certificats.

```
cd /usr/lib/vmware-vmafd/bin/vecs-cli
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
```

5 Créez un fichier `castore.pem` contenant ce qui se trouve dans le magasin TRUSTED_ROOTS et placez le fichier 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 ESXi du système vCenter Server sur **`Personnalisé`**.

Reportez-vous à la section 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 génère un certificat. Le serveur Auto Deploy utilise le certificat racine que vous venez d'ajouter au magasin TRUSTED_ROOTS.

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

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 les panneaux Profil de sécurité, Services et Pare-feu disponibles dans vSphere 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 **Configurer > Pare-feu** pour chaque hôte dans vSphere 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 VIB Author disponible dans VMware Labs. Pour installer le VIB personnalisé, vous devez modifier le niveau d'acceptation de l'hôte ESXi sur CommunitySupported.

  Note Si vous contactez le support technique VMware pour examiner un problème sur un hôte ESXi sur lequel un VIB CommunitySupported est installé, le support VMware peut vous demander de désinstaller ce VIB. Une telle demande est une étape de dépannage permettant de déterminer si ce VIB est lié au problème examiné.

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 Client ou sur la ligne de commande.

Cette tâche explique comment utiliser l'instance de vSphere Client pour configurer des paramètres de pare-feu ESXi. Vous pouvez utiliser les commandes d'ESXi Shell ou d'ESXCLI pour configurer ESXi sur la ligne de commande afin d'automatiser la configuration du pare-feu. Reportez-vous à *Démarrage avec ESXCLI* pour une introduction et à *Concepts et exemples d'ESXCLI* pour des exemples d'utilisation d'ESXCLI pour manipuler des pare-feu et des règles de pare-feu.

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.
2. Cliquez sur **Configurer**, puis cliquez sur **Pare-feu** sous Système.

   L'écran affiche la liste des connexions entrantes et sortantes actives avec les ports de pare-feu correspondants.
3. 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.
4. Sélectionnez les ensembles de règles à activer, ou désélectionnez ceux à désactiver.
5. Pour certains services, vous pouvez également gérer les détails du service en accédant à **Configurer > Services** sous Système.

   Pour plus d'informations sur le démarrage, l'arrêt et le redémarrage des services, reportez-vous à la section Activer ou désactiver un service.
6. Pour certains services, vous pouvez spécifier explicitement les adresses IP à partir desquelles les connexions sont autorisées.

   Reportez-vous à la section Ajouter des adresses IP autorisées pour un hôte ESXi.
7. 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 Client, ESXCLI 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. Cette tâche explique comment utiliser vSphere Client. Pour obtenir des instructions sur l'utilisation d'ESXCLI, consultez la section sur la gestion du pare-feu dans *Concepts et exemples d'ESXCLI* sur https://code.vmware.com/.

Ajout d'adresses IP autorisées au pare-feu ESXi (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_ipaddress)

Procédure

1. Connectez-vous à vCenter Server en utilisant vSphere Client.
2. Accédez à l'hôte ESXi.
3. Cliquez sur **Configurer**, puis cliquez sur **Pare-feu** sous Système.
4. Dans la section Pare-feu, cliquez sur **Modifier**, puis sélectionnez un service dans la liste.
5. 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 Client et VMware Host Client vous permettent d'ouvrir et de fermer les ports de pare-feu pour chaque service ou encore d'autoriser le trafic provenant d'adresses IP sélectionnées.

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. Pour obtenir la liste des ports et protocoles pris en charge dans le pare-feu ESXi, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/.

L'outil VMware Ports and Protocols répertorie les informations de port pour les services installés par défaut. Il est possible de disposer de services et de ports de pare-feu supplémentaires en installant d'autres VIB sur l'hôte. Ces informations s'adressent principalement aux services visibles dans vSphere Client mais l'outil VMware Ports and Protocols inclut aussi d'autres ports.

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 être 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, automatisez la configuration du pare-feu à l'aide des commandes ESXCLI ou de vSphere Web Services SDK.

Référence des commandes de pare-feu

Vous pouvez utiliser les commandes d'ESXi Shell ou d'ESXCLI pour configurer ESXi sur la ligne de commande afin d'automatiser la configuration du pare-feu. Pour obtenir une présentation, consultez *Démarrage avec ESXCLI* et, pour des exemples d'utilisation d'ESXCLI afin de gérer les pare-feux et les règles de pare-feu, consultez *Concepts et exemples ESXCLI*. Pour plus d'informations sur la création de règles de pare-feu personnalisées, reportez-vous à l'article 2008226 de la base de connaissances VMware.

Tableau 3-4. Commandes du pare-feu

Commande	Description
`esxcli network firewall get`	Renvoie l'état activé ou désactivé du pare-feu et répertorie les actions par défaut.
`esxcli network firewall set --default-action`	Définir sur True pour définir Passer comme action par défaut. Définir sur False pour définir Abandonner comme action par défaut.
`esxcli network firewall set --enabled`	Activer ou désactiver le pare-feu d'ESXi.
`esxcli network firewall load`	Charger le module du pare-feu et les fichiers de configuration d'ensemble de règles.
`esxcli network firewall refresh`	Actualiser la configuration du pare-feu en lisant les fichiers d'ensemble de règles si le module du pare-feu est chargé.
`esxcli network firewall unload`	Détruire les filtres et décharger le module du pare-feu.
`esxcli network firewall ruleset list`	Répertorier les informations des ensembles de règles.
`esxcli network firewall ruleset set --allowed-all`	Définir sur True pour permettre l'accès à toutes les adresses IP. Définir sur False pour utiliser une liste d'adresses IP autorisées.
`esxcli network firewall ruleset set --enabled --ruleset-id=<string>`	Définir la propriété sur True pour activer l'ensemble de règles spécifié. Définir la propriété sur False pour désactiver l'ensemble de règles spécifié.
`esxcli network firewall ruleset allowedip list`	Répertorier les adresses IP autorisées de l'ensemble de règles spécifié.
`esxcli network firewall ruleset allowedip add`	Autoriser l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.
`esxcli network firewall ruleset allowedip remove`	Supprimer l'accès à l'ensemble de règles à partir de l'adresse IP ou de la plage d'adresses IP spécifiée.
`esxcli network firewall ruleset rule list`	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. Si votre stratégie d'entreprise le permet, vous pouvez désactiver les services à partir du profil de sécurité ou activer les services.

Activer ou désactiver un service 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 Client.

Tableau 3-5. Services ESXi du profil de sécurité

Service	Par défaut	Description
Interface utilisateur de la console directe	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.
attestd	Arrêté	Service d'attestation de Autorité d'approbation vSphere .
kmxd	Arrêté	Service de fournisseur de clés de Autorité d'approbation vSphere .
Service Active Directory	Arrêté	Lorsque vous configurez ESXi pour Active Directory, ce service démarre.
Processus NTP	Arrêté	Démon NTP (Network Time Protocol).
Démon de carte à puce PC/SC	Arrêté	Lorsque vous activez l'hôte pour l'authentification par carte à puce, ce service démarre. Reportez-vous à la section Configuration de l'authentification par carte à puce pour ESXi.
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 *Surveillance et performances de vSphere* pour obtenir des informations sur la configuration de SNMP v1, v2 et v3.

Tableau 3-5. Services ESXi du profil de sécurité (suite)

Service	Par défaut	Description
Serveur Syslog	Arrêté	Démon Syslog. Vous pouvez activer syslog à partir des Paramètres système avancés de vSphere Client. Reportez-vous à la section *Installation et configuration de vCenter Server*.
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

Vous pouvez activer ou désactiver des services depuis vSphere Client.

Après l'installation, certains services s'exécutent par défaut, tandis que d'autres sont arrêtés. Une configuration supplémentaire est parfois nécessaire avant qu'un service devienne disponible dans l'interface utilisateur. 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 Client.

Procédure

1. Accédez à un hôte dans l'inventaire.
2. Cliquez sur **Configurer**, puis cliquez sur **Services** sous Système.
3. Sélectionnez le service que vous souhaitez modifier.
   a. Sélectionnez **Redémarrer**, **Démarrer** ou **Arrêter** pour une modification ponctuelle de l'état de l'hôte.
   b. Pour modifier l'état de l'hôte lors de redémarrages successifs, cliquez sur **Modifier la stratégie de démarrage** et sélectionnez une stratégie.
   - **Démarrer et arrêter avec hôte** : le service démarre peu après le démarrage de l'hôte, et s'arrête peu après l'arrêt de l'hôte. À l'instar de **Démarrer et arrêter avec l'utilisation de port**, cette option signifie que le service tente régulièrement d'effectuer ses tâches, telles que contacter le serveur NTP spécifié. Si le port a été fermé, mais est rouvert ultérieurement, le client commence à effectuer sa tâche peu après.
   - **Démarrer et arrêter manuellement** : l'hôte conserve les paramètres de service déterminés par l'utilisateur, que les ports soient ouverts ou non. Lorsqu'un utilisateur

démarre le service NTP, l'exécution de ce service se poursuit si 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. Lorsque l'hôte est mis sous tension, le service est redémarré, ce qui conserve l'état déterminé par l'utilisateur.

- **Démarrer et arrêter avec l'utilisation de port** : 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.

Note Ces paramètres s'appliquent uniquement aux paramètres de service configurés par le biais de l'interface utilisateur ou d'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).

4 Cliquez sur **OK**.

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.

Vous pouvez sélectionner le mode de verrouillage normal ou le mode de verrouillage strict, ce qui offre différents degrés de verrouillage. Vous pouvez également utiliser la liste des utilisateurs exceptionnels. 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.

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 Client ou de vSphere Web Services SDK.
- Le comportement de l'interface de console directe du mode de verrouillage strict et 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 présents dans la liste des utilisateurs exceptionnels peuvent accéder à l'interface DCUI s'ils disposent des privilèges d'administrateur. En outre, tous les utilisateurs qui sont spécifiés dans le paramètre système avancé `DCUI.Access` peuvent accéder à l'interface DCUI.

- Si ESXi Shell ou SSH est activé et que l'hôte est placé en mode de verrouillage, 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. Les sessions ESXi ou SSH des utilisateurs qui ne disposent pas de privilèges d'administrateur sont fermées.

Tout accès est connecté à la fois pour le mode de verrouillage strict et normal.

Tableau 3-6. Comportement du mode de verrouillage

Service	Mode normal	Mode de verrouillage normal	Mode de 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.
ESXi Shell (s'il est activé) et 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

Les utilisateurs peuvent se connecter à ESXi Shell ou accéder à l'hôte via SSH avant que le mode de verrouillage soit activé. Dans ce cas, les utilisateurs présents dans la liste des utilisateurs exceptionnels et disposant de privilèges d'administrateur sur l'hôte restent connectés. La session est fermée pour tous les autres utilisateurs. Ce comportement s'applique à la fois au mode de verrouillage normal et strict.

Activer le mode verrouillage

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.

Si vous souhaitez 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 la section Comportement du mode de verrouillage.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
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
Normal	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 est activé, il peut être possible d'y accéder.
Strict	Vous ne pouvez accéder à l'hôte que via vCenter Server. Si SSH ou ESXi Shell est activé, 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 fermées.

6. Cliquez sur **OK**.

Désactiver le mode de verrouillage

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.

Vous pouvez désactiver le mode de verrouillage comme suit :

Depuis l'interface utilisateur graphique

Les utilisateurs peuvent désactiver à la fois le mode de verrouillage normal et strict dans vSphere 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 un hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, sélectionnez **Profil de sécurité**.
4. Dans le panneau mode verrouillage, cliquez sur **Modifier**.
5. Cliquez sur **Mode verrouillage** et sélectionnez **Désactiver** pour désactiver le mode de verrouillage.
6. Cliquez sur **OK**.

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 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.

Les autorisations de l'utilisateur sont conservées lorsque vous activez le mode de verrouillage. Les autorisations de l'utilisateur sont restaurées lorsque vous désactivez le mode de verrouillage à partir de l'interface de la 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 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 la 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.

La version vSphere détermine ce que les différents comptes peuvent faire par défaut lorsque le mode de verrouillage est activé et comment vous pouvez modifier le comportement par défaut.

- Dans vSphere 5.0 et versions antérieures, 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. L'option est utilisée en cas de défaillance irrémédiable de vCenter Server. Les sociétés verrouillent généralement le mot de passe de l'utilisateur disposant de cet accès dans un coffre-fort. Un utilisateur figurant dans 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 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 perdre leurs autorisations lorsque l'hôte est en mode de verrouillage.

Option avancée Ajouter des utilisateurs à DCUI.Access

En cas de défaillance irrémédiable, l'option avancée `DCUI.Access` vous permet de quitter le mode de verrouillage lorsque vous ne pouvez pas accéder à l'hôte depuis vCenter Server. Vous ajoutez des utilisateurs à la liste en modifiant les paramètres avancés de l'hôte à partir de vSphere Client.

Note Les utilisateurs de la liste DCUI.Access peuvent modifier les paramètres du mode de verrouillage, quels que soient leurs privilèges. La possibilité de changer les modes de verrouillage peut affecter 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 la section Spécifier les utilisateurs exceptionnels du mode de verrouillage.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans la section Système, cliquez sur **Paramètres système avancés**, puis sur **Modifier**.
4. Appliquez le filtre à l'interface DCUI.
5. Dans la zone de texte **DCUI.Access**, entrez les noms d'utilisateur ESXi locaux, séparés par des virgules.

   L'utilisateur racine est inclus par défaut. Pensez à supprimer l'utilisateur racine de la liste DCUI.Access et à spécifier un compte nommé pour un meilleur contrôle.
6. Cliquez sur **OK**.

Spécifier les utilisateurs exceptionnels du mode de verrouillage

Vous pouvez ajouter des utilisateurs à la liste des utilisateurs exceptionnels depuis vSphere 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 Client.
2. Cliquez sur **Configurer**.
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 **Ajouter utilisateur** pour ajouter des utilisateurs exceptionnels.

Vérifier les niveaux d'acceptation des hôtes et des fichiers VIB

Le niveau d'acceptation d'un VIB dépend du montant de certification de ce VIB. Le niveau d'acceptation de l'hôte dépend du niveau du VIB inférieur. Si vous souhaitez autoriser des VIB de niveau inférieur, vous pouvez modifier le niveau d'acceptation de l'hôte. Vous pouvez supprimer les VIB CommunitySupported pour modifier le niveau d'acceptation de l'hôte.

Les VIB sont des modules logiciels qui incluent une signature de VMware ou d'un partenaire VMware. 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.

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. Par exemple, si le niveau d'acceptation de l'hôte est VMwareAccepted, vous ne pouvez pas installer les VIB au niveau PartnerSupported. Vous pouvez utiliser des commandes ESXCLI pour définir le niveau de l'acceptation d'un 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.

Le niveau d'acceptation d'un hôte ESXi s'affiche dans le **Profil de sécurité** dans vSphere Client.

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. Aujourd'hui, seuls les pilotes de programmes IOVP (I/O Vendor Program) 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 invite les clients disposant d'appels d'assistance pour les VIB avec ce niveau d'acceptation à contacter 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 invite les clients disposant d'appels d'assistance pour les VIB avec ce niveau d'acceptation à contacter 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, VMwareAccepted ou PartnerSupported en exécutant la commande suivante.

```
esxcli software acceptance get
```

2 Si le niveau d'acceptation de l'hôte est CommunitySupported, déterminez si un ou plusieurs VIB sont au niveau CommunitySupported en exécutant les commandes suivantes.

```
esxcli software vib list
esxcli software vib get –n vibname
```

3 Supprimez les VIB CommunitySupported en exécutant la commande suivante.

```
esxcli software vib remove --vibname vib
```

4 Modifiez le niveau d'acceptation de l'hôte en utilisant l'une des méthodes suivantes.

Option	Description
Commande de l'interface de ligne de commande	`esxcli software acceptance set --level level` Le paramètre `level` est nécessaire et spécifie le niveau d'acceptation à définir. Les niveaux possibles sont les suivants : **`VMwareCertified`**, **`VMwareAccepted`**, **`PartnerSupported`** ou **`CommunitySupported`**. Consultez *Référence d'ESXCLI* pour plus d'informations.
vSphere Client	a Sélectionnez un hôte dans l'inventaire. b Cliquez sur **Configurer**. c Dans Système, sélectionnez **Profil de sécurité**. d Cliquez sur **Modifier** pour le niveau d'acceptation du profil d'image hôte et choisissez le niveau d'acceptation.

Résultats

Le nouveau niveau d'acceptation est en vigueur.

Note ESXi effectue des vérifications d'intégrité des VIB régis par le niveau d'acceptation. Vous pouvez utiliser le paramètre `VMkernel.Boot.execInstalledOnly` pour demander à ESXi d'exécuter uniquement les binaires provenant d'un VIB valide installé sur l'hôte. Combiné au démarrage sécurisé, ce paramètre garantit que chaque processus exécuté sur un hôte ESXi est signé, autorisé et attendu. Par défaut, le paramètre `VMkernel.Boot.execInstalledOnly` est désactivé pour la compatibilité des partenaires dans vSphere 7. L'activation de ce paramètre lorsque cela est possible améliore la sécurité. Pour plus d'informations sur la configuration des options avancées pour ESXi, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/1038578.

Attribution de privilèges pour les hôtes 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 Client.

Vous pouvez sélectionner l'objet hôte ESXi dans la hiérarchie d'objets vCenter Server et attribuer le rôle d'administrateur à un nombre limité d'utilisateurs. Ces utilisateurs peuvent ensuite effectuer une gestion directe sur l'hôte ESXi. Reportez-vous à la section 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

Dans l'onglet Gestion de VMware Host Client, vous pouvez ajouter des utilisateurs locaux et définir des rôles personnalisés. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

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. Ce rôle est le rôle par défaut. Vous pouvez remplacer le rôle par défaut.

Vous pouvez gérer les utilisateurs et les groupes locaux et ajouter des rôles personnalisés locaux à un hôte ESXi à l'aide d'une instance de VMware Host Client directement connectée à l'hôte ESXi. Consultez la documentation de *Gestion individuelle des hôtes vSphere - VMware Host Client*.

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'utilisateur ESXi, il n'est pas attribué à l'utilisateur vCenter Server.

Privilèges prédéfinis

Si votre environnement ne comprend pas de système vCenter Server, les utilisateurs suivants sont prédéfinis.

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.

L'attribution du privilège d'utilisateur racine peut faciliter l'accès à un hôte ESXi, car le nom est déjà connu. Un compte racine commun rend également plus difficile la mise en correspondance des actions avec les utilisateurs.

Pour optimiser l'audit, créez des comptes individuels avec des privilèges d'administrateur. 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. Pour plus d'informations sur l'attribution d'autorisations à un utilisateur pour un hôte ESXi, consultez la documentation *Gestion individuelle des hôtes vSphere - VMware Host Client*.

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 fonctionnalités Active Directory d'ESXi, qui vous permettent de gérer les informations d'identification Active Directory.

Important Vous pouvez supprimer les privilèges d'accès pour l'utilisateur racine. Cependant, vous devez d'abord créer une autre autorisation au niveau de la racine, puisqu'un autre utilisateur est affecté au rôle d'administrateur.

Utilisateur vpxuser

vCenter Server utilise les privilèges vpxuser pour gérer les activités de l'hôte.

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. Seul un utilisateur disposant des privilèges d'administrateur peut effectuer ces tâches directement sur un 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.

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.

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 la section 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 l'heure entre ESXi et le système de service d'annuaire.

   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 l'inventaire de vSphere Client.
   b. Cliquez sur **Configurer**.
   c. Sous Mise en réseau, cliquez sur **Configuration TCP/IP**.
   d. Sous Pile TCP/IP : par défaut, cliquez sur **DNS** et vérifiez que le nom d'hôte et les informations relatives au serveur DNS de l'hôte sont correctes.

Étape suivante

Joignez l'hôte à un domaine de service d'annuaire. Reportez-vous à Ajouter un hôte à un domaine de service d'annuaire. Pour les hôtes provisionnés avec Auto Deploy, configurez vSphere Authentication Proxy. Reportez-vous à Utiliser vSphere Authentication Proxy. Vous pouvez configurer les autorisations afin que des utilisateurs et des groupes du domaine Active Directory joint puissent accéder aux composants de vCenter Server. Pour plus d'informations sur la gestion des autorisations, reportez-vous à Ajouter une autorisation à un objet d'inventaire .

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 conteneur 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 un hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
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.

Étape suivante

Vous pouvez configurer les autorisations afin que des utilisateurs et des groupes du domaine Active Directory joint puissent accéder aux composants de vCenter Server. Pour plus d'informations sur la gestion des autorisations, reportez-vous à Ajouter une autorisation à un objet d'inventaire .

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 Client.
2. Cliquez sur **Configurer**.
3. Sous Système, sélectionnez **Services d'authentification**.

   La page Services d'authentification affiche le service d'annuaire et les paramètres du domaine.

Étape suivante

Vous pouvez configurer les autorisations afin que des utilisateurs et des groupes du domaine Active Directory joint puissent accéder aux composants de vCenter Server. Pour plus d'informations sur la gestion des autorisations, reportez-vous à Ajouter une autorisation à un objet d'inventaire .

Utiliser vSphere Authentication Proxy

Vous pouvez ajouter des hôtes ESXi à un domaine Active Directory en utilisant vSphere Authentication Proxy plutôt que d'ajouter les hôtes explicitement au domaine Active Directory.

Vous devez simplement configurer l'hôte de sorte qu'il connaisse le nom de domaine du serveur Active Directory et l'adresse IP de vSphere Authentication Proxy. Lorsque vSphere Authentication Proxy est activé, il ajoute automatiquement les hôtes qui sont en cours de provisionnement avec Auto Deploy au domaine Active Directory. Vous pouvez également utiliser vSphere Authentication Proxy avec des hôtes qui ne sont pas provisionnés en utilisant Auto Deploy.

Pour plus d'informations sur les ports TCP utilisés par vSphere Authentication Proxy, reportez-vous à la section Ports requis pour vCenter Server.

Auto Deploy

Si vous provisionnez des hôtes avec Auto Deploy, vous pouvez configurer un hôte de référence qui pointe vers Authentication Proxy. Vous pouvez configurer une règle qui applique le profil de l'hôte de référence à un hôte ESXi qui est provisionné avec Auto Deploy. vSphere Authentication Proxy stocke les adresses IP de tous les hôtes qu'Auto Deploy provisionne à l'aide de PXE dans sa liste de contrôle d'accès. Lorsque l'hôte démarre, il contacte vSphere Authentication Proxy, et vSphere Authentication Proxy joint ces hôtes, qui se trouvent déjà dans sa liste de contrôle d'accès, sur le domaine Active Directory.

Même si vous utilisez vSphere Authentication Proxy dans un environnement utilisant des certificats provisionnés par VMCA ou des certificats tiers, le processus se déroule de manière

transparente si vous suivez les instructions d'utilisation des certificats personnalisés avec Auto Deploy.

Reportez-vous à la section Utiliser des certificats personnalisés avec Auto Deploy.

Autres hôtes ESXi

Vous pouvez configurer d'autres hôtes pour qu'ils utilisent vSphere Authentication Proxy si vous souhaitez que l'hôte puisse joindre le domaine sans utiliser les informations d'identification Active Directory. Cela signifie que vous n'avez pas besoin de transmettre les informations d'identification d'Active Directory à l'hôte, et que vous n'enregistrez pas les informations d'identification d'Active Directory dans le profil hôte.

Dans ce cas, vous ajoutez l'adresse IP de l'hôte à la liste de contrôle d'accès de vSphere Authentication Proxy, et vSphere Authentication Proxy autorise l'hôte basé sur son adresse IP par défaut. Vous pouvez activer l'autentification client de sorte que vSphere Authentication Proxy vérifie le certificat de l'hôte.

Note Vous ne pouvez pas utiliser vSphere Authentication Proxy dans un environnement qui prend uniquement en charge IPv6.

Activer vSphere Authentication Proxy

Le service vSphere Authentication Proxy est disponible sur chaque système vCenter Server. Par défaut, ce service ne s'exécute pas. Si vous souhaitez utiliser vSphere Authentication Proxy dans votre environnement, vous pouvez démarrer ce service depuis l'interface de gestion de vCenter Server ou depuis la ligne de commande.

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 vCenter Server peut être sur une machine hôte dans un environnement réseau exclusivement IPv4 ou mixte, IPv4/IPv6. Cependant, lorsque vous spécifiez l'adresse de vSphere Authentication Proxy, vous devez spécifier une adresse IPv4.

Conditions préalables

Vous devez utiliser vCenter Server 6.5 ou une version plus récente. Dans les versions précédentes de vSphere, vSphere Authentication Proxy est installé séparément. Reportez-vous à la documentation de la version précédente du produit pour connaître les instructions.

Procédure

1 Démarrez le service VMware vSphere Authentication Proxy.

Option	Description
Interface de gestion de vCenter Server	a Dans un navigateur Web, accédez à l'interface de gestion de vCenter Server, https://*appliance-IP-address-or-FQDN*:5480. b Connectez-vous en tant qu'utilisateur racine. Le mot de passe racine par défaut est le mot de passe que vous définissez lors du déploiement de vCenter Server. c Cliquez sur **Services**, puis sur le service **VMware vSphere Authentication Proxy**. d Cliquez sur **Démarrer**. e (Facultatif) Une fois le service démarré, cliquez sur **Définir le type de démarrage** et cliquez sur **Automatique** pour démarrer automatiquement le service par la suite.
CLI	`service-control --start vmcam`

2 Vérifiez que le service a démarré correctement.

Résultats

Vous pouvez désormais définir le domaine vSphere Authentication Proxy. Ensuite, vSphere Authentication Proxy traite tous les hôtes qui sont provisionnés avec Auto Deploy et vous pouvez ajouter explicitement des hôtes à vSphere Authentication Proxy.

Ajouter un domaine à vSphere Authentication Proxy avec vSphere Client

Vous pouvez ajouter un domaine vSphere Authentication Proxy depuis vSphere Client ou en exécutant la commande `camconfig`.

Vous pouvez ajouter un domaine à vSphere Authentication Proxy uniquement après avoir activé le proxy. Dès que vous avez ajouté le domaine, vSphere Authentication Proxy ajoute à celui-ci tous les hôtes que vous provisionnez avec Auto Deploy. Pour les autres hôtes, vous pouvez également utiliser vSphere Authentication Proxy si vous ne souhaitez pas leur accorder des privilèges de domaine.

Procédure

1 Connectez-vous à un système vCenter Server avec vSphere Client.

2 Sélectionnez l’instance de vCenter Server, puis cliquez sur **Configurer**.

3 Cliquez sur **proxy d'authentification**, puis sur **Modifier**.

4 Entrez le nom du domaine dans lequel le service vSphere Authentication Proxy ajoutera les hôtes, ainsi que le nom et le mot de passe d'un utilisateur qui dispose de privilèges Active Directory permettant d'ajouter des hôtes dans ce domaine.

5 Cliquez sur **Enregistrer**.

Ajouter un domaine à vSphere Authentication Proxy avec la commande camconfig

Vous pouvez ajouter un domaine à vSphere Authentication à l'aide de la commande `camconfig`.

Vous pouvez ajouter un domaine à vSphere Authentication Proxy uniquement après avoir activé le proxy. Dès que vous avez ajouté le domaine, vSphere Authentication Proxy ajoute à celui-ci tous les hôtes que vous provisionnez avec Auto Deploy. Pour les autres hôtes, vous pouvez également utiliser vSphere Authentication Proxy si vous ne souhaitez pas leur accorder des privilèges de domaine.

Procédure

1 Connectez-vous au système vCenter Server en tant qu'utilisateur disposant des privilèges d'administrateur.

2 Exécutez la commande pour activer l'accès à l'interpréteur de commandes de dépistage.

```
shell
```

3 Accédez au répertoire `/usr/lib/VMware-vmcam/bin/` dans lequel se trouve le script **camconfig**.

4 Pour ajouter le domaine et les informations d'identification Active Directory à la configuration du serveur proxy d'authentification, exécutez la commande suivante.

```
camconfig add-domain -d domain -u user
```

Vous êtes invité à entrer un mot de passe.

vSphere Authentication Proxy place en mémoire cache ce nom d'utilisateur et ce mot de passe. Vous pouvez supprimer et recréer l'utilisateur en fonction des besoins. Le domaine doit être accessible par DNS, mais ne doit pas nécessairement être une source d'identité vCenter Single Sign-On.

vSphere Authentication Proxy utilise le nom d'utilisateur spécifié par l'*utilisateur* pour créer les comptes destinés aux hôtes ESXi dans Active Directory. L'utilisateur doit disposer de privilèges suffisants pour créer des comptes dans le domaine Active Directory auquel vous ajoutez les hôtes. Lors de la rédaction de ce manuel, l'article 932455 de la base de connaissances Microsoft disposait des informations nécessaires concernant les privilèges de création de compte.

5 Si vous décidez par la suite de supprimer les informations relatives au domaine et à l'utilisateur de vSphere Authentication Proxy, exécutez la commande suivante.

```
camconfig remove-domain -d domain
```

Utiliser vSphere Authentication Proxy pour ajouter un hôte à un domaine

Le serveur Auto Deploy ajoute tous les hôtes qu'il provisionne à vSphere Authentication Proxy, et vSphere Authentication Proxy ajoute ces hôtes au domaine. Si vous voulez ajouter d'autres hôtes à un domaine à l'aide de vSphere Authentication Proxy, vous pouvez ajouter explicitement ces hôtes à vSphere Authentication Proxy. Le serveur vSphere Authentication Proxy ajoute ensuite ces hôtes au domaine. Par conséquent, les informations d'identification fournies par l'utilisateur n'ont plus besoin d'être transmises au système vCenter Server.

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 conteneur 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

- Si ESXi utilise un certificat signé par VMCA, vérifiez que l'hôte a été ajouté à vCenter Server. Dans le cas contraire, le service Authentication Proxy ne peut pas approuver l'hôte ESXi.
- Si l'hôte ESXi utilise un certificat racine signé par une autorité de certification, vérifiez que le certificat approprié a été ajouté au système vCenter Server. Reportez-vous à la section Gestion de certificats pour les hôtes ESXi.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans la section **Système**, sélectionnez **Services d'authentification**.
4. Cliquez sur **Joindre le domaine**.
5. Entrez un domaine.

   Utilisez le formulaire **`name.tld`**, par exemple **`mydomain.com`**, ou **`name.tld/container/path`**, par exemple, **`mydomain.com/organizational_unit1/organizational_unit2`**.
6. Sélectionnez **Utilisation du serveur proxy**.
7. Entrez l'adresse IP du serveur Authentication Proxy, qui est toujours la même que l'adresse IP du système vCenter Server.
8. Cliquez sur **OK**.

Activer l'authentification du client pour vSphere Authentication Proxy

Par défaut, vSphere Authentication Proxy ajoute les hôtes lorsqu'il dispose de leur adresse dans sa liste de contrôle d'accès. Pour une sécurité renforcée, vous pouvez activer l'authentification

du client. Lorsque l'authentification du client est activée, vSphere Authentication Proxy vérifie également le certificat de l'hôte.

Conditions préalables

- Assurez-vous que le système vCenter Server considère l'hôte comme fiable. Par défaut, lorsque vous ajoutez un hôte dans vCenter Server, cet hôte est associé à un certificat qui est signé par une autorité de certification racine fiable de vCenter Server. vSphere Authentication Proxy fait confiance à l'autorité de certification racine fiable de vCenter Server.
- Si vous prévoyez de remplacer les certificats ESXi dans votre environnement, effectuez ce remplacement avant d'activer vSphere Authentication Proxy. Les certificats de l'hôte ESXi doivent correspondre à ceux de l'enregistrement de l'hôte.

Procédure

1. Connectez-vous au système vCenter Server en tant qu'utilisateur disposant des privilèges d'administrateur.
2. Exécutez la commande pour activer l'accès à l'interpréteur de commandes de dépistage.

   ```
   shell
   ```

3. Accédez au répertoire `/usr/lib/VMware-vmcam/bin/` dans lequel se trouve le script **camconfig**.
4. L'exécution de la commande suivante permet d'activer l'authentification du client.

   ```
   camconfig ssl-cliAuth -e
   ```

   Ensuite, vSphere Authentication Proxy vérifie le certificat de tout nouvel hôte.
5. Si vous décidez par la suite de désactiver l'authentification de l'hôte, exécutez la commande suivante.

   ```
   camconfig ssl-cliAuth -n
   ```

Importer le certificat vSphere Authentication Proxy sur l'hôte ESXi

Par défaut, les hôtes ESXi nécessitent une vérification explicite du certificat vSphere Authentication Proxy. Si vous utilisez vSphere Auto Deploy, le service Auto Deploy se charge d'ajouter le certificat dans les hôtes qu'il provisionne. Pour les autres hôtes, vous devez ajouter le certificat de façon explicite.

Conditions préalables

- Téléchargez le certificat de vSphere Authentication Proxy vers une banque de données accessible à l'hôte de ESXi. À l'aide d'une application SFTP telle que WinSCP, vous pouvez télécharger le certificat de l'hôte vCenter Server à l'emplacement suivant.

  `/var/lib/vmware/vmcam/ssl/rui.crt`

- Assurez-vous que le paramètre avancé `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi est défini sur 1 (valeur par défaut).

Procédure

1. Sélectionnez l'hôte ESXi et cliquez sur **Configurer**.
2. Dans la section **Système**, sélectionnez **Services d'authentification**.
3. Cliquez sur **Importer un certificat**.
4. Entrez le chemin du fichier de certificat au format [*banque de données*]/*chemin/nom du certificat*.crt et cliquez sur **OK**.

Générer un nouveau certificat pour vSphere Authentication Proxy

Vous pouvez générer un nouveau certificat provisionné par VMCA ou un nouveau certificat incluant VMCA en tant que certificat subordonné.

Reportez-vous à Configurer vSphere Authentication Proxy pour utiliser des certificats personnalisés si vous souhaitez utiliser des certificats personnalisés qui sont signés par une autorité de certification tierce ou d'entreprise.

Conditions préalables

Vous devez disposer de privilèges racine ou d'administration dans le système qui sert à exécuter vSphere Authentication Proxy.

Procédure

1. Créez une copie de `certool.cfg`.

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2. Modifiez cette copie avec des informations sur votre organisation, comme dans l'exemple suivant.

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3. Générez la nouvelle clé privée dans `/var/lib/vmware/vmcam/ssl/`.

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

Pour *localhost*, fournissez le nom de domaine complet de vCenter Server.

4 Générez le nouveau certificat dans `/var/lib/vmware/vmcam/ssl/`, en utilisant la clé et le fichier `vmcam.cfg` que vous avez créés au cours des étapes 1 et 2.

```
/usr/lib/vmware-vmca/bin/certool --server=localhost --gencert --privkey=/var/lib/vmware/vmcam/ssl/
rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/vmcam/ssl/vmcam.cfg
```

Pour *localhost*, fournissez le nom de domaine complet de vCenter Server.

Configurer vSphere Authentication Proxy pour utiliser des certificats personnalisés

L'utilisation des certificats personnalisés avec vSphere Authentication Proxy se compose de plusieurs étapes. Tout d'abord, vous générez une demande de signature de certificat (CSR) et vous l'envoyez à votre autorité de certification pour signature. Ensuite, vous placez le certificat signé et le fichier de clé dans un emplacement auquel vSphere Authentication Proxy peut accéder.

Par défaut, vSphere Authentication Proxy génère un CSR lors du premier démarrage et demande à VMCA de signer ce CSR. vSphere Authentication Proxy s'enregistre avec vCenter Server à l'aide de ce certificat. Vous pouvez utiliser des certificats personnalisés dans votre environnement, si vous ajoutez ces certificats à vCenter Server.

Procédure

1 Générez un CSR pour vSphere Authentication Proxy.

a Créez un fichier de configuration, `/var/lib/vmware/vmcam/ssl/vmcam.cfg`, comme dans l'exemple suivant.

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:dns.static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

b Exécutez `openssl` pour générer un fichier CSR et un fichier de clé, en transitant par le fichier de configuration.

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/vmcam/ssl/
rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

2 Sauvegardez le certificat `rui.crt`, ainsi que les fichiers `rui.key`, qui sont stockés à l'emplacement suivant.

`/var/lib/vmware/vmcam/ssl/rui.crt`

3 Annulez l'enregistrement de vSphere Authentication Proxy.

a Accédez au répertoire `/usr/lib/vmware-vmcam/bin/` dans lequel se trouve le script `camregister`.

b Exécutez la commande suivante.

```
camregister --unregister -a VC_address -u user
```

user doit être un utilisateur vCenter Single Sign-On disposant d'autorisations d'administrateur sur vCenter Server.

4 Arrêtez le service vSphere Authentication Proxy.

Outil	Étapes
Interface de gestion de la configuration de vCenter Server	a Dans un navigateur Web, accédez à l'interface de gestion de la configuration de vCenter Server, https://*vcenter-IP-address-or-FQDN*:5480. b Connectez-vous en tant qu'utilisateur racine. Le mot de passe racine par défaut est le mot de passe que vous définissez lors du déploiement de vCenter Server. c Cliquez sur **Services**, puis sur le **service VMware vSphere Authentication Proxy**. d Cliquez sur **Arrêter**.
CLI	`service-control --stop vmcam`

5 Remplacez le certificat `rui.crt` et les fichiers `rui.key` existants par les fichiers que vous avez reçus de votre autorité de certification.

6 Redémarrez le service vSphere Authentication Proxy.

7 Réenregistrez vSphere Authentication Proxy explicitement avec vCenter Server en utilisant le nouveau certificat et la clé.

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k full_path_to_rui.key
```

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 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 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 code PIN. Cette invite remplace l'invite par défaut qui 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 code 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 Client pour ajouter des certificats racines. Reportez-vous à la section Gestion de certificats pour les hôtes ESXi.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
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).

   Les certificats doivent être au format PEM.
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. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
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**.

S'authentifier avec le nom d'utilisateur et le mot de passe 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. Dans ce cas, vous pouvez vous connecter à l'interface DCUI ESXi en utilisant les informations d'identification d'un utilisateur administrateur local d'ESXi. Une fois connecté, vous pouvez exécuter des diagnostics ou toute autre mesure d'urgence. 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 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.

Utilisation du ESXi Shell

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.

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 à ESXi Shell.

SSH

Activez ce service pour accéder à ESXi Shell à distance en utilisant SSH.

L'utilisateur racine et les utilisateurs disposant du rôle d'administrateur peuvent accéder à 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 ESXi Shell si n'avez pas réellement besoin d'un accès.

- Activer l'accès à ESXi Shell

  Les interfaces ESXi Shell et SSH sont désactivées par défaut. Maintenez ces interfaces désactivées, sauf si vous effectuez des activités de dépannage ou de prise en charge. Pour les activités quotidiennes, utilisez vSphere Client, où l'activité est soumise à des méthodes de contrôle d'accès basé sur les rôles et modernes.

- Utiliser l'interface utilisateur de la console directe 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 service ESXi Shell pour une opération de dépannage

  Effectuez les tâches de configuration d'ESXi avec vSphere Client, ESXCLI ou VMware PowerCLI. Connectez-vous au ESXi Shell (anciennement mode support technique ou TSM) uniquement à des fins de dépannage.

Activer l'accès à ESXi Shell

Les interfaces ESXi Shell et SSH sont désactivées par défaut. Maintenez ces interfaces désactivées, sauf si vous effectuez des activités de dépannage ou de prise en charge. Pour les activités quotidiennes, utilisez vSphere Client, où l'activité est soumise à des méthodes de contrôle d'accès basé sur les rôles et modernes.

Note Accédez à l'hôte à l'aide de vSphere Client, d'outils de ligne de commande à distance (ESXCLI 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.
2. Cliquez sur **Configurer**, puis cliquez sur **Services** sous Système.
3. Gérez les services ESXi, SSH ou d'interface utilisateur de la console directe (DCUI).
   a. Dans le volet Services, sélectionnez le service.
   b. Cliquez sur **Modifier la stratégie de démarrage** et sélectionnez la stratégie de démarrage **Démarrer et arrêter manuellement**.
   c. Pour activer le service, cliquez sur **Démarrer**.

   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**.

Étape suivante

Définissez le délai d'attente de disponibilité et le délai d'inactivité pour ESXi Shell. Reportez-vous aux sections Créer un délai d'attente de disponibilité pour ESXi Shell et Créer un délai d'expiration pour des sessions ESXi Shell inactives.

Créer un délai d'attente de disponibilité pour ESXi Shell

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 votre connexion suite à l'activation d'ESXi Shell. Lorsque le délai est écoulé, le service est désactivé et les utilisateurs ne peuvent plus se connecter.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, sélectionnez **Paramètres système avancés**.
4. Cliquez sur **Modifier** et sélectionnez `UserVars.ESXiShellTimeOut`.
5. Entrez la valeur 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 des sessions ESXi Shell inactives

Si vous activez ESXi Shell sur un hôte, mais que vous oubliez de vous déconnecter de la session, la session inactive demeure connectée indéfiniment. La connexion restée ouverte augmente 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 Client.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, sélectionnez **Paramètres système avancés**.
4. Cliquez sur **Modifier**, sélectionnez `UserVars.ESXiShellInteractiveTimeOut` et entrez le paramètre de délai d'expiration.

   Une valeur de zéro (0) désactive le délai d'inactivité.
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 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 (DCUI) pour activer l'accès local et distant au service ESXi Shell. Accédez à l'interface DCUI (Direct Console User Interface) à partir de la console physique attachée à l'hôte. Après le redémarrage de l'hôte et le chargement d'ESXi, appuyez sur F2 pour vous connecter à l'interface DCUI. Entrez les informations d'identification que vous avez créées lors de l'installation d'ESXi.

Note Les modifications apportées à l'hôte en utilisant l'interface utilisateur de la console directe, vSphere 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. Si l'hôte échoue avant que les modifications ne soient validées, celles-ci risquent d'être perdues.

Procédure

1. Depuis 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 pour ESXi Shell. Reportez-vous à la section Définir le délai d'expiration de disponibilité ou le délai d'inactivité de ESXi Shell.

Définir le délai d'expiration de disponibilité ou le délai d'inactivité de ESXi Shell

ESXi Shell est désactivé par défaut. Pour renforcer la sécurité lorsque vous activez l'interpréteur de commandes, vous pouvez définir un délai d'attente de disponibilité, un délai d'inactivité ou les deux.

Les deux types de délais d'expiration s'appliquent selon différentes situations.

Délai d'inactivité

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 cette situation en paramétrant un délai d'expiration des sessions inactives.

Délai d'expiration de la disponibilité

Le délai d'attente de disponibilité détermine le délai pouvant s'écouler avant que vous vous connectiez après avoir activé initialement l'interpréteur de commandes. Si vous dépassez ce délai, le service est désactivé et vous ne pouvez pas vous connecter à ESXi Shell.

Conditions préalables

Activez le ESXi Shell. Reportez-vous à la section Utiliser l'interface utilisateur de la console directe pour activer l'accès au service ESXi Shell.

Procédure

1 Connectez-vous à ESXi Shell.

2 Dans le menu des options de mode de dépannage, sélectionnez **Modifier les délais d'ESXi Shell et de SSH** et cliquez sur Entrée.

3 Entrez le délai d'inactivité (en secondes) ou 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.

4 Appuyez sur Entrée et Échap jusqu'à ce que vous reveniez au menu principal de l'interface utilisateur de console directe.

5 Cliquez sur **OK**.

Résultats

- Si vous définissez le délai d'inactivité, les utilisateurs sont déconnectés une fois la session devenue inactive pendant la durée spécifiée.
- Si vous définissez le délai d'attente de disponibilité, mais que vous ne vous connectez pas avant que ce délai d'expiration soit écoulé, les connexions sont à nouveau désactivées.

Connexion au service ESXi Shell pour une opération de dépannage

Effectuez les tâches de configuration d'ESXi avec vSphere Client, ESXCLI ou VMware 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.

Démarrage sécurisé UEFI des hôtes ESXi

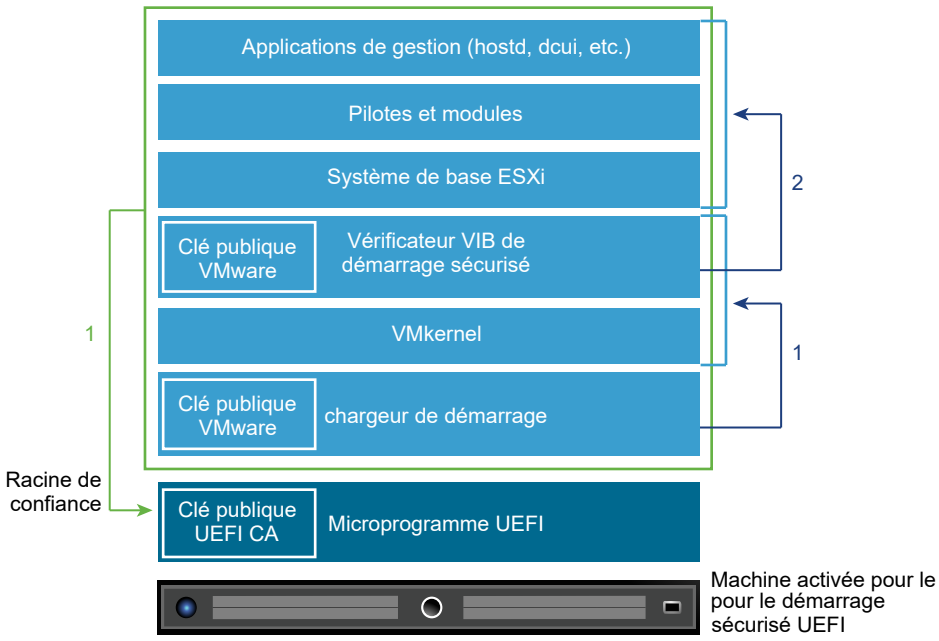
Le démarrage sécurisé est une fonctionnalité standard du microprogramme UEFI. Lorsque le démarrage sécurisé est activé, si le chargeur de démarrage du système d'exploitation n'est pas signé par chiffrement, la machine refuse de charger un pilote ou une application UEFI. À partir de vSphere 6.5, ESXi prend en charge le démarrage sécurisé s'il est activé dans le matériel.

Présentation du démarrage sécurisé UEFI

ESXi 6.5 et versions ultérieures prend en charge le démarrage sécurisé UEFI à chaque niveau de la pile de démarrage.

Note Avant d'utiliser le démarrage sécurisé UEFI sur un hôte qui a été mis à niveau, vérifiez la compatibilité en suivant les instructions de la section Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau.

Figure 3-1. Démarrage sécurisé UEFI



Lorsque le démarrage sécurisé est activé, la séquence de démarrage se déroule de la manière suivante.

1 À partir de vSphere 6.5, le chargeur de démarrage ESXi contient une clé publique VMware. Le chargeur de démarrage utilise cette clé pour vérifier la signature du noyau et un petit sous-ensemble du système incluant un vérificateur VIB de démarrage sécurisé.

2 Le vérificateur VIB vérifie chaque module VIB installé sur le système.

L'ensemble du système démarre alors, avec la racine d'approbation dans les certificats faisant partie du microprogramme UEFI.

Note Lorsque vous installez ou mettez à niveau vers vSphere 7.0 Update 2 et qu'un hôte ESXi dispose d'un TPM, le TPM scelle les informations sensibles en utilisant une stratégie TPM basée sur des valeurs PCR pour le démarrage sécurisé UEFI. Cette valeur est chargée lors des redémarrages suivants si la stratégie est satisfaite avec la valeur true. Pour désactiver ou activer le démarrage sécurisé UEFI dans vSphere 7.0 Update 2, consultez Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée.

Dépannage du démarrage sécurisé UEFI

Si le démarrage sécurisé échoue à un niveau de la séquence de démarrage, une erreur se produit.

Le message d'erreur dépend du fournisseur du matériel et du niveau où la vérification a échoué.

- Si vous tentez de démarrer la machine avec un chargeur de démarrage non signé ou qui a été falsifié, une erreur se produit lors de la séquence de démarrage. Le message exact dépend du fournisseur du matériel. Il peut être similaire au message d'erreur suivant.

  ```
  UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
  ```

- Si le noyau a été falsifié, une erreur similaire à la suivante se produit.

  ```
  Fatal error: 39 (Secure Boot Failed)
  ```

- Si un module (VIB ou pilote) a été falsifié, un écran violet avec le message suivant s'affiche.

  ```
  UEFI Secure Boot failed:
  Failed to verify signatures of the following vibs (XX)
  ```

Pour résoudre les problèmes de démarrage sécurisé, suivez la procédure suivante.

1 Redémarrez l'hôte avec le démarrage sécurisé désactivé.

2 Exécutez le script de vérification du démarrage sécurisé (voir Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau).

3 Examinez les informations dans le fichier `/var/log/esxupdate.log`.

Exécuter le script de validation du démarrage sécurisé sur un hôte ESXi mis à niveau

Après la mise à niveau d'un hôte ESXi depuis une ancienne version d'ESXi qui ne prenait pas en charge le démarrage sécurisé UEFI, vous pouvez éventuellement activer le démarrage sécurisé. Cela dépendra de la manière dont vous avez effectué la mise à niveau et de si celle-ci a remplacé tous les VIB existants ou si certains VIB sont restés inchangés. Pour savoir si le démarrage

sécurisé est pris en charge sur l'installation mise à niveau, vous pouvez exécuter un script de validation après avoir effectué la mise à niveau.

Pour que le démarrage sécurisé réussisse, la signature de chaque VIB installé doit être disponible sur le système. Les versions antérieures d'ESXi n'enregistrent pas les signatures lors de l'installation des VIB.

- Si vous procédez à la mise à niveau à l'aide des commandes ESXCLI, l'ancienne version d'ESXi effectue l'installation des nouveaux VIB, de sorte que leurs signatures ne soient pas enregistrées et que le démarrage sécurisé ne soit pas possible.
- Si vous procédez à la mise à niveau à l'aide de l'image ISO, les signatures des nouveaux VIB sont enregistrées. Cela est également vrai pour les mises à niveau de vSphere Lifecycle Manager qui utilisent l'ISO.
- Si des anciens VIB restent sur le système, leurs signatures ne sont pas disponibles et le démarrage sécurisé n'est pas possible.
  - Si le système utilise un pilote tiers et si la mise à niveau de VMware n'inclut pas de nouvelle version du VIB pilote, l'ancien VIB est conservé sur le système après la mise à niveau.
  - Dans de rares cas, VMware peut stopper le développement d'un VIB spécifique sans fournir un nouveau VIB qui le remplace ou le rend obsolète, l'ancien VIB est donc conservé sur le système après la mise à niveau.

Note Le démarrage sécurisé UEFI nécessite également un chargeur de démarrage à jour. Ce script ne vérifie pas si le chargeur de démarrage est à jour.

Conditions préalables

- Vérifiez si le matériel prend en charge le démarrage sécurisé UEFI.
- Vérifiez si tous les VIB sont signés avec le niveau d'acceptation minimum PartnerSupported. Si vous incluez des VIB au niveau CommunitySupported, vous ne pouvez pas utiliser le démarrage sécurisé.

Procédure

1. Mettez à niveau le dispositif ESXi et exécutez la commande suivante.

   ```
   /usr/lib/vmware/secureboot/bin/secureBoot.py –c
   ```

2. Vérifiez le résultat.

   Le résultat inclut `Secure boot can be enabled` ou `Secure boot CANNOT be enabled`.

Sécurisation des hôtes ESXi avec un module de plate-forme sécurisée

Les hôtes ESXi peuvent utiliser des puces TPM (Trusted Platform Modules), il s'agit de cryptoprocesseurs sécurisés qui améliorent la sécurité de l'hôte en fournissant une assurance confiance ancrée dans le matériel et non dans le logiciel.

Les TPM constituent un standard dans le secteur des cryptoprocesseurs sécurisés. Des puces TPM se trouvent aujourd'hui dans la plupart des ordinateurs, des ordinateurs portables aux ordinateurs de bureau et aux serveurs. vSphere 6.7 et version ultérieure prennent en charge la version 2.0 du TPM.

Une puce TPM 2.0 atteste de l'identité d'un hôte ESXi. L'attestation par hôte est le processus d'authentification et d'attestation de l'état du logiciel hôte à un moment précis. Le démarrage sécurisé UEFI, qui garantit que le logiciel signé uniquement est chargé au moment du démarrage, est nécessaire pour que l'attestation soit réussie. La puce TPM 2.0 enregistre et stocke de manière sécurisée des mesures de modules logiciels démarrés dans le système, que vCenter Server vérifie à distance.

Les principales étapes du processus d'attestation à distance sont les suivantes :

1 Établissez la fiabilité du TPM distant et créez une clé d'attestation (AK) sur celui-ci.

   Lorsqu'un hôte ESXi est ajouté à, redémarré depuis ou s'est reconnecté à vCenter Server, vCenter Server demande une AK à l'hôte. Une partie du processus de création de l'AK implique également la vérification du matériel TPM lui-même, pour vous assurer qu'il a été produit par un fournisseur connu (et approuvé).

2 Récupérez le rapport d'attestation à partir de l'hôte.

   vCenter Server demande que l'hôte envoie un rapport d'attestation, contenant un extrait des registres PCR (Platform Configuration Registers) signé par le TPM et d'autres métadonnées binaires hôte signées. En vérifiant que les informations correspondent à une configuration qu'il estime approuvée, vCenter Server identifie la plate-forme d'hôte précédemment non approuvé.

3 Vérifiez l'authenticité de l'hôte.

   vCenter Server vérifie l'authenticité du devis signé, déduit les versions de logiciel et détermine la fiabilité de ces dernières. Si vCenter Server détermine que le devis signé n'est pas valide, l'attestation à distance échoue et l'hôte n'est pas approuvé.

Pour utiliser une puce TPM 2.0, votre environnement vCenter Server doit respecter certaines conditions requises :

- vCenter Server 6.7 ou une version ultérieure
- Hôte ESXi 6.7 ou version ultérieure avec une puce TPM 2.0 installée et activée en mode UEFI
- Démarrage sécurisé UEFI activé

Assurez-vous que le module TPM est configuré dans le BIOS de l'hôte ESXi pour utiliser l'algorithme de hachage SHA-256 et l'interface TIS/FIFO (First-In, First-Out, premier entré, premier sorti), mais pas le CRB (Command Response Buffer, tampon de réponse de la commande). Pour plus d'informations sur la définition de ces options BIOS requises, consultez la documentation du fournisseur.

Consultez les puces TPM 2.0 certifiées par VMware à l'emplacement suivant :

https://www.vmware.com/resources/compatibility/search.php

Lorsque vous démarrez un hôte ESXi avec une puce TPM 2.0, vCenter Server surveille l'état de l'attestation de l'hôte. vSphere Client affiche l'état de confiance du matériel dans l'onglet **Résumé** de vCenter Server, sous **Sécurité**, avec les alarmes suivantes :

- Vert : état normal, indique une confiance totale.
- Rouge : échec de l'attestation.

Note Si vous ajoutez une puce TPM 2.0 à un hôte ESXi déjà géré par vCenter Server, vous devez d'abord déconnecter l'hôte, puis le reconnecter. Pour plus d'informations sur la déconnexion et la reconnexion des hôtes, consultez la documentation *Gestion de vCenter Server et des hôtes*.

Démonstration des fonctionnalités ESXi et Trusted Platform Module 2.0 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_67_esxi_tmp20)

Afficher l'état de l'attestation de l'hôte ESXi

Lors de l'ajout à un hôte ESXi, une puce TPM 2.0 atteste de l'intégrité de la plate-forme. Vous pouvez afficher l'état de l'attestation de l'hôte dans vSphere Client. Vous pouvez également afficher l'état Intel Trusted Execution Technology (TXT).

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Accédez à un centre de données et cliquez sur l'onglet **Surveiller**.
3. Cliquez sur **Sécurité**.
4. Vérifiez l'état de l'hôte dans la colonne Attestation et lisez le message qui l'accompagne dans la colonne **Message**.
5. Si cet hôte est un hôte approuvé, consultez Afficher l'état d'attestation du cluster approuvé pour plus d'informations.

Étape suivante

Pour un état de l'attestation sur Échec ou Avertissement, reportez-vous à la section Résoudre les problèmes d'attestation de l'hôte ESXi. Pour les hôtes approuvés, consultez Résoudre les problèmes d'attestation d'hôte approuvé.

Résoudre les problèmes d'attestation de l'hôte ESXi

Lorsque vous installez un périphérique TPM (module de plate-forme sécurisée) sur un hôte ESXi, l'attestation de l'hôte peut échouer. Vous pouvez résoudre les causes potentielles de ce problème.

Procédure

1. Permet d'afficher l'état de l'alarme de l'hôte ESXi et le message d'erreur qui l'accompagne. Reportez-vous à la section Afficher l'état de l'attestation de l'hôte ESXi.
2. Si le message d'erreur est `Le démarrage sécurisé hôte a été désactivé`, vous devez réactiver le démarrage sécurisé pour résoudre le problème.
3. Si l'état d'attestation de l'hôte est Échec, vérifiez le message suivant dans le fichier vCenter Server `vpxd.log` :

   `Aucune clé d'identité en cache, chargement depuis la base de données`

   Ce message indique que vous ajoutez une puce TPM 2.0 à un hôte ESXi déjà géré par vCenter Server. Vous devez d'abord déconnecter l'hôte, puis le reconnecter. Pour plus d'informations sur la déconnexion et la reconnexion des hôtes, consultez la documentation *Gestion de vCenter Server et des hôtes*.

   Pour plus d'informations sur les fichiers journaux de vCenter Server, notamment l'emplacement et la rotation des journaux, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/1021804.
4. Pour tous les autres messages d'erreur, contactez le support technique.

Fichiers journaux ESXi

Les fichiers journaux constituent un élément important dans le dépannage des attaques et l'obtention d'informations relatives aux failles. 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.

Pour renforcer la sécurité de l'hôte, procédez comme suit.

- Configurez la journalisation permanente d'une banque de données. Les journaux des hôtes ESXi sont stockés par défaut dans le système de fichiers en mémoire. 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 de l'hôte.
- La connexion à distance à un hôte central vous permet de rassembler les fichiers journaux sur celui-ci. À partir de cet hôte, vous pouvez surveiller tous les hôtes à l'aide d'un outil unique, effectuer une analyse regroupée et rechercher des données dans les journaux. Cette approche facilite la surveillance et révèle des informations sur les attaques coordonnées sur plusieurs hôtes.

- Configurez le protocole syslog sécurisé à distance sur les hôtes ESXi en utilisant une interface de ligne de commande comme ESXCLI ou PowerCLI ou une API de client.
- Effectuez une requête dans la configuration syslog pour vous assurer que le serveur et le port syslog sont valides.

Pour des informations sur la configuration du protocole syslog, reportez à la documentation *Surveillance et performances de vSphere* sur les fichiers journaux ESXi.

Configurer Syslog sur des hôtes ESXi

Vous pouvez utiliser vSphere Client ou la commande `esxcli system syslog` pour configurer le service syslog.

Pour plus d'informations sur l'utilisation de la commande `esxcli system syslog` et d'autres commandes ESXCLI, consultez *Démarrage avec ESXCLI*.

Procédure

1. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, cliquez sur **Paramètres système avancés**.
4. Cliquez sur **Modifier**.
5. Filtre pour **`syslog`**.
6. Pour configurer la journalisation de façon globale, sélectionnez le paramètre à modifier et entrez la valeur.

Option	Description
Syslog.global.defaultRotate	Nombre maximal d'archives à conserver. Vous pouvez définir ce nombre de façon globale et pour les sous-unités d'enregistrement automatique.
Syslog.global.defaultSize	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 `/scratch` situé sur le système de fichiers local subsiste après des redémarrages. Spécifiez le répertoire sous la forme [*nom_banque_de_données*]*chemin_du_fichier*, le chemin étant relatif à la racine du volume qui assure la sauvegarde de la banque de données. Par exemple, le chemin `[storage1] /systemlogs` crée un mappage vers le chemin `/ vmfs/volumes/storage1/systemlogs.`

Option	Description
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, `ssl://hostName1:1514`. Les protocoles UDP (uniquement sur le port 514), TCP et SSL sont pris en charge. L'hôte distant doit avoir un syslog installé et correctement configuré pour recevoir les messages syslog transférés. Pour plus d'informations sur la configuration de l'hôte distant, reportez-vous à la documentation du service syslog installé sur l'hôte distant. Vous pouvez utiliser un nombre illimité d'hôtes distants pour recevoir des messages syslog.

7 (Facultatif) Pour remplacer la taille et la rotation des journaux par défaut d'un journal quelconque :

   a Cliquez sur le nom du journal que vous souhaitez personnaliser.

   b Entrez le nombre de rotations et la taille de journal souhaités.

8 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.

Tableau 3-7. Emplacements des fichiers journaux ESXi

Composant	Emplacement	Objectif
Authentification	`/var/log/auth.log`	Contient tous les événements relatifs à l'authentification pour le système local.
Journal de l'agent hôte ESXi	`/var/log/hostd.log`	Contient des informations sur l'agent gérant et configurant les hôtes ESXi et leurs machines virtuelles.
Journal du shell	`/var/log/shell.log`	Contient un enregistrement de toutes les commandes tapées dans ESXi Shell et les événements de shell (par exemple, le moment où le shell a été activé).
Messages système	`/var/log/syslog.log`	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.

Tableau 3-7. Emplacements des fichiers journaux ESXi (suite)

Composant	Emplacement	Objectif
Journal de l'agent vCenter Server	`/var/log/vpxa.log`	Contient des informations sur l'agent communiquant avec vCenter Server (si l'hôte est géré par vCenter Server).
Machines virtuelles	Le même répertoire que les fichiers de configuration de la machine virtuelle, appelés `vmware.log` et `vmware*.log`. Par exemple, `/vmfs/volumes/datastore/virtual machine/vwmare.log`	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.
VMkernel	`/var/log/vmkernel.log`	Enregistre les activités relatives aux machines virtuelles et à ESXi.
Résumé VMkernel	`/var/log/vmksummary.log`	Utilisé pour déterminer les statistiques de temps de fonctionnement et de disponibilité pourESXi (virgule séparée).
Avertissements VMkernel	`/var/log/vmkwarning.log`	Enregistre les activités relatives aux machines virtuelles.
Démarrage rapide	`/var/log/loadESX.log`	Contient tous les événements liés au redémarrage d'un hôte ESXi via le démarrage rapide.
Agent d'infrastructure approuvé	`/var/run/log/kmxa.log`	Enregistre les activités liées au service client sur l'hôte approuvé ESXi.
Service de fournisseur de clés	`/var/run/log/kmxd.log`	Enregistre les activités liées au service de fournisseur de clés de Autorité d'approbation vSphere .
Service d'attestation	`/var/run/log/attestd.log`	Enregistre les activités liées au service d'attestation de Autorité d'approbation vSphere .
Service de jeton ESX	`/var/run/log/esxtokend.log`	Enregistre les activités liées au service de jeton ESX de Autorité d'approbation vSphere .
Redirecteur d'API ESX	`/var/run/log/esxapiadapter.log`	Enregistre les activités liées au redirecteur d'API de Autorité d'approbation vSphere .

Trafic de la journalisation de la tolérance aux pannes

VMware Fault Tolerance (FT) capture les entrées et les événements qui se produisent sur une machine virtuelle principale et les transmet à la machine virtuelle secondaire qui s'exécute 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 « intermédiaires ». Par exemple, vous pouvez utiliser un réseau privé pour le trafic de la journalisation de la tolérance aux pannes.

Sécurisation de la configuration ESXi

À partir de vSphere 7.0 Update 2, la configuration ESXi est protégée par chiffrement. Lorsqu'un hôte ESXi est éventuellement protégé par un TPM, la clé de chiffrement de la configuration ESXi est scellée par le TPM.

De nombreux services ESXi stockent des secrets dans leurs fichiers de configuration. Ces configurations sont persistantes dans la banque de démarrage d'un hôte ESXi en tant que fichier archivé. À partir de vSphere 7.0 Update 2, ce fichier archivé est chiffré. Par conséquent, les pirates ne peuvent pas lire ou modifier ce fichier directement, même s'ils ont un accès physique au stockage de l'hôte ESXi.

En plus d'empêcher aux pirates d'accéder aux secrets, une configuration ESXi sécurisée utilisée avec un TPM peut enregistrer les clés de chiffrement de la machine virtuelle lors des redémarrages. Par conséquent, les charges de travail chiffrées peuvent continuer à fonctionner lorsqu'un serveur de clés est indisponible ou inaccessible. Reportez-vous à la section Présentation de la persistance des clés.

Présentation de la sécurisation de la configuration ESXi

Vous n'avez pas besoin d'activer le chiffrement de la configuration d'ESXi manuellement. Lorsque vous installez ou mettez à niveau vers vSphere 7.0 Update 2 ou version ultérieure, le fichier de configuration ESXi archivé est chiffré.

Avant vSphere 7.0 Update 2, le fichier de configuration ESXi archivé n'était pas chiffré. Dans vSphere 7.0 Update 2 et versions ultérieures, le fichier de configuration archivé est chiffré. Lorsque l'hôte ESXi est configuré avec un module de plate-forme sécurisée (TPM), le TPM est utilisé pour « sceller » la configuration sur l'hôte, fournissant ainsi une garantie de sécurité renforcée.

Présentation des fichiers de configuration ESXi avant vSphere 7.0 Update 2

La configuration d'un hôte ESXi se compose de fichiers de configuration pour chaque service qui s'exécute sur l'hôte. Les fichiers de configuration résident généralement dans le répertoire `/etc/`, mais ils peuvent également résider dans d'autres espaces de noms. Les fichiers de configuration contiennent des informations d' run-time sur l'état des services . Au fil du temps, les valeurs par défaut dans les fichiers de configuration peuvent être modifiées. Par exemple, lorsque vous modifiez les paramètres sur l'hôte ESXi. Une tâche cron sauvegarde régulièrement les fichiers de configuration ESXi ou lorsque ESXi s'arrête normalement ou à la demande, puis de crée un fichier de configuration archivé dans la banque de démarrage. Lorsque ESXi redémarre, il lit le

fichier de configuration archivé et recrée l'état dans lequel ESXi était lors de la sauvegarde. Avant vSphere 7.0 Update 2, le fichier de configuration archivé n'était pas chiffré. Par conséquent, il est possible pour un pirate ayant accès au stockage ESXi physique de lire et de modifier ce fichier lorsque le système est hors ligne.

Présentation de la configuration ESXi sécurisée

Lors du premier démarrage après l'installation ou la mise à niveau de l'hôte ESXi vers vSphere 7.0 Update 2, les événements suivants se produisent :

- Si l'hôte ESXi dispose d'un TPM et qu'il est activé dans le microprogramme, le fichier de configuration archivé est chiffré par une clé de chiffrement stockée dans le TPM. À partir de ce moment, la configuration de l'hôte est scellée par le TPM.
- Si l'hôte ESXi n'a pas de TPM, ESXi utilise une fonction KDF (fonction de dérivation de clés) pour générer une clé de chiffrement de la configuration sécurisée pour le fichier de configuration archivé. Les entrées du fichier KDF sont stockées sur le disque dans le fichier `encryption.info`.

Note Lorsque l'hôte ESXi dispose d'un périphérique TPM activé, vous obtenez une protection supplémentaire.

Lorsque l'hôte ESXi redémarre après le premier démarrage, les événements suivants se produisent :

- Si l'hôte ESXi dispose d'un TPM, l'hôte doit obtenir la clé de chiffrement à partir du TPM pour cet hôte spécifique. Si les mesures TPM répondent à la stratégie de scellement qui a été utilisée lors de la création de la clé de chiffrement, l'hôte obtient la clé de chiffrement à partir du TPM.
- Si l'hôte ESXi n'a pas de TPM, ESXi lit les informations du fichier `encryption.info` pour déverrouiller la configuration sécurisée.

Exigences relatives à la configuration ESXi sécurisée

- ESXi 7.0 Update 2
- TPM 2.0 pour le chiffrement de la configuration et la possibilité d'utiliser une stratégie de scellement

Clé de récupération de la configuration ESXi sécurisée

Une configuration ESXi sécurisée inclut une clé de récupération. Si vous devez récupérer la configuration ESXi sécurisée, vous devez utiliser une clé de récupération dont vous entrez le contenu comme option de démarrage de la ligne de commande. Vous pouvez lister la clé de récupération pour créer une sauvegarde de clé de récupération. Vous pouvez également effectuer une rotation de la clé de récupération dans le cadre de vos exigences de sécurité.

La sauvegarde de la clé de récupération est un élément important dans la gestion de votre configuration ESXi sécurisée. vCenter Server génère une alarme pour vous rappeler de sauvegarder la clé de récupération.

Alarme de la clé de récupération

La sauvegarde de la clé de récupération est un élément important dans la gestion de votre configuration ESXi sécurisée. Chaque fois qu'un hôte ESXi en mode TPM est connecté ou reconnecté à vCenter Server, vCenter Server génère une alarme pour vous rappeler de sauvegarder la clé de récupération. Lorsque vous réinitialisez l'alarme, elle ne se déclenche plus, sauf si les conditions changent.

Meilleures pratiques pour la configuration ESXi sécurisée

Suivez ces recommandations pour la clé de récupération :

- Lorsque vous ré listez une clé de récupération, elle est temporairement affichée dans un environnement non sécurisé et se trouve dans la mémoire. Supprimez les traces de la clé.
  - Le redémarrage de l'hôte supprime la clé résiduelle dans la mémoire.
  - Pour une protection améliorée, vous pouvez activer le mode de chiffrement sur l'hôte. Reportez-vous à la section Activer explicitement le mode de chiffrement de l'hôte.
- Lorsque vous effectuez une récupération :
  - Pour éliminer toute trace de la clé de récupération dans un environnement non sécurisé, redémarrez l'hôte.
  - Pour une sécurité renforcée, faites pivoter la clé de récupération pour utiliser une nouvelle clé après avoir récupéré la clé une première fois.

Présentation des stratégies de scellement TPM

À partir de vSphere 7.0 Update 2, un hôte ESXi utilise le TPM pour sceller la configuration de l'hôte par rapport à une stratégie PCR (Platform Configuration Register). La stratégie PCR peut être configurée pour appliquer le démarrage sécurisé UEFI et d'autres paramètres.

Un TPM peut utiliser des mesures PCR (Platform Configuration Register) pour mettre en œuvre des stratégies qui limitent l'accès non autorisé aux données sensibles. Lorsque vous installez ou mettez à niveau un hôte ESXi avec un TPM vers vSphere 7.0 Update 2, le TPM scelle les informations sensibles à l'aide d'une stratégie qui intègre le paramètre de démarrage sécurisé. Cette stratégie vérifie que si le démarrage sécurisé a été activé lorsque les données ont été scellées pour la première fois avec le TPM, alors le démarrage sécurisé doit toujours être activé lors de la tentative de descellement des données au cours d'un démarrage ultérieur.

Le démarrage sécurisé est une fonctionnalité standard du microprogramme UEFI. Lorsque le démarrage sécurisé UEFI est activé, si le chargeur de démarrage du système d'exploitation ne possède pas de signature numérique valide, l'hôte refuse de charger un pilote ou une application UEFI.

Vous pouvez choisir de désactiver ou d'activer l'application du démarrage sécurisé UEFI. Reportez-vous à la section Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée.

Note Si vous n'avez pas activé un TPM lors de l'installation ou de la mise à niveau vers vSphere 7.0 Update 2, vous pouvez le faire ultérieurement à l'aide de la commande suivante.

```
esxcli system settings encryption set --mode=TPM
```

Après avoir activé le TPM, vous ne pouvez plus annuler ce paramètre.

La commande `esxcli system settings encryption set` échoue sur certains TPM, tels que ceux provenant de NationZ (NTZ) et d'Infineon Technologies (IFX), même lorsque le TPM est activé pour l'hôte.

Si une installation ou une mise à niveau de vSphere 7.0 Update 2 ne parvient pas à utiliser le TPM lors du premier démarrage, l'installation ou la mise à niveau se poursuit et le mode est défini par défaut sur AUCUN (c'est-à-dire `--mode=NONE`). Le comportement qui en résulte est comme si le TPM n'était pas activé.

Le TPM peut également appliquer le paramètre pour l'option de démarrage execInstalledOnly dans la stratégie de scellement. L'application execInstalledOnly est une option de démarrage ESXi avancée qui garantit que VMkernel exécute uniquement les fichiers binaires qui ont été correctement empaquetés et signés dans le cadre d'un VIB. L'option de démarrage execInstalledOnly est dépendante de l'option de démarrage sécurisé. L'application du démarrage sécurisé doit être activée avant de pouvoir appliquer l'option de démarrage execInstalledOnly dans la stratégie de scellement. Reportez-vous à la section Activer ou désactiver l'application d'execInstalledOnly pour une configuration ESXi sécurisée.

Gestion d'une configuration ESXi sécurisée

Vous pouvez utiliser les commandes ESXCLI pour répertorier la clé de récupération de la configuration ESXi sécurisée, faire pivoter la clé de récupération et modifier les stratégies TPM (par exemple, l'application du démarrage sécurisé UEFI).

Répertorier le contenu de la clé de récupération de la configuration ESXi sécurisée

Vous pouvez utiliser ESXCLI pour afficher le contenu de la clé de récupération de la configuration ESXi sécurisée.

Cette tâche s'applique uniquement à un hôte ESXi qui dispose d'un TPM. En général, vous répertoriez le contenu de la clé de récupération de la configuration ESXi sécurisée pour créer une sauvegarde ou dans le cadre de la rotation des clés de récupération.

Conditions préalables

- A accès à l'ensemble de commandes ESXCLI. Vous pouvez exécuter des commandes ESXCLI à distance ou les exécuter dans ESXi Shell.

- Privilège requis pour utiliser la version autonome d'ESXCLI ou via PowerCLI : **Hôte.Configuration.Paramètres**

Procédure

1. Exécutez la commande suivante sur l'hôte ESXi.

```
esxcli system settings encryption recovery list
```

2. Enregistrez la sortie dans un emplacement distant sécurisé en tant que sauvegarde, dans le cas où vous devez récupérer la configuration sécurisée.

Résultats

L'ID de clé de récupération et la clé sont affichés.

Exemple : Répertorier la clé de récupération de la configuration ESXi sécurisée

```
[root@host1] esxcli system settings encyption recovery list

Recovery ID                             Key
--------------------------------------  ---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}  478269-039194-473926-430939-686855-231401-642208-184477-602511
-225586-551660-586542-338394-092578-687140-267425
```

Effectuer une rotation de la clé de récupération de la configuration ESXi sécurisée

Vous pouvez utiliser ESXCLI pour effectuer une rotation de la clé de récupération de la configuration ESXi sécurisée à l'aide de l'interface de ligne de commande.

Cette tâche s'applique uniquement à un hôte ESXi qui dispose d'un TPM. Vous souhaitez peut-être effectuer une rotation de la clé de récupération de la configuration ESXi sécurisée dans le cadre des recommandations en matière de sécurité.

Conditions préalables

- A accès à l'ensemble de commandes ESXCLI. Vous pouvez exécuter des commandes ESXCLI à distance ou les exécuter dans ESXi Shell.
- Privilège requis pour utiliser la version autonome d'ESXCLI ou via PowerCLI : **Hôte.Configuration.Paramètres**

Procédure

1. Répertoriez la clé de récupération.

   Reportez-vous à la section Répertorier le contenu de la clé de récupération de la configuration ESXi sécurisée.

2. Exécutez la commande suivante.

```
esxcli system settings encryption recovery rotate -k keyID -u uuid
```

Dans cette commande, *keyID* est l'ID de clé dans le cache de clés VMkernel et *uuid* est l'ID de récupération (obtenu à partir de la commande `esxcli system settings encyption recovery list`).

Résultats

La clé de récupération est maintenant définie sur le contenu de la clé référencée par l'ID de clé.

Dépannage et récupération de la configuration ESXi sécurisée

Vous pouvez résoudre et récupérer des problèmes de démarrage que vous pouvez rencontrer avec une configuration ESXi sécurisée.

Si vous effacez un TPM (c'est-à-dire que les valeurs initiales dans le TPM sont réinitialisées) ou si un TPM échoue, vous devez prendre des mesures pour récupérer la configuration ESXi sécurisée. Vous devez avoir la clé de récupération pour récupérer la configuration. Tant que vous n'avez pas récupéré la configuration, l'hôte ESXi ne peut pas démarrer. Reportez-vous à la section Récupérer la configuration ESXi sécurisée.

Bien que cela soit rare, il est possible qu'un hôte ESXi ne réussisse pas à restaurer ou à déchiffrer la configuration sécurisée, empêchant ainsi l'hôte de démarrer. Cela est possible dans les situations suivantes :

- Modification du paramètre de démarrage sécurisé (ou autre stratégie)
- Altération réelle
- Clé de récupération non disponible

Pour résoudre ces situations, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/81446.

Récupérer la configuration ESXi sécurisée

Si un TPM échoue ou si vous en effacez un, vous devez récupérer la configuration ESXi sécurisée. Tant que vous n'avez pas récupéré la configuration, l'hôte ESXi ne peut pas démarrer.

La récupération de la configuration ESXi sécurisée fait référence aux situations suivantes :

- Vous avez effacé le TPM (c'est-à-dire que les valeurs initiales du TPM ont été réinitialisées).
- Le TPM a échoué.

Pour résoudre d'autres problèmes liés à la configuration ESXi sécurisée, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/81446.

Effectuez la récupération manuellement. N'effectuez pas la récupération dans le cadre d'un script d'installation ou de mise à niveau.

Conditions préalables

Obtenez votre clé de récupération. Vous devez avoir précédemment répertorié et stocké la clé de récupération. Reportez-vous à la section Répertorier le contenu de la clé de récupération de la configuration ESXi sécurisée.

Procédure

1. (Facultatif) Si le TPM a échoué, déplacez le disque (avec la banque de démarrage) vers un autre hôte avec un TPM.
2. Démarrez l'hôte ESXi.
3. Lorsque la fenêtre du programme d'installation ESXi s'affiche, appuyez sur les touches Maj.+O pour éditer les options de démarrage.
4. À l'invite de commande, entrez l'option de démarrage pour récupérer la configuration.

```
encryptionRecoveryKey=recovery_key
```

Résultats

La configuration ESXi sécurisée est récupérée et l'hôte ESXi démarre.

Étape suivante

Lorsque vous entrez la clé de récupération, celle-ci s'affiche temporairement dans un environnement non sécurisé et se trouve dans la mémoire. Vous pouvez supprimer les traces résiduelles de la clé dans la mémoire en redémarrage de l'hôte. Vous pouvez également effectuer une rotation de la clé. Reportez-vous à la section Effectuer une rotation de la clé de récupération de la configuration ESXi sécurisée.

Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée

Vous pouvez choisir d'activer l'application du démarrage sécurisé UEFI ou de désactiver une application de démarrage sécurisé UEFI précédemment activée. Vous devez utiliser ESXCLI pour modifier ce paramètre dans le TPM sur l'hôte ESXi.

Cette tâche s'applique uniquement aux hôtes ESXi qui contiennent un TPM. Le démarrage sécurisé UEFI est un paramètre du microprogramme qui permet de s'assurer que le logiciel lancé par le microprogramme est approuvé. L'activation du démarrage sécurisé UEFI peut être appliquée à chaque démarrage à l'aide du TPM.

Conditions préalables

- A accès à l'ensemble de commandes ESXCLI. Vous pouvez exécuter des commandes ESXCLI à distance ou les exécuter dans ESXi Shell.
- Privilège requis pour utiliser la version autonome d'ESXCLI ou via PowerCLI : **Hôte.Configuration.Paramètres**

Procédure

1 Répertoriez les paramètres actuels sur l'hôte ESXi.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Si l'application du démarrage sécurisé est activée, l'option Exiger le démarrage sécurisé affiche la valeur true. Si l'application du démarrage sécurisé est désactivée, l'option Exiger le démarrage sécurisé affiche la valeur false.

2 Activez ou désactivez l'application du démarrage sécurisé.

Option	Description

Activer	a Arrêtez l'hôte de manière normale.
	Par exemple, cliquez avec le bouton droit sur l'hôte ESXi dans vSphere Client et sélectionnez **Alimentation > Arrêter**.
	b Activez le démarrage sécurisé dans le microprogramme de l'hôte.
	Consultez la documentation matérielle de votre fournisseur.
	c Redémarrez l'hôte.
	d Exécutez la commande ESXCLI suivante.
	`esxcli system settings encryption set --require-secure-boot=T`
	e Vérifiez la modification.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirmez que l'option Exiger le démarrage sécurisé affiche la valeur true.
	f Pour enregistrer le paramètre, exécutez la commande suivante.
	`/sbin/auto-backup.sh`

Désactiver	a Exécutez la commande ESXCLI suivante.
	`esxcli system settings encryption set --require-secure-boot=F`
	b Vérifiez la modification.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	Confirmez que l'option Exiger le démarrage sécurisé affiche la valeur false.
	c Pour enregistrer le paramètre, exécutez la commande suivante.
	`/sbin/auto-backup.sh`
	Vous pouvez choisir de désactiver le démarrage sécurisé dans le microprogramme de l'hôte, mais la dépendance entre le paramètre du microprogramme et l'application du TPM n'est plus définie à ce stade.

Résultats

L'hôte ESXi s'exécute avec l'application du démarrage sécurisé activée ou désactivée, selon votre choix.

Note Si vous n'avez pas activé un TPM lors de l'installation ou de la mise à niveau vers vSphere 7.0 Update 2, vous pouvez le faire ultérieurement à l'aide de la commande suivante.

```
esxcli system settings encryption set --mode=TPM
```

Après avoir activé le TPM, vous ne pouvez plus annuler ce paramètre.

La commande `esxcli system settings encryption set` échoue sur certains TPM, tels que ceux provenant de NationZ (NTZ) et d'Infineon Technologies (IFX), même lorsque le TPM est activé pour l'hôte.

Si une installation ou une mise à niveau de vSphere 7.0 Update 2 ne parvient pas à utiliser le TPM lors du premier démarrage, l'installation ou la mise à niveau se poursuit et le mode est défini par défaut sur AUCUN (c'est-à-dire `--mode=NONE`). Le comportement qui en résulte est comme si le TPM n'était pas activé.

Activer ou désactiver l'application d'execInstalledOnly pour une configuration ESXi sécurisée

Vous pouvez choisir d'activer l'application d'execInstalledOnly ou de désactiver une application d'execInstalledOnly précédemment activée. Vous devez utiliser ESXCLI pour modifier ce paramètre dans le TPM sur l'hôte ESXi. L'application du démarrage sécurisé UEFI doit être activée avant de pouvoir activer l'application d'execInstalledOnly.

Cette tâche s'applique uniquement aux hôtes ESXi qui contiennent un TPM. L'option de démarrage ESXi avancée execInstalledOnly, lorsqu'elle est définie sur TRUE, garantit que VMkernel exécute uniquement les fichiers binaires qui ont été empaquetés et signés dans le cadre d'un VIB. L'activation de cette option de démarrage peut être appliquée à chaque démarrage à l'aide du TPM.

Conditions préalables

- Pour activer l'application d'execInstalledOnly, vous devez d'abord activer l'application du démarrage sécurisé UEFI. L'application d'execInstalledOnly est intégrée à l'application du démarrage sécurisé UEFI. Reportez-vous à la section Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée.
- A accès à l'ensemble de commandes ESXCLI. Vous pouvez exécuter des commandes ESXCLI à distance ou les exécuter dans ESXi Shell.
- Privilège requis pour utiliser la version autonome d'ESXCLI ou via PowerCLI : **Hôte.Configuration.Paramètres**

Procédure

1 Répertoriez les paramètres actuels sur l'hôte ESXi.

```
esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: false
   Require Secure Boot: true
```

Si l'application d'execInstalledOnly est activée, l'option Exiger les exécutables à partir des VIB installés uniquement affiche la valeur true. Si l'application d'execInstalledOnly est déactivée, l'option Exiger les exécutables à partir des VIB installés uniquement affiche la valeur false. Pour activer l'application d'execInstalledOnly, l'application du démarrage sécurisé doit être activée et l'option Exiger le démarrage sécurisé affiche alors la valeur true.

2 Activez ou désactivez l'application execInstalledOnly.

Option	Description

Activer	a Vérifiez que l'option de démarrage sécurisé est appliquée.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirmez que l'option Exiger le démarrage sécurisé affiche la valeur true. Si ce n'est pas le cas, consultez la section Activer ou désactiver l'application du démarrage sécurisé pour une configuration ESXi sécurisée.
	b Pour définir la valeur d'exécution de l'option de démarrage execInstalledOnly sur TRUE, exécutez la commande ESXCLI suivante.
	`esxcli system settings kernel set –s execInstalledOnly –v TRUE`
	c Arrêtez l'hôte de manière normale.
	Par exemple, cliquez avec le bouton droit sur l'hôte ESXi dans vSphere Client et sélectionnez **Alimentation > Arrêter**.
	d Redémarrez l'hôte.
	e Pour définir l'option de démarrage execInstalledOnly, exécutez la commande ESXCLI suivante.
	`esxcli system settings encryption set –require–exec–installed–only=T`
	f Vérifiez la modification.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	Confirmez que l'option Exiger les exécutables à partir des VIB installés uniquement affiche la valeur true.
	g Pour enregistrer le paramètre, exécutez la commande suivante.
	`/sbin/auto–backup.sh`

Désactiver	a Exécutez la commande ESXCLI suivante.
	`esxcli system settings encryption set ––require–exec–installed–only=F`
	b Vérifiez la modification.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	Confirmez que l'option Exiger les exécutables à partir des VIB installés uniquement affiche la valeur false.

Option	Description
	c Pour enregistrer le paramètre, exécutez la commande suivante. `/sbin/auto-backup.sh` Le TPM n'applique plus l'option de démarrage execInstalledOnly.

Résultats

L'hôte ESXi s'exécute avec l'application d'execInstalledOnly activée ou désactivée, selon votre choix.

Sécurisation des systèmes vCenter Server

4

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
- Ports requis pour vCenter Server

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

- N'accordez le rôle Administrateur qu'aux administrateurs nommés qui doivent en bénéficier. Vous pouvez créer des rôles personnalisés ou utiliser le rôle Aucun administrateur de chiffrement pour les administrateurs qui disposent de privilèges plus restreints. N'appliquez pas ce rôle à un groupe dont la composition ne fait pas l'objet d'un contrôle strict.
- Assurez-vous que les applications utilisent des comptes de service uniques lors d'une connexion à un système vCenter Server.

Surveiller 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.

Minimiser l'accès

N'autorisez pas les utilisateurs à se connecter directement à la machine hôte vCenter Server. Les utilisateurs qui sont connectés à la machine hôte vCenter Server peuvent provoquer des dommages, intentionnels ou non, en modifiant les paramètres et les processus. Ils ont également potentiellement accès 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 vérifiés.

Accorder 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.

Certains privilèges ne sont nécessaires que pour l'installation et la mise à niveau. Après l'installation ou la mise à niveau de vCenter Server, vous pouvez supprimer ces privilèges du rôle d'administrateur de base de données.

Restreindre l'accès au navigateur de la banque de données

Attribuez le privilège **Banque de données.Parcourir la banque de données** uniquement aux utilisateurs ou aux groupes qui en ont réellement besoin. Les utilisateurs qui disposent de ce privilège peuvent afficher, charger ou télécharger les fichiers des banques de données associées au déploiement de vSphere par l'intermédiaire du navigateur Web ou de vSphere Client.

Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle

Par défaut, un utilisateur avec le rôle Administrateur de vCenter Server peut interagir avec les fichiers et les 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 personnalisé, dépourvu du privilège **Systèmes invités**. Reportez-vous à la section Empêcher des utilisateurs d'exécuter des commandes dans une machine virtuelle.

Envisager de modifier la stratégie de mot de passe pour vpxuser

Par défaut, vCenter Server modifie automatiquement le mot de passe vpxuser tous les 30 jours. Assurez-vous que ce paramètre correspond à la stratégie de l'entreprise ou configurez la stratégie de mot de passe de vCenter Server. Reportez-vous à la section 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.

Vérifier les privilèges après le redémarrage de vCenter Server

Vérifiez la réaffectation des privilèges lorsque vous redémarrez vCenter Server. Si l'utilisateur ou le groupe qui a le rôle Administrateur sur le dossier racine ne peut pas être validé lors d'un redémarrage, le rôle est supprimé de cet utilisateur ou de ce groupe. À la place, vCenter Server accordez le rôle Administrateur à l'administrateur de vCenter Single Sign-On (par défaut, administrator@vsphere.local). Ce compte peut alors agir en tant qu'administrateur de vCenter Server.

Rétablissez un compte d'administrateur nommé et attribuez-lui le rôle Administrateur pour éviter d'utiliser le compte d'administrateur de vCenter Single Sign-On anonyme (par défaut, administrator@vsphere.local).

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.

Vérifier les certificats vSphere Client

Demandez aux utilisateurs de vSphere Client ou d'autres applications client de tenir compte des 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 Client.

Procédure

1. Connectez-vous au système vCenter Server à l'aide de vSphere Client.
2. Sélectionnez le système vCenter Server dans la hiérarchie des objets.
3. Cliquez sur **Configurer**.
4. Cliquez sur **Paramètres avancés**, puis sur **Modifier les paramètres**.
5. Cliquez sur l'icône **Filtre** et entrez **`VimPasswordExpirationInDays`**.
6. Configurez `VirtualCenter.VimPasswordExpirationInDays` pour qu'il soit conforme à vos exigences.

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 Client, un système Windows sous lequel vous utilisez PowerCLI ou tout autre client SDK.
- Des services d'infrastructure, tels que DNS, Active Directory et PTP ou NTP.
- D'autres systèmes qui exécutent des composants essentiels à la fonctionnalité du système vCenter Server.

Utilisez le pare-feu sur l'instance de vCenter Server. Incluez des restrictions d'accès basées sur l'IP, afin que seuls les composants nécessaires puissent communiquer avec le système vCenter Server.

Évaluer l'utilisation de clients Linux avec des interfaces de lignes de commande et des SDK

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.

Pour améliorer la sécurité, vous pouvez remplacer les certificats signés par VMCA sur le système vCenter Server et sur les hôtes ESXi avec des certificats signés par une entreprise ou une autorité de certification tierce. Cependant, certaines communications avec les clients Linux peuvent toujours être vulnérables aux attaques MITM (Man in the Middle). Les composants suivants sont vulnérables lorsqu'ils fonctionnent sur le système d'exploitation Linux.

- Commandes ESXCLI
- Scripts vSphere SDK for 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.

Examiner les plug-ins des clients

Les extensions vSphere 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 améliorer la sécurité, utilisez une installation qui comporte uniquement des extensions autorisées provenant de sources fiables.

Une installation vCenter comprend une infrastructure d'extensibilité pour vSphere Client. Vous pouvez utiliser cette infrastructure pour développer le client avec des sélections du menu ou des icônes de la barre d'outils. Les extensions peuvent donner accès à des composants vCenter complémentaires ou des fonctionnalités externes basées sur le Web.

L'utilisation de l'infrastructure d'extensibilité peut risquer d'introduire des fonctionnalités non souhaitées. Par exemple, si un administrateur installe un plug-in dans une instance de vSphere Client, le plug-in peut exécuter des commandes arbitraires grâce au niveau de privilège de cet administrateur.

Pour éviter que votre vSphere Client puisse être compromis, examinez périodiquement tous les plug-ins installés et assurez-vous que chaque plug-in provient 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 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 de sécurité de vCenter Server

Suivez toutes les meilleures pratiques de sécurisation d'un système vCenter Server. Des procédures supplémentaires vous permettent de renforcer la sécurité de votre dispositif vCenter Server.

Configurer PTP ou NTP

Assurez-vous que tous les systèmes utilisent la même source de temps relatif. Cette source de temps doit être en synchronisation avec une norme de temps convenue, par exemple UTC (temps universel coordonné). La synchronisation des systèmes est essentielle pour la validation des certificats. PTP et NTP simplifient également le suivi d'un éventuel intrus dans les fichiers journaux. Des réglages d'heure incorrects compliquent l'analyse et la corrélation de fichiers journaux pour détecter d'éventuelles attaques et compromettent la précision des audits. Reportez-vous à la section Synchroniser l'heure dans vCenter Server avec un serveur NTP.

Limiter l'accès au réseau de vCenter Server

Limitez l'accès aux composants qui sont nécessaires pour communiquer avec le dispositif vCenter Server. En bloquant l'accès des systèmes non essentiels, vous réduisez les risques d'attaque sur le système d'exploitation.

Pour obtenir la liste de tous les ports et protocoles pris en charge dans les produits VMware, y compris vSphere et vSAN, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/. Vous pouvez rechercher des ports selon le produit VMware, créer une liste personnalisée de ports et imprimer ou enregistrer des listes de ports.

Exigences de mots de passe et comportement de verrouillage de vCenter

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

Cette section traite des mots de passe vCenter Single Sign-On. Reportez-vous à Verrouillage des mots de passe et des comptes ESXi pour une description des mots de passe des utilisateurs locaux d'ESXi.

Mot de passe d'administrateur vCenter Single Sign-On

Le mot de passe de l'administrateur de vCenter Single Sign-On, administrator@vsphere.local par défaut, est spécifié par la stratégie de mot de passe de vCenter Single Sign-On. Par défaut, ce mot de passe doit répondre aux exigences suivantes :

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

Le mot de passe de cet utilisateur ne peut pas dépasser 20 caractères. Les caractères non-ASCII sont autorisés. Les administrateurs peuvent modifier la stratégie de mot de passe par défaut. Consultez la documentation de *Authentification vSphere*.

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 ou OpenLDAP.

Comportement de verrouillage de vCenter Single Sign-On

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 de vCenter Single Sign-On. Consultez la documentation de *Authentification vSphere*.

L'administrateur du domaine vCenter Single Sign-On, administrator@vsphere.local par défaut, n'est pas affecté par la stratégie de verrouillage. L'utilisateur est affecté par la stratégie de mot de passe.

Modifications du mot de passe

Si vous connaissez votre mot de passe, vous pouvez le modifier à l'aide de la commande `dir-cli password change`. Si vous avez oublié votre mot de passe, un administrateur vCenter Single Sign-On peut le réinitialiser à l'aide de la commande `dir-cli password reset`.

Pour obtenir des informations sur l'expiration du mot de passe et d'autres rubriques associés dans différentes versions de vSphere, reportez-vous à la base de connaissances VMware.

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 Client.

Note Les certificats sont conservés par défaut entre les mises à niveau.

Procédure

1. Accédez à vCenter Server dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans **Paramètres**, cliquez sur **Général**.
4. Cliquez sur **Modifier**.
5. Cliquez sur **Paramètres SSL**.
6. 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.
7. Si l'empreinte correspond, cochez la case **Vérifier** à côté de l'hôte.

   Les hôtes non sélectionnés sont déconnectés après avoir cliqué sur **OK**.
8. Cliquez sur **Enregistrer**.

Ports requis pour vCenter Server

Le système vCenter Server doit pouvoir envoyer des données à chaque hôte géré et recevoir des données de vSphere Client. Pour autoriser les activités de migration et de provisionnement entre les hôtes gérés, les hôtes source et de destination doivent pouvoir recevoir des données l'un de l'autre par le biais de ports TCP et UDP prédéterminés.

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. Pour obtenir la liste de tous les ports et protocoles pris en charge dans vSphere, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com.

Lors de l'installation, si un port est en cours d'utilisation ou est bloqué à l'aide d'une liste d'exclusion, le programme d'installation de vCenter Server affiche un message d'erreur. Vous devez utiliser un autre numéro de port pour poursuivre l'installation. Des ports internes sont utilisés uniquement pour la communication entre processus.

VMware utilise des ports désignés pour la communication. En outre, les hôtes gérés surveillent des ports désignés pour détecter l'arrivée de données en provenance de vCenter Server. Si un pare-feu intégré existe entre ces éléments, le programme d'installation ouvre les ports pendant le processus d'installation ou de mise à niveau. Pour les pare-feu personnalisés, vous devez ouvrir les ports requis. Si vous avez un pare-feu entre deux hôtes gérés et que vous désirez effectuer des activités source ou cible, comme une migration ou un clonage, vous devez configurer un moyen pour que les hôtes gérés puissent recevoir des données.

Pour configurer le système vCenter Server de manière à utiliser un autre port pour recevoir les données de vSphere Client, reportez-vous à la documentation *Gestion de vCenter Server et des hôtes*.

Sécurisation des machines virtuelles

5

Le système d'exploitation client qui est exécuté dans la machine virtuelle est exposé aux mêmes risques de sécutité qu'une machine physique. Sécurisez les machines virtuelles de la même manière que pour les machines physiques et appliquez les recommandations présentées dans ce document et dans le *Guide de configuration de sécurité* (nommé auparavant *Guide de sécurisation renforcée*).

Le *Guide de configuration de la sécurité* est disponible à l'adresse https://core.vmware.com/security.

Ce chapitre contient les rubriques suivantes :

- Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle
- 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
- Sécurisation des machines virtuelles avec Intel Software Guard Extensions
- Sécurisation des machines virtuelles avec SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD

Activer ou désactiver le démarrage sécurisé UEFI pour une machine virtuelle

Le démarrage sécurisé UEFI est une norme de sécurité qui permet de vérifier que votre ordinateur démarre uniquement avec les logiciels approuvés par le fabricant. Pour certaines versions matérielles et certains systèmes d'exploitation de machines virtuelles, vous pouvez activer le démarrage sécurisé de la même manière que pour une machine physique.

Dans un système d'exploitation qui prend en charge le démarrage sécurisé UEFI, chaque logiciel de démarrage est signé, notamment le chargeur de démarrage, le noyau du système d'exploitation et les pilotes du système d'exploitation. La configuration par défaut de la machine virtuelle inclut plusieurs certificats de signature de code.

- Un certificat Microsoft utilisé uniquement pour démarrer Windows.

- Un certificat Microsoft utilisé pour le code tiers qui est signé par Microsoft, comme les chargeurs de démarrage Linux.
- Un certificat VMware qui est utilisé uniquement pour démarrer ESXi dans une machine virtuelle.

La configuration par défaut de la machine virtuelle inclut un certificat pour authentifier les demandes de modification de la configuration du démarrage sécurisé, notamment la liste de révocation de démarrage sécurisé, depuis la machine virtuelle, qui est un certificat Microsoft KEK (Key Exchange Key).

Dans la plupart des cas, il n'est pas nécessaire de remplacer les certificats existants. Si vous souhaitez remplacer les certificats, reportez-vous au système de la base de connaissances VMware.

La version 10.1 ou ultérieure de VMware Tools est requise pour les machines virtuelles qui utilisent le démarrage sécurisé UEFI. Vous pouvez mettre à niveau ces machines virtuelles vers une version ultérieure de VMware Tools, le cas échéant.

Pour les machines virtuelles Linux, VMware Host-Guest Filesystem n'est pas pris en charge en mode de démarrage sécurisé. Supprimez VMware Host-Guest Filesystem de VMware Tools avant d'activer le démarrage sécurisé.

Note Si vous activez le démarrage sécurisé pour une machine virtuelle, vous ne pouvez charger que des pilotes signés sur cette machine virtuelle.

Cette tâche décrit comment utiliser vSphere Client pour activer et désactiver le démarrage sécurisé d'une machine virtuelle. Vous pouvez également créer des scripts pour gérer les paramètres de machine virtuelle. Par exemple, vous pouvez automatiser le basculement du microprogramme du BIOS vers l'EFI pour les machines virtuelles disposant du code PowerCLI suivant :

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Pour plus d'informations, reportez-vous à la section *Guide de l'utilisateur de VMware PowerCLI*.

Conditions préalables

Vous pouvez activer le démarrage sécurisé uniquement si toutes les conditions préalables sont remplies. Si les conditions préalables ne sont pas remplies, la case à cocher n'est pas visible dans vSphere Client.

- Vérifiez que le système d'exploitation et le micrologiciel de la machine virtuelle prennent en charge le démarrage UEFI.
  - Micrologiciel EFI
  - Matériel virtuel version 13 ou ultérieure.

- Système d'exploitation prenant en charge le démarrage sécurisé UEFI.

Note Certains systèmes d'exploitation invités ne prennent pas en charge le remplacement du démarrage BIOS par le démarrage UEFI sans que des modifications leur soient apportées. Consultez la documentation de votre système d'exploitation invité avant de passer au démarrage UEFI. Si vous mettez à niveau une machine virtuelle qui utilise déjà le démarrage UEFI vers un système d'exploitation prenant en charge le démarrage sécurisé UEFI, vous pouvez activer le démarrage sécurisé pour cette machine virtuelle.

- Désactivez la machine virtuelle. Si la machine virtuelle est en cours d'exécution, la case est grisée.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Cliquez sur l'onglet **Options de VM** et développez **Options de démarrage**.
4. Sous **Options de démarrage**, assurez-vous que le microprogramme est défini sur **EFI**.
5. Sélectionnez votre tâche.
   - Sélectionnez la case à cocher **Démarrage sécurisé** pour activer le démarrage sécurisé.
   - Désélectionnez la case à cocher **Démarrage sécurisé** pour désactiver le démarrage sécurisé.
6. Cliquez sur **OK**.

Résultats

Lorsque la machine virtuelle démarre, seuls les composants ayant des signatures valides sont autorisés. Le processus de démarrage s'arrête avec une erreur s'il rencontre un composant ayant une signature manquante ou non valide.

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 quantité d'informations excède la capacité de la banque de données.

La limite par défaut du fichier de configuration de machine virtuelle (fichier VMX) est de 1 Mo. Cette capacité est généralement suffisante, mais vous pouvez modifier cette valeur si nécessaire. Par exemple, vous pouvez augmenter la limite si vous stockez des quantités importantes d'informations personnalisées dans le fichier.

Note Étudiez soigneusement le volume d'informations dont vous avez besoin. Si la quantité d'informations excède la capacité de la banque de données, un déni de service peut survenir.

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. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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 invité 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. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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
`isolation.tools.diskWiper.disable`	TRUE
`isolation.tools.diskShrink.disable`	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.

- Minimiser 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 ont accès à la console de machine virtuelle ont accès à la gestion de l'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. L'accès à la console peut donc permettre une attaque malveillante sur une machine virtuelle.

- 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 exécuté sur une machine virtuelle peut entraîner l'attaque de cette dernière. En désactivant les composants du système qui ne sont pas nécessaires pour prendre en charge l'application ou le service exécuté sur le système, vous réduisez les risques d'attaque.

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*.

Minimiser 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 ont accès à la console de machine virtuelle ont accès à la gestion de l'alimentation des machines virtuelles et aux contrôles de la connectivité des périphériques amovibles. L'accès à la console peut donc permettre une attaque malveillante sur une machine virtuelle.

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 de machine virtuelle.

   Par exemple, dans un environnement hautement sécurisé, limitez ce nombre à une connexion. Dans certains environnements, vous pouvez augmenter la limite si plusieurs connexions simultanées sont requises pour effectuer des tâches normales.

   a. Dans vSphere Client, mettez la machine virtuelle hors tension.

   b. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

   c. Cliquez sur l'onglet **Options VM** et développez les **Options de VMware Remote Console**.

   d. Entrez le nombre maximum de sessions, par exemple, **2**.

   e. Cliquez sur **OK**.

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.

Ne définissez pas de limites ou n'utilisez pas de pools de ressources 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 exécuté sur une machine virtuelle peut entraîner l'attaque de cette dernière. En désactivant les composants du système qui ne sont pas nécessaires pour prendre en charge l'application ou le service exécuté sur le système, vous réduisez les risques d'attaque.

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.

Note Lorsque cela est possible, installez les systèmes d'exploitation invités en utilisant les modes d'installation « minimal » ou « core » pour réduire la taille, la complexité et la surface d'attaque du système d'exploitation invité.

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 de CD/DVD, les lecteurs de disquettes et les adaptateurs USB.
- Désactivez les fonctionnalités non utilisées, telles que les fonctionnalités d'affichage ou la fonctionnalité de dossiers partagés VMware, qui permet le partage de fichiers de l'hôte sur la machine virtuelle (HGFS, Host Guest File System).
- Désactivez les écrans de veille.
- N'exécutez pas le système X Window sous des systèmes d'exploitation invités 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 disposant de privilèges 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 peut aider à la prévention des attaques.

Un pirate ayant accès à une machine virtuelle peut connecter un périphérique matériel déconnecté et accéder à des informations sensibles sur n'importe quel média qui est laissé dans celui-ci. Il peut également déconnecter une carte réseau pour isoler la machine virtuelle de son réseau, ce qui constitue un déni de service.

- Ne connectez pas des périphériques non autorisés à la machine virtuelle.
- Retirez les périphériques matériels inutiles ou inutilisés.
- Désactivez les périphériques virtuels inutiles au sein d'une machine virtuelle.
- Vérifiez que seuls les périphériques requis sont connectés à une machine virtuelle. Les machines virtuelles utilisent rarement les ports série ou parallèles. En règle générale, les lecteurs CD/DVD ne sont connectés que temporairement lors de l'installation du logiciel.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.
3. Désactivez les périphériques matériels qui ne sont pas nécessaires.

   Vérifiez notamment les périphériques suivants :

   - Ports série
   - Ports parallèles
   - Contrôleurs USB

- Lecteurs de CD-ROM

Note Vous devez utiliser des commandes PowerCLI pour gérer les périphériques de lecteur de disquettes dans vSphere 7.0 et versions ultérieures.

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.

Conditions préalables

Mettez la machine virtuelle hors tension.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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. Le cas échéant, ajoutez ou modifiez les paramètres suivants.

Option	Description
svga.vgaonly	Si vous définissez ce paramètre sur TRUE, les fonctions graphiques avancées ne fonctionnent plus. Seul le mode de console en cellule de caractère est disponible. Si vous utilisez ce paramètre, `mks.enable3d` n'a aucun effet. **Note** Appliquez ce paramètre uniquement aux machines virtuelles n'ayant pas besoin d'une carte vidéo virtualisée.
mks.enable3d	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 peuvent fonctionner dans un environnement vSphere et sur des plates-formes de virtualisation hébergées comme VMware Workstation et VMware Fusion. Certains paramètres de machine virtuelle ne nécessitent pas d'être activés lorsque vous exécutez une machine virtuelle dans un environnement vSphere. Désactivez ces paramètres afin de réduire les possibilités de vulnérabilités.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.

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 la fonctionnalité de dossiers partagés VMware pour le partage des fichiers de l'hôte sur la machine virtuelle

Dans les environnements hautement sécurisés, vous pouvez désactiver certains composants pour minimiser le risque d'utilisation du système HGFS (Host Guest File System) par un pirate pour transférer des fichiers dans le système d'exploitation invité.

Modifier les paramètres décrits dans cette section affecte uniquement la fonctionnalité de dossiers partagés et n'affecte pas le serveur HGFS exécuté dans le cadre des outils des machines virtuelles invitées. En outre, ces paramètres n'affectent pas la mise à niveau automatique et les commandes VIX qui utilisent les transferts de fichiers des outils.

Procédure

1 Accédez à la machine virtuelle dans l'inventaire de vSphere Client.

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.

La valeur TRUE empêche le processus VMX de recevoir une notification des processus de mise à niveau, du démon ou du service de chaque outil informant des capacités du serveur HGFS.

6 (Facultatif) Vérifiez que le paramètre `isolation.tools.hgfs.disable` est défini sur TRUE.

La valeur TRUE désactive la fonctionnalité de dossiers partagés VMware inutilisée pour le partage des fichiers de l'hôte sur la machine virtuelle.

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 utilisantvSphere Client.

Les valeurs par défaut de ces options sont définies pour garantir un environnement sécurisé. 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. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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. Assurez-vous que les valeurs suivantes sont utilisées dans les colonnes Nom et Valeur, ou ajoutez les.

Nom	Valeur
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

   Ces options écrasent les valeurs entrées dans Panneau de configuration de VMware Tools, sur le système d'exploitation invité.
6. Cliquez sur **OK**.
7. (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. Lorsque la fenêtre de console s'affiche, les processus en cours d'exécution dans la machine virtuelle et les utilisateurs sans privilèges peuvent accéder au presse-papiers

de la console de machine virtuelle. Si un utilisateur copie des informations sensibles dans le presse-papiers avant d'utiliser la console, son utilisation peut exposer 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 Administrateur de vCenter Server peut interagir avec les fichiers et les applications 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**. Attribuez ce rôle aux administrateurs qui n'ont pas besoin d'avoir accès aux fichiers de la machine virtuelle.

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. Appliquez un rôle personnalisé qui désactive l'accès invité aux utilisateurs qui ont besoin de privilèges d'administrateur mais qui ne sont pas autorisés à interagir avec les fichiers et les applications du système d'exploitation invité.

Prenons, par exemple, une configuration composée d'une machine virtuelle placée dans une infrastructure contenant des informations sensibles.

Si des tâches telles que la migration avec vMotion nécessitent que les administrateurs de centre de données puissent accéder à la machine virtuelle, désactivez certaines opérations sur le système d'exploitation invité afin que ces administrateurs ne puissent pas accéder 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 Client en tant qu'utilisateur possédant des privilèges **Administrateur** sur le système vCenter Server sur lequel vous souhaitez créer le rôle.
2. Sélectionnez **Administration**, puis cliquez sur **Rôles**.
3. Cliquez sur le rôle d'administrateur et sur l'icône **Cloner une action de rôle**.
4. Tapez un nom de rôle et une description, puis cliquez sur **OK**.

   Par exemple, entrez **`Accès non-invité administrateur`**.
5. Sélectionnez le rôle cloné et cliquez sur l'icône **Modifier une action de rôle**.
6. Sous le privilège **Machine virtuelle**, désélectionnez les **Opérations des invités** et cliquez sur **Suivant**.
7. Cliquez sur **Terminer**.

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 Administrateur.

Interdiction pour les utilisateurs ou les processus de machines virtuelles de déconnecter les périphériques

Les utilisateurs et les processus sans privilèges racine ou d'administrateur au sein des machines virtuelles ont la possibilité de connecter ou déconnecter des périphériques, comme les adaptateurs réseau et les lecteurs de CD-ROM, et peuvent modifier leurs paramètres. Afin de renforcer la sécurité des machines virtuelles, supprimez ces périphériques.

Vous pouvez empêcher les utilisateurs de machine virtuelle dans le système d'exploitation invité et les processus en cours d'exécution dans le système d'exploitation invité d'apporter des modifications aux périphériques en modifiant les paramètres avancés de la machine virtuelle.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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. Assurez-vous que les valeurs suivantes sont utilisées dans les colonnes Nom et Valeur, ou ajoutez-les.

Nom	Valeur
isolation.device.connectable.disable	vrai
isolation.device.edit.disable	vrai

   Ces paramètres n'affectent pas la capacité d'un administrateur vSphere à connecter ou déconnecter les périphériques attachés à la machine virtuelle.
6. Cliquez sur **OK** pour fermer la boîte de dialogue Paramètres de configuration, puis cliquez de nouveau sur **OK**.

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

Pour vous assurer que le système d'exploitation invité ne modifie par les paramètres de configuration, vous pouvez empêcher ces processus d'écrire des paires nom-valeur dans le fichier de configuration.

Conditions préalables

Désactivez la machine virtuelle.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.
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 le paramètre de configuration** et tapez les valeurs suivantes dans les colonnes Nom et Valeur.

Colonne	Valeur
Nom	`isolation.tools.setinfo.disable`
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 des machines virtuelles avec Intel Software Guard Extensions

vSphere vous permet de configurer vSGX (Virtual Intel® Software Guard Extensions) pour les machines virtuelles. L'utilisation de vSGX vous permet de fournir une sécurité supplémentaire à vos charges de travail.

Certains processeurs Intel modernes mettent en œuvre une extension de sécurité appelée Intel® Software Guard Extensions (Intel® SGX). Intel SGX est une technologie spécifique au processeur pour les développeurs d'applications qui cherchent à protéger une sélection de code et de données contre la divulgation ou la modification. Intel SGX permet de définir des régions privées de mémoire, appelées enclaves, pour le code au niveau utilisateur. Le contenu de l'enclave est protégé afin que le code exécuté en dehors de l'enclave ne puisse pas accéder au contenu de l'enclave.

vSGX permet aux machines virtuelles d'utiliser la technologie Intel SGX si elle est disponible sur le matériel. Pour utiliser vSGX l'hôte ESXi doit être installé sur un CPU compatible SGX et SGX doit être activé dans le BIOS de l'hôte ESXi. Vous pouvez utiliser vSphere Client pour activer SGX pour une machine virtuelle.

Présentation de vSGX

Les machines virtuelles peuvent utiliser la technologie Intel SGX, si elle disponible sur le matériel.

Conditions requises pour vSGX

Pour utiliser vSGX, votre environnement vSphere doit répondre aux exigences suivantes :

- Configuration requise pour la machine virtuelle :
  - Micrologiciel EFI
  - Version matérielle 17
- Configuration requise pour le composant :
  - vCenter Server 7.0
  - ESXi 7.0
- Prise en charge du système d'exploitation invité :
  - Linux
  - Windows Server 2016 (64 bits) et versions ultérieures
  - Windows 10 (64 bits) et versions ultérieures

Matériel Intel

Utilisez le matériel Intel suivant pour vSGX :

- Processeur Coffee Lake ou ultérieur.

Vous devrez peut-être désactiver l'hyperthreading sur certains CPU pour activer SGX sur l'hôte ESXi. Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/71367.

Fonctionnalités de VMware non prises en charge sur vSGX

Les fonctionnalités suivantes ne sont pas prises en charge dans une machine virtuelle lorsque vSGX est activé :

- Migration vMotion/DRS
- Interruption et reprise de machine virtuelle
- Snapshots de machines virtuelles (les snapshots de machine virtuelle sont pris en charge si vous ne prenez pas de snapshot de la mémoire de la machine virtuelle.)
- Fault Tolerance
- Intégrité de l'invité (GI, fondation de plateforme pour VMware AppDefense™ 1.0)

Note Ces fonctionnalités VMware ne sont pas prises en charge en raison de la manière dont l'architecture Intel SGX fonctionne. Cela n'est pas dû à une insuffisance de VMware.

Activer vSGX sur une machine virtuelle

Vous pouvez activer vSGX sur une machine virtuelle au moment de la création d'une machine virtuelle.

Conditions préalables

L'hôte ESXi doit être installé sur un processeur compatible SGX et SGX doit être activé dans le BIOS de l'hôte. Reportez-vous à Présentation de vSGX pour en savoir plus sur les processeurs Intel pris en charge.

Créez une machine virtuelle qui utilise la version matérielle 17 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Linux
- Windows 10 (64 bits) et versions ultérieures
- Windows Server 2016 (64 bits) et versions ultérieures

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.

3 Cliquez avec le bouton droit sur l'objet, sélectionnez **Nouvelle machine virtuelle** et suivez les invites pour créer une machine virtuelle.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom et un emplacement cible
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous disposez des privilèges de création de machines virtuelles.
Sélectionner le stockage	Dans la stratégie de stockage VM, sélectionnez la stratégie de stockage. Sélectionnez une banque de données compatible.
Sélectionner une compatibilité	Assurez-vous qu'**ESXi 7.0 et versions ultérieures** est sélectionné.
Sélectionner un système d'exploitation invité	Sélectionnez Linux, Windows 10 (64 bits) ou Windows Server 2016 (64 bits).
Personnalisation du matériel	Sous Périphériques de sécurité, cochez la case **Activer** pour SGX. Sous **Options VM > Options de démarrage > Microprogramme**, assurez- vous qu'EFI est sélectionné. Entrez la taille du cache EPC (Enclave Page Cache, cache de la page d'enclave) et sélectionnez le mode FLC (Flexible Launch Control, contrôle de lancement flexible) en conséquence.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Activer vSGX sur une machine virtuelle existante

Vous pouvez activer vSGX sur une machine virtuelle existante.

Vous pouvez activer vSGX pour les machines virtuelles s'exécutant sur vSphere 7.0 et versions ultérieures.

Conditions préalables

- L'hôte ESXi doit être installé sur un processeur compatible SGX et SGX doit être activé dans le BIOS de l'hôte. Reportez-vous à Présentation de vSGX pour en savoir plus sur les processeurs Intel pris en charge.
- Le SE invité que vous utilisez doit être Linux, Windows Server 2016 (64 bits) ou version ultérieure, ou Windows 10 (64 bits) ou version ultérieure.
- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être ESXi 7.0 ou version ultérieure.
- Vérifiez si la machine virtuelle est désactivée.
- La machine virtuelle doit utiliser le microprogramme EFI.
- La machine virtuelle doit utiliser la version matérielle 17 ou ultérieure.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Client.

2 Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.

3 Dans la boîte de dialogue **Modifier les paramètres**, sous **Périphériques de sécurité**, cochez la case **Activer** pour SGX.

4 Entrez la taille du cache EPC (Enclave Page Cache, cache de la page d'enclave) et sélectionnez le mode FLC (Flexible Launch Control, contrôle de lancement flexible) en conséquence.

5 Sous **Options VM > Options de démarrage > Microprogramme**, assurez- vous qu'EFI est sélectionné.

6 Cliquez sur **OK**.

Supprimer vSGX d'une machine virtuelle

Vous pouvez supprimer vSGX d'une machine virtuelle.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Client.

2 Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.

3 Dans la boîte de dialogue **Modifier les paramètres**, sous **Périphériques de sécurité**, décochez la case **Activer** pour SGX.

4 Cliquez sur **OK**.

Vérifiez que l'entrée vSGX n'apparaît plus dans l'onglet **Résumé** de la machine virtuelle, dans le volet **Matériel VM**.

Sécurisation des machines virtuelles avec SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD

SEV-ES est une fonctionnalité matérielle activée dans les CPU AMD récents qui maintient l'état chiffré de la mémoire et du registre du système d'exploitation invité, ce qui le protège contre tout accès depuis l'hyperviseur.

Vous pouvez ajouter SEV-ES à vos machines virtuelles en tant qu'amélioration de la sécurité. SEV-ES empêche les fuites d'informations des registres de CPU dans des registres de composants tels que l'hyperviseur. SEV-ES peut également détecter les modifications malveillantes apportées à un état de registre de CPU.

Présentation de l'état chiffré sécurisé SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD

Dans vSphere 7.0 Update 1 et versions ultérieures, vous pouvez activer SEV-ES (Secure Encrypted Virtualization-Encrypted State) sur les CPU AMD et les systèmes d'exploitation invités pris en charge.

Actuellement, SEV-ES prend uniquement en charge les CPU AMD EPYC 7xx2 (nom de code « Rome ») et les CPU ultérieurs, et uniquement les versions des noyaux Linux qui incluent une prise en charge spécifique de SEV-ES.

Composants et architecture de SEV-ES

L'architecture SEV-ES comprend les composants suivants.

- CPU AMD, en particulier le processeur PSP (Platform Security Processor) qui gère les clés de chiffrement et le chiffrement.
- Système d'exploitation recommandé, c'est-à-dire système d'exploitation qui utilise des appels initiés par l'invité à l'hyperviseur.
- Moniteur de machine virtuelle (VMM) et exécutable de machine virtuelle (VMX), pour initialiser un état de machine virtuelle chiffré pendant la mise sous tension de la machine virtuelle et pour gérer les appels du système d'exploitation invité.
- Pilote VMkernel, pour échanger des données non chiffrées entre l'hyperviseur et le système d'exploitation invité.

Implémentation et gestion de SEV-ES sur ESXi

Vous devez d'abord activer SEV-ES dans la configuration du BIOS d'un système. Reportez-vous à la documentation de votre système pour plus d'informations sur l'accès à la configuration du BIOS. Après avoir activé SEV-ES dans le BIOS du système, vous pouvez ajouter SEV-ES à une machine virtuelle.

Utilisez vSphere Client (à partir de vSphere 7.0 Update 2) ou les commandes PowerCLI pour activer et désactiver SEV-ES sur les machines virtuelles. Vous pouvez créer des machines virtuelles avec SEV-ES ou activer SEV-ES sur des machines virtuelles existantes. Les privilèges de gestion des machines virtuelles activées disposant de SEV-ES sont les mêmes que pour la gestion de machines virtuelles standard.

Fonctionnalités de VMware non prises en charge sur SEV-ES

Les fonctionnalités suivantes ne sont pas prises en charge lorsque SEV-ES est activé.

- Mode de gestion du système
- vMotion
- Snapshots sous tension (les snapshots de mémoire ne sont toutefois pas pris en charge)
- Ajouter ou supprimer à chaud un CPU ou de la mémoire

- Interrompre/reprendre
- VMware Fault Tolerance
- Clones et clones instantanés
- Intégrité d'invité

Ajouter un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD à une machine virtuelle avec vSphere Client

À partir de vSphere 7.0 Update 2, vous pouvez utiliser vSphere Client pour ajouter SEV-ES à une machine virtuelle afin de fournir une sécurité renforcée au système d'exploitation invité.

Vous pouvez ajouter SEV-ES aux machines virtuelles exécutées sur ESXi 7.0 Update 1 ou version ultérieure.

Conditions préalables

- Un CPU AMD EPYC 7xx2 (nom de code « Rome ») ou version ultérieure et prenant en charge le BIOS doit être installé sur le système.
- SEV-ES doit être activé dans le BIOS.
- Le nombre de machines virtuelles SEV-ES par hôte ESXi est contrôlé par le BIOS. Lors de l'activation de SEV-ES dans le BIOS, entrez une valeur pour le paramètre **Minimum SEV non-ES ASID** correspondant au nombre de machines virtuelles SEV-ES plus un. Par exemple, si vous disposez de 12 machines virtuelles que vous souhaitez exécuter simultanément, entrez **13**. Des paramètres aussi élevés que 500 sont pris en charge par ESXi.

  Note vSphere 7.0 Update 1 prend en charge 16 machines virtuelles compatibles SEV par hôte ESXi. L'utilisation d'un paramètre plus élevé dans le BIOS n'empêche pas SEV-ES de fonctionner. Cependant, la limite de 16 s'applique toujours.

- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être à la version ESXi 7.0 Update 1 ou version ultérieure.
- L'instance de vCenter Server doit être à la version vSphere 7.0 Update 2 ou une version ultérieure.
- Le système d'exploitation invité doit prendre en charge SEV-ES.

  Actuellement, seuls les noyaux Linux avec une prise en charge spécifique de SEV-ES sont pris en charge.
- Le démarrage sécurisé UEFI doit être activé sur la machine virtuelle.
- La machine virtuelle doit être à la version matérielle 18 ou ultérieure.
- L'option **Réserver toute la mémoire de l'invité** doit être activée sur la machine virtuelle, sinon la mise sous tension échoue.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Cliquez avec le bouton droit sur l'objet, sélectionnez **Nouvelle machine virtuelle** et suivez les invites pour créer une machine virtuelle.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom et un emplacement cible
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous disposez des privilèges de création de machines virtuelles.
Sélectionner le stockage	Dans la stratégie de stockage VM, sélectionnez la stratégie de stockage. Sélectionnez une banque de données compatible.
Sélectionner une compatibilité	Assurez-vous qu'**ESXi 7.0 et versions ultérieures** est sélectionné.
Sélectionner un système d'exploitation invité	Sélectionnez Linux et choisissez une version de Linux avec une prise en charge spécifique de SEV-ES.
Personnalisation du matériel	Sous **Options VM > Options de démarrage > Microprogramme**, assurez-vous qu'EFI est sélectionné. Sous **Options de VM > Chiffrement**, cochez la case **Activer** pour AMD SEV-ES.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Résultats

La machine virtuelle est créée avec SEV-ES.

Ajouter un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD à une machine virtuelle

Vous pouvez ajouter SEV-ES (Secure Encrypted Virtualization-Encrypted State) à une machine virtuelle pour apporter une sécurité renforcée au système d'exploitation invité.

Vous pouvez ajouter SEV-ES aux machines virtuelles exécutées sur ESXi 7.0 Update 1 ou version ultérieure.

Conditions préalables

- Un CPU AMD EPYC 7xx2 (nom de code « Rome ») ou version ultérieure et prenant en charge le BIOS doit être installé sur le système.
- SEV-ES doit être activé dans le BIOS.

- Le nombre de machines virtuelles SEV-ES par hôte ESXi est contrôlé par le BIOS. Lors de l'activation de SEV-ES dans le BIOS, entrez une valeur pour le paramètre **Minimum SEV non-ES ASID** correspondant au nombre de machines virtuelles SEV-ES plus un. Par exemple, si vous disposez de 12 machines virtuelles que vous souhaitez exécuter simultanément, entrez **13**. Des paramètres aussi élevés que 500 sont pris en charge par ESXi.

  Note vSphere 7.0 Update 1 prend en charge 16 machines virtuelles compatibles SEV par hôte ESXi. L'utilisation d'un paramètre plus élevé dans le BIOS n'empêche pas SEV-ES de fonctionner. Cependant, la limite de 16 s'applique toujours.

- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être à la version ESXi 7.0 Update 1 ou version ultérieure.
- Le système d'exploitation invité doit prendre en charge SEV-ES.

  Actuellement, seuls les noyaux Linux avec une prise en charge spécifique de SEV-ES sont pris en charge.
- Le démarrage sécurisé UEFI doit être activé sur la machine virtuelle.
- La machine virtuelle doit être à la version matérielle 18 ou ultérieure.
- L'option **Réserver toute la mémoire de l'invité** doit être activée sur la machine virtuelle, sinon la mise sous tension échoue.
- PowerCLI 12.1.0 ou version ultérieure doit être installé sur un système ayant accès à votre environnement.

Procédure

1 Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu'administrateur à l'instance de vCenter Server qui gère l'hôte ESXi sur lequel vous souhaitez ajouter une machine virtuelle avec SEV-ES.

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 Créez la machine virtuelle avec l'applet de commande `New-VM`, en spécifiant `-SEVEnabled $true`.

Par exemple, attribuez d'abord les informations de l'hôte à une variable, puis créez la machine virtuelle.

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

Si vous devez spécifier la version du matériel virtuel, exécutez l'applet de commande `New-VM` avec le paramètre `-HardwareVersion vmx-18`. Par exemple :

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true -HardwareVersion
vmx-18
```

Résultats

La machine virtuelle est créée avec SEV-ES.

Activer un état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle existante avec vSphere Client

À partir de vSphere 7.0 Update 2, vous pouvez utiliser vSphere Client pour ajouter SEV-ES à une machine virtuelle existante afin de fournir une sécurité renforcée au système d'exploitation invité.

Vous pouvez ajouter SEV-ES aux machines virtuelles exécutées sur ESXi 7.0 Update 1 ou version ultérieure.

Conditions préalables

- Un CPU AMD EPYC 7xx2 (nom de code « Rome ») ou version ultérieure et prenant en charge le BIOS doit être installé sur le système.
- SEV-ES doit être activé dans le BIOS.
- Le nombre de machines virtuelles SEV-ES par hôte ESXi est contrôlé par le BIOS. Lors de l'activation de SEV-ES dans le BIOS, entrez une valeur pour le paramètre **Minimum SEV non-ES ASID** correspondant au nombre de machines virtuelles SEV-ES plus un. Par exemple, si vous disposez de 12 machines virtuelles que vous souhaitez exécuter simultanément, entrez **13**. Des paramètres aussi élevés que 500 sont pris en charge par ESXi.

  Note vSphere 7.0 Update 1 prend en charge 16 machines virtuelles compatibles SEV par hôte ESXi. L'utilisation d'un paramètre plus élevé dans le BIOS n'empêche pas SEV-ES de fonctionner. Cependant, la limite de 16 s'applique toujours.
- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être à la version ESXi 7.0 Update 1 ou version ultérieure.
- L'instance de vCenter Server doit être à la version vSphere 7.0 Update 2 ou une version ultérieure.
- Le système d'exploitation invité doit prendre en charge SEV-ES.

  Actuellement, seuls les noyaux Linux avec une prise en charge spécifique de SEV-ES sont pris en charge.
- Le démarrage sécurisé UEFI doit être activé sur la machine virtuelle.
- La machine virtuelle doit être à la version matérielle 18 ou ultérieure.
- L'option **Réserver toute la mémoire de l'invité** doit être activée sur la machine virtuelle, sinon la mise sous tension échoue.
- Assurez-vous que la machine virtuelle est hors tension.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.
3. Sous **Options VM > Options de démarrage > Microprogramme**, assurez- vous qu'EFI est sélectionné.
4. Dans la boîte de dialogue **Modifier les paramètres**, sous **Options de VM > Chiffrement**, cochez la case **Activer** pour AMD SEV-ES.
5. Cliquez sur **OK**.

Résultats

SEV-ES est ajouté à la machine virtuelle.

Activer SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle existante

Vous pouvez ajouter un SEV-ES (Secure Encrypted Virtualization-Encrypted State) à une machine virtuelle existante pour apporter une sécurité renforcée au système d'exploitation invité.

Vous pouvez ajouter SEV-ES aux machines virtuelles exécutées sur ESXi 7.0 Update 1 ou version ultérieure.

Conditions préalables

- Un CPU AMD EPYC 7xx2 (nom de code « Rome ») ou version ultérieure et prenant en charge le BIOS doit être installé sur le système.
- SEV-ES doit être activé dans le BIOS.
- Le nombre de machines virtuelles SEV-ES par hôte ESXi est contrôlé par le BIOS. Lors de l'activation de SEV-ES dans le BIOS, entrez une valeur pour le paramètre **Minimum SEV non-ES ASID** correspondant au nombre de machines virtuelles SEV-ES plus un. Par exemple, si vous disposez de 12 machines virtuelles que vous souhaitez exécuter simultanément, entrez **13**. Des paramètres aussi élevés que 500 sont pris en charge par ESXi.

  Note vSphere 7.0 Update 1 prend en charge 16 machines virtuelles compatibles SEV-ES par hôte ESXi. L'utilisation d'un paramètre plus élevé dans le BIOS n'empêche pas SEV-ES de fonctionner. Cependant, la limite de 16 s'applique toujours.

- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être à la version ESXi 7.0 Update 1 ou version ultérieure.
- Le système d'exploitation invité doit prendre en charge SEV-ES.

  Actuellement, seuls les noyaux Linux avec une prise en charge spécifique de SEV-ES sont pris en charge.
- Le démarrage sécurisé UEFI doit être activé sur la machine virtuelle.

- La machine virtuelle doit être à la version matérielle 18 ou ultérieure.
- L'option **Réserver toute la mémoire de l'invité** doit être activée sur la machine virtuelle, sinon la mise sous tension échoue.
- PowerCLI 12.1.0 ou version ultérieure doit être installé sur un système ayant accès à votre environnement.
- Assurez-vous que la machine virtuelle est hors tension.

Procédure

1. Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu'administrateur à l'instance de vCenter Server qui gère l'hôte ESXi avec la machine virtuelle à laquelle vous souhaitez ajouter des SEV-ES.

   Par exemple :

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. Ajoutez SEV-ES à la machine virtuelle avec l'applet de commande `Set-VM`, en spécifiant `-SEVEnabled $true`.

   Par exemple :

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
   ```

   Si vous devez spécifier la version du matériel virtuel, exécutez l'applet de commande `Set-VM` avec le paramètre `-HardwareVersion vmx-18`. Par exemple :

   ```
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
   ```

Résultats

SEV-ES est ajouté à la machine virtuelle.

Désactiver l'état chiffré SEV-ES (Secure Encrypted Virtualization-Encrypted State) AMD sur une machine virtuelle avec vSphere Client

À partir de vSphere 7.0 Update 2, vous pouvez utiliser vSphere Client pour désactiver SEV-ES sur une machine virtuelle.

Conditions préalables

- Assurez-vous que la machine virtuelle est hors tension.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.

3 Dans la boîte de dialogue **Modifier les paramètres**, sous **Options de VM > Chiffrement**, décochez la case **Activer** pour AMD SEV-ES.

4 Cliquez sur **OK**.

Résultats

SEV-ES est désactivé sur la machine virtuelle.

Désactiver l'état SEV-ES AMD (Secure Encrypted Virtualization-Encrypted State) sur une machine virtuelle

Vous pouvez désactiver SEV-ES sur une machine virtuelle.

Conditions préalables

- Assurez-vous que la machine virtuelle est hors tension.
- PowerCLI 12.1.0 ou version ultérieure doit être installé sur un système ayant accès à votre environnement.

Procédure

1 Dans une session PowerCLI, exécutez l'applet de commande `Connect–VIServer` pour vous connecter en tant qu'administrateur à l'instance de vCenter Server qui gère l'hôte ESXi avec la machine virtuelle sur laquelle vous souhaitez supprimer SEV-ES.

Par exemple :

```
Connect–VIServer –server vCenter_Server_ip_address –User admin_user –Password 'password'
```

2 Désactivez SEV-ES sur la machine virtuelle avec l'applet de commande `Set–VM`, en spécifiant `–SEVEnabled $false`.

Par exemple, attribuez d'abord les informations de l'hôte à une variable, puis désactivez SEV-ES pour la machine virtuelle.

```
$vmhost = Get–VMHost –Name 10.193.25.83
Set–VM –Name MyVM2 $vmhost –SEVEnabled $false
```

Résultats

SEV-ES est désactivé sur la machine virtuelle.

Chiffrement des machines virtuelles

6

Avec le chiffrement de machines virtuelles vSphere, vous pouvez chiffrer vos charges de travail sensibles de manière encore plus sécurisée. L'accès aux clés de chiffrement peut être subordonné à l'état d'approbation de l'hôte ESXi.

Avant de pouvoir commencer avec des tâches de chiffrement de machine virtuelle, vous devez configurer un fournisseur de clés. Les types de fournisseurs de clés suivants sont disponibles.

Tableau 6-1. Fournisseurs de clés vSphere

Fournisseur de clés	Description	Pour plus d'informations
Fournisseur de clés standard	Disponible dans vSphere 6.5 et les versions ultérieures, le fournisseur de clés standard utilise vCenter Server pour demander des clés à partir d'un serveur de clés externe. Ce dernier génère et stocke les clés, et les transmet à vCenter Server pour distribution.	Reportez-vous à la section Chapitre 7 Configuration et gestion d'un fournisseur de clés standard.
Fournisseur de clés approuvé	Disponible dans vSphere 7.0 et les versions ultérieures, le fournisseur de clés approuvé Autorité d'approbation vSphere conditionne l'accès aux clés de chiffrement à l'état d'attestation d'un cluster de charge de travail. Autorité d'approbation vSphere nécessite un serveur de clés externe.	Reportez-vous à la section Chapitre 9 Autorité d'approbation vSphere .
VMware vSphere® Native Key Provider™	Disponible à partir de vSphere 7.0 Update 2, vSphere Native Key Provider est inclus dans toutes les éditions de vSphere et ne nécessite pas de serveur de clés externe.	Reportez-vous à la section Chapitre 8 Configuration et gestion de vSphere Native Key Provider.

Ce chapitre contient les rubriques suivantes :

- Comparaison des fournisseurs de clés vSphere
- Méthodologie utilisée par le chiffrement de machine virtuelle vSphere pour protéger votre environnement

- Composants du chiffrement des machines virtuelles vSphere
- Flux de chiffrement
- Chiffrement des disques virtuels
- Erreurs de chiffrement des machines virtuelles
- Conditions préalables et privilèges requis pour les tâches de chiffrement
- vSphere vMotion chiffré
- Meilleures pratiques de chiffrement, mises en garde et interopérabilité
- Présentation de la persistance des clés

Comparaison des fournisseurs de clés vSphere

Une présentation générale des fonctionnalités des fournisseurs de clés vSphere nécessite votre attention pour vous aider à planifier votre stratégie de chiffrement.

En général, il existe peu de différences entre les fournisseurs de clés dans les opérations quotidiennes de prise en charge des fonctionnalités ou des produits. Bien que les fournisseurs de clés se ressemblent et se comportent de manière similaire, vous pouvez avoir des exigences et des réglementations à prendre en compte lors du choix d'un fournisseur de clés, comme indiqué dans le tableau suivant.

Tableau 6-2. Considération relatives au fournisseur de clés

Fournisseur de clés	Retour sur investissement du matériel ?	Serveur de clés externe requis ?	Configuration rapide ?	Fonctionne uniquement avec vSphere ?
Fournisseur de clés standard	Non	Oui	Non	Non
Fournisseur de clés approuvé	Oui	Oui	Non	Non
vSphere Native Key Provider	Non	Non	Oui	Oui

Fonctionnalités de chiffrement

Les fonctionnalités de chiffrement suivantes sont supportées par chaque type de fournisseur de clés.

- Renouvellement de clés à l'aide du même fournisseur de clés ou d'un autre fournisseur de clés
- Rotation des clés
- vTPM (Virtual Trusted Platform Module)
- Chiffrement de disque
- Chiffrement des machines virtuelles vSphere

- Coexistence avec d'autres fournisseurs de clés
- Mise à niveau vers un fournisseur de clés différent

Fonctionnalités de vSphere

Ce qui suit décrit la prise en charge par le fournisseur de clés de certaines fonctionnalités vSphere importantes.

- Chiffrement vSphere vMotion : pris en charge par tous les types de fournisseurs de clés. Le même fournisseur de clés doit être disponible sur l'hôte de destination. Reportez-vous à la section vSphere vMotion chiffré.
- Sauvegarde et restauration basée sur des fichiers vCenter Server : le fournisseur de clés standard et vSphere Native Key Provider prennent en charge la sauvegarde et la restauration basées sur des fichiers vCenter Server. Étant donné que la plupart des informations de configuration de Autorité d'approbation vSphere sont stockées sur les hôtes ESXi, le mécanisme de sauvegarde basé sur des fichiers de vCenter Server ne sauvegarde pas ces informations. Pour vous assurer que les informations de configuration de votre déploiement de Autorité d'approbation vSphere sont enregistrées, reportez-vous à Sauvegarde de la configuration de Autorité d'approbation vSphere .

Produits VMware

Le tableau suivant compare la prise en charge par les fournisseurs de clés de certains produits VMware.

Tableau 6-3. Comparaison de la prise en charge des produits VMware

Fournisseur de clés	vSAN	Site Recovery Manager	vSphere Replication
Fournisseur de clés standard	Oui	Oui	Oui
Fournisseur de clés approuvé	Oui	Oui Si la même configuration de services Autorité d'approbation vSphere est disponible côté récupération, SRM avec réplication basée sur la baie est pris en charge.	Non
vSphere Native Key Provider	Oui	Oui	Oui

Matériel requis

Le tableau suivant compare certaines exigences matérielles minimales du fournisseur de clés.

Tableau 6-4. Comparaison du matériel requis

Fournisseur de clés	TPM sur hôte ESXi
Fournisseur de clés standard	Non requis
Fournisseur de clés approuvé	Requis sur les hôtes approuvés (hôtes du cluster approuvé). **Note** Actuellement, les hôtes ESXi du cluster d'autorité d'approbation ne requièrent pas de TPM. Cependant, il convient d'envisager d'installer de nouveaux hôtes ESXi disposant de TPM.
vSphere Native Key Provider	Non requis La disponibilité de vSphere Native Key Provider peut éventuellement être limitée aux hôtes avec un TPM.

Méthodologie utilisée par le chiffrement de machine virtuelle vSphere pour protéger votre environnement

Quel que soit le fournisseur de clés utilisé, avec le chiffrement des machines virtuelles vSphere, vous pouvez créer des machines virtuelles chiffrées et chiffrer des machines virtuelles existantes. Étant donné que tous les fichiers de machine virtuelle contenant des informations sensibles sont chiffrés, la machine virtuelle est protégée. Seuls les administrateurs disposant de privilèges de chiffrement peuvent effectuer des tâches de chiffrement et de déchiffrement.

Éléments pris en charge par le chiffrement des machines virtuelles vSphere

Le chiffrement des machines virtuelles vSphere fonctionne avec n'importe quel type de stockage pris en charge (NFS, iSCSI, Fibre Channel, stockage directement raccordé, etc.), y compris VMware vSAN. Pour plus d'informations sur l'utilisation du chiffrement sur un cluster vSAN, consultez la documentation *Administration de VMware vSAN*.

Le chiffrement des machines virtuelles vSphere et vSAN utilisent les mêmes bibliothèques de chiffrement, mais elles ont des profils différents. Le chiffrement des machines virtuelles est un chiffrement au niveau de la machine virtuelle et vSAN est un chiffrement au niveau de la banque de données.

Clés de chiffrement utilisées par chaque type de fournisseur de clés

Selon le type de fournisseur de clés, différentes clés de chiffrement sont utilisées et différentes méthodes sont utilisées pour les créer et les gérer.

Le fournisseur de clés standard utilise les clés suivantes.

1 L'hôte ESXi génère et utilise des clés internes pour chiffrer des machines virtuelles et des disques. Ces clés sont utilisées en tant que clés de chiffrement de données. Ce sont des clés XTS AES 256 bits.

2 vCenter Server demande les clés au serveur de clés (KMS). Ces clés sont utilisées en tant que clés de chiffrement de clés (KEK) et sont des clés AES 256 bits. vCenter Server stocke uniquement l'identifiant de chaque KEK et non la clé elle-même.

3 ESXi utilise la clé KEK pour chiffrer les clés internes et stocke la clé interne chiffrée sur le disque. ESXi ne stocke pas la clé KEK sur le disque. Lorsqu'un hôte redémarre, vCenter Server demande la clé KEK avec l'ID correspondant au serveur de clés et la met à la disposition du produit ESXi. ESXi peut alors déchiffrer les clés internes si nécessaire.

Le fournisseur de clés approuvé Autorité d'approbation vSphere utilise les clés suivantes.

1 L'instance de vCenter Server du cluster approuvé vérifie si le fournisseur de clés approuvé par défaut est accessible à l'hôte ESXi sur lequel la machine virtuelle chiffrée doit être créée.

2 L'instance de vCenter Server du cluster approuvé ajoute le fournisseur de clés approuvé à la machine virtuelle ConfigSpec.

3 La demande de création de la machine virtuelle est envoyée à l'hôte ESXi.

4 Si un jeton d'attestation n'est pas déjà disponible pour l'hôte ESXi, il en demande un à partir du service d'attestation.

5 Le service de fournisseur de clés valide le jeton d'attestation et crée une clé de chiffrement de clés (clé KEK) à envoyer à l'hôte ESXi. La clé KEK est encapsulée (chiffrée) avec la clé principale qui est configurée sur le fournisseur de clés. Les deux types de texte chiffré KEK et de texte brut KEK sont renvoyés à l'hôte approuvé.

6 L'hôte ESXi génère une clé de chiffrement de données (DEK) pour chiffrer les disques de la machine virtuelle.

7 La clé KEK est utilisé pour encapsuler les DEK générés par l'hôte ESXi et le texte chiffré du fournisseur de clés est stocké avec les données chiffrées.

8 La machine virtuelle est chiffrée et écrite dans le stockage.

Note Si vous supprimez ou annulez l'enregistrement d'une machine virtuelle chiffrée, le cluster et l'hôte ESXi suppriment la clé KEK du cache. L'hôte ESXi ne peut plus utiliser la clé KEK. Ce comportement est le même pour les fournisseurs de clés standard et les fournisseurs de clés approuvés.

vSphere Native Key Provider utilise les clés suivantes.

1 Lorsque vous créez le fournisseur de clés, vCenter Server génère une clé principale et la transmet aux hôtes ESXi du cluster.

2 Les hôtes ESXi génèrent une clé de chiffrement de données (DEK) à la demande.

3 Lorsque vous effectuez une activité de chiffrement, les données sont chiffrées avec la clé DEK.

   Les clés DEK chiffrées sont stockées avec les données chiffrées.

4 Lorsque vous déchiffrez des données, la clé principale est utilisée pour déchiffrer la clé DEK, puis les données.

Éléments chiffrés

Le chiffrement de machine virtuelle vSphere prend en charge le chiffrement des fichiers de machine virtuelle, les fichiers de disque virtuel et les fichiers de vidage de mémoire.

Fichiers de machine virtuelle

La plupart des fichiers de machine virtuelle, notamment les données invitées qui ne sont pas stockées dans le fichier VMDK, sont chiffrés. Cet ensemble de fichiers inclut les fichiers NVRAM, VSWP et VMSN, sans se limiter à ceux-ci. La clé provenant du fournisseur de clés déverrouille un bundle chiffré dans le fichier VMX qui contient des clés internes et d'autres secrets. La récupération de la clé fonctionne comme suit, selon le fournisseur de clés :

- Fournisseur de clés standard : vCenter Server gère les clés depuis le serveur de clés et les hôtes ESXi ne peuvent pas accéder directement au fournisseur de clés. Les hôtes attendent que vCenter Server transmette les clés.
- Fournisseur de clés approuvé et vSphere Native Key Provider : les hôtes ESXi accèdent directement aux fournisseurs de clés et récupèrent donc les clés demandées directement depuis le service Autorité d'approbation vSphere ou le vSphere Native Key Provider.

Lorsque vous utilisez vSphere Client pour créer une machine virtuelle chiffrée, vous pouvez chiffrer et déchiffrer des disques virtuels distincts à partir des fichiers de machine virtuelle. Tous les disques virtuels sont chiffrés par défaut. Pour d'autres tâches de chiffrement, comme le chiffrement d'une machine virtuelle existante, vous pouvez chiffrer et déchiffrer des disques virtuels distincts des fichiers de machine virtuelle.

Note Vous ne pouvez pas associer un disque virtuel chiffré à une machine virtuelle qui n'est pas chiffrée.

Fichiers de disque virtuel

Les données se trouvant dans un fichier de disque virtuel (VMDK) chiffré ne sont jamais écrites en texte clair dans le stockage ou le disque physique, et elles ne sont jamais transmises sur le réseau en texte clair. Le fichier descripteur VMDK est principalement en texte clair, mais il contient un ID de clé pour la clé KEK et la clé interne (DEK) dans le bundle chiffré.

Vous pouvez utiliser vSphere API pour effectuer une opération de rechiffrement de premier niveau avec une nouvelle clé KEK ou une opération de rechiffrement approfondi avec une nouvelle clé interne.

Vidages de mémoire

Les vidages de mémoire sur un hôte ESXi pour lequel le mode de chiffrement est activé sont toujours chiffrés. Reportez-vous à la section Chiffrement de machines virtuelles vSphere et vidages mémoire. Les vidages de mémoire sur le système vCenter Server ne sont pas chiffrés. Protégez l'accès au système vCenter Server.

Note Pour plus d'informations sur certaines des limites relatives aux dispositifs et aux fonctionnalités avec lesquels le chiffrement de machine virtuelle vSphere peut interagir, reportez-vous à la section Interopérabilité du chiffrement des machines virtuelles.

Éléments non chiffrés

Certains des fichiers associés à une machine virtuelle ne sont pas chiffrés ou sont partiellement chiffrés.

Fichiers de journalisation

Les fichiers de journalisation ne sont pas chiffrés, car ils ne contiennent pas de données sensibles.

Fichiers de configuration de la machine virtuelle

La plupart des informations de configuration de machine virtuelle stockées dans les fichiers VMX et VMSD ne sont pas chiffrées.

Fichier descripteur du disque virtuel

Pour permettre la gestion de disque sans clé, la plus grande partie du fichier descripteur du disque virtuel n'est pas chiffrée.

Personnes habilitées à effectuer des opérations cryptographiques

Seuls les utilisateurs auxquels des privilèges d'**opérations cryptographiques** ont été attribués peuvent effectuer des opérations de chiffrement. L'ensemble de privilèges est détaillé. Le rôle d'administrateur système par défaut possède tous les privilèges d'**opérations cryptographiques**. Le rôle d'administrateur sans droits de chiffrement prend en charge tous les privilèges d'administrateur à l'exception des privilèges **Opérations de chiffrement**.

En plus d'utiliser les privilèges **Cryptographer.***, vSphere Native Key Provider peut utiliser le privilège **Cryptographer.ReadKeyServersInfo**, qui est spécifique à vSphere Native Key Provider.

Consultez Privilèges d'opérations de chiffrement pour plus d'informations.

Vous pouvez créer des rôles personnalisés supplémentaires, par exemple pour autoriser un groupe d'utilisateurs à chiffrer des machines virtuelles tout en les empêchant de déchiffrer des machines virtuelles.

Méthodologie pour effectuer des opérations cryptographiques

vSphere Client prend en charge de nombreuses opérations cryptographiques. Pour d'autres tâches, vous pouvez utiliser vSphere API.

Tableau 6-5. Interfaces pour l'exécution d'opérations cryptographiques

Interface	Opérations	Informations
vSphere Client	Créer une machine virtuelle chiffrée Chiffrer et déchiffrer des machines virtuelles	Ce document
PowerCLI	Créer une machine virtuelle chiffrée Chiffrer et déchiffrer des machines virtuelles Configurer Autorité d'approbation vSphere	*Référence des applets de commande VMware PowerCLI*
vSphere Web Services SDK	Créer une machine virtuelle chiffrée Chiffrer et déchiffrer des machines virtuelles Effectuer un rechiffrement approfondi d'une machine virtuelle (utilisez une clé DEK différente) Effectuer un rechiffrement de premier niveau d'une machine virtuelle (utilisez une clé KEK différente)	*Guide de programmation de vSphere Web Services SDK* *Référence de l'API vSphere Web Services*
`crypto-util`	Déchiffrer les vidages de mémoire chiffrés Vérifier si les fichiers sont chiffrés ou non Effectuer d'autres tâches de gestion directement sur l'hôte ESXi	Aide relative à la ligne de commande Chiffrement de machines virtuelles vSphere et vidages mémoire

Rechiffrement des machines virtuelles

Vous pouvez recrypter une machine virtuelle avec de nouvelles clés, par exemple, au cas où une clé expire ou serait compromise. Les options suivantes sont disponibles.

- Un rechiffrement approfondi, qui remplace à la fois la clé de chiffrement de disque (DEK) et la clé de chiffrement de clé (KEK)
- Un rechiffrement superficiel qui remplace uniquement la clé KEK

Vous devez effectuer un rechiffrement d'une machine virtuelle à l'aide de l'API. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Un rechiffrement approfondi nécessite que la machine virtuelle soit mise hors tension et ne contienne aucun snapshot. Vous pouvez effectuer une opération de rechiffrement superficielle alors que la machine virtuelle est sous tension et si des snapshots sont présents sur la machine virtuelle. Le rechiffrement superficiel d'une machine virtuelle chiffrée avec des snapshots n'est autorisé que sur une seule branche de snapshot (chaîne de disques). Plusieurs branches de snapshot ne sont pas prises en charge. De plus, le rechiffrement superficiel n'est pas pris en charge sur un clone lié d'une machine virtuelle ou d'un disque. Si le rechiffrement superficiel échoue avant la mise à jour de tous les liens de la chaîne avec la nouvelle clé KEK, vous pouvez toujours accéder à la machine virtuelle chiffrée si vous disposez de l'ancienne et de la nouvelle clé KEK. Cependant, il est préférable d'émettre une nouvelle opération de rechiffrement superficiel avant d'effectuer des opérations de snapshot.

Composants du chiffrement des machines virtuelles vSphere

Selon le fournisseur de clés que vous utilisez, un serveur de clés externe, le système vCenter Server et vos hôtes ESXi contribuent potentiellement à la solution de chiffrement.

Les composants suivants comprennent le chiffrement de machines virtuelles vSphere:

- Un serveur de clés externe, également appelé KMS (non requis pour vSphere Native Key Provider)
- vCenter Server
- hôtes ESXi

Serveur de clés

Le serveur de clés est un serveur de gestion KMIP (Key Management Interoperability Protocol) associé à un fournisseur de clés. Un fournisseur de clés standard et un fournisseur de clés approuvé nécessitent un serveur de clés. vSphere Native Key Provider ne nécessite pas de serveur de clés. Le tableau suivant décrit les différences entre le fournisseur de clés et le serveur de clés.

Tableau 6-6. Interaction entre le fournisseur de clés et le serveur de clés

Fournisseur de clés	Interaction avec le serveur de clés
Fournisseur de clés standard	Un fournisseur de clés standard utilise vCenter Server pour demander des clés à partir d'un serveur de clés. Ce dernier génère et stocke les clés, et les transmet à vCenter Server pour distribution aux hôtes ESXi.
Fournisseur de clés approuvé	Un fournisseur de clés approuvé utilise un service de fournisseur de clés qui permet aux hôtes ESXi approuvés d'extraire les clés directement. Reportez-vous à la section À propos du service de fournisseur de clés de Autorité d'approbation vSphere.
vSphere Native Key Provider	vSphere Native Key Provider ne nécessite pas de serveur de clés. vCenter Server génère une clé principale et la transmet aux hôtes ESXi. Les hôtes ESXi génèrent ensuite des clés de chiffrement de données (même lorsqu'ils ne sont pas connectés à vCenter Server). Reportez-vous à la section Présentation de vSphere Native Key Provider.

Vous pouvez utiliser vSphere Client ou vSphere API pour ajouter des d'instances de fournisseurs de clés au système vCenter Server. Si vous utilisez plusieurs instances de fournisseurs de clés, toutes les instances doivent provenir du même fournisseur et doivent répliquer des clés.

Si votre environnement utilise différents fournisseurs de serveurs de clés dans différents environnements, vous pouvez ajouter un fournisseur de clés pour chaque serveur de clés et spécifier un fournisseur de clés par défaut. Le premier fournisseur de clés que vous ajoutez devient le fournisseur de clés par défaut. Vous pouvez spécifier la valeur par défaut ultérieurement.

En tant que client KMIP, vCenter Server utilise le protocole KMIP (Key Management Interoperability Protocol) pour faciliter l'utilisation du serveur de clés de votre choix.

vCenter Server

Le tableau suivant décrit le rôle du système vCenter Server dans le processus de chiffrement.

Tableau 6-7. Fournisseurs de clés et vCenter Server

Fournisseur de clés	Rôle de vCenter Server	Vérification des privilèges
Fournisseur de clés standard	Seul le système vCenter Server dispose des informations d'identification pour établir la connexion au serveur de clés. Vos hôtes ESXi ne possèdent pas ces informations d'identification. Le système vCenter Server obtient des clés du serveur de clés et les transmet aux hôtes ESXi. Le système vCenter Server ne stocke pas les clés du serveur de clés, mais conserve une liste des ID de clés.	vCenter Server vérifie les privilèges des utilisateurs qui effectuent des opérations de chiffrement.
Fournisseur de clés approuvé	Avec Autorité d'approbation vSphere , le système vCenter Server n'a plus besoin de demander de clés auprès du serveur de clés et conditionne l'accès aux clés de chiffrement à l'état d'attestation d'un cluster de charge de travail. Vous devez utiliser des systèmes vCenter Server séparés pour le cluster approuvé et le cluster d'autorité d'approbation.	vCenter Server vérifie les privilèges des utilisateurs qui effectuent des opérations de chiffrement. Seuls les utilisateurs membres du groupe SSO TrustedAdmins peuvent effectuer des opérations administratives.
vSphere Native Key Provider	L'instance de vCenter Server génère les clés.	vCenter Server vérifie les privilèges des utilisateurs qui effectuent des opérations de chiffrement.

Vous pouvez utiliser vSphere Client pour attribuer des privilèges pour les opérations de chiffrement ou pour attribuer le rôle personnalisé **Administrateur sans droits de chiffrement** aux groupes d'utilisateurs. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.

vCenter Server ajoute des événements cryptographiques à la liste des événements que vous pouvez afficher et exporter à partir de la console des événements de vSphere Client. Chaque événement inclut l'utilisateur, l'heure, l'ID de clé et l'opération de chiffrement.

Les clés provenant du serveur de clés sont utilisées comme clés de chiffrement de clés (KEK).

Hôtes ESXi

Les hôtes ESXi sont responsables de plusieurs aspects du workflow de chiffrement.

Tableau 6-8. Hôtes ESXi

Fournisseur de clés	Aspects de l'hôte ESXi
Fournisseur de clés standard	■ vCenter Server transmet les clés à un hôte ESXi lorsque ce dernier en a besoin. Le mode de chiffrement doit être activé pour l'hôte. Le rôle de l'utilisateur actuel doit inclure des privilèges d'opération de chiffrement. Reportez-vous aux sections Conditions préalables et privilèges requis pour les tâches de chiffrement et Privilèges d'opérations de chiffrement. ■ Garantir que les données de l'invité pour les machines virtuelles chiffrées sont chiffrées lorsqu'elles sont stockées sur disque. ■ Garantir que les données de l'invité pour les machines virtuelles chiffrées ne sont pas envoyées sur le réseau sans être chiffrées.
Fournisseur de clés approuvé	Les hôtes ESXi exécutent les services Autorité d'approbation vSphere , selon qu'il s'agit d'hôtes approuvés ou d'hôtes d'autorité d'approbation. Les hôtes ESXi approuvés exécutent des machines virtuelles de charge de travail qui peuvent être chiffrées à l'aide de fournisseurs de clés publiés par les hôtes d'autorité d'approbation. Reportez-vous à la section Présentation de l'infrastructure approuvée.
vSphere Native Key Provider	Les hôtes ESXi extraient des clés directement depuis vSphere Native Key Provider.

Les clés générées par l'hôte ESXi sont appelées clés internes dans ce document. Ces clés jouent généralement le rôle de clés de chiffrement de données (DEK).

Flux de chiffrement

Après avoir installé un fournisseur de clés, les utilisateurs ayant les privilèges requis peuvent créer des machines virtuelles et des disques chiffrés. Ces utilisateurs peuvent également chiffrer des machines virtuelles existantes et déchiffrer des machines virtuelles chiffrées, mais aussi ajouter des vTPM (Virtual Trusted Platform Modules) aux machines virtuelles.

Selon le type de fournisseur de clés, le flux de processus peut impliquer un serveur de clés, l'instance de vCenter Server et l'hôte ESXi.

Flux de chiffrement du fournisseur de clés standard

Pendant le processus de chiffrement, différents composants vSphere interagissent de la façon suivante.

1 Lorsque l'utilisateur exécute une tâche de chiffrement, par exemple pour créer une machine virtuelle, vCenter Server demande une nouvelle clé au serveur de clés par défaut. Cette clé est utilisée en tant que certificat KEK (Key Exchange Key).

2 vCenter Server stocke l'identifiant de clé et transmet la clé à l'hôte ESXi. Si l'hôte ESXi fait partie d'un cluster, vCenter Server envoie le certificat KEK à chacun des hôtes du cluster.

   La clé, quant à elle, n'est pas stockée sur le système vCenter Server. Seul l'identifiant de clé est connu.

3 L'hôte ESXi génère des clés internes (DEK) pour la machine virtuelle et ses disques. Les clés internes sont conservées uniquement en mémoire et l'hôte utilise les certificats KEK pour chiffrer les clés internes.

   Les clés internes non chiffrées ne sont jamais stockées sur disque. Seules les données chiffrées sont stockées. Dans la mesure où les certificats KEK proviennent du fournisseur de clés, l'hôte continue d'utiliser les mêmes KEK.

4 L'hôte ESXi chiffre la machine virtuelle avec la clé interne chiffrée.

   Tous les hôtes qui ont le certificat KEK et peuvent accéder au fichier de clé chiffrée peuvent exécuter des opérations sur la machine virtuelle chiffrée ou le disque.

Flux de chiffrement du fournisseur de clés approuvé

Le flux de chiffrement de Autorité d'approbation vSphere inclut les services Autorité d'approbation vSphere , les fournisseurs de clés approuvés, les instances de vCenter Server et les hôtes ESXi.

Le chiffrement d'une machine virtuelle avec un fournisseur de clés approuvé ressemble à l'expérience utilisateur de chiffrement des machines virtuelles lors de l'utilisation d'un fournisseur de clés standard. Le chiffrement de machines virtuelles sous Autorité d'approbation vSphere continue de reposer sur des stratégies de stockage de chiffrement des machines virtuelles ou sur la présence d'un périphérique vTPM pour décider du chiffrement d'une machine virtuelle. Vous continuez d'utiliser un fournisseur de clés configuré par défaut (appelé cluster KMS dans vSphere 6.5 et 6.7) lors du chiffrement d'une machine virtuelle à partir de vSphere Client. De plus, vous pouvez toujours utiliser les API de manière similaire pour spécifier manuellement le fournisseur de clés. Les privilèges de chiffrement existants ajoutés à vSphere 6.5 sont toujours pertinents dans vSphere 7.0 pour Autorité d'approbation vSphere .

Le processus de chiffrement du fournisseur de clés approuvé présente d'importantes différences par rapport au fournisseur de clés standard :

- Les administrateurs d'autorité d'approbation ne spécifient pas d'informations directement lors de la configuration d'un serveur de clés pour une instance de vCenter Server et ils n'établissent pas l'approbation du serveur de clés. Au lieu de cela, Autorité d'approbation vSphere publie les fournisseurs de clés approuvés que les hôtes approuvés peuvent utiliser.
- vCenter Server n'envoie plus de clés aux hôtes ESXi et peut traiter plutôt chaque fournisseur de clés approuvé comme une clé de niveau supérieur unique.
- Seuls les hôtes approuvés peuvent demander des opérations de chiffrement à partir d'hôtes d'autorité d'approbation

Flux de chiffrement de vSphere Native Key Provider

vSphere Native Key Provider est inclus dans vSphere à partir de la version 7.0 Update 2. Lorsque vous configurez un vSphere Native Key Provider, vCenter Server transmet une clé principale à tous les hôtes ESXi du cluster. En outre, si vous mettez à jour ou supprimez un vSphere Native Key Provider, la modification est transmise aux hôtes du cluster. Le flux de chiffrement est semblable au fonctionnement d'un fournisseur de clés approuvé. La différence est que vSphere Native Key Provider génère les clés et les encapsule avec la clé principale, puis les remet pour effectuer le chiffrement.

Attributs personnalisés pour les serveurs de clés

Le protocole KMIP (Key Management Interoperability Protocol) prend en charge l'ajout d'attributs personnalisés destinés à des fins spécifiques au fournisseur. Les attributs personnalisés vous permettent d'identifier plus spécifiquement les clés stockées dans votre serveur de clés. vCenter Server ajoute les attributs personnalisés suivants pour les clés de machine virtuelle et les clés d'hôte.

Tableau 6-9. Attributs personnalisés de chiffrement des machines virtuelles

Attribut personnalisé	Valeur
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	Version de vCenter Server
`x-Component`	Machine virtuelle
`x-Name`	Nom de la machine virtuelle (collecté à partir de ConfigInfo ou ConfigSpec)
`x-Identifier`	InstanceUuid de la machine virtuelle (collecté à partir de ConfigInfo ou ConfigSpec)

Tableau 6-10. Attributs personnalisés de chiffrement de l'hôte

Attribut personnalisé	Valeur
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	Version de vCenter Server
`x-Component`	Serveur ESXi
`x-Name`	Nom d'hôte
`x-Identifier`	UUID matériel de l'hôte

vCenter Server ajoute les attributs `x-Vendor`, `x-Product` et `x-Product_Version` lorsque le serveur de clés crée une clé. Lorsque la clé est utilisée pour chiffrer une machine virtuelle ou un hôte, vCenter Server définit les attributs `x-Component`, `x-Identifier` et `x-Name`. Vous pourrez peut-être afficher ces attributs personnalisés dans l'interface utilisateur de votre serveur de clés. Vérifiez auprès de votre fournisseur de serveur de clés.

La clé d'hôte et la clé de machine virtuelle disposent des six attributs personnalisés. `x-Vendor`, `x-Product` et `x-Product_Version` peuvent être identiques pour les deux clés. Ces attributs sont définis lors de la génération de la clé. Selon que la clé est destinée à une machine virtuelle ou à un hôte, il est possible que les attributs `x-Component`, `x-Identifier` et `x-Name` soient ajoutés.

Erreurs de clé

Lorsqu'une erreur se produit lors de l'envoi de clés du serveur de clés à un hôte ESXi, vCenter Server génère un message dans le journal des événements pour les événements suivants :

- L'ajout de clés à l'hôte ESXi a échoué en raison de problèmes de connexion à l'hôte ou de prise en charge de l'hôte.
- Échec de l'obtention des clés depuis le serveur de clés en raison d'une clé manquante dans le serveur de clés.
- Échec de l'obtention des clés depuis le serveur de clés en raison de la connexion au serveur de clés.

Déchiffrement des machines virtuelles chiffrées

Si vous souhaitez déchiffrer ultérieurement une machine virtuelle chiffrée, vous modifiez sa stratégie de stockage. Vous pouvez modifier la stratégie de stockage de la machine virtuelle et de l'ensemble des disques. Si vous souhaitez déchiffrer des composants individuels, déchiffrez les disques sélectionnés en premier, puis déchiffrez la machine virtuelle en modifiant la stratégie de stockage d'Accueil VM. Les deux clés sont requises pour le déchiffrement de chaque composant. Reportez-vous à la section Déchiffrer une machine ou un disque virtuel.

Chiffrement des disques virtuels

Lorsque vous créez une machine virtuelle chiffrée à partir de vSphere Client, vous pouvez décider des disques à exclure du chiffrement. Vous pouvez, par la suite, ajouter des disques et définir leur stratégies de chiffrement. Vous ne pouvez pas ajouter un disque chiffré à une machine virtuelle qui n'est pas chiffrée, et vous ne pouvez pas chiffrer un disque si la machine virtuelle n'est pas chiffrée.

Le chiffrement d'une machine virtuelle et de ses disques est contrôlé à l'aide de stratégies de stockage. La stratégie de stockage d'Accueil VM gouverne la machine virtuelle elle-même, et chaque disque virtuel a une stratégie de stockage associée.

- Définir la stratégie de stockage d'Accueil VM sur une stratégie de chiffrement chiffre uniquement la machine virtuelle en elle-même.
- Définir la stratégie de stockage d'Accueil VM et de tous les disques sur une stratégie de chiffrement chiffre l'ensemble des composants.

Examinez les cas d'utilisation suivants.

Tableau 6-11. Cas d'utilisation de chiffrement des disques virtuels

Cas d'utilisation	Détails
Créer une machine virtuelle chiffrée	Si vous ajoutez des disques pendant que vous créez une machine virtuelle chiffrée, les disques sont chiffrés par défaut. Vous pouvez modifier la stratégie de manière afin de ne pas chiffrer un ou plusieurs disques. Après la création de la machine virtuelle, vous pouvez modifier explicitement la stratégie de stockage de chaque disque. Reportez-vous à la section Modifier la stratégie de chiffrement des disques virtuels.
Chiffrer une machine virtuelle	Pour chiffrer une machine virtuelle existante, vous modifiez sa stratégie de stockage. Vous pouvez modifier la stratégie de stockage pour la machine virtuelle et pour tous les disques virtuels. Pour chiffrer uniquement la machine virtuelle, vous pouvez spécifier une stratégie de chiffrement d'Accueil VM et sélectionnez une stratégie de stockage différente, comme Valeur par défaut de la banque de données, pour chaque disque virtuel. Reportez-vous à la section Créer une machine virtuelle chiffrée.
Ajoutez un disque non chiffré existant à une machine virtuelle chiffrée (stratégie de stockage de chiffrement).	Échoue avec une erreur. Vous devez ajouter le disque avec la stratégie de stockage par défaut, mais vous pourrez modifier la stratégie de stockage ultérieurement. Reportez-vous à la section Modifier la stratégie de chiffrement des disques virtuels.
Ajouter un disque non chiffré existant à une machine virtuelle chiffrée avec une stratégie de stockage qui n'inclut pas le chiffrement (valeur par défaut de la banque de données, par exemple)	Le disque utilise la stratégie de stockage par défaut. Vous pouvez modifier explicitement la stratégie de stockage après avoir ajouté le disque si vous souhaitez un disque chiffré. Reportez-vous à la section Modifier la stratégie de chiffrement des disques virtuels.

Tableau 6-11. Cas d'utilisation de chiffrement des disques virtuels (suite)

Cas d'utilisation	Détails
Ajouter un disque chiffré à une machine virtuelle chiffrée (stratégie de stockage d'Accueil VM : Chiffrement)	Lorsque vous ajoutez le disque, il reste chiffré. vSphere Client affiche la taille et d'autres attributs, y compris l'état de chiffrement.
Ajouter un disque chiffré existant à une machine virtuelle non chiffrée.	Ce cas d'utilisation n'est pas pris en charge.
Enregistrer une machine virtuelle chiffrée.	Si vous supprimez une machine virtuelle chiffrée de vCenter Server mais que vous ne la supprimez pas du disque, vous pouvez la replacer dans l'inventaire vCenter Server en enregistrant le fichier de configuration de machine virtuelle (.vmx) de la machine virtuelle. Pour enregistrer la machine virtuelle chiffrée, l'utilisateur doit disposer du privilège **Opérations de chiffrement.Enregistrer une VM**. Si la machine virtuelle a été chiffrée à l'aide d'un fournisseur de clés standard, lorsque la machine virtuelle chiffrée est enregistrée, vCenter Server transmet les clés requises à l'hôte ESXi. Si l'utilisateur qui enregistre la machine virtuelle ne dispose pas du privilège **Opérations de chiffrement.Enregistrer une VM**, vCenter Server verrouille la machine virtuelle lors de l'enregistrement et celle-ci n'est pas utilisable tant qu'elle n'est pas déverrouillée. Si la machine virtuelle a été chiffrée à l'aide d'un fournisseur de clés approuvé ou de vSphere Native Key Provider, lorsque la machine virtuelle chiffrée est enregistrée, vCenter Server ne transmet plus les clés à l'hôte ESXi. Au lieu de cela, les clés sont extraites de l'hôte lors de l'enregistrement de la machine virtuelle. Si l'utilisateur qui enregistre la machine virtuelle ne dispose pas du privilège **Opérations de chiffrement.Enregistrer une VM**, vCenter Server n'autorise pas l'opération.

Erreurs de chiffrement des machines virtuelles

Si vCenter Server détecte une erreur critique avec le chiffrement des machines virtuelles, il crée un événement. Vous pouvez afficher ces événements pour faciliter le dépannage et résoudre les erreurs de chiffrement.

vCenter Server crée des événements pour les erreurs critiques de chiffrement des machines virtuelles suivantes.

- Échec de la génération d'une clé KEK.
- Espace disque insuffisant sur la banque de données pour créer une machine virtuelle chiffrée.
- Privilège d'utilisateur insuffisant pour initier l'opération de chiffrement.
- La clé spécifiée est manquante sur le fournisseur de clés et, par conséquent, la clé de l'hôte ESXi est renouvelée avec une nouvelle clé.

- Une erreur s'est produite sur le fournisseur de clés avec la clé spécifiée et, par conséquent, la clé de l'hôte ESXi est renouvelée avec une nouvelle clé.

Conditions préalables et privilèges requis pour les tâches de chiffrement

Les tâches de chiffrement sont possibles uniquement dans les environnements qui incluent vCenter Server. De plus, le mode de chiffrement doit être activé sur l'hôte ESXi pour la plupart des tâches de chiffrement. L'utilisateur qui exécute la tâche doit disposer des privilèges appropriés. Un ensemble de privilèges **Opérations de chiffrement** permet d'effectuer un contrôle plus précis. Si des tâches de chiffrement de machines virtuelles nécessitent de modifier le mode de chiffrement de l'hôte, des privilèges supplémentaires sont requis.

Note Autorité d'approbation vSphere dispose de conditions préalables supplémentaires et de privilèges requis. Reportez-vous à la section Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere.

Privilèges de chiffrement et rôles

Par défaut, l'utilisateur ayant le rôle d'vCenter Serveradministrateur détient tous les privilèges. Le rôle **Administrateur sans droits de chiffrement** ne dispose pas des privilèges suivant qui sont requis pour les opérations de chiffrement.

- Ajoutez des privilèges **Opérations de chiffrement**.
- **Global.Diagnostics**
- **Hôte.Inventaire.Ajouter un hôte au cluster**
- **Hôte.Inventaire.Ajouter un hôte autonome**
- **Hôte.Opérations locales.Gérer des groupes d'utilisateurs**

Vous pouvez attribuer le rôle **Administrateur sans droits de chiffrement** à des vCenter Server administrateurs qui n'ont pas besoin de privilèges **Opérations de chiffrement**.

Pour imposer plus de limites à ce que les utilisateurs sont autorisés à faire, vous pouvez cloner le rôle **Administrateur sans droits de chiffrement** et créer un rôle personnalisé avec certains privilèges **Opérations de chiffrement** uniquement. Par exemple, vous pouvez créer un rôle qui permet aux utilisateurs de chiffrer des machines virtuelles, mais de ne pas les déchiffrer. Reportez-vous à la section Utilisation des rôles pour assigner des privilèges.

Mode de chiffrement de l'hôte

Le mode de chiffrement de l'hôte détermine si un hôte ESXi est prêt à accepter du matériel cryptographique pour le chiffrage des machines virtuelles et des disques virtuels. Avant des opérations de chiffrement sur un hôte, le mode de chiffrement de l'hôte doit être activé. Le mode de chiffrement de l'hôte est souvent activé automatiquement lorsqu'il est requis, mais vous pouvez l'activer explicitement. Vous pouvez vérifier et définir explicitement le mode de chiffrement de l'hôte actuel depuis vSphere Client ou à l'aide de vSphere API.

Lorsque le mode de chiffrement de l'hôte est activé, l'instance de vCenter Server installe une clé d'hôte sur l'hôte afin de garantir que celui-ci est « sécurisé » au niveau cryptographique. La clé d'hôte permet d'effectuer d'autres opérations cryptographiques. Elle permet notamment à l'instance de vCenter Server d'obtenir des clés à partir du fournisseur de clés et de les envoyer aux hôtes ESXi.

En mode « sécurisé », les vidages de mémoire des mondes d'utilisateur (autrement dit, hostd) et des machines virtuelles chiffrées sont chiffrés. Les vidages de mémoire des machines virtuelles non chiffrées ne sont pas chiffrés.

Pour plus d'informations sur les vidages de mémoire chiffrés et leur utilisation par le support technique de VMware, consultez l'article de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/2147388.

Voir Activer explicitement le mode de chiffrement de l'hôte pour des instructions.

Une fois le mode de chiffrement de l'hôte activé, celui-ci ne peut pas être désactivé facilement. Reportez-vous à la section Désactiver le mode de chiffrement de l'hôte.

Des modifications automatiques se produisent lorsque des opérations de chiffrement tentent d'activer le mode de chiffrement de l'hôte. Supposez par exemple que vous ajoutez une machine virtuelle chiffrée à un hôte autonome. Le mode de chiffrement de l'hôte n'est pas activé. Si vous disposez des privilèges requis sur l'hôte, le mode de chiffrement devient automatiquement activé.

Supposons qu'un cluster dispose de trois hôtes ESXi, A, B et C. Vous créez une machine virtuelle chiffrée sur l'hôte A. L'effet produit dépend de plusieurs facteurs.

- Si le chiffrement pour les hôtes A, B et C est déjà activé, vous avez uniquement besoin des privilèges **Opérations de chiffrement.Chiffrer nouvel élément** pour pouvoir créer la machine virtuelle.
- Si les hôtes A et B sont activés pour le chiffrement et que C n'est pas activé, le système procède de la manière suivante.
  - Supposons que vous possédiez les privilèges **Opérations de chiffrement.Chiffrer nouvel élément** et **Opérations cryptographiques.Enregistrer l'hôte** sur chaque hôte. Dans ce cas, le processus de création de la machine virtuelle active le chiffrement sur l'hôte C. Le processus de chiffrement active le mode de chiffrement de l'hôte sur l'hôte C et envoie la clé à chaque hôte dans le cluster.

Dans ce cas, vous pouvez également activer explicitement le chiffrement de l'hôte sur l'hôte C.

- Supposons que vous disposiez des privilèges **Opérations cryptographiques.Chiffrer nouvel élément** uniquement sur la machine virtuelle ou le dossier de machines virtuelles. Dans ce cas, la création de la machine virtuelle aboutit et la clé devient disponible sur l'hôte A et l'hôte B. Le chiffrement reste désactivé sur l'hôte C et il n'obtient pas la clé de la machine virtuelle.

- Si aucun des hôtes n'est activé pour le chiffrement et que vous disposez des privilèges **Opérations de chiffrement.Enregistrer l'hôte** sur l'hôte A, le processus de création de machine virtuelle active le chiffrement de l'hôte sur cet hôte. Sinon, une erreur se produit.
- Vous pouvez également utiliser vSphere API pour définir le mode de chiffrement d'un cluster sur « Forcer l'activation ». « Forcer l'activation » garantit que tous les hôtes du cluster sont « sécurisés » au niveau du chiffrement, c'est-à-dire que vCenter Server a installé une clé d'hôte sur cet hôte. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Conditions requises en matière d'espace disque

Lorsque vous chiffrez une machine virtuelle existante, vous avez besoin d'au moins deux fois l'espace en cours d'utilisation par la machine virtuelle.

vSphere vMotion chiffré

vSphere vMotion applique systématiquement le chiffrement lors de la migration de machines virtuelles chiffrées. Pour les machines virtuelles qui ne sont pas chiffrées, vous pouvez sélectionner l'une des options chiffrées de vSphere vMotion.

La version chiffrée de vSphere vMotion garantit la confidentialité, l'intégrité et l'authenticité des données qui sont transférées avec vSphere vMotion. vSphere prend en charge la migration vMotion chiffrée des machines virtuelles non chiffrées et chiffrées sur des instances de vCenter Server.

Éléments chiffrés

Concernant les disques chiffrés, les données sont transmises chiffrées. Pour les disques qui ne sont pas chiffrés, le chiffrement par Storage vMotion n'est pas pris en charge.

Lorsque les machines virtuelles sont chiffrées, la migration avec vSphere vMotion utilise systématiquement la version chiffrée de vSphere vMotion. Vous ne pouvez pas désactiver le chiffrement de vSphere vMotion pour les machines virtuelles chiffrées.

États de vSphere vMotion chiffrés

Concernant les machines virtuelles qui ne sont pas chiffrées, vous pouvez définir vSphere vMotion à l'un des états suivants. La valeur par défaut est Opportuniste.

Désactivé

N'utilisez pas vSphere vMotion chiffré.

Opportuniste

Utilisez vSphere vMotion chiffré si les hôtes source et de destination le prennent en charge. Seules les versions 6.5 et ultérieures de ESXi utilisent vSphere vMotion chiffré.

Requis

Autorisez uniquement vSphere vMotion chiffré. Si l'hôte source ou de destination ne prend pas en charge vSphere vMotion chiffré, la migration avec vSphere vMotion est interdite.

Lorsque vous chiffrez une machine virtuelle, cette dernière conserve une trace du paramètre vSphere vMotion actuellement chiffré. Si vous désactivez par la suite le chiffrement de la machine virtuelle, le paramètre vMotion chiffré demeure au niveau Requis jusqu'à ce que vous le changiez de façon explicite. Vous pouvez modifier les paramètres avec l'option **Modifier les paramètres**.

Reportez-vous à la documentation de *Gestion de vCenter Server et des hôtes* pour plus d'informations sur l'activation et la désactivation de vSphere vMotion pour les machines virtuelles qui ne sont pas chiffrées.

Note Actuellement, vous devez utiliser les vSphere API pour migrer ou cloner des machines virtuelles chiffrées sur des instances de vCenter Server. Consultez *Guide de programmation de vSphere Web Services SDK* et *Référence de l'API vSphere Web Services*.

Migration ou clonage de machines virtuelles chiffrées entre des instances de vCenter Server

vSphere vMotion prend en charge la migration et le clonage de machines virtuelles chiffrées entre des instances de vCenter Server.

Lors de la migration ou du clonage de machines virtuelles chiffrées entre des instances de vCenter Server, les instances source et de destination de vCenter Server doivent être configurées pour partager le fournisseur de clés qui a été utilisé pour chiffrer la machine virtuelle. En outre, le nom du fournisseur de clés doit être le même sur les instances source et de destination de vCenter Server et présenter les caractéristiques suivantes :

- Fournisseur de clés standard : le même serveur de clés (ou serveurs de clés) doit se trouver dans le fournisseur de clés.
- Fournisseur de clés approuvé : le même service Autorité d'approbation vSphere doit être configuré sur l'hôte de destination.
- vSphere Native Key Provider : doit avoir la même clé KDK.

L'instance de destination de vCenter Server garantit que le mode de chiffrement est activé sur l'hôte ESXi de destination, ce qui garantit que l'hôte est « sécurisé » au niveau du chiffrement.

Les privilèges suivants sont requis lors de l'utilisation de vSphere vMotion pour la migration ou le clonage d'une machine virtuelle chiffrée entre des instances de vCenter Server.

- Migration : **Opérations de chiffrement.Migrer** sur la machine virtuelle
- Clonage : **Opérations de chiffrement.Cloner** sur la machine virtuelle

En outre, l'instance de destination de vCenter Server doit disposer du privilège **Opérations de chiffrement.EncryptNew**. Si l'hôte de destination de ESXi n'est pas en mode « sécurisé », le privilège **Opérations de chiffrement.RegisterHost** doit également se trouver sur l'instance de destination de vCenter Server.

Certaines tâches ne sont pas autorisées lors de la migration de machines virtuelles chiffrées sur des instances de vCenter Server.

- Vous ne pouvez pas modifier la stratégie de stockage de machine virtuelle.
- Vous ne pouvez pas effectuer une modification de la clé.

Configuration minimale requise pour la migration ou le clonage de machines virtuelles chiffrées entre des instances de vCenter Server

La configuration minimale requise pour la migration ou le clonage de machines virtuelles chiffrées du fournisseur de clés standard entre des instances de vCenter Server à l'aide de vSphere vMotion est la suivante :

- Les instances source et de destination de vCenter Server doivent être de version 7.0 ou ultérieure.
- Les hôtes source et de destination d'ESXi doivent être de version 6.7 ou ultérieure.

La configuration minimale requise pour la migration ou le clonage de machines virtuelles chiffrées du fournisseur de clés approuvé entre des instances de vCenter Server à l'aide de vSphere vMotion est la suivante :

- Le service Autorité d'approbation vSphere doit être configuré pour l'hôte de destination et l'hôte de destination doit être attesté.
- Le chiffrement ne peut pas être modifié lors de la migration. Par exemple, un disque non chiffré ne peut pas être chiffré lors de la migration de la machine virtuelle vers un nouveau stockage.
- Vous pouvez migrer une machine virtuelle chiffrée de type standard vers un hôte approuvé. Le nom du fournisseur de clés doit être le même sur les instances source et de destination de vCenter Server.
- Vous ne pouvez pas migrer une machine virtuelle chiffrée de type Autorité d'approbation vSphere vers un hôte non approuvé.

Fournisseur de clés approuvé vMotion et Cross-vCenter Server vMotion

Le fournisseur de clés approuvé prend entièrement en charge vMotion sur les hôtes ESXi.

La fonction Cross-vCenter Server vMotion est prise en charge, mais avec les restrictions suivantes.

1 Le service approuvé requis doit être configuré sur l'hôte de destination et l'hôte de destination doit être attesté.

2 Le chiffrement ne peut pas être modifié lors de la migration. Par exemple, un disque ne peut pas être chiffré lors de la migration de la machine virtuelle vers le nouveau stockage.

Lors de l'exécution de Cross-vCenter Server vMotion, vCenter Server vérifie que le fournisseur de clés approuvé est disponible sur l'hôte de destination et que l'hôte y a accès.

vSphere Native Key Provider vMotion et Cross-vCenter Server vMotion

vSphere Native Key Provider prend en charge vMotion et vMotion chiffré sur les hôtes ESXi. Cross-vCenter Server vMotion est pris en charge si vSphere Native Key Provider est configuré sur l'hôte de destination.

Meilleures pratiques de chiffrement, mises en garde et interopérabilité

Les meilleures pratiques et mises en garde relatives au chiffrement des machines physiques s'appliquent également aux machines virtuelles. L'architecture de chiffrement de machine virtuelle donne lieu à des recommandations supplémentaires. Tenez compte des limitations d'interopérabilité pendant la phase de planification de la stratégie de chiffrement des machines virtuelles.

Note Pour plus d'informations sur l'interopérabilité de Autorité d'approbation vSphere , consultez Meilleures pratiques de Autorité d'approbation vSphere , mises en garde et interopérabilité.

Meilleures pratiques de chiffrement des machines virtuelles

Suivez les meilleures pratiques de chiffrement des machines virtuelles pour éviter les problèmes ultérieurement, par exemple, lorsque vous générez un bundle `vm-support`.

Meilleures pratiques générales

Suivez les meilleures pratiques générales suivantes pour éviter les problèmes.

- Ne chiffrez pas les machines virtuelles d'un dispositif vCenter Server Appliance.

- Si votre hôte ESXi échoue, récupérez le bundle de support dès que possible. La clé de l'hôte doit être disponible pour générer un bundle de support qui utilise un mot de passe, ou pour déchiffrer un vidage de mémoire. Si l'hôte est redémarré, il est possible que sa clé change. En pareil cas, vous ne pouvez plus générer un bundle de support avec un mot de passe ni déchiffrer les vidages de mémoire dans le bundle de support avec la clé de l'hôte.
- Gérez les noms de fournisseurs de clés avec précaution. Si le nom du fournisseur de clés change pour un serveur de clés déjà utilisé, une machine virtuelle chiffrée à l'aide de ce serveur de clés prend un état verrouillé pendant la mise sous tension ou l'enregistrement. Dans ce cas, supprimez le serveur de clés de vCenter Server et ajoutez-le avec le nom du fournisseur de clés que vous avez utilisé au départ.
- Ne modifiez pas les fichiers VMX et les fichiers descripteurs VMDK. Ces fichiers contiennent le bundle de chiffrement. Il est possible que vos modifications rendent la machine virtuelle irrécupérable et que le problème de récupération ne puisse pas être résolu.
- Le processus de chiffrement chiffre les données sur l'hôte avant qu'elles soient écrites dans le stockage. Les fonctionnalités de stockage back-end telles que la déduplication et la compression peuvent ne pas être efficaces pour les machines virtuelles chiffrées. Lorsque vous utilisez le chiffrement des machines virtuelles vSphere, envisagez d'effectuer des compromis de stockage.
- Le chiffrement nécessite une utilisation importante du CPU. AES-NI améliore de manière significative les performances du chiffrement. Activez AES-NI dans votre BIOS.

Meilleures pratiques pour les vidages de mémoire chiffrés

Suivez ces meilleures pratiques pour éviter les problèmes lorsque vous voulez examiner un vidage de mémoire dans le cadre du diagnostic d'un incident.

- Établissez une stratégie concernant les vidages de mémoire. Les vidages de mémoire sont chiffrés, car ils peuvent contenir des informations sensibles telles que des clés. Si vous déchiffrez un vidage de mémoire, prenez en compte ses informations sensibles. Les vidages de mémoire ESXi peuvent contenir des clés de l'hôte ESXi des machines virtuelles qui s'y trouvent. Envisagez de modifier la cl de l'hôte et de rechiffrer les machines virtuelles chiffrées après avoir déchiffré un vidage de mémoire. Vous pouvez effectuer ces deux tâches à l'aide de vSphere API.

  Reportez-vous à Chiffrement de machines virtuelles vSphere et vidages mémoire pour plus de détails.

- Utilisez toujours un mot de passe lorsque vous collectez un bundle `vm-support`. Vous pouvez spécifier le mot de passe lorsque vous générez le bundle de support à partir de vSphere Client ou à l'aide de la commande `vm-support`.

  Le mot de passe rechiffre les vidages de mémoire utilisant des clés internes de façon à utiliser les clés reposant sur le mot de passe. Vous pouvez utiliser ultérieurement le mot de passe pour déchiffrer les vidages de mémoire chiffrés susceptibles d'être intégrés dans le bundle de support. Les vidages de mémoire et les journaux non chiffrés ne sont pas affectés par l'utilisation de l'option de mot de passe.

- Le mot de passe que vous spécifiez pendant la création du bundle `vm-support` n'est pas conservé dans les composants vSphere. Vous êtes responsable du suivi des mots de passe pour les bundles de support.
- Avant de modifier la clé de l'hôte, générez un bundle `vm-support` avec un mot de passe. Vous pourrez ultérieurement utiliser le mot de passe pour accéder à tous les vidages de mémoire susceptibles d'avoir été chiffrés avec l'ancienne clé de l'hôte.

Meilleures pratiques de gestion du cycle de vie des clés

Implémenter des meilleures pratiques qui garantissent la disponibilité du serveur de clés et surveillent les clés sur le serveur de clés.

- Vous êtes responsable de la mise en place de stratégies qui garantissent la disponibilité du serveur de clés.

  Si le serveur de clés n'est pas disponible, il est impossible d'effectuer les opérations liées aux machines virtuelles nécessitant que vCenter Server demande la clé auprès du serveur de clés. Cela signifie que l'exécution des machines virtuelles se poursuit et que vous pouvez les mettre sous tension, les mettre hors tension et les reconfigurer. Toutefois, vous ne pouvez pas les déplacer vers un hôte qui ne dispose pas des informations concernant la clé.

  La plupart des solutions de serveur clés incluent des fonctionnalités de haute disponibilité. Vous pouvez utiliser vSphere Client ou l'API pour spécifier un fournisseur de clés et les serveurs de clés associés.

  Note À partir de la version 7.0 Update 2, les machines virtuelles chiffrées et les TPM virtuels peuvent continuer à fonctionner même lorsque le serveur de clés est temporairement hors ligne ou indisponible. Les hôtes ESXi peuvent faire persister les clés de chiffrement afin de poursuivre et les opérations de chiffrement et vTPM. Reportez-vous à la section Présentation de la persistance des clés.

- Vous êtes responsable du suivi des clés et de l'application de corrections sur les clés de machines virtuelles existantes ne sont pas à l'état Active.

  Le standard KMIP définit les états suivants pour les clés.

  - Pré-active
  - Active
  - Désactivée
  - Compromise
  - Détruite
  - Détruite compromise

Le chiffrement des machines virtuelles vSphere utilise uniquement les clés à l'état Active pour la chiffrement. Si une clé est à l'état Pré-active, le chiffrement des machines virtuelles vSphere l'active. Si l'état de la clé est Désactivée, Compromise, Détruite ou Détruite compromise, cela signifie que vous ne pouvez pas chiffrer la machine virtuelle ou le disque virtuel présentant cet état.

Pour les clés ayant un autre état, les machines virtuelles qui les utilisent continuent de fonctionner. La réussite d'une opération de clonage ou de migration varie selon que la clé est déjà dans l'hôte ou non.

- Si la clé se trouve sur l'hôte de destination, l'opération réussit même si la clé n'est pas active sur le serveur de clés.
- Si les clés requises de la machine virtuelle et du disque virtuel ne sont pas sur l'hôte de destination, vCenter Server doit extraire les clés du serveur de clés. Si l'état de la clé est Désactivée, Compromise, Détruite ou Détruite compromise, vCenter Server affiche une erreur et l'opération échoue.

Une opération de clonage ou de migration réussit si la clé est déjà dans l'hôte. L'opération échoue si vCenter Server doit extraire les clés du serveur de clés.

Si une clé n'est pas à l'état Active, effectuez une opération de rechiffrement à l'aide de l'API. Reportez-vous au *Guide de programmation de vSphere Web Services SDK*.

- Élaborez des stratégies de rotation des clés pour effectuer un retrait et une rotation des clés après une période spécifique.
  - Fournisseur de clés approuvé : modifiez la clé principale d'un fournisseur de clés approuvé.
  - vSphere Native Key Provider : modifiez le paramètre `key_id` d'un périphérique vSphere Native Key Provider.

Meilleures pratiques en matière de sauvegarde et de restauration

Configurez des stratégies pour les opérations de sauvegarde et de restauration.

- Toutes les architectures de sauvegarde ne sont pas prises en charge. Reportez-vous à la section Interopérabilité du chiffrement des machines virtuelles.
- Configurez des stratégies pour les opérations de restauration. Étant donné que les sauvegardes sont toujours en texte clair, envisagez de chiffrer les machines virtuelles immédiatement après la fin de la restauration. Vous pouvez spécifier que la machine virtuelle est chiffrée dans le cadre de l'opération de restauration. Si possible, chiffrez la machine virtuelle dans le cadre de l'opération de restauration pour éviter toute exposition des informations sensibles. Pour modifier la stratégie de chiffrement pour les disques associés à la machine virtuelle, modifiez la stratégie de stockage du disque.
- Étant donné que les fichiers de base de machine virtuelle sont chiffrés, assurez-vous que les clés de chiffrement sont disponibles au moment de la restauration.

Meilleures pratiques en matière de performances

- Les performances du chiffrement dépendent du CPU et de la vitesse du stockage.
- Le chiffrement de machines virtuelles existantes prend plus de temps que le chiffrement d'un machine virtuelle lors de sa création. Si possible, chiffrez une machine virtuelle au moment de la créer.

Meilleures pratiques en matière de stratégie de stockage

Ne modifiez pas l'exemple de stratégie de stockage du bundle de chiffrement des machines virtuelles. Au lieu de cela, clonez la stratégie et modifiez le clone.

Note Il n'existe aucun moyen automatisé de rétablir les paramètres d'origine de la stratégie de chiffrement des machines virtuelles.

Pour plus de détails sur la personnalisation des stratégies de stockage, reportez-vous à la documentation *Stockage vSphere*.

Meilleures pratiques de suppression des clés de chiffrement

Pour vous assurer que les clés de chiffrement sont supprimées d'un cluster, après la suppression, la désinscription ou le déplacement de la machine virtuelle chiffrée vers un autre périphérique vCenter Server, redémarrez les hôtes ESXi dans le cluster.

Mises en garde concernant le chiffrement des machines virtuelles

Prenez en compte les mises en garde concernant le chiffrement des machines virtuelles pour éviter l'apparition de problèmes.

Pour en savoir plus sur les dispositifs et les fonctionnalités qui ne peuvent pas être utilisés avec le chiffrement des machines virtuelles, reportez-vous à Interopérabilité du chiffrement des machines virtuelles.

Limitations

Prenez en compte les mises en garde suivantes lorsque vous planifiez votre stratégie de chiffrement des machines virtuelles.

- Lorsque vous clonez une machine virtuelle chiffrée ou effectuez une opération Storage vMotion, vous pouvez tenter de modifier le format de disque. Ces conversions ne sont pas toujours concluantes. Par exemple, si vous clonez une machine virtuelle et tentez de remplacer le format de disque en remplaçant le format statique mis à zéro en différé par le format dynamique, le disque de la machine virtuelle conserve le format statique mis à zéro en différé.

- Si vous détachez un disque d'une machine virtuelle, les informations sur la stratégie de stockage du disque virtuel ne sont pas conservées.
  - Si le disque virtuel est chiffré, vous devez explicitement définir la stratégie de stockage sur la stratégie de chiffrement des machines virtuelles ou sur une stratégie de stockage qui englobe le chiffrement.
  - Si le disque virtuel n'est pas chiffré, vous pouvez modifier la stratégie de stockage lorsque vous ajoutez le disque à la machine virtuelle.

  Reportez-vous à Chiffrement des disques virtuels pour plus de détails.
- Déchiffrez les vidages de mémoire avant de déplacer une machine virtuelle vers un autre cluster.

  vCenter Server ne stocke pas les clés KMS, mais assure uniquement le suivi des ID de clé. Par conséquent, vCenter Server ne stocke pas la clé de l'hôte ESXi de manière persistante.

  Dans certaines circonstances, par exemple lors du déplacement de l'hôte ESXi vers un autre cluster et du redémarrage de l'hôte, vCenter Server attribue une nouvelle clé d'hôte à l'hôte. Il est impossible de déchiffrer des vidages de mémoire existants avec la nouvelle clé d'hôte.
- L'exportation OVF n'est pas prise en charge pour une machine virtuelle chiffrée.
- L'utilisation de VMware Host Client pour enregistrer une machine virtuelle chiffrée n'est pas prise en charge.

État de verrouillage des machines virtuelles

Si la clé de la machine virtuelle ou une ou plusieurs clés de disque virtuel sont manquantes, la machine virtuelle passe à l'état verrouillé. Si la machine est à l'état verrouillé, vous ne pouvez pas effectuer ses opérations.

- Si vous chiffrez une machine virtuelle et ses disques à l'aide de vSphere Client, la même clé est utilisée pour les deux.
- Lorsque vous effectuez le chiffrement à l'aide de l'API, vous pouvez utiliser différentes clés de chiffrement pour la machine virtuelle et ses disques. Dans ce cas, si vous tentez de mettre sous tension une machine virtuelle et si une des clés de disque est manquante, l'opération de mise sous tension échoue. Pour remédier à cela, retirez le disque virtuel.

Pour obtenir des suggestions de dépannage, reportez-vous à Résoudre les problèmes de clés manquantes.

Interopérabilité du chiffrement des machines virtuelles

Le chiffrement des machines virtuelles vSphere présente des limitations quant à la compatibilité avec certains périphériques et certaines fonctionnalités.

Limitations de certaines tâches de chiffrement

Vous ne pouvez pas effectuer certaines tâches sur une machine virtuelle chiffrée.

- Pour la plupart des opérations de chiffrement de machines virtuelles, la machine virtuelle doit être mise hors tension. Vous pouvez cloner une machine virtuelle chiffrée et vous pouvez procéder à un rechiffrement superficiel tandis que la machine virtuelle est sous tension.
- Vous pouvez effectuer un rechiffrement superficiel sur une machine virtuelle incluant des snapshots. Vous ne pouvez pas effectuer un rechiffrement en profondeur sur une machine virtuelle incluant des snapshots.

Vous pouvez reprendre depuis un état suspendu d'une machine virtuelle chiffrée ou restaurer un snapshot de mémoire d'une machine chiffrée. Vous pouvez migrer une machine virtuelle chiffrée avec le snapshot de mémoire et l'état suspendu entre des hôtes ESXi.

Chiffrement de machines virtuelles vSphere et IPv6

Vous pouvez utiliser le chiffrement de machines virtuelles vSphere avec le mode IPv6 pur ou en mode mixte. Vous pouvez configurer le serveur de clés avec des adresses IPv6. L'instance de vCenter Server et le serveur de clés peuvent être configurés avec des adresses IPv6 uniquement.

Limitations des fonctionnalités de chiffrement de machines virtuelles vSphere

Certaines fonctionnalités ne sont pas compatibles avec le chiffrement des machines virtuelles vSphere.

- vSphere Fault Tolerance
- Pour un fournisseur de clés standard, le clonage est pris en charge sous condition.
  - Le clone intégral est pris en charge. Le clone hérite de l'état de chiffrement parent, y compris des clés. Vous pouvez chiffrer le clone intégral, rechiffrer le clone intégral de façon qu'il utilise de nouvelles clés ou déchiffrer le clone intégral.

    Les clones liés sont pris en charge et le clone hérite de l'état de chiffrement parent, y compris des clés. Vous ne pouvez pas déchiffrer le clone lié ou rechiffrer un clone lié avec différentes clés.
- Pour un fournisseur de clés approuvé, le clonage est pris en charge, mais les clés de chiffrement ne peuvent pas être modifiées sur le clone. Ce comportement contraste avec le chiffrement standard, où les clés peuvent être modifiées lors de la création d'un clone. Les opérations suivantes ne sont pas prises en charge par Autorité d'approbation vSphere lors du clonage d'une machine virtuelle :
  - Clonage d'une machine virtuelle non chiffrée vers une machine virtuelle chiffrée
  - Clonage d'une machine virtuelle chiffrée et modification des clés de chiffrement
- Instant Clone est pris en charge par tous les types de fournisseurs de clés, mais vous ne pouvez pas modifier les clés de chiffrement sur le clone.
- vSphere ESXi Dump Collector

- Bibliothèque de contenu
- Toutes les solutions de sauvegarde reposant sur VMware vSphere Storage API - Data Protection (VADP) pour la sauvegarde de disques virtuels ne sont pas prises en charge.
  - Les solutions de sauvegarde VADP SAN ne sont pas prises en charge.
  - Les solutions d'ajout de sauvegarde à chaud VADP sont prises en charge si le fournisseur prend en charge le chiffrement de la machine virtuelle proxy créée dans le cadre du workflow de sauvegarde. Le fournisseur doit disposer du privilège **Opérations de chiffrement.Chiffrer la machine virtuelle**.
  - Les solutions de sauvegarde VADP NBD-SSL sont prises en charge. L'application du fournisseur doit disposer du privilège **Opérations de chiffrement.Accès direct**.
- Vous ne pouvez pas utiliser le chiffrement des machines virtuelles vSphere pour le chiffrement sur d'autres produits VMware tels que VMware Workstation.
- Vous ne pouvez pas envoyer de sortie d'une machine virtuelle chiffrée vers un port en série ou un port parallèle. Même si la configuration semble concluante, la sortie est envoyée vers un fichier.

Certains types de configurations de disque de machine virtuelle ne sont pas pris en charge avec le chiffrement des machines virtuelles vSphere.

- Disque RDM (mappage de périphériques bruts).
- Disques en mode multi-écriture ou disques partagés (MSCS, WSFC ou Oracle RAC). Si un disque virtuel est chiffré et si vous tentez de sélectionner le mode multi-écriture dans la page **Modifier les paramètres** de la machine virtuelle, le bouton **OK** est désactivé.

Présentation de la persistance des clés

À partir de la version 7.0 Update 2, les machines virtuelles chiffrées et les TPM virtuels peuvent continuer à fonctionner même lorsque le serveur de clés est temporairement hors ligne ou indisponible. Les hôtes ESXi peuvent faire persister les clés de chiffrement afin de poursuivre et les opérations de chiffrement et vTPM.

Avant vSphere 7.0 Update 2, les machines virtuelles et les vTPM chiffrés avaient besoin que le serveur de clés soit disponible en permanence pour fonctionner. Dans vSphere 7.0 Update 2 et version ultérieure, les terminaux chiffrés peuvent fonctionner même lorsque l'accès à un serveur de clés est interrompu.

Persistance des clés sur l'hôte ESXi

Lors de l'utilisation d'un fournisseur de clés standard, l'hôte ESXi s'appuie sur vCenter Server pour gérer les clés de chiffrement. Lors de l'utilisation d'un fournisseur de clés approuvé, l'hôte ESXi s'appuie directement sur les hôtes d'autorité d'approbation pour gérer les clés et vCenter Server n'est pas impliqué.

Quel que soit le type de fournisseur de clés, l'hôte ESXi obtient d'abord les clés et les conserve dans son cache de clés. Si l'hôte ESXi redémarre, il perd son cache de clés. Ensuite, l'hôte ESXi demande à nouveau les clés, soit au serveur de clés (fournisseur de clés standard) soit aux hôtes d'autorité d'approbation (fournisseur de clés approuvé). Lorsque l'hôte ESXi tente d'obtenir les clés et que le serveur de clés est hors ligne ou inaccessible, les vTPM et le chiffrement de la charge de travail ne peuvent pas fonctionner. Pour les déploiements de type Edge, pour lesquels un serveur de clés n'est généralement pas déployé sur le site, une perte de connectivité avec un serveur de clés peut entraîner une indisponibilité superflue pour les charges de travail chiffrées.

À partir de vSphere 7.0 Update 2, les charges de travail chiffrées peuvent continuer à fonctionner même lorsque le serveur de clés est hors ligne ou inaccessible. Si l'hôte ESXi dispose d'un TPM, les clés de chiffrement sont persistantes sur le TPM lors des redémarrages. Par exemple, même si un hôte ESXi redémarre, l'hôte n'a pas besoin de demander des clés de chiffrement. En outre, les opérations de chiffrement et de déchiffrement peuvent se poursuivre lorsque le serveur de clés est indisponible, car les clés sont persistantes sur le TPM. En d'autres mots, lorsque le serveur de clés ou les hôtes d'autorité d'approbation sont indisponibles, vous pouvez continuer à gérer les charges de travail chiffrées « sans serveur de clés ». En outre, les vTPM peuvent continuer à fonctionner même lorsque le serveur de clés est inaccessible.

À partir de vSphere 7.0 Update 2, vSphere Native Key Provider prend en charge la persistance des clés. Lorsque vous utilisez un vSphere Native Key Provider, l'instance de vCenter Server génère les clés et aucun serveur de clés n'est requis. Les hôtes ESXi obtiennent une clé KDK (clé de dérivation de clés) de vCenter Server, qui est utilisée pour dériver d'autres clés. Après avoir reçu la clé KDK et généré d'autres clés, les hôtes ESXi n'ont pas besoin d'accéder à vCenter Server pour les opérations de chiffrement. En d'autres mots, un vSphere Native Key Provider s'exécute toujours « sans serveur de clés ».

Pour activer ou désactiver la persistance des clés, consultez la section Activer ou désactiver la persistance de clé sur un hôte ESXi.

Configuration et gestion d'un fournisseur de clés standard 7

L'utilisation d'un fournisseur de clés standard dans votre environnement vSphere nécessite une certaine préparation. Après avoir configuré votre environnement, vous pouvez créer des machines virtuelles et des disques virtuels chiffrés et chiffrer les machines virtuelles et les disques existants.

Après avoir configuré votre environnement pour un fournisseur de clés standard, vous pouvez utiliser vSphere Client pour créer des machines virtuelles et des disques virtuels chiffrés et chiffrer des machines virtuelles et des disques existants. Reportez-vous à la section Chapitre 10 Utiliser le chiffrement dans votre environnement vSphere.

Vous pouvez effectuer d'autres tâches à l'aide de l'API et de l'interface de ligne de commande crypto-util. Consultez *Guide de programmation de vSphere Web Services SDK* pour obtenir de la documentation sur l'API et l'aide de la ligne de commande `crypto–util` pour plus d'informations sur cet outil.

Ce chapitre contient les rubriques suivantes :

- Présentation du fournisseur de clés standard
- Configurer le fournisseur de clés standard
- Configurer des fournisseurs de clés distincts pour différents utilisateurs

Présentation du fournisseur de clés standard

Vous pouvez utiliser un fournisseur de clés standard pour effectuer des tâches de chiffrement de machine virtuelle.

Qu'est-ce qu'un fournisseur de clés standard ?

Dans vSphere, un fournisseur de clés standard obtient des clés de chiffrement directement à partir d'un serveur de clés et vCenter Server distribue des clés aux hôtes ESXi requis dans un centre de données.

Vous pouvez ajouter des fournisseurs de clés standard distincts pour différents utilisateurs et définir le fournisseur de clés standard par défaut.

Exigences relatives au fournisseur de clés standard vSphere

- vSphere 6.5 ou version ultérieure
- Un serveur de clés externe (KMS)

Le serveur de gestion de clés doit prendre en charge la norme KMIP (Key Management Interoperability Protocol) 1.1. Reportez-vous à *Matrices de compatibilité vSphere* pour plus de détails.

Vous pouvez trouver plus d'informations sur les fournisseurs KMS certifiés VMware dans le Guide de compatibilité VMware, sous la section Plate-forme et calcul. Si vous sélectionnez Guides de compatibilité, vous pouvez accéder à de la documentation sur la compatibilité du serveur de gestion des clés (KMS). Cette documentation est régulièrement mise à jour.

Privilèges du fournisseur de clés standard

Les fournisseurs de clés standard utilisent les privilèges **Cryptographer.***. Reportez-vous à la section Privilèges d'opérations de chiffrement.

Configurer le fournisseur de clés standard

Avant de pouvoir commencer avec des tâches de chiffrement de machine virtuelle, vous devez configurer le fournisseur de clés standard.

La configuration d'un fournisseur de clés standard inclut l'ajout du fournisseur de clés et l'établissement d'une relation de confiance avec le serveur de clés. Lorsque vous ajoutez un fournisseur de clés, vous êtes invité à le définir comme cluster par défaut. Vous pouvez modifier explicitement le fournisseur de clés par défaut. vCenter Server provisionne des clés à partir du fournisseur de clés par défaut.

Note Ce qui était précédemment appelé un cluster de serveur de gestion des clés dans vSphere 6.5 et 6.7 est désormais appelé fournisseur de clés.

Chiffrement de la machine virtuelle pour la configuration d'un fournisseur de clés standard (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere7_keyprovider)

Ajouter un fournisseur de clés standard à l'aide de vSphere Client

Vous pouvez ajouter un fournisseur de clés standard à votre système vCenter Server depuis vSphere Client ou au moyen de l'API publique.

vSphere Client vous permet d'ajouter un fournisseur de clés standard à votre système vCenter Server et d'établir une relation de confiance entre le serveur de clés et vCenter Server.

- Vous pouvez ajouter plusieurs serveurs de clés à partir du même fournisseur.

- Si votre environnement prend en charge des solutions de différents fournisseurs, vous pouvez ajouter plusieurs fournisseur de clés.
- Si votre environnement inclut plusieurs fournisseurs de clés et si vous supprimez le fournisseur de clés par défaut, vous devez en définir un autre de façon explicite.
- Vous pouvez configurer le serveur de clés avec des adresses IPv6.
  - Le système vCenter Server et le serveur de clés ne peuvent être configurés qu'avec des adresses IPv6.

Conditions préalables

- Vérifiez que le serveur de clés (KMS) figure dans le *Guide de compatibilité VMware pour les serveurs de gestion des clés (KMS)*, qu'il est conforme à KMIP 1.1 et qu'il peut être un profil Symmetric Key Foundry And Server.
- Assurez-vous que vous disposez des privilèges requis : **Opérations de chiffrement.Gérer les serveurs de clés**.
- Assurez-vous que le serveur de clés dispose de la haute disponibilité. La perte de connexion au serveur de clés, telle qu'une coupure de courant ou un événement de récupération d'urgence, rend inaccessibles les machines virtuelles chiffrées.

  Note À partir vSphere 7.0 mise à jour 2, les machines virtuelles chiffrées et les TPM virtuels peuvent continuer à fonctionner même lorsque le serveur de clés est temporairement hors ligne ou indisponible. Reportez-vous à la section Présentation de la persistance des clés.
- Examinez attentivement les dépendances de votre infrastructure sur le serveur de clés. Certaines solutions KMS sont fournies en tant que dispositifs virtuels, ce qui permet de créer une boucle de dépendance ou d'autres problèmes de disponibilité entraînant un mauvais placement du dispositif KMS.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer** et, sous **Sécurité**, cliquez sur **Fournisseurs de clés**.
4. Cliquez sur **Ajouter un fournisseur de clés standard** et entrez les informations du fournisseur de clés.

Option	Valeur
Nom	Nom du fournisseur de clés.
KMS	Alias du serveur de clés (KMS).
Adresse	Adresse IP ou nom de domaine complet du serveur de clés.
Port	Port sur lequel vCenter Server se connecte au serveur de clés.
Serveur proxy	Adresse facultative du serveur proxy pour la connexion au serveur de clés.

Option	Valeur
Port du proxy	Port proxy facultatif pour la connexion au serveur de clés.
Nom d'utilisateur	Certains fournisseurs de serveurs de clés permettent aux utilisateurs d'isoler les clés de chiffrement utilisées par différents utilisateurs ou groupes en spécifiant un nom d'utilisateur et un mot de passe. Spécifiez un nom d'utilisateur uniquement si votre serveur de clés prend en charge cette fonctionnalité et si vous prévoyez de l'utiliser.
Mot de passe	Certains fournisseurs de serveurs de clés permettent aux utilisateurs d'isoler les clés de chiffrement utilisées par différents utilisateurs ou groupes en spécifiant un nom d'utilisateur et un mot de passe. Spécifiez un mot de passe uniquement si votre serveur de clés prend en charge cette fonctionnalité et si vous prévoyez de l'utiliser.

Vous pouvez cliquer sur **Ajouter un KMS** pour ajouter d'autres serveurs de clés.

5 Cliquez sur **Ajouter un fournisseur de clés**.

6 Cliquez sur **Approuver**.

vCenter Server ajoute le fournisseur de clés et affiche l'état Connecté.

Étape suivante

Reportez-vous à la section Établissement d'une connexion approuvée de fournisseur de clés standard en échangeant des certificats.

Établissement d'une connexion approuvée de fournisseur de clés standard en échangeant des certificats

Après avoir ajouté le fournisseur de clés standard au système vCenter Server, vous pouvez établir une connexion approuvée. Le processus exact dépend des certificats acceptés par le fournisseur de clés, et de la stratégie de votre entreprise.

Conditions préalables

Ajoutez le fournisseur de clés standard.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés.

Le serveur KMS du fournisseur de clés s'affiche.

4 Sélectionnez le KMS.

5 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

6 Sélectionnez l'option correspondant à votre serveur et suivez la procédure.

Option	Reportez-vous au
Certificat d'autorité de certification racine vCenter Server	Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance avec le fournisseur de clés standard.
Certificat vCenter Server	Utiliser l'option de certificat pour établir une connexion de confiance avec le fournisseur de clés standard.
Télécharger le certificat et la clé privée	Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance avec le fournisseur de clés standard.
Demande de signature du nouveau certificat	Utiliser l'option Nouvelle demande de signature de certificat pour établir une connexion de confiance avec un fournisseur de clés standard.

Utiliser l'option Certificat d'autorité de certification racine pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveurs de gestion de clés (KMS) imposent le téléchargement du certificat d'autorité de certification racine sur le serveur KMS. Tous les certificats qui sont signés par votre autorité de certification racine sont alors approuvés par ce KMS.

Le certificat d'autorité de certification racine que le chiffrement de machines virtuelles vSphere utilise est un certificat autosigné qui est stocké dans un magasin distinct du VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Note Générez un certificat d'autorité de certification uniquement si vous souhaitez remplacer des certificats existants. Si vous le faites en effet, les autres certificats signés par cette autorité de certification racine deviennent non valides. Vous pouvez générer un nouveau certificat d'autorité de certification racine dans le cadre de ce workflow.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

Le serveur KMS du fournisseur de clés s'affiche.

4 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

5 Sélectionnez **Certificat d'autorité de certification racine vCenter** et cliquez sur **Suivant**.

La boîte de dialogue Télécharger un certificat d'autorité de certification est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

6 Copiez le certificat dans le presse-papiers ou téléchargez-le comme un fichier.

7 Suivez les instructions de votre fournisseur de KMS pour télécharger le certificat sur son système.

Note Certains fournisseurs de KMS exigent que le fournisseur de KMS redémarre le KMS pour détecter le certificat racine que vous téléchargez.

Étape suivante

Finalisez l'échange de certificat. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option de certificat pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveurs de gestion de clés (KMS) imposent le téléchargement du certificat de vCenter Server sur le serveur KMS. Une fois le téléchargement effectué, le KMS accepte le trafic provenant d'un système avec ce certificat.

vCenter Server génère un certificat pour protéger les connexions avec le KMS. Le certificat est stocké dans un magasin de clés distinct dans VECS (VMware Endpoint Certificate Store) sur le système vCenter Server.

Procédure

1 Accédez à l'instance de vCenter Server.

2 Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.

3 Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

Le serveur KMS du fournisseur de clés s'affiche.

4 Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.

5 Sélectionnez **Certificat vCenter** et cliquez sur **Suivant**.

La boîte de dialogue Télécharger le certificat est renseignée avec le certificat racine utilisé par vCenter Server pour le chiffrement. Ce certificat est stocké dans VECS.

Note Ne générez pas de nouveau certificat sauf si vous souhaitez remplacer des certificats existants.

6 Copiez le certificat dans le presse-papier ou téléchargez-le comme un fichier.

7 Suivez les instructions de votre fournisseur de KMS pour mettre à jour le certificat sur le KMS.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option Télécharger le certificat et la clé privée pour établir une connexion de confiance avec le fournisseur de clés standard

Certains fournisseurs de serveur de gestion de clés (KMS) exigent que vous téléchargiez le certificat et la clé privée du serveur KMS sur le système vCenter Server.

Certains fournisseurs de KMS génèrent un certificat et une clé privée pour la connexion et les mettent à votre disposition. Après le téléchargement des fichiers, le KMS approuve votre instance de vCenter Server.

Conditions préalables

- Demandez un certificat et une clé privée au fournisseur de KMS. Les fichiers sont des fichiers X509 au format PEM.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

   Le serveur KMS du fournisseur de clés s'affiche.
4. Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.
5. Sélectionnez **Certificat KMS et clé privée** et cliquez sur **Suivant**.
6. Collez le certificat que vous avez reçu du fournisseur KMS dans la zone de texte supérieure ou cliquez sur **Télécharger un fichier** pour télécharger le fichier de certificat.
7. Collez le fichier de clé dans la zone de texte supérieure ou cliquez sur **Télécharger un fichier** pour télécharger le fichier de clé.
8. Cliquez sur **établir la confiance**.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Utiliser l'option Nouvelle demande de signature de certificat pour établir une connexion de confiance avec un fournisseur de clés standard

Certains fournisseurs de serveur de gestion de clés (KMS) exigent que vCenter Server génère une demande de signature de certificat (CSR) et envoie cette demande CSR au KMS. Le KMS signe le CSR et renvoie le certificat signé. Vous pouvez télécharger le certificat signé sur vCenter Server.

L'utilisation de l'option **Demande de signature du nouveau certificat** se fait en deux étapes. Dans un premier temps, vous générez le CSR et vous l'envoyez au fournisseur de KMS. Vous téléchargez ensuite le certificat signé que vous avez reçu du fournisseur de KMS sur vCenter Server.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

   Le serveur KMS du fournisseur de clés s'affiche.
4. Dans le menu déroulant **Établir une approbation**, sélectionnez **Établir une relation de confiance entre le KMS et l'instance de vCenter**.
5. Sélectionnez **Nouvelle demande de signature de certificat (CSR)**, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue, copiez dans le Presse-papiers le certificat complet contenu dans la zone de texte ou téléchargez-le sous la forme d'un fichier.

   Utilisez le bouton **Générer un nouveau CSR** dans la zone de dialogue uniquement si vous souhaitez générer explicitement un CSR. L'utilisation de cette option rend les certificats signés basés sur l'ancien CSR non valides.
7. Suivez les instructions fournies par votre fournisseur de KMS pour envoyer le CSR.
8. Lorsque vous recevez le certificat signé du fournisseur KMS, cliquez de nouveau sur **Fournisseurs de clés**, sélectionnez le fournisseur de clés et, dans le menu déroulant **Établir une relation de confiance**, sélectionnez **Télécharger le certificat CSR signé**.
9. Collez le certificat signé dans la zone de texte du bas ou cliquez sur **Télécharger le fichier** et télécharger le fichier, puis cliquez sur **Télécharger**.

Étape suivante

Finalisez la relation de confiance. Reportez-vous à la section Terminer la configuration de l'approbation pour un fournisseur de clés standard.

Définir le fournisseur de clés par défaut

Vous devez définir le fournisseur de clés par défaut si vous ne configurez pas le premier cluster comme fournisseur de clés par défaut, ou si votre environnement utilise plusieurs fournisseurs de clés et que vous supprimez le fournisseur par défaut.

Conditions préalables

Nous vous recommandons de vérifier que l'état de la connexion dans l'onglet **Fournisseurs de clés** indique Connecté, et présente une coche verte.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés.
4. Cliquez sur **Définir en tant que valeur par défaut**.

   Une boîte de dialogue de confirmation apparaît.
5. Cliquez sur **Définir en tant que valeur par défaut**.

   Le fournisseur de clés s'affiche en tant que valeur par défaut actuelle.

Terminer la configuration de l'approbation pour un fournisseur de clés standard

À moins que la boîte de dialogue **Ajouter un serveur de clés standard** ne vous ait invité à approuver le KMS, vous devez explicitement établir la confiance une fois l'échange de certificats terminé.

Vous pouvez terminer la configuration de la confiance, c'est-à-dire indiquer à vCenter Server de faire confiance au certificat KMS, soit en faisant confiance au KMS, soit en téléchargeant un certificat KMS. Deux options s'offrent à vous :

- Faire explicitement confiance au certificat en utilisant l'option **Télécharger un certificat KMS**.
- Télécharger un certificat KMS feuille ou le certificat KMS de l'autorité de certification sur vCenter Server à l'aide de l'option **Établir une relation de confiance entre l'instance de vCenter et le KMS**.

Note Si vous téléchargez le certificat de l'autorité de certification racine ou le certificat de l'autorité de certification intermédiaire, vCenter Server fait confiance à tous les certificats signés par cette autorité de certification. Pour une sécurité renforcée, téléchargez un certificat feuille ou un certificat d'autorité de certification intermédiaire contrôlé par le fournisseur KMS.

Procédure

1. Accédez à l'instance de vCenter Server.
2. Cliquez sur **Configurer** et sélectionnez **Fournisseurs de clés** sous **Sécurité**.
3. Sélectionnez le fournisseur de clés auquel vous souhaitez établir une connexion approuvée.

   Le serveur KMS du fournisseur de clés s'affiche.
4. Sélectionnez le KMS.

5 Sélectionnez une des options suivantes à partir du menu déroulant **Établir une relation de confiance**.

Option	Action
Établir une relation de confiance entre l'instance de vCenter et le KMS	Dans la boîte de dialogue qui apparaît, cliquez sur **Faire confiance**.
Télécharger un certificat KMS	a Dans la boîte de dialogue qui s'affiche, collez le certificat ou cliquez sur **Télécharger un fichier** et accédez au fichier de certificat. b Cliquez sur **Télécharger**.

Configurer des fournisseurs de clés distincts pour différents utilisateurs

Vous pouvez configurer votre environnement avec des fournisseurs de clés distincts pour différents utilisateurs de la même instance de KMS. Il peut s'avérer utile de disposer de plusieurs fournisseurs de clés, par exemple si vous voulez accorder à différents départements de votre entreprise un accès à différents ensembles de clés de chiffrement.

Vous pouvez utiliser plusieurs fournisseurs de clés pour le même KMS pour distinguer les clés. Il est essentiel de disposer d'ensembles distincts de clés, par exemple pour les cas avec d'utilisation avec différents BU ou différents clients.

Note Tous les fournisseurs KMS ne prennent pas en charge plusieurs utilisateurs.

Conditions préalables

Configurez la connexion avec KMS.

Procédure

1 Créez deux utilisateurs avec les noms d'utilisateur et mots de passe correspondants, par exemple C1 et C2, sur KMS.

2 Connectez-vous à vCenter Server et créez le premier fournisseur de clés.

3 Lorsque vous êtes invité à entrer un nom d'utilisateur et un mot de passe, fournissez des informations qui sont uniques au premier utilisateur.

4 Créez un second fournisseur de clés et ajoutez le même KMS, mais utilisez les seconds nom d'utilisateur et mot de passe (C2).

Résultats

Les deux fournisseurs de clés disposent d'une connexion indépendante au KMS et utilisent un ensemble différent de clés.

Configuration et gestion de vSphere Native Key Provider

8

L'utilisation d'un vSphere® Native Key Provider™ VMware dans votre environnement vSphere nécessite une certaine préparation. Après avoir configuré vSphere Native Key Provider, vous pouvez créer des vTPM (virtual Trusted Platform Modules) sur vos machines virtuelles.

Une fois que votre environnement est configuré pour vSphere Native Key Provider, vous pouvez utiliser le vSphere Client et l'API pour créer des vTPM. Si vous achetez VMware vSphere® Enterprise Plus Edition™, vous pouvez également chiffrer des machines virtuelles et des disques virtuels, et chiffrer des machines virtuelles et des disques existants.

Ce chapitre contient les rubriques suivantes :

- Présentation de vSphere Native Key Provider
- Flux de processus vSphere Native Key Provider
- Configurer un fournisseur vSphere Native Key Provider
- Sauvegarder un vSphere Native Key Provider
- Récupération d'un vSphere Native Key Provider
- Configurer une instance de vSphere Native Key Provider
- Supprimer un vSphere Native Key Provider

Présentation de vSphere Native Key Provider

À partir de vSphere 7.0 Update 2, vous pouvez utiliser le périphérique vSphere Native Key Provider intégré pour activer des technologies de chiffrement, comme des TPM virtuels (vTPM).

vSphere Native Key Provider est inclus dans toutes les éditions de vSphere et ne nécessite pas de serveur de clés externe (également appelé serveur de gestion des clés dans le secteur). Vous pouvez également utiliser vSphere Native Key Provider pour le chiffrement de machine virtuelle vSphere, mais vous devez acheter l'édition VMware vSphere® Enterprise Plus™.

Qu'est-ce que vSphere Native Key Provider ?

Avec un fournisseur de clés standard ou un fournisseur de clés approuvé, vous devez configurer un serveur de clés externe. Dans une configuration de fournisseur de clés standard, vCenter Server extrait les clés du serveur de clés externe et les distribue aux hôtes ESXi. Dans une configuration de fournisseur de clés approuvé (Autorité d'approbation vSphere), les hôtes ESXi approuvés extraient les clés directement.

Avec vSphere Native Key Provider, vous n'avez plus besoin d'un serveur de clés externe. vCenter Server génère une clé principale, appelée clé de dérivation de clé (KDK), et la transmet à tous les hôtes ESXi du cluster. Les hôtes ESXi génèrent ensuite des clés de chiffrement des données (même si elles ne sont pas connectées à vCenter Server) pour activer des fonctionnalités de sécurité telles que des vTPM. La fonctionnalité vTPM est incluse dans toutes les éditions vSphere. Pour utiliser vSphere Native Key Provider pour le chiffrement de machine virtuelle vSphere, vous devez avoir acheté l'édition vSphere Enterprise Plus. vSphere Native Key Provider peut coexister avec une infrastructure de serveur de clés existante.

vSphere Native Key Provider :

- Permet d'utiliser des vTPM, le chiffrement de machine virtuelle vSphere et vSAN le chiffrement des données au repos, lorsque vous n'avez pas besoin ou ne souhaitez pas de serveur de clés externe.
- Fonctionne uniquement avec les produits d'infrastructure VMware.
- Ne fournit pas d'interopérabilité externe, de support KMIP, de modules de sécurité matérielle ou les autres fonctionnalités qu'un serveur de clés externe tiers traditionnel peut fournir pour assurer l'interopérabilité ou le respect de la réglementation. Si votre organisation cette fonctionnalité pour les produits et composants non-VMware, installez un serveur de clés tiers traditionnel.
- Permet de répondre aux besoins des organisations qui ne peuvent pas utiliser ou ne souhaitent pas utiliser un serveur de clés externe.
- Améliore les pratiques de nettoyage des données et de réutilisation du système en permettant l'utilisation antérieure de technologies de chiffrement sur des supports difficiles à nettoyer, tels que Flash et SSD.
- Fournit un chemin de transition entre les fournisseurs de clés. vSphere Native Key Provider est compatible avec le fournisseur de clés VMware standard et le fournisseur de clés approuvé vSphere Trust Authority.
- Fonctionne avec plusieurs systèmes vCenter Server en utilisant une configuration Enhanced Linked Mode ou une configuration vCenter Server High Availability.
- Peut être utilisé pour activer un vTPM dans toutes les éditions de vSphere et chiffrer les machines virtuelles avec l'achat de l'édition vSphere Enterprise Plus qui inclut le chiffrement de machine virtuelle vSphere. Le chiffrement de machines virtuelles vSphere fonctionne avec un périphérique vSphere Native Key Provider, comme il le fait avec les fournisseurs de clés approuvés et standard VMware.

- Peut être utilisé pour activer le chiffrement des données au repos vSAN avec l'utilisation d'une licence vSAN appropriée.
- Peut utiliser un module de plate-forme sécurisée (TPM) pour renforcer la sécurité lorsqu'un module est installé sur un hôte ESXi. Vous pouvez également configurer vSphere Native Key Provider pour qu'il soit disponible uniquement pour les hôtes sur lesquels un TPM est installé.

Comme pour toutes les solutions de sécurité, tenez compte de la conception du système, des éléments à prendre en compte pour la mise en œuvre et des compromis liés à l'utilisation d'un fournisseur de clés natif. Par exemple, la persistance des clés ESXi évite que la dépendance sur un serveur de clés soit toujours disponible. Cependant, étant donné que la persistance des clés stocke les informations de chiffrement du fournisseur de clés natif sur les hôtes en cluster, vous êtes toujours exposé à un risque si des acteurs malveillants dérobent les données des hôtes ESXi eux-mêmes. Étant donné que les environnements diffèrent, évaluez et mettez en œuvre vos contrôles de sécurité conformément aux besoins réglementaires et de sécurité de votre organisation, aux exigences opérationnelles et à la tolérance aux risques.

Conditions requises pour vSphere Native Key Provider

Pour utiliser vSphere Native Key Provider :

- Assurez-vous que le système vCenter Server et les hôtes ESXi exécutent vSphere 7.0 Update 2 ou une version ultérieure.
- Configurez les hôtes ESXi dans un cluster.
- Utilisez le nom de domaine complet (FQDN) du système vCenter Server lorsque vous y accédez avec l'instance de vSphere Client.
- Configurez la sauvegarde et la restauration basées sur des fichiers vCenter Server et stockez les sauvegardes de manière sécurisée, car elles contiennent la clé de dérivation de clé. Reportez-vous à la rubrique sur la sauvegarde et la restauration de vCenter Server dans *Installation et configuration de vCenter Server*.

Pour effectuer le chiffrement de machine virtuelle vSphere ou le chiffrement de vSAN à l'aide de vSphere Native Key Provider, vous devez acheter l'édition de ces produits contenant la licence appropriée.

vSphere Native Key Provider et Enhanced Linked Mode

Vous pouvez configurer un seul périphérique vSphere Native Key Provider pouvant être partagé entre les systèmes vCenter Server configurés dans une configuration Enhanced Linked Mode. Les étapes générales de ce scénario sont les suivantes :

1 Création du périphérique vSphere Native Key Provider sur l'un des systèmes vCenter Server

2 Sauvegarde du fournisseur de clés natif sur le vCenter Server sur lequel il a été créé

3 Exportation du fournisseur de clés natif

4 Importation du fournisseur de clés natif dans les autres systèmes vCenter Server dans la configuration Enhanced Linked Mode

Privilèges vSphere Native Key Provider

Comme pour les fournisseurs de clés standard et approuvés, vSphere Native Key Provider utilise le **cryptographe.***. En outre, vSphere Native Key Provider utilise le privilège **Cryptographer.ReadKeyServersInfo**, qui est spécifique aux périphériques vSphere Native Key Providers, pour répertorier les périphériques vSphere Native Key Providers. Reportez-vous à la section Privilèges d'opérations de chiffrement.

Alarmes vSphere Native Key Provider

Vous devez sauvegarder un périphérique vSphere Native Key Provider. Lorsqu'un périphérique vSphere Native Key Provider n'est pas sauvegardé, vCenter Server génère une alarme. Lorsque vous sauvegardez un périphérique vSphere Native Key Provider pour lequel une alarme a été générée, vCenter Server réinitialise l'alarme. Par défaut, vCenter Server recherche les périphériques vSphere Native Key Provider sauvegardés une fois par jour. Vous pouvez modifier l'intervalle de vérification en modifiant l'option `vpxd.KMS.backupCheckInterval`.

Vérification de correction périodique de vSphere Native Key Provider

vCenter Server vérifie périodiquement que la configuration de vSphere Native Key Provider sur les hôtes vCenter Server et ESXi correspond. Lorsqu'un état d'un hôte change, par exemple, lorsque vous ajoutez un hôte au cluster, la configuration du fournisseur de clés sur le cluster s'écarte de la configuration sur l'hôte. Si la configuration (keyID) diffère sur l'hôte, vCenter Server met à jour la configuration de l'hôte automatiquement. Aucune intervention manuelle n'est requise.

Par défaut, vCenter Server vérifie la configuration toutes les cinq minutes. Vous pouvez modifier l'intervalle en utilisant l'option `vpxd.KMS.remediationInterval`.

Flux de processus vSphere Native Key Provider

Comprendre les flux de processus vSphere Native Key Provider vSphere est essentiel pour apprendre à configurer et à gérer votre vSphere Native Key Provider vSphere.

Vous pouvez utiliser le périphérique vSphere Native Key Provider vSphere intégré pour alimenter des TPM virtuels basés sur le chiffrement (vTPM). vSphere Native Key Provider est inclus dans toutes les éditions de vSphere et ne nécessite pas de serveur de clés externe (KMS). Pour utiliser vSphere Native Key Provider pour le chiffrement de machine virtuelle vSphere, vous devez acheter l'édition vSphere Enterprise+.

Configuration de vSphere Native Key Provider

La configuration de vSphere Native Key Provider implique les opérations de base ci-après :

1 Un utilisateur ayant les privilèges administratifs appropriés utilise vSphere Client pour créer un périphérique vSphere Native Key Provider sur une instance de vCenter Server.

2 vCenter Server configure ensuite vSphere Native Key Provider pour tous les clusters des hôtes ESXi.

   Dans cette étape, vCenter Server transmet une clé principale à tous les hôtes ESXi du cluster. En outre, si vous mettez à jour ou supprimez un vSphere Native Key Provider, la modification est transmise aux hôtes du cluster.

3 Les utilisateurs ayant les privilèges de chiffrement appropriés créent des vTPM et des machines virtuelles chiffrées (à condition d'avoir acheté l'édition vSphere Enterprise+).

   Reportez-vous aux sections Chapitre 11 Sécurisation des machines virtuelles avec le TPM et Chapitre 10 Utiliser le chiffrement dans votre environnement vSphere.

Flux de chiffrement de vSphere Native Key Provider

Pour comprendre comment différents composants interagissent pour effectuer une tâche de chiffrement à l'aide de vSphere Native Key Provider, reportez-vous à la section Flux de chiffrement.

Configurer un fournisseur vSphere Native Key Provider

Avant de pouvoir commencer avec des tâches de chiffrement, vous devez configurer un vSphere Native Key Provider sur vCenter Server.

vSphere 7.0 mise à jour 2 inclut un fournisseur de clés appelé vSphere Native Key Provider. vSphere Native Key Provider permet d'utiliser les fonctionnalités liées au chiffrement sans nécessiter de serveur de clés externe (KMS). Initialement, vCenter Server n'est pas configuré avec un vSphere Native Key Provider. Vous devez configurer manuellement un vSphere Native Key Provider.

Un hôte ESXi n'a pas besoin d'un TPM pour utiliser un vSphere Native Key Provider. Toutefois, un TPM offre une sécurité améliorée.

Note Lorsque vous configurez vSphere Native Key Provider, les fournisseurs de clés sont disponibles sur tous les clusters pour le vCenter Server sur lequel vous les configurez. Par conséquent, tous les hôtes attachés au vCenter Server ont accès à tous les vSphere Native Key Providers que vous configurez.

Conditions préalables

Privilège nécessaire : **Opérations de chiffrement. Gérer des serveurs de clés**

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer** et, sous **Sécurité**, cliquez sur **Fournisseurs de clés**.
4. Cliquez sur **Ajouter** puis cliquez sur **Ajouter un fournisseur de clés natif**.

5 Entrez un nom pour le vSphere Native Key Provider.

6 Si vous souhaitez que ce vSphere Native Key Provider soit utilisé uniquement par les hôtes avec un TPM, cochez la case **Utiliser le fournisseur de clés uniquement avec des hôtes ESXi protégés par TPM**.

   Si cette option est activée, le vSphere Native Key Provider n'est disponible que sur les hôtes avec un TPM.

7 Cliquez sur **Ajouter un fournisseur de clés**.

Note Il faut environ cinq minutes pour que tous les hôtes ESXi en cluster d'un centre de données obtiennent le fournisseur de clés et que le vCenter Server mette à jour son cache. En raison de la façon dont les informations sont propagées, vous devrez peut-être attendre quelques minutes pour utiliser le fournisseur de clés pour les opérations de clés sur certains hôtes.

Résultats

Le vSphere Native Key Provider est ajouté et s'affiche dans le volet Fournisseur de clés. À ce stade, le vSphere Native Key Provider n'est pas sauvegardé. Vous devez sauvegarder le vSphere Native Key Provider avant de pouvoir l'utiliser.

Étape suivante

Reportez-vous à la section Sauvegarder un vSphere Native Key Provider.

Sauvegarder un vSphere Native Key Provider

Si vous devez restaurer la configuration du fournisseur de clés, vous devez sauvegarder un vSphere Native Key Provider dans le cadre d'un scénario de récupération d'urgence. Vous pouvez utiliser vSphere Client, PowerCLI ou l'API pour sauvegarder le vSphere Native Key Provider.

Le vSphere Native Key Provider est sauvegardé dans le cadre de la sauvegarde basée sur fichier de vCenter Server. Toutefois, vous devez sauvegarder le vSphere Native Key Provider au moins une fois avant de pouvoir l'utiliser. Lorsque vous créez un vSphere Native Key Provider, il n'est pas sauvegardé.

Une sauvegarde est nécessaire si vous devez restaurer la configuration. Conservez le fichier de sauvegarde dans un emplacement sécurisé. Vous pouvez protéger la sauvegarde par mot de passe lorsque vous la créez. Le fichier de sauvegarde est au format PKCS#12.

vCenter Server crée une alarme si un vSphere Native Key Provider n'a pas été sauvegardé. Vous pouvez acquitter l'alarme, mais elle réapparaît toutes les 24 heures jusqu'à ce que vous ayez sauvegardé le vSphere Native Key Provider.

Conditions préalables

Privilège nécessaire : **Opérations de chiffrement. Gérer des serveurs de clés**

Note Pour enregistrer le vSphere Native Key Provider, vous devez vous connecter à l'aide du nom de domaine complet vCenter Server. Si vous vous connectez à l'aide de l'adresse IP de vCenter Server, la sauvegarde ne se termine pas. Dans une configuration Enhanced Link Mode, vous devez effectuer la sauvegarde sur le vCenter Server auquel le fournisseur de clés appartient.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.

   Connectez-vous à l'aide du nom de domaine complet de vCenter Server. Si vous utilisez l'adresse IP pour vous connecter, la sauvegarde ne se termine pas.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer** et, sous **Sécurité**, cliquez sur **Fournisseurs de clés**.
4. Sélectionnez le vSphere Native Key Provider que vous souhaitez sauvegarde.

   L'état « Non sauvegardé » s'affiche pour les fournisseurs de clés que vous n'avez pas sauvegardés.
5. Cliquez sur **Sauvegarder**.
6. Pour protéger par mot de passe la sauvegarde, cochez la case **Protéger les données du fournisseur de clés natif avec un mot de passe**.
   a. Entrez un mot de passe et enregistrez-le dans un emplacement sécurisé.
   b. Cochez la case **J'ai enregistré le mot de passe dans un lieu sûr** pour indiquer que vous avez enregistré le mot de passe dans un endroit sécurisé.
7. Cliquez sur **Sauvegarder le fournisseur de clés**.

   Le fichier de sauvegarde est au format PKCS#12.
8. Enregistrez le fichier de sauvegarde dans un emplacement sécurisé.

Résultats

L'état du vSphere Native Key Provider change de Non sauvegardé, en Avertissement, en Actif. Avertissement indique que le vCenter Server continue à envoyer les informations vers tous les hôtes ESXi dans le centre de données. Actif signifie que les informations ont été envoyées vers tous les hôtes.

Étape suivante

Pour ajouter des vTPM à vos hôtes ESXi, consultez Chapitre 11 Sécurisation des machines virtuelles avec le TPM. Pour chiffrer des machines virtuelles, consultez Chapitre 10 Utiliser le chiffrement dans votre environnement vSphere.

Récupération d'un vSphere Native Key Provider

Vous pouvez récupérer le vSphere Native Key Provider via vSphere Client ou à partir de la sauvegarde de vCenter Server Appliance.

Si nécessaire, vous pouvez récupérer un vSphere Native Key Provider de l'une des manières suivantes.

1 Si vous n'avez pas besoin de recréer votre dispositif vCenter Server Appliance, utilisez vSphere Client pour restaurer le fournisseur de clés. Reportez-vous à la section Restaurer un vSphere Native Key Provider à l'aide de vSphere Client.

2 Si vous devez recréer votre dispositif vCenter Server Appliance, vous devez restaurer le fournisseur de clés à partir de votre sauvegarde de vCenter Server Appliance. Lorsque vous effectuez une sauvegarde de vCenter Server Appliance, celle-ci enregistre le vSphere Native Key Provider. Pour plus d'informations sur la restauration de vCenter Server Appliance à partir de la sauvegarde, reportez-vous à la rubrique https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html.

Restaurer un vSphere Native Key Provider à l'aide de vSphere Client

Vous pouvez utiliser vSphere Client pour restaurer le vSphere Native Key Provider.

Vous pouvez restaurer un fournisseur de clés natif au cas où il a été supprimé accidentellement ou si vous devez effectuer une récupération d'urgence.

Lorsque vous restaurez un vSphere Native Key Provider, vous n'avez pas besoin de sauvegarder le fournisseur de clés à nouveau. La sauvegarde initiale est suffisante. Continuez à conserver le fichier de sauvegarde dans un emplacement sécurisé.

Conditions préalables

- Privilège nécessaire : **Opérations de chiffrement. Gérer des serveurs de clés**
- Fichier de sauvegarde du fournisseur de clés.
- Mot de passe du fichier de fournisseur de clés, si vous en avez entré un lorsque vous avez sauvegardé le fournisseur de clés.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer** et, sous **Sécurité**, cliquez sur **Fournisseurs de clés**.
4. Sélectionnez le vSphere Native Key Provider et cliquez sur **Restaurer**.
5. Accédez à l'emplacement du fichier et sélectionnez le fichier de clé chiffré de sauvegarde.

   Le fichier a été enregistré au format PKCS#12.
6. (Facultatif) Si le fichier est protégé par mot de passe, entrez le mot de passe.

7 Cliquez sur **Suivant**.

8 (Facultatif) Si vous avez décidé d'utiliser ce fournisseur de clés uniquement avec des hôtes ESXi protégés par TPM, cochez la case.

9 Cliquez sur **Terminer**.

Résultats

Le vSphere Native Key Provider est restauré.

Configurer une instance de vSphere Native Key Provider

Dans le cadre de vos plans de rotation des clés standard, vous pouvez utiliser PowerCLI pour mettre à jour une instance de vSphere Native Key Provider.

Si vous disposez d'une stratégie pour la rotation des clés, vous pouvez mettre à jour l'instance de vSphere Native Key Provider et renouveler les clés des machines virtuelles que vous avez chiffrées avec ce fournisseur de clés. Vous pouvez également renouveler la clé des machines virtuelles chiffrées sans mettre à jour le fournisseur de clés. Dans ce cas, seules les clés de machine virtuelle sont modifiées. Pour mettre à jour vSphere Native Key Provider, vous devez utiliser PowerCLI.

Conditions préalables

- Privilège nécessaire : **Opérations de chiffrement. Gérer des serveurs de clés**
- PowerCLI 12.3.0

Procédure

1 Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu'utilisateur administrateur au vCenter Server sur lequel vous avez généré l'instance de vSphere Native Key Provider que vous souhaitez mettre à jour.

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 Pour mettre à jour le fournisseur de clés, exécutez l'applet de commande `Set-KeyProvider`.

```
Set-KeyProvider -KeyProvider providerId -KeyId keyUuid
```

Un avertissement s'affiche concernant la sauvegarde de la configuration.

3 Pour sauvegarder le fournisseur de clés, exécutez l'applet de commande `Export-KeyProvider`.

```
Export-KeyProvider -FilePath path_file_name
```

Vous pouvez également sauvegarder le fournisseur de clés à l'aide du vSphere Client. Reportez-vous à la section Sauvegarder un vSphere Native Key Provider.

Résultats

Lorsqu'un fournisseur de clés est mis à jour, son état passe à Non sauvegardé. Après la sauvegarde du fournisseur de clés, son état devient Actif.

Supprimer un vSphere Native Key Provider

Vous pouvez supprimer un vSphere Native Key Provider de vCenter Server.

Après la suppression d'un vSphere Native Key Provider, les machines virtuelles qui ont des vTPM ou qui sont chiffrées continuent à s'exécuter. Si vous redémarrez l'hôte ESXi, ses machines virtuelles chiffrées passent à un état verrouillé. Une fois que vous avez désinscrit ces machines virtuelles, elles entrent dans un état verrouillé lorsque vous tentez de les réenregistrer. La seule façon de déverrouiller les machines virtuelles consiste à restaurer le vSphere Native Key Provider précédent.

Conditions préalables

Privilège nécessaire : **Opérations de chiffrement. Gérer des serveurs de clés**

Avant de supprimer un vSphere Native Key Provider, renouvelez les clés des machines virtuelles et des banques de données chiffrées avec ce fournisseur de clés avec un autre fournisseur de clés. Conservez une sauvegarde du fournisseur vSphere Native Key Provider au cas où vous devez renouveler la clé d'une machine virtuelle chiffrée après la suppression du fournisseur de clés.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Parcourez la liste d'inventaire et sélectionnez l'instance vCenter Server.
3. Cliquez sur **Configurer** et, sous **Sécurité**, cliquez sur **Fournisseurs de clés**.
4. Sélectionnez le fournisseur de clés que vous souhaitez supprimer.
5. Cliquez sur **Supprimer**.
6. Lisez le message d'avertissement et faites glisser le curseur complètement à droite.
7. Cliquez sur **Supprimer**.

Résultats

Le vSphere Native Key Provider est supprimé du vCenter Server.

Autorité d'approbation vSphere

9

Avec vSphere 7.0 et les versions ultérieures, vous pouvez bénéficier de VMware® vSphere Trust Authority™. Autorité d'approbation vSphere est une technologie de base qui améliore la sécurité des charges de travail. Autorité d'approbation vSphere établit un niveau de confiance amélioré dans votre organisation en associant une racine matérielle d'approbation de l'hôte ESXi à la charge de travail elle-même.

Ce chapitre contient les rubriques suivantes :

- Concepts et fonctionnalités de Autorité d'approbation vSphere
- Configuration de Autorité d'approbation vSphere
- Gestion de Autorité d'approbation vSphere dans votre environnement vSphere

Concepts et fonctionnalités de Autorité d'approbation vSphere

Autorité d'approbation vSphere sécurise votre SDDC contre les attaques malveillantes en étendant la fiabilité d'une base informatique approuvée à l'ensemble de l'infrastructure informatique de votre organisation. Autorité d'approbation vSphere utilise l'attestation à distance et l'accès contrôlé pour offrir des fonctionnalités de chiffrement avancées.

Autorité d'approbation vSphere est un ensemble de services qui répond à des exigences de sécurité élevées. Avec Autorité d'approbation vSphere , vous pouvez configurer et gérer une infrastructure sécurisée. Vous pouvez vous assurer que les charges de travail sensibles s'exécutent uniquement sur les hôtes ESXi reconnus comme ayant démarré un logiciel authentique.

Protection de votre environnement par l'autorité d'approbation vSphere

Vous configurez des services Autorité d'approbation vSphere pour attester vos hôtes ESXi, qui deviennent ensuite capables d'effectuer des opérations de chiffrement approuvées.

Autorité d'approbation vSphere utilise l'attestation à distance pour les hôtes ESXi afin de prouver l'authenticité de leur logiciel démarré. L'attestation vérifie que les hôtes ESXi exécutent un logiciel VMware authentique ou un logiciel partenaire signé par VMware. L'attestation s'appuie sur des mesures qui sont enracinées dans une puce TPM 2.0 (Trusted Platform Module) installée dans l'hôte ESXi. Dans Autorité d'approbation vSphere , une instance d'ESXi peut accéder aux clés de chiffrement et effectuer des opérations de chiffrement uniquement après avoir été attestée.

Glossaire de Autorité d'approbation vSphere

Autorité d'approbation vSphere introduit des termes et définitions spécifiques importants à comprendre.

Tableau 9-1. Glossaire de Autorité d'approbation vSphere

Terme	Définition
Autorité d'approbation™ vSphere® de VMware	Spécifie un ensemble de services qui active une infrastructure d'approbation. Elle est chargée de s'assurer que les hôtes ESXi exécutent des logiciels approuvés et de libérer des clés de chiffrement uniquement pour les hôtes ESXi approuvés.
Composants de l'autorité d'approbation vSphere	Les composants de l'autorité d'approbation vSphere sont les suivants : ■ Service d'attestation ■ Service de fournisseur de clés
Service d'attestation	Atteste de l'état d'un hôte ESXi distant. Utilise TPM 2.0 pour établir une racine matérielle d'approbation et vérifie les mesures logicielles par rapport à une liste de versions d'ESXi approuvées par l'administrateur.
Service de fournisseur de clés	Encapsule un ou plusieurs serveurs de clés et expose les fournisseurs de clés approuvés qui peuvent être spécifiés lors du chiffrement des machines virtuelles. Actuellement, les serveurs de clés sont limités au protocole KMIP.
Infrastructure approuvée	Une infrastructure approuvée comprend les éléments suivants : ■ Une autorité d'approbation vCenter Server ■ Une instance de vCenter Server de charge de travail ■ Au moins un cluster d'autorité d'approbation vSphere (configuré comme autorité d'approbation vCenter Server) ■ Au moins un cluster approuvé (configuré comme instance de vCenter Server de charge de travail) ■ Des machines virtuelles de charge de travail chiffrées qui s'exécutent dans le cluster approuvé ■ Au moins un serveur de gestion des clés compatible KMIP **Note** Vous devez utiliser des systèmes vCenter Server séparés pour le cluster d'autorité d'approbation et le cluster approuvé.
Cluster d'autorité d'approbation	Se compose d'un cluster vCenter Server d'hôtes ESXi qui exécutent les composants de l'autorité d'approbation vSphere (le service d'attestation et le service de fournisseur de clés).
Hôte d'autorité d'approbation	Hôte ESXi exécutant des composants d'autorité d'approbation vSphere (le service d'attestation et le service de fournisseur de clés).

Tableau 9-1. Glossaire de Autorité d'approbation vSphere (suite)

Terme	Définition
Cluster approuvé	Se compose d'un cluster vCenter Server d'hôtes ESXi approuvés qui sont attestés à distance par le cluster d'autorité d'approbation. Bien qu'il ne soit pas strictement requis, un service de fournisseur de clés configuré augmente fortement la valeur fournie par un cluster approuvé.
Hôte approuvé	Hôte ESXi dont le logiciel a été validé par le service d'attestation du cluster d'autorité d'approbation. Cet hôte exécute des machines virtuelles de charge de travail qui peuvent être chiffrées à l'aide de fournisseurs de clés publiés par le service de fournisseur de clés du cluster d'autorité d'approbation.
Chiffrement vSphere pour des machines virtuelles	Le chiffrement de machine virtuelle vSphere vous permet de créer des machines virtuelles chiffrées et de chiffrer des machines virtuelles existantes. ■ À partir de vSphere 6.5, l'instance de vCenter Server demande des clés à partir d'un serveur de clés externe. Ce dernier génère et stocke les clés, et les transmet à vCenter Server pour distribution. ■ À partir de vSphere 7.0, la connexion approuvée peut être configurée entre vSphere Trust Authority et un serveur de clés. Cette configuration supprime la nécessité pour l'instance de vCenter Server et les hôtes ESXi de charge de travail d'exiger des informations d'identification de serveur de clés directes, et ajoute une couche supplémentaire de sécurité en profondeur.
Fournisseur de clés approuvé	Fournisseur de clés qui encapsule une clé de chiffrement unique sur un serveur de clés. L'accès à la clé de chiffrement nécessite que le service d'attestation confirme que le logiciel ESXi ait été vérifié sur l'hôte approuvé.
Fournisseur de clés standard	Fournisseur de clés qui obtient des clés de chiffrement directement à partir d'un serveur de clés et distribue des clés aux hôtes requis dans un centre de données. Précédemment référencé dans vSphere en tant que cluster KMS.
Serveur de clés	Un serveur de gestion de clés (KMS) KMIP associé à un fournisseur de clés.
vCenter Server de charge de travail	Instance de vCenter Server qui gère un ou plusieurs clusters approuvés et qui est utilisée pour les configurer.

Principes de base de Autorité d'approbation vSphere

Avec Autorité d'approbation vSphere , vous pouvez :

- Fournir des hôtes ESXi avec une racine matérielle d'approbation et des capacités d'attestation à distance
- Limiter la gestion des clés de chiffrement en libérant des clés uniquement pour les hôtes ESXi attestés
- Créer un environnement d'administration plus sécurisé pour la gestion des approbations
- Centraliser la gestion de plusieurs serveurs de clés
- Continuer à effectuer des opérations de chiffrement sur les machines virtuelles, mais avec un niveau de gestion des clés de chiffrement amélioré

Dans vSphere 6.5 et 6.7, le chiffrement des machines virtuelles dépend du système vCenter Server pour obtenir des clés de chiffrement à partir d'un serveur de clés et les transférer à des hôtes ESXi selon les besoins. Le système vCenter Server s'authentifie auprès du serveur de clés à l'aide de certificats de client et de serveur, qui sont stockés dans VECS (VMware Endpoint Certificate Store). Les clés de chiffrement qui sont envoyées à partir du serveur de clés sont transmises via la mémoire du système vCenter Server aux hôtes ESXi requis (avec un chiffrement des données fourni par TLS sur le réseau). En outre, vSphere dépend des contrôles de privilèges dans le système vCenter Server pour valider les autorisations des utilisateurs et appliquer les restrictions d'accès au serveur de clés. Bien que cette architecture soit sécurisée, elle ne prend pas en compte les éventualités d'une instance de vCenter Server compromise, d'un administrateur de vCenter Server malveillant ou d'une erreur de gestion ou de configuration pouvant entraîner une divulgation ou une perte de secrets.

Dans vSphere 7.0, Autorité d'approbation vSphere résout ces problèmes. Vous pouvez créer une base de calcul approuvée, qui se compose d'un ensemble sécurisé et gérable d'hôtes ESXi. Autorité d'approbation vSphere implémente un service d'attestation à distance pour les hôtes ESXi que vous souhaitez approuver. En outre, Autorité d'approbation vSphere améliore la prise en charge de la certification TPM 2.0 (ajoutée à vSphere à partir de la version 6.7) afin de mettre en œuvre des restrictions d'accès sur les clés de chiffrement et donc de mieux protéger les secrets de charge de travail des machines virtuelles. En outre, Autorité d'approbation vSphere autorise uniquement les administrateurs d'autorité d'approbation autorisés à configurer des services Autorité d'approbation vSphere et à configurer des hôtes d'autorité d'approbation. L'administrateur d'autorité d'approbation peut être le même utilisateur que l'utilisateur administrateur vSphere ou un autre utilisateur.

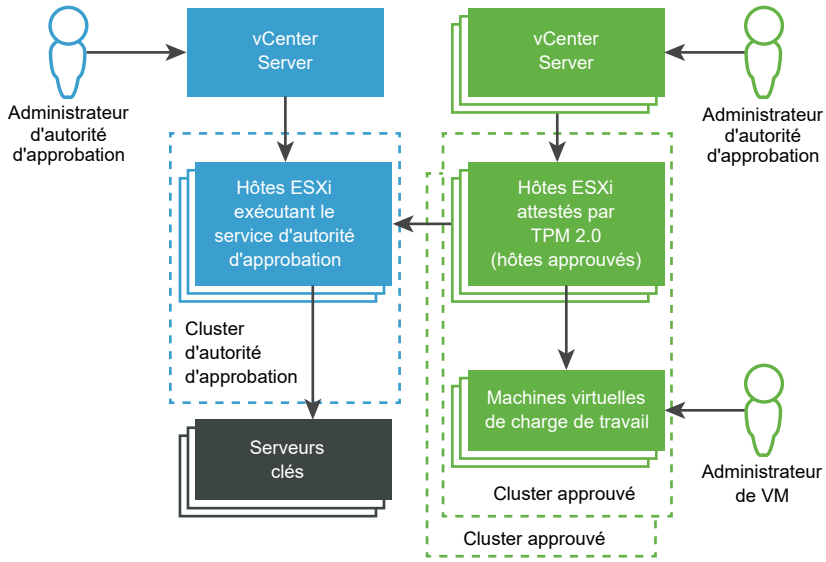
En fin de compte, Autorité d'approbation vSphere vous permet d'exécuter vos charges de travail dans un environnement plus sécurisé en effectuant les actions suivantes :

- Détection des falsifications
- Interdiction des modifications non autorisées
- Prévention des logiciels malveillants et des modifications
- Limitation des charges de travail sensibles pour qu'elles s'exécutent uniquement sur une pile matérielle et logicielle vérifiée et sécurisée

Architecture de Autorité d'approbation vSphere

La figure suivante illustre une vue simplifiée de l'architecture Autorité d'approbation vSphere .

Figure 9-1. Architecture de Autorité d'approbation vSphere



Dans cette figure :

1 Systèmes vCenter Server

Des systèmes vCenter Server distincts gèrent le cluster d'autorité d'approbation et les clusters approuvés.

2 Cluster d'autorité d'approbation

Ce cluster comprend les hôtes ESXi exécutant les composants de Autorité d'approbation vSphere .

3 Serveurs de clés

Les serveurs de clés stockent les clés de chiffrement qui sont utilisées par le service de fournisseur de clés lorsque des opérations de chiffrement sont effectuées. Les serveurs de clés sont externes à Autorité d'approbation vSphere .

4 Clusters approuvés

Ces clusters se composent des hôtes approuvés ESXi qui ont été attestés à distance par un TPM, et qui exécutent des charges de travail chiffrées.

5 Administrateur d'autorité d'approbation

Cet administrateur est membre du groupe TrustedAdmins de vCenter Server et configure l'infrastructure approuvée.

Autorité d'approbation vSphere offre une flexibilité dans la manière dont vous désignez les administrateurs d'autorité d'approbation. Les administrateurs d'autorité d'approbation de la figure peuvent être des utilisateurs distincts. Il est également possible que les administrateurs d'autorité d'approbation soient le même utilisateur, en utilisant les informations d'identification qui sont liées entre les systèmes vCenter Server. Dans ce cas, il s'agit du même utilisateur et du même groupe TrustedAdmins.

6 Administrateur de machine virtuelle

Cet administrateur a obtenu des privilèges pour gérer les machines virtuelles de charge de travail chiffrées sur les hôtes approuvés.

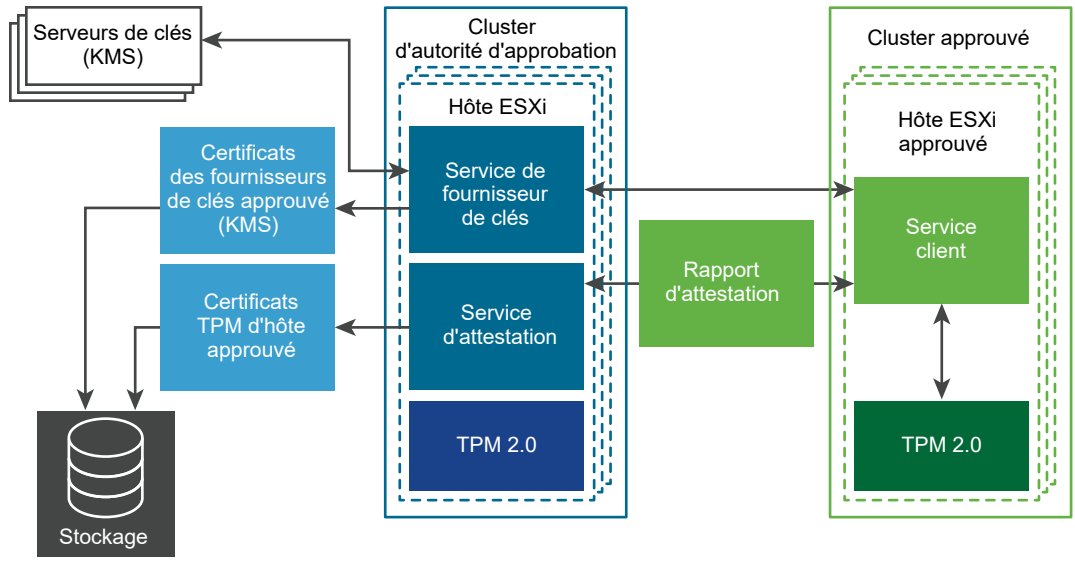
Présentation de l'infrastructure approuvée

Les services Autorité d'approbation vSphere , au moins un serveur de clés externe compatible KMIP, les systèmes vCenter Server et vos hôtes ESXi contribuent à l'infrastructure approuvée.

À propos de l'infrastructure approuvée

Une infrastructure approuvée se compose d'au moins un cluster vSphere Trust Authority, d'au moins un cluster approuvé et d'au moins un serveur de clés compatible KMIP externe. Chaque cluster contient des hôtes ESXi qui exécutent des services Autorité d'approbation vSphere spécifiques, comme indiqué dans la figure suivante.

Figure 9-2. Services Autorité d'approbation vSphere



La configuration du cluster d'autorité d'approbation active deux services :

- Service d'attestation
- Service de fournisseur de clés

Lorsque vous configurez Autorité d'approbation vSphere , les hôtes ESXi dans le cluster approuvé communiquent avec le service d'attestation. Le service de fournisseur de clés interagit entre les hôtes approuvés et un ou plusieurs fournisseurs de clés approuvés.

Note Actuellement, les hôtes ESXi du cluster d'autorité d'approbation ne requièrent pas de TPM. Cependant, il convient d'envisager d'installer de nouveaux hôtes ESXi disposant de TPM.

À propos du service d'attestation de Autorité d'approbation vSphere

Le service d'attestation génère un document signé contenant des assertions décrivant l'état binaire et de configuration des hôtes ESXi distants dans le cluster approuvé. Le service d'attestation atteste de l'état des hôtes ESXi en utilisant une puce TPM (Trusted Platform Module) 2.0 comme base pour la mesure et la génération de rapports de logiciel. Le TPM sur l'hôte ESXi distant mesure la pile logicielle et envoie les données de configuration au service d'attestation. Le service d'attestation vérifie que la signature de mesure du logiciel peut être attribuée à une clé d'approbation TPM (EK) précédemment approuvée. Le service d'attestation garantit également que la mesure du logiciel correspond à l'une des images ESXi d'un ensemble précédemment validé. Le service d'attestation signe un jeton Web JSON (JWT) qu'il envoie à l'hôte ESXi, en fournissant les assertions sur l'identité, la validité et la configuration de l'hôte ESXi.

À propos du service de fournisseur de clés de Autorité d'approbation vSphere

Le service de fournisseur de clés libère vCenter Server et les hôtes ESXi de la nécessité d'exiger des informations d'identification de serveur de clés directes. Dans Autorité d'approbation vSphere , pour qu'un hôte ESXi ait accès à une clé de chiffrement, il doit s'authentifier auprès du service de fournisseur de clés.

Pour que le service de fournisseur de clés se connecte à un serveur de clés, l'administrateur de l'autorité d'approbation doit effectuer une configuration d'approbation. Pour la plupart des serveurs compatibles KMIP, une configuration d'approbation implique la configuration de certificats de client et de serveur.

Pour s'assurer que les clés sont uniquement publiées sur des hôtes ESXi approuvés, le service de fournisseur de clés agit comme un contrôleur d'accès aux serveurs de clés. Le service de fournisseur de clés masque les spécificités du serveur de clés du reste de la pile logicielle du centre de données en utilisant le concept de fournisseur de clés approuvé. Chaque fournisseur de clés approuvé dispose d'une clé de chiffrement principale configurée unique (précédemment appelée clé de chiffrement principale) et fait référence à un ou plusieurs serveurs de clés. Le service de fournisseur de clés peut avoir plusieurs fournisseurs de clés approuvés configurés. Par exemple, vous souhaiterez éventuellement disposer d'un fournisseur de clés approuvé distinct pour chaque service d'une organisation. Chaque fournisseur de clés approuvé utilise une clé principale différente, mais peut faire référence au même serveur de clés de sauvegarde.

Une fois que vous avez créé un fournisseur de clés approuvé, le service de fournisseur de clés peut accepter des demandes d'hôtes ESXi approuvés pour exécuter des opérations de chiffrement sur ce fournisseur de clés approuvé.

Lorsqu'un hôte ESXi approuvé demande des opérations à un fournisseur de clés approuvé, le service de fournisseur de clés s'assure que l'hôte ESXi qui tente d'obtenir la clé de chiffrement est attesté. Après avoir passé tous les contrôles, l'hôte ESXi approuvé reçoit des clés de chiffrement du service de fournisseur de clés.

Port utilisés par Autorité d'approbation vSphere

Les services Autorité d'approbation vSphere écoutent les connexions derrière le proxy inverse de l'hôte ESXi. Toutes les communications s'effectuent sur HTTPS sur le port 443.

À propos de Autorité d'approbation vSphere et des hôtes approuvés

Les hôtes ESXi approuvés sont configurés pour utiliser des fournisseurs de clés approuvés afin d'effectuer des opérations de chiffrement. Les hôtes ESXi approuvés effectuent des opérations de clés en communiquant avec le service de fournisseur de clés et le service d'attestation. Pour l'authentification et l'autorisation, les hôtes ESXi approuvés utilisent un jeton obtenu du service d'attestation. Pour obtenir un jeton valide, l'hôte ESXi approuvé doit attester correctement le service d'attestation. Le jeton contient des déclarations utilisées pour décider si l'hôte ESXi approuvé est autorisé à accéder à un fournisseur de clés approuvé.

À propos des serveurs de clés

Autorité d'approbation vSphere nécessite l'utilisation d'au moins un serveur de clés. Dans les versions précédentes de vSphere, un serveur de clés s'appelait un serveur de gestion des clés ou KMS. Actuellement, la solution de chiffrement des machines virtuelles vSphere prend en charge les serveurs de clés conformes à KMIP 1.1.

À propos de la configuration et des informations d'état de Autorité d'approbation vSphere

vCenter Server est principalement un service de relais pour les informations de configuration et d'état de Autorité d'approbation vSphere . La plupart des informations de configuration et d'état de Autorité d'approbation vSphere sont stockées sur les hôtes ESXi dans la base de données ConfigStore. Certaines informations d'état sont également stockées dans la base de données vCenter Server.

Note Étant donné que la plupart des informations de configuration de Autorité d'approbation vSphere sont stockées sur les hôtes ESXi, le mécanisme de sauvegarde basé sur fichier de vCenter Server ne sauvegarde pas ces informations. Pour vous assurer que les informations de configuration de votre déploiement de Autorité d'approbation vSphere sont enregistrées, reportez-vous à Sauvegarde de la configuration de Autorité d'approbation vSphere .

À propos de l'intégration de vCenter Server

Vous configurez des instances de vCenter Server distinctes pour gérer le cluster d'autorité d'approbation et le cluster approuvé. Reportez-vous à la section Configuration de Autorité d'approbation vSphere .

Sur un cluster approuvé, vCenter Server gère les appels d'API de l'autorité d'approbation et les transmet aux hôtes ESXi. vCenter Server réplique les appels d'API sur tous les hôtes ESXi du cluster approuvé.

Après la configuration initiale de Autorité d'approbation vSphere , vous pouvez ajouter ou supprimer des hôtes ESXi d'un cluster d'autorité d'approbation ou d'un cluster approuvé. Reportez-vous à la section Ajout et suppression d'hôtes Autorité d'approbation vSphere .

Flux de processus de l'autorité d'approbation vSphere

La compréhension des flux de processus de Autorité d'approbation vSphere est essentielle pour apprendre à configurer et à administrer votre infrastructure approuvée.

Activation Autorité d'approbation vSphere

Autorité d'approbation vSphere n'est pas activée par défaut. Vous devez configurer manuellement Autorité d'approbation vSphere dans votre environnement. Reportez-vous à la section Configuration de Autorité d'approbation vSphere .

Lorsque vous activez Autorité d'approbation vSphere , vous devez spécifier les versions du logiciel ESXi que le service d'attestation accepte, ainsi que les modules de plate-forme sécurisée (TPM) dignes de confiance.

TPM et attestation

Ce guide utilise les définitions suivantes lors de la présentation de TPM et de l'attestation.

Tableau 9-2. Glossaire de TPM et de l'attestation

Terme	Définition
Clé d'approbation (EK)	Un TPM est fabriqué avec une paire de clés publique/privée RSA intégrée au matériel, appelée clé d'approbation (EK). La clé EK est propre à un TPM particulier.
Clé publique EK	Partie publique de la paire de clés EK.
Clé privée EK	Partie privée de la paire de clés EK.
Certificat EK	Clé publique EK encapsulée avec une signature. Le certificat EK est créé par le fabricant TPM qui utilise sa clé privée d'autorité de certification pour signer la clé publique EK. Tous les TPM ne contiennent pas un certificat EK. Dans ce cas, la clé publique EK n'est pas signée.
Attestation TPM	Capacité du service d'attestation à vérifier le logiciel exécuté sur un hôte distant. L'attestation TPM est effectuée par des mesures de chiffrement effectuées par le TPM pendant le démarrage de l'hôte distant et est relayée vers le service d'attestation sur demande. Le service d'attestation établit une relation de confiance dans le TPM via la clé publique EK ou le certificat EK.

Configuration de l'approbation TPM sur les hôtes approuvés

Un hôte approuvé ESXi doit contenir un TPM. Un TPM est fabriqué avec une paire de clés publique/privée intégrée au matériel, appelée clé d'approbation (EK). Bien que TPM 2.0 autorise de nombreuses paires de clé/certificat, le plus courant est une paire de clés RSA-2048. Lorsqu'une clé publique EK de TPM est signée par une autorité de certification, le résultat est le certificat EK. Le fabricant de TPM pré-génère normalement au moins un EK, signe la clé publique auprès d'une autorité de certification et incorpore le certificat signé dans la mémoire non volatile du TPM.

Vous pouvez configurer le service d'attestation pour approuver les TPM comme suit :

- Approuvez tous les certificats d'autorité de certification avec lesquels le fabricant a signé le TPM (la clé publique EK). Le paramètre par défaut du service d'attestation consiste à approuver les certificats d'autorité de certification. De cette manière, le même certificat d'autorité de certification couvre de nombreux hôtes ESXi, ce qui réduit votre charge administrative.
- Approuvez le certificat d'autorité de certification TPM et la clé publique EK de l'hôte ESXi. Ce dernier peut être le certificat EK ou la clé publique EK. Bien que cette approche offre davantage de sécurité, elle nécessite de configurer des informations sur chaque hôte approuvé.
- Certains TPM ne contiennent pas de certificat EK. Dans ce cas, vous devez approuver la clé publique EK.

Le fait d'approuver tous les certificats d'autorité de certification TPM est pratique d'un point de vue opérationnel. Vous configurez de nouveaux certificats uniquement lorsque vous ajoutez une nouvelle classe de matériel à votre centre de données. En approuvant des certificats EK de manière individuelle, vous pouvez limiter l'accès à des hôtes ESXi spécifiques.

Vous pouvez également décider de ne pas approuver les certificats d'autorité de certification TPM. Dans une situation peu courante, vous pouvez utiliser cette configuration lorsqu'un EK n'est pas signé par une autorité de certification. Cette fonctionnalité n'est pas entièrement implémentée pour le moment.

Note Certains TPM n'incluent pas de certificats EK. Si vous souhaitez approuver des hôtes ESXi de manière individuelle, le TPM doit inclure un certificat EK.

Attestation de plusieurs TPM

Pour commencer le processus d'attestation, l'hôte approuvé ESXi dans le cluster approuvé envoie la clé publique EK et le certificat EK préconfigurés au service d'attestation sur le cluster d'autorité d'approbation. Lorsque le service d'attestation reçoit la demande, il recherche l'EK dans sa configuration. Il peut s'agir de la clé publique EK, du certificat EK ou des deux, selon la configuration. Si aucun de ces cas n'est valide, le service d'attestation rejette la demande d'attestation.

L'EK n'est pas utilisé directement pour la signature, c'est pourquoi une clé d'attestation (AK ou AIK) est négociée. Le protocole de négociation garantit qu'un AK récemment créé est lié à l'EK précédemment vérifié, empêchant les potentiels intercepteurs ou usurpateurs. Après la négociation d'un AK, celui-ci est réutilisé lors de demandes d'attestation ultérieures plutôt que de devoir en générer un nouveau à chaque fois.

L'hôte approuvé ESXi lit les valeurs de l'opération quote et de PCR à partir du TPM. L'opération quote est signée par l'AK. L'hôte approuvé ESXi lit également le journal des événements TCG, qui inclut tous les événements ayant généré l'état PCR actuel. Ces informations de TPM sont envoyées au service d'attestation pour validation. Le service d'attestation vérifie les valeurs de PCR à l'aide du journal des événements.

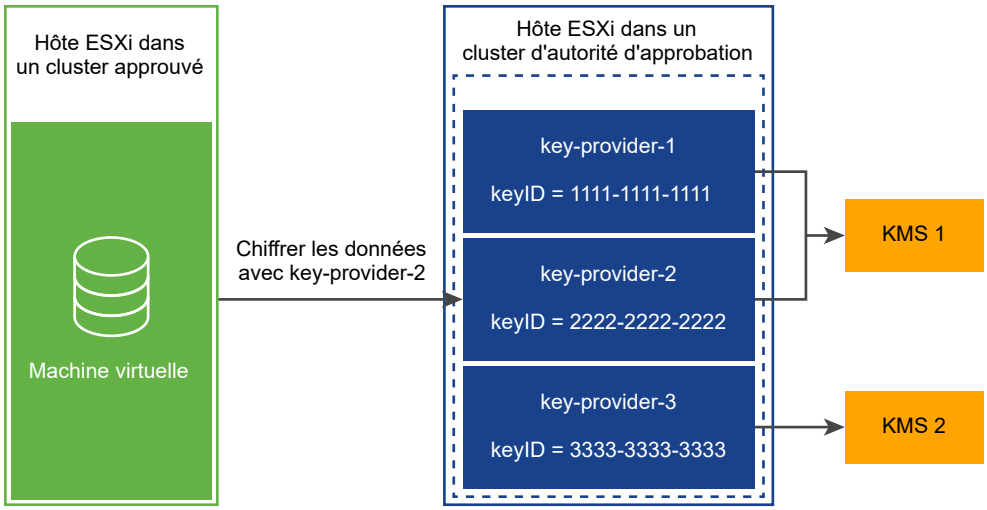
Fournisseurs de clés et serveurs de clés

Le service de fournisseur de clés utilise le concept d'un fournisseur de clés approuvé pour masquer les spécificités du serveur de clés par rapport au reste du logiciel de centre de données. Chaque fournisseur de clés approuvé dispose d'une clé de chiffrement principale configurée unique (précédemment appelée clé de chiffrement principale) et fait référence à un ou plusieurs serveurs de clés. La clé de chiffrement principale est présente dans les serveurs de clés. Dans le cadre de la configuration de Autorité d'approbation vSphere , vous devez provisionner la clé principale en tant qu'activité distincte et l'activer. Le service de fournisseur de clés peut avoir plusieurs fournisseurs de clés approuvés configurés. Chaque fournisseur de clés approuvé utilise une clé principale différente, mais peut référencer le même serveur de clés de sauvegarde.

Lorsqu'un nouveau fournisseur de clés approuvé est ajouté, l'administrateur de l'autorité d'approbation doit spécifier le serveur de clés et un identifiant de clé existant sur ce serveur de clés.

La figure suivante illustre la relation entre le service de fournisseur de clés et les serveurs de clés.

Figure 9-3. Fournisseur de clés et serveur de clés



Après avoir configuré un fournisseur de clés approuvé pour un cluster approuvé, le service de fournisseur de clés peut accepter des demandes pour exécuter des opérations de chiffrement sur ce fournisseur de clés approuvé. Par exemple, dans cette figure, trois fournisseurs de clés approuvés sont configurés, deux pour KMS-1 et un pour KMS-2. L'hôte approuvé demande une opération de chiffrement par rapport à key-provider-2. L'hôte approuvé demande une clé de chiffrement à générer et à renvoyer, puis utilise cette clé de chiffrement pour effectuer des opérations de chiffrement.

Le service de fournisseur de clés utilise la clé principale référencée par key-provider-2 pour chiffrer les données en texte brut spécifiées et renvoyer le texte chiffré correspondant. Par la suite, l'hôte approuvé peut fournir le même texte chiffré à une opération de déchiffrement et récupérer le texte brut d'origine.

Authentification et autorisation

Les opérations administratives de Autorité d'approbation vSphere nécessitent un utilisateur membre du groupe TrustedAdmins. Avoir uniquement des privilèges d'administrateur d'autorité d'approbation n'est pas suffisant pour effectuer toutes les opérations administratives impliquant les hôtes ESXi. Pour plus d'informations, consultez Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere.

Ajout d'un hôte approuvé à un cluster approuvé

Les étapes de l'ajout initial d'hôtes ESXi au cluster approuvé sont décrites dans Configuration de Autorité d'approbation vSphere .

Par la suite, si vous souhaitez ajouter des hôtes ESXi au cluster approuvé, le workflow est différent. Reportez-vous à la section Ajout et suppression d'hôtes Autorité d'approbation vSphere .

Lors de l'ajout initial d'hôtes ESXi au cluster approuvé, vous devez réunir les informations suivantes :

- Certificat TPM pour chaque type de matériel dans le cluster
- Image ESXi pour chaque version d'ESXi dans le cluster
- Informations de principal de vCenter Server

Si vous ajoutez ultérieurement des hôtes ESXi à un cluster approuvé, vous devrez peut-être collecter des informations supplémentaires. En effet, si les nouveaux hôtes ESXi diffèrent dans la version matérielle ou ESXi des hôtes d'origine, vous devez collecter les nouvelles informations sur l'hôte ESXi et les importer dans le cluster d'autorité d'approbation. Vous ne devez collecter les informations de principal de vCenter Server qu'une seule fois par système vCenter Server.

Topologie de Autorité d'approbation vSphere

Autorité d'approbation vSphere nécessite des systèmes vCenter Server séparés pour le cluster d'autorité d'approbation et le cluster approuvé.

Le cluster d'autorité d'approbation est configuré et géré sur une instance de vCenter Server isolée et indépendante. L'instance de vCenter Server du cluster d'autorité d'approbation ne peut pas être également l'instance de vCenter Server du cluster approuvé. Le cluster approuvé doit disposer de ses propres instances de vCenter Server séparées. Une instance unique de vCenter Server peut gérer plusieurs clusters approuvés. Plusieurs systèmes vCenter Server pour les clusters approuvés peuvent participer en mode Enhanced Linked Mode. L'instance de vCenter Server du cluster d'autorité d'approbation ne peut pas participer en mode Enhanced Linked Mode avec d'autres systèmes vCenter Server de clusters d'autorité d'approbation ou d'autres systèmes vCenter Server de cluster approuvés.

L'administrateur d'autorité d'approbation gère le cluster d'autorité d'approbation et ses instances de vCenter Server associées indépendamment des autres instances de vCenter Server, car cette approche fournit la meilleure isolation de sécurité.

L'administrateur d'autorité d'approbation documente ou publie les noms d'hôte et les certificats SSL que les administrateurs de cluster approuvés utilisent pour configurer leurs clusters. L'administrateur d'autorité d'approbation provisionne également des fournisseurs de clés approuvés pour l'organisation et ses services ou même des administrateurs individuels.

Vous ne pouvez pas déployer des services Autorité d'approbation vSphere directement sur le cluster approuvé géré par l'instance de vCenter Server de charge de travail, car l'administrateur de charge de travail dispose d'un accès de privilège élevé aux hôtes ESXi. Ce type de déploiement ne parvient pas à la séparation des rôles requise pour répondre aux objectifs de sécurité de Autorité d'approbation vSphere .

Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere

Vous devez tenir compte de la configuration matérielle et logicielle requise pour configurer Autorité d'approbation vSphere . Vous devez définir des privilèges de chiffrement et des rôles pour utiliser le chiffrement. L'utilisateur qui exécute les tâches Autorité d'approbation vSphere doit disposer des privilèges appropriés.

Conditions requises pour Autorité d'approbation vSphere

Pour utiliser Autorité d'approbation vSphere , votre environnement vSphere doit répondre aux exigences suivantes :

- Configuration matérielle requise pour l'hôte approuvé ESXi :
  - TPM 2.0
  - Le démarrage sécurisé doit être activé
  - Micrologiciel EFI
- Configuration requise pour le composant :
  - vCenter Server 7.0 ou une version ultérieure

- Un système vCenter Server dédié pour le cluster d'autorité d'approbation vSphere et les hôtes ESXi
- Un système vCenter Server distinct pour le cluster approuvé et les hôtes ESXi approuvés
- Un serveur de clés (appelé serveur de gestion des clés ou KMS dans les versions antérieures de vSphere)

- Configuration requise pour la machine virtuelle :
  - Micrologiciel EFI
  - Démarrage sécurisé activé

Note Avant de pouvoir commencer à configurer Autorité d'approbation vSphere , assurez-vous d'avoir configuré vos systèmes vCenter Server pour le cluster autorité d'approbation et le cluster approuvé et ajouté des hôtes ESXi à chaque cluster.

Privilèges de chiffrement

Autorité d'approbation vSphere n'introduit aucun nouveau privilège de chiffrement. Les mêmes privilèges de chiffrement décrits dans Privilèges de chiffrement et rôles s'appliquent à Autorité d'approbation vSphere .

Mode de chiffrement de l'hôte

Autorité d'approbation vSphere n'introduit aucune nouvelle configuration requise pour l'activation du mode de chiffrement de l'hôte sur les hôtes approuvés ESXi. Pour plus d'informations sur le mode de chiffrement de l'hôte, consultez Conditions préalables et privilèges requis pour les tâches de chiffrement.

À propos des rôles de Autorité d'approbation vSphere et du groupe TrustedAdmins

Les opérations de Autorité d'approbation vSphere nécessitent un utilisateur membre du groupe TrustedAdmins. Cet utilisateur est appelé administrateur de l'autorité d'approbation. Les administrateurs vSphere doivent s'ajouter eux-mêmes au groupe TrustedAdmins ou ajouter d'autres utilisateurs au groupe pour obtenir le rôle d'administrateur d'infrastructure approuvée. Le rôle d'administrateur d'infrastructure approuvée est nécessaire pour l'autorisation de vCenter Server. Le groupe TrustedAdmins est nécessaire pour l'authentification sur les hôtes ESXi faisant partie de l'infrastructure approuvée. Les utilisateurs ayant le privilège **Opérations de chiffrement.Enregistrer l'hôte** sur les hôtes ESXi peuvent gérer le cluster approuvé. Les

autorisations vCenter Server ne sont pas propagées aux hôtes d'autorité d'approbation, mais uniquement aux hôtes approuvés. Seuls les membres du groupe TrustedAdmins disposent de privilèges sur les hôtes d'autorité d'approbation. L'appartenance au groupe est vérifiée sur l'hôte ESXi lui-même.

Note Le rôle d'administrateur d'infrastructure approuvée est attribué aux administrateurs vSphere et aux membres du groupe Administrateurs, mais ce rôle n'autorise pas un utilisateur à effectuer des opérations de Autorité d'approbation vSphere . L'appartenance au groupe TrustedAdmins est également requise.

Une fois Autorité d'approbation vSphere activé, les administrateurs d'autorité d'approbation peuvent attribuer des fournisseurs de clés approuvés à des hôtes approuvés. Ces hôtes approuvés peuvent ensuite utiliser les fournisseurs de clés approuvés pour effectuer des tâches de chiffrement.

En plus du rôle d'administrateur d'infrastructure approuvée, Autorité d'approbation vSphere fournit le rôle Administrateur sans droits sur l'infrastructure approuvée, qui contient tous les privilèges dans vCenter Server à l'exception de ceux qui appellent les API de Autorité d'approbation vSphere .

Les groupes, les rôles et les utilisateurs de Autorité d'approbation vSphere fonctionnent de la manière suivante :

- Lors du premier démarrage, vSphere accorde au groupe TrustedAdmins le rôle Administrateur d'infrastructure approuvée, qui dispose des autorisations globales.
- Le rôle Administrateur d'infrastructure approuvée est un rôle système qui dispose des privilèges requis pour appeler les API de Autorité d'approbation vSphere (`TrustedAdmin.*`) et les privilèges système **System.Read**, **System.View** et **System.Anonymous** pour afficher les objets d'inventaire.
- Le rôle d'administrateur sans droits sur l'infrastructure approuvée est un rôle système qui contient tous les privilèges dans vCenter Server à l'exception de ceux nécessaires pour appeler les API de Autorité d'approbation vSphere . L'ajout de nouveaux privilèges à vCenter Server les ajoute également au rôle Administrateur sans droits sur l'infrastructure approuvée. (Le rôle Administrateur sans droits sur l'infrastructure approuvée est similaire au rôle Administrateur sans droits de chiffrement.)
- Les privilèges de Autorité d'approbation vSphere (les API `TrustedAdmin.*`) ne sont pas inclus dans le rôle Administrateur sans droits de chiffrement, ce qui empêche les utilisateurs disposant de ce rôle de configurer une infrastructure approuvée ou d'effectuer des opérations de chiffrement.

Les cas d'utilisation de ces utilisateurs, groupes et rôles sont présentés dans le tableau suivant.

Tableau 9-3. Utilisateurs, groupes et rôles de l'autorité d'approbation vSphere

Utilisateur, groupe ou rôle	**Peut appeler l'API de Autorité d'approbation vSphere vCenter Server (inclut les appels à l'API de Autorité d'approbation vSphere ESXi)**	**Peut appeler l'API de Autorité d'approbation vSphere vCenter Server (n'inclut pas les appels à l'API de Autorité d'approbation vSphere ESXi)**	**Peut effectuer des opérations d'hôte dans un cluster non lié à Autorité d'approbation vSphere**	**Commentaire**
Utilisateur dans le groupe Administrators@*system.domain* et le groupe TrustedAdmins@*system.domain*	Oui	Oui	Oui	S/O
Utilisateur dans le groupe TrustedAdmins@*system.domain* uniquement	Oui	Oui	Non	Ce type d'utilisateur ne peut pas effectuer d'opérations de gestion de cluster standard.
Utilisateur dans le groupe Administrators@*system.domain* uniquement	Oui	Non	Oui	S/O
Utilisateur disposant du rôle d'administrateur d'infrastructure approuvée, mais ne faisant pas partie du groupe TrustedAdmins@*system.domain*	Oui	Non	Non	L'hôte ESXi vérifie l'appartenance au groupe de l'utilisateur pour accorder les autorisations.
Utilisateur disposant du rôle d'administrateur sans droits sur l'infrastructure approuvée	Non	Non	Oui	Ce type d'utilisateur est semblable à un administrateur qui ne peut pas effectuer d'opérations de Autorité d'approbation vSphere .

Meilleures pratiques de Autorité d'approbation vSphere , mises en garde et interopérabilité

L'architecture de Autorité d'approbation vSphere donne lieu à des recommandations supplémentaires. Tenez compte des limitations d'interopérabilité pendant la phase de planification de la stratégie de Autorité d'approbation vSphere .

Interopérabilité de l'infrastructure approuvée

Pour les versions d'ESXi, le service d'attestation est compatible en amont et en aval. Par exemple, vous pouvez avoir un cluster d'hôtes ESXi exécutant ESXi 7.0 dans le cluster d'autorité d'approbation vSphere, et mettre à niveau ou appliquer des correctifs aux hôtes ESXi du cluster approuvé vers une version plus récente d'ESXi. De même, vous pouvez mettre à niveau ou corriger les hôtes ESXi dans le cluster d'autorité d'approbation tout en conservant les hôtes ESXi dans le cluster approuvé à la version actuelle.

Vous ne pouvez pas avoir de cluster fonctionnant à la fois comme cluster d'autorité d'approbation et cluster approuvé. Cette configuration n'est pas prise en charge.

Limitation de la configuration du cluster approuvé

Vous ne pouvez configurer qu'un seul cluster d'autorité d'approbation par cluster approuvé. Autrement dit, un cluster approuvé ne peut pas être configuré pour référencer plusieurs clusters d'autorité d'approbation.

Autre

Autorité d'approbation vSphere prend en charge les éléments suivants :

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM, en comprenant les points suivants :
  - SRM avec réplication basée sur la baie est pris en charge, si la même configuration de services Autorité d'approbation vSphere est disponible du côté de la récupération.
  - SPPG
- VADP
  - La prise en charge est la même que pour le chiffrement standard. Les modes d'ajout à chaud et NFC sont pris en charge, mais pas le mode SAN. Les sauvegardes sont déchiffrées. Les partenaires VADP ont la possibilité de récupérer la machine virtuelle sauvegardée avec la même clé de chiffrement que la machine virtuelle d'origine.
- vSAN
  - Le chiffrement de la machine virtuelle est entièrement pris en charge en plus de vSAN.

- OVF
  - Les machines virtuelles chiffrées ne peuvent pas être exportées vers OVF. Cependant, les machines virtuelles peuvent être chiffrées lors de leur importation à partir d'un fichier OVF.
- vVol

Actuellement, Autorité d'approbation vSphere ne prend pas en charge les éléments suivants :

- Chiffrement vSAN
- Chiffrement de disque de première classe (FCD)
- vSphere Replication
- Profils d'hôte vSphere

Cycle de vie de l'autorité d'approbation vSphere

Les services Autorité d'approbation vSphere sont conditionnés et installés dans le cadre de l'image ESXi de base.

Démarrage et arrêt des services

Dans vSphere Client, vous pouvez démarrer, arrêter et redémarrer des services Autorité d'approbation vSphere qui s'exécutent sur un hôte ESXi. Vous pouvez redémarrer des services lors d'une modification de configuration ou si vous suspectez la présence de problèmes fonctionnels ou de performances. Pour redémarrer le service sur un hôte ESXi approuvé, vous devez vous connecter à l'hôte lui-même pour redémarrer le service. Reportez-vous à la section Démarrer, arrêter et redémarrer les services Autorité d'approbation vSphere .

Mise à niveau et application de correctifs

Chaque fois que vous mettez à niveau ou corrigez un hôte ESXi approuvé, vous devez mettre à jour le cluster Autorité d'approbation vSphere avec les nouvelles informations de version d'ESXi. Pour cela, vous pouvez mettre à niveau ou corriger un hôte ESXi de test, exporter les informations d'image de base d'ESXi, importer le fichier image dans le cluster d'autorité d'approbation, puis mettre à niveau ou corriger les hôtes ESXi approuvés.

Meilleures pratiques de mise à niveau

La meilleure pratique pour la mise à niveau d'une infrastructure Autorité d'approbation vSphere consiste à d'abord mettre à niveau l'instance de vCenter Server de l'autorité d'approbation et les hôtes de l'autorité d'approbation. De cette manière, vous tirer le maximum des toutes dernières fonctionnalités de Autorité d'approbation vSphere . Cependant, vous pouvez effectuer des mises à niveau autonomes distinctes des hôtes vCenter Server et ESXi pour des raisons commerciales spécifiques.

En règle générale, suivez cet ordre pour mettre à niveau de votre infrastructure Autorité d'approbation vSphere :

1 Mettez à niveau le cluster d'autorité d'approbation vCenter Server.

2 Mettez à niveau les hôtes d'autorité d'approbation.

3 Mettez à niveau le cluster approuvé vCenter Server.

4 Mettez à niveau les hôtes approuvés.

Pour garantir un processus fluide, mettez à niveau vos hôtes d'autorité d'approbation et vos hôtes approuvés progressivement, un par un.

Dépannage des problèmes de mise à niveau

Si vous la mise à niveau d'un hôte d'autorité d'approbation échoue, procédez comme suit.

1 Supprimez l'hôte d'autorité d'approbation du cluster approuvé.

2 Restaurez la version précédente de ESXi.

3 Ajoutez à nouveau l'hôte d'autorité d'approbation au cluster comme décrit dans l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/77234.

4 Vérifiez que la configuration de l'hôte d'autorité d'approbation est cohérente avec celle des autres hôtes d'autorité d'approbation dans le cluster d'autorité d'approbation. Reportez-vous à la section Vérifier la santé du cluster approuvé.

Lorsque vous effectuez une mise à niveau vers une nouvelle version d'ESXi sur un hôte approuvé, l'attestation échoue jusqu'à ce que vous ayez mis à jour le cluster d'autorité d'approbation avec les nouvelles informations de l'image de base de ESXi. Ce comportement est normal. Vous ne pourrez plus chiffrer des machines virtuelles ni utiliser les machines virtuelles existantes qui avaient été chiffrées avant la mise à niveau tant que vous n'aurez pas résolu le problème. Les messages d'erreur d'attestation figurent dans le volet **Tâches récentes** de vSphere Client et dans les fichiers `attestd.log`, `kmxa.log`, `vpxd.log`.

Pour corriger le problème, procédez comme suit.

1 Exécutez l'applet de commande `Export-VMHostImageDb` pour ré-exporter les images de base d'ESXi. Reportez-vous à l'étape 5 dans Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

2 Exécutez l'applet de commande `New-TrustAuthorityVMHostBaseImage` pour réimporter la nouvelle image de base vers l'instance de vCenter Server du cluster d'autorité d'approbation. Reportez-vous à l'étape 8 dans Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.

3 Si vous n'avez plus besoin d'attester les anciennes versions de ESXi (tous les hôtes approuvés ont été mis à niveau), exécutez l'applet de commande `Remove-TrustAuthorityVMHostBaseImage` pour supprimer les versions. Par exemple :

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

Sauvegarde de la configuration de Autorité d'approbation vSphere

Étant donné que la plupart des informations de configuration de Autorité d'approbation vSphere sont stockées sur les hôtes ESXi, la sauvegarde de vCenter Server ne sauvegarde pas ces informations de Autorité d'approbation vSphere . Reportez-vous à la section Sauvegarde de la configuration de Autorité d'approbation vSphere .

Configuration de Autorité d'approbation vSphere

Autorité d'approbation vSphere n'est pas activée par défaut. Vous devez configurer votre environnement pour Autorité d'approbation vSphere avant de pouvoir commencer à l'utiliser.

Activez les services Autorité d'approbation vSphere sur un cluster vCenter Server dédié, appelé le cluster Autorité d'approbation vSphere . Le cluster d'autorité d'approbation agit comme une plateforme de gestion centralisée et sécurisée. Ensuite, activez un cluster vCenter Server de charge de travail comme cluster approuvé. Le cluster approuvé contient les hôtes approuvés par ESXi.

Le cluster d'autorité d'approbation certifie les hôtes ESXi dans le cluster approuvé à distance. Le cluster d'autorité d'approbation publie des clés de chiffrement uniquement pour les hôtes ESXi attestés dans le cluster approuvé pour chiffrer des machines virtuelles et des disques virtuels à l'aide de fournisseurs de clés approuvés.

Avant de commencer la configuration de Autorité d'approbation vSphere , pour plus d'informations sur la configuration requise des systèmes vCenter Server et des hôtes ESXi, consultez Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere.

Pour gérer les différents aspects de Autorité d'approbation vSphere , l'une des manières suivantes vous est proposée.

- Configurez les services et les connexions approuvées Autorité d'approbation vSphere à l'aide des applets de commande PowerCLI ou des vSphere API. Consultez la *Référence des applets de commande VMware PowerCLI* et le *Guide de programmation des vSphere Automation SDK*.
- Gérez la configuration des fournisseurs de clés approuvées à l'aide des applets de commande PowerCLI ou de vSphere Client.
- Exécutez des workflows de chiffrement, comme dans les versions précédentes de vSphere, à l'aide de vSphere Client et d'API.

En général, vous utilisez VMware PowerCLI pour configurer et gérer Autorité d'approbation vSphere , bien que certaines fonctionnalités soient disponibles dans vSphere Client.

Lorsque vous configurez Autorité d'approbation vSphere , vous devez effectuer des tâches de configuration sur le cluster d'autorité d'approbation et le cluster approuvé. Certaines de ces tâches doivent être réalisées dans un ordre spécifique. Utilisez la séquence de tâches suivante pour configurer Autorité d'approbation vSphere .

1 Sur un système ayant accès à votre environnement Autorité d'approbation vSphere :
   - Installez PowerCLI 12.1.0 ou version ultérieure. Consultez le *Guide de l'utilisateur de PowerCLI*.
   - Vérifiez que Microsoft .NET Framework 4.8 ou version ultérieure est installé.
   - Créez un dossier local dans lequel enregistrer les informations de l'autorité d'approbation que vous exportez en tant que fichiers.
2 Ajoutez l'administrateur d'autorité d'approbation au groupe TrustedAdmins sur l'instance de vCenter Server du cluster d'autorité d'approbation.
3 Ajoutez l'administrateur d'autorité d'approbation au groupe TrustedAdmins sur l'instance de vCenter Server du cluster approuvé.
4 Activez l'état de l'autorité d'approbation.
5 Collectez des informations sur les hôtes à approuver (les hôtes approuvés) sur le cluster approuvé.
6 Importez les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
7 Créez le fournisseur de clés sur le cluster d'autorité d'approbation.
8 Exportez les informations du cluster d'autorité d'approbation à partir du cluster d'autorité d'approbation.
9 Importez les informations du cluster d'autorité d'approbation exportées vers le cluster d'autorité d'approbation.
10 Configurez le fournisseur de clés approuvé pour les hôtes approuvés sur le cluster approuvé.

Note Lors de l'ajout d'hôtes ESXi au cluster approuvé après avoir terminé la configuration initiale de Autorité d'approbation vSphere , vous devrez peut-être exporter et importer à nouveau les informations de l'hôte approuvé. En effet, si les nouveaux hôtes ESXi diffèrent des hôtes d'origine, vous devez collecter les nouvelles informations sur l'hôte ESXi et les importer dans le cluster d'autorité d'approbation. Reportez-vous à la section Ajout et suppression d'hôtes Autorité d'approbation vSphere .

Procédure

1 Activer l'administrateur de l'autorité d'approbation

   Pour activer Autorité d'approbation vSphere , vous devez ajouter un utilisateur au groupe TrustedAdmins de vSphere. Cet utilisateur devient l'administrateur de l'autorité d'approbation. Utilisez l'administrateur de l'autorité d'approbation pour la plupart des tâches de configuration de Autorité d'approbation vSphere .

2 Activer l'état de l'autorité d'approbation

La création d'un cluster vCenter Server dans un cluster Autorité d'approbation vSphere (également appelé activation de l'état de l'autorité d'approbation) démarre les services d'autorité d'approbation requis sur les hôtes ESXi du cluster.

3 Collecter des informations sur les hôtes ESXi et vCenter Server à approuver

Pour établir l'approbation, le cluster Autorité d'approbation vSphere nécessite des informations sur les hôtes ESXi et le système vCenter Server du cluster approuvé. Exportez ces informations sous forme de fichiers à importer dans le cluster d'autorité d'approbation. Vous devez vous assurer de maintenir ces fichiers confidentiels et de les transporter en toute sécurité.

4 Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation

Vous importez l'hôte ESXi exporté et les informations de l'instance de vCenter Server dans le cluster Autorité d'approbation vSphere , de sorte que le cluster d'autorité d'approbation puisse déterminer les hôtes qu'il peut attester.

5 Créer le fournisseur de clés sur le cluster d'autorité d'approbation

Pour que le service de fournisseur de clés se connecte à un fournisseur de clés, vous devez d'abord créer un fournisseur de clés approuvé, puis configurer une configuration d'approbation entre le cluster Autorité d'approbation vSphere et le serveur de clés (KMS). Pour la plupart des serveurs de clés compatibles KMIP, cette configuration implique la configuration de certificats de client et de serveur.

6 Exporter les informations du cluster d'autorité d'approbation

Pour que le cluster approuvé se connecte au cluster Autorité d'approbation vSphere , exportez les informations de service du cluster d'autorité d'approbation sous la forme d'un fichier, puis importez celui-ci dans le cluster approuvé. Vous devez vous assurer de protéger la confidentialité de ces fichiers et de les transporter en toute sécurité.

7 Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés

Une fois que vous avez importé les informations du cluster Autorité d'approbation vSphere sur le cluster approuvé, les hôtes approuvés démarrent le processus d'attestation avec le cluster d'autorité d'approbation.

8 Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de vSphere Client

Vous pouvez configurer le fournisseur de clés approuvé à l'aide de vSphere Client.

9 Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de la ligne de commande

Vous pouvez configurer des fournisseurs de clés approuvés à l'aide de la ligne de commande. Vous pouvez configurer le fournisseur de clés approuvé par défaut pour vCenter Server, ou au niveau du cluster ou du dossier dans la hiérarchie d'objets vCenter.

Activer l'administrateur de l'autorité d'approbation

Pour activer Autorité d'approbation vSphere , vous devez ajouter un utilisateur au groupe TrustedAdmins de vSphere. Cet utilisateur devient l'administrateur de l'autorité d'approbation. Utilisez l'administrateur de l'autorité d'approbation pour la plupart des tâches de configuration de Autorité d'approbation vSphere .

Utilisez un utilisateur distinct de l'administrateur vCenter Server comme administrateur de l'autorité d'approbation. Le fait de choisir un utilisateur distinct améliore la sécurité de votre environnement. Vous devez activer un administrateur d'autorité d'approbation au cluster d'autorité d'approbation et au cluster approuvé.

Conditions préalables

Créez un utilisateur ou identifiez un utilisateur existant, comme administrateur d'autorité d'approbation.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster d'autorité d'approbation à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur.
3. Dans le menu **Accueil**, sélectionnez **Administration**.
4. Sous **Single Sign-On**, cliquez sur **Utilisateurs et groupes**.
5. Cliquez sur **Groupes** et cliquez sur le groupe **TrustedAdmins**.

   Si le groupe TrustedAdmins ne s'affiche pas initialement, utilisez l'icône **Filtre** pour le filtrer ou parcourez les groupes en cliquant sur la flèche de droite en bas du volet.
6. Dans la zone **Membres du groupe**, cliquez sur **Ajouter des membres**.

   Assurez-vous que la source d'identité locale est sélectionnée (vsphere.local est la valeur par défaut, mais vous avez peut-être sélectionné un domaine différent au cours de l'installation) et recherchez le membre (utilisateur) à ajouter au groupe en tant qu'administrateur d'autorité d'approbation.
7. Sélectionnez le membre.
8. Cliquez sur **Enregistrer**.
9. Répétez les étapes 1 à 8 pour l'instance de vCenter Server du cluster approuvé.

Étape suivante

Continuez avec Activer l'état de l'autorité d'approbation.

Activer l'état de l'autorité d'approbation

La création d'un cluster vCenter Server dans un cluster Autorité d'approbation vSphere (également appelé activation de l'état de l'autorité d'approbation) démarre les services d'autorité d'approbation requis sur les hôtes ESXi du cluster.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.

Procédure

1. Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu'utilisateur administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster d'autorité d'approbation.

   ```
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

2. Pour vérifier l'état actuel du cluster, exécutez l'applet de commande `Get-TrustAuthorityCluster`.

   Par exemple, cette commande affiche le cluster, `vTA Cluster`, et que son état est désactivé.

   ```
   Get-TrustAuthorityCluster

   Name                 State                Id
   ----                 -----                --
   vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
   ```

   La sortie indique Désactivé ou Activé dans la colonne État pour chaque cluster trouvé. Désactivé signifie que les services d'autorité d'approbation ne sont pas en cours d'exécution.

3. Pour activer le cluster d'autorité d'approbation, exécutez l'applet de commande `Set-TrustAuthorityCluster`.

   Par exemple, cette commande active le cluster `vTA Cluster`.

   ```
   Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
   ```

   Le système répond par une invite de confirmation.

   ```
   Confirmation
   Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
   ```

4 Lorsque vous êtes invité à confirmer, appuyez sur Entrée. (La valeur par défaut est **Y**.)

La sortie affiche l'état du cluster. L'exemple suivant montre que le cluster `vTA Cluster` a été activé :

```
Name                State               Id
----                -----               --
vTA Cluster         Enabled             TrustAuthorityCluster-domain-c8
```

Résultats

Deux services démarrent sur les hôtes ESXi dans le cluster d'autorité d'approbation : le service d'attestation et le service de fournisseur de clés.

Exemple : Activer l'état approuvé sur le cluster d'autorité d'approbation

Cet exemple montre comment utiliser PowerCLI pour activer des services sur le cluster d'autorité d'approbation. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-4. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Instance de vCenter Server pour le cluster d'autorité d'approbation	192.168.210.22
Nom du cluster d'autorité d'approbation	Cluster vTA
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State
Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
```

```
----                 -----              --
vTA Cluster          Enabled            TrustAuthorityCluster-domain-c8
```

Étape suivante

Continuez avec Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

Collecter des informations sur les hôtes ESXi et vCenter Server à approuver

Pour établir l'approbation, le cluster Autorité d'approbation vSphere nécessite des informations sur les hôtes ESXi et le système vCenter Server du cluster approuvé. Exportez ces informations sous forme de fichiers à importer dans le cluster d'autorité d'approbation. Vous devez vous assurer de maintenir ces fichiers confidentiels et de les transporter en toute sécurité.

Vous utilisez les applets de commande PowerCLI de Autorité d'approbation vSphere pour exporter les informations suivantes sous forme de fichiers à partir des hôtes ESXi dans le cluster approuvé pour que le cluster d'autorité d'approbation sache quels logiciels et matériels sont à approuver.

- Version de ESXi
- Fabricant de TPM (certificat d'autorité de certification)
- (Facultatif) TPM unique (certificat EK)

Note Stockez ces fichiers exportés dans un endroit sûr, au cas où vous devez restaurer la configuration de Autorité d'approbation vSphere .

Si vous disposez d'hôtes du même type et du même fournisseur fabriqués dans la même période et au même emplacement, vous pouvez être en mesure de faire confiance à tous les TPM en obtenant le certificat d'autorité de certification d'un seul des TPM. Pour approuver un TPM unique, vous devez obtenir le certificat EK du TPM.

Vous devez également obtenir les informations de principal depuis l'instance de vCenter Server du cluster approuvé. Les informations de principal contiennent l'utilisateur de solution vpxd et sa chaîne de certificats. Les informations de principal permettent à l'instance de vCenter Server du cluster approuvé de détecter les fournisseurs de clés approuvés disponibles et configurés sur le cluster d'autorité d'approbation.

Pour configurer initialement Autorité d'approbation vSphere , vous devez collecter la version d'ESXi et les informations de TPM. Vous devez collecter la version d'ESXi chaque fois que vous déployez une nouvelle version d'ESXi, y compris lorsque vous effectuez une mise à niveau ou appliquez un correctif.

Vous collectez les informations de principal de vCenter Server une seule fois par système vCenter Server.

Conditions préalables

- Identifiez les versions d'ESXi et les types de matériel TPM qui se trouvent dans le cluster approuvé et définissez si vous souhaitez approuver tous les types de matériel TPM, seulement certains d'entre eux ou uniquement des hôtes individuels.
- Sur la machine à partir de laquelle vous exécutez les applets de commande PowerCLI, créez un dossier local dans lequel enregistrer les informations que vous exportez en tant que fichiers.
- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.

Procédure

1. Dans une session PowerCLI, exécutez l'applet de commande pour vous connecter en tant qu'utilisateur racine à l'un des hôtes ESXi dans le cluster approuvé.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server host_ip_address -User root -Password 'password'
   ```

2. Exécutez l'applet de commande `Get-VMHost` pour confirmer l'hôte ESXi.

   ```
   Get-VMHost
   ```

   Les informations de l'hôte s'affichent.

3. Attribuez `Get-VMHost` à une variable.

   Par exemple :

   ```
   $vmhost = Get-VMHost
   ```

4 Exécutez l'applet de commande `Export-Tpm2CACertificate` pour exporter le certificat d'autorité de certification d'un fabricant TPM spécifique.

   a Attribuez `Get-Tpm2EndorsementKey -VMHost $vmhost` à une variable.

   Par exemple, cette commande attribue `Get-Tpm2EndorsementKey -VMHost $vmhost` à la variable `$tpm2`.

   ```
   $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
   ```

   b Exécutez la cmdlet `Export-Tpm2CACertificate`.

   Par exemple, cette commande exporte le certificat du TPM vers le fichier `cacert.zip`. Assurez-vous que le répertoire de destination existe avant d'exécuter cette commande.

   ```
   Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
   ```

   Le fichier est créé.

   c Répétez cette opération pour chaque type de matériel TPM du cluster que vous souhaitez approuver. Utilisez un nom de fichier différent pour chaque type de matériel TMP afin de ne pas remplacer un fichier précédemment exporté.

5 Exécutez l'applet de commande `Export-VMHostImageDb` pour exporter la description de l'hôte ESXi du logiciel (l'image ESXi).

Par exemple, cette commande exporte les informations vers le fichier `image.tgz`. Assurez-vous que le répertoire de destination existe avant d'exécuter cette commande.

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

Note L'applet de commande `Export-VMHostImageDb` fonctionne également si vous préférez vous connecter à l'instance de vCenter Server du cluster approuvé.

Le fichier est créé.

Répétez la procédure pour chaque version d'ESXi dans le cluster que vous souhaitez approuver. Utilisez un nom de fichier différent pour chaque version afin de ne pas remplacer un fichier précédemment exporté.

6 Exportez les informations principales de vCenter Server sur le cluster approuvé.

a Déconnectez-vous de l'hôte ESXi.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de l'utilisateur administrateur de l'autorité d'approbation. (Vous pouvez également utiliser un utilisateur disposant de privilèges d'**Administrateur**.)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c Pour exporter les informations principales de vCenter Server sur le cluster approuvé, exécutez l'applet de commande `Export-TrustedPrincipal`.

Par exemple, cette commande exporte les informations vers le fichier `principal.json`. Assurez-vous que le répertoire de destination existe avant d'exécuter cette commande.

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

Le fichier est créé.

7 (Facultatif) Si vous souhaitez approuver un hôte individuel, vous devez exporter le certificat de clé publique EK du TPM.

Reportez-vous à la section Exportation et importation d'un certificat de paire de clés de type EK (Endorsement Key) du TPM.

Résultats

Les fichiers suivants sont créés :

- Fichier de certificat d'autorité de certification TPM (extension de fichier .zip)
- Fichier image d'ESXi (extension de fichier .tgz)
- Fichier principal de vCenter Server (extension de fichier .json)

Exemple : Collecte d'informations sur les hôtes ESXi et vCenter Server à approuver

Cet exemple explique comment utiliser PowerCLI pour exporter les informations de l'hôte ESXi et le principal vCenter Server. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-5. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Hôte ESXi dans un cluster approuvé	192.168.110.51
vCenter Server du cluster approuvé	192.168.110.22
Variable `$vmhost`	`Get-VMHost`

Tableau 9-5. Exemple de configuration de Autorité d'approbation vSphere (suite)

Composant	Valeur
Variable `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local
Répertoire local contenant des fichiers de sortie	`C:\vta`

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576         1.614
7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

Étape suivante

Continuez avec Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.

Exportation et importation d'un certificat de paire de clés de type EK (Endorsement Key) du TPM

Vous pouvez exporter un certificat de paire de clés de type EK (Endorsement Key) du TPM à partir d'un hôte ESXi et l'importer dans le cluster Autorité d'approbation vSphere . C'est le cas lorsque vous souhaitez approuver un hôte ESXi individuel dans le cluster approuvé.

Pour importer un certificat de paire de clés de type EK (Endorsement Key) du TPM dans le cluster d'autorité d'approbation, vous devez modifier le type d'attestation par défaut du cluster d'autorité d'approbation pour accepter les certificats de type EK. Le type d'attestation par défaut accepte les certificats d'autorité de certification (CA) du TPM. Certains TPM n'incluent pas de certificats EK. Si vous souhaitez approuver des hôtes ESXi de manière individuelle, le TPM doit inclure un certificat EK.

Note Stockez les fichiers exportés de certificats EK à un emplacement sûr, au cas où vous deviez restaurer la configuration de Autorité d'approbation vSphere .

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.

Procédure

1. Assurez-vous que vous êtes connecté en tant qu'administrateur d'autorité d'approbation à l'instance de vCenter Server du cluster d'autorité d'approbation.

   Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3 Pour modifier le type d'attestation du cluster d'autorité d'approbation :

a Exécutez l'applet de commande `Get-TrustAuthorityCluster` pour afficher les clusters gérés par cette instance de vCenter Server.

```
Get-TrustAuthorityCluster
```

Les clusters s'affichent.

b Attribuez les informations de `Get-TrustAuthorityCluster` à une variable.

Par exemple, cette commande attribue le cluster nommé `vTA Cluster` à la variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

c Attribuez les informations de `Get-TrustAuthorityTpm2AttestationSettings` à une variable.

Par exemple, cette commande attribue les informations à la variable `$tpm2Settings`.

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d Exécutez l'applet de commande `Set-TrustAuthorityTpm2AttestationSettings`, en spécifiant `RequireEndorsementKey` ou `RequireCertificateValidation`, ou les deux.

Par exemple, cette commande spécifie `RequireEndorsementKey`.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

Le système répond avec une invite de confirmation semblable à la suivante.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e Lorsque vous êtes invité à confirmer, appuyez sur Entrée. (La valeur par défaut est **Y**.)

La sortie indique l'état True pour le paramètre spécifié. Par exemple, cet état indique True pour exiger une de paire de clés de type EK (Endorsement Key) et False pour exiger la validation du certificat.

```
Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 Pour exporter le certificat de paire de clés de type EK (Endorsement Key) du TPM :

a Déconnectez-vous de l'instance de vCenter Server du cluster d'autorité d'approbation.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu'utilisateur racine à l'un des hôtes ESXi dans le cluster approuvé.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c Exécutez l'applet de commande `Get-VMHost` pour confirmer l'hôte ESXi.

```
Get-VMHost
```

Les informations de l'hôte s'affichent.

d Attribuez `Get-VMHost` à une variable.

Par exemple :

```
$vmhost = Get-VMHost
```

e Exécutez l'applet de commande `Export-Tpm2EndorsementKey` pour exporter le certificat de type EK (Endorsement Key) de l'hôte ESXi.

Par exemple, cette commande exporte le certificat de type EK (Endorsement Key) vers le fichier `tpm2ek.json`.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

Le fichier est créé.

5 Pour importer la paire de clés de type EK (Endorsement Key) du TPM :

a Déconnectez-vous de l'hôte ESXi dans le cluster approuvé.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de l'utilisateur administrateur de l'autorité d'approbation.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c Exécutez la cmdlet `Get-TrustAuthorityCluster`.

```
Get-TrustAuthorityCluster
```

Les clusters du cluster d'autorité d'approbation s'affichent.

d Attribuez les informations « *cluster* » `Get-TrustAuthorityCluster` à une variable.

Par exemple, cette commande attribue les informations sur le cluster `vTA Cluster` à la variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

e Exécutez la cmdlet `New-TrustAuthorityTpm2EndorsementKey`.

Par exemple, cette commande utilise le fichier de `tpm2ek.json` précédemment exporté à l'étape 4.

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath C:\vta\tpm2ek.json
```

Les informations sur la paire de clés de type EK (Endorsement Key) importée s'affichent.

Résultats

Le type d'attestation du cluster d'autorité d'approbation est modifié pour accepter les certificats de type EK (Endorsement Key). Le certificat de type EK (Endorsement Key) est exporté à partir du cluster approuvé et importé dans le cluster d'autorité d'approbation.

Exemple : Exportation et importation d'un certificat de paire de clés de type EK (Endorsement Key) du TPM

Cet exemple montre comment utiliser PowerCLI pour modifier le type d'attestation par défaut du cluster de l'autorité d'approbation pour accepter les certificats de type EK (Endorsement Key), exporter le certificat du TPM de l'hôte ESXi dans le cluster approuvé et l'importer dans le cluster d'autorité d'approbation. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-6. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Instance de vCenter Server pour le cluster d'autorité d'approbation	192.168.210.22
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
Variable `$vmhost`	`Get-VMHost`
Hôte ESXi dans un cluster approuvé	192.168.110.51
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local
Répertoire local contenant le fichier de sortie	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
-Password 'VMware1!'

Name                           Port  User
```

```
----                            ----  ----
192.168.210.22                  443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with the
following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz   MemoryUsageGB
MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------   -------------
------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
```

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
-Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

Étape suivante

Continuez avec Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.

Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation

Vous importez l'hôte ESXi exporté et les informations de l'instance de vCenter Server dans le cluster Autorité d'approbation vSphere , de sorte que le cluster d'autorité d'approbation puisse déterminer les hôtes qu'il peut attester.

Si vous suivez ces tâches dans l'ordre, vous êtes toujours connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

Procédure

1. Assurez-vous que vous êtes connecté en tant qu'administrateur d'autorité d'approbation à l'instance de vCenter Server du cluster d'autorité d'approbation.

   Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2 (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

3 Pour afficher les clusters gérés par cette instance de vCenter Server, exécutez l'applet de commande `Get-TrustAuthorityCluster`.

```
Get-TrustAuthorityCluster
```

Les clusters s'affichent.

4 Attribuez les informations « *cluster* » `Get-TrustAuthorityCluster` à une variable.

Par exemple, cette commande attribue les informations sur le cluster `vTA Cluster` à la variable `$vTA`.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 Pour importer les informations de principal de l'instance de vCenter Server du cluster approuvé dans le cluster d'autorité d'approbation, exécutez l'applet de commande `New-TrustAuthorityPrincipal`.

Par exemple, la commande suivante importe le fichier `principal.json` précédemment exporté dans Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

Les informations sur TrustAuthorityPrincipal s'affichent.

6 Pour vérifier l'importation, exécutez l'applet de commande `Get-TrustAuthorityPrincipal`.

Par exemple :

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

Les informations sur TrustAuthorityPrincipal importé s'affichent.

7 Pour importer les informations du certificat de l'autorité de certification du module de plateforme sécurisée (TPM), exécutez l'applet de commande `New-TrustAuthorityTpm2CACertificate`.

Par exemple, la commande suivante importe les informations du certificat de l'autorité de certification du module de plateforme sécurisée à partir du fichier `cacert.zip` précédemment exporté dans Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
```

Les informations sur le certificat importé s'affichent.

8 Pour importer les informations sur l'image de base de l'hôte ESXi, exécutez l'applet de commande `New-TrustAuthorityVMHostBaseImage`.

Par exemple, la commande suivante importe les informations sur l'image à partir du fichier `image.tgz` précédemment exporté dans Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

Les informations de l'image importée s'affichent.

Résultats

Le cluster d'autorité d'approbation détermine les hôtes ESXi qu'il peut attester à distance, ainsi que les hôtes qu'il peut approuver.

Exemple : Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation

Cet exemple montre comment utiliser PowerCLI pour importer les informations du principal vCenter Server du cluster approuvé et les fichiers d'informations de l'hôte approuvé dans le cluster d'autorité d'approbation. Il suppose que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation en tant qu'administrateur d'autorité d'approbation. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-7. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
Instance de vCenter Server pour le cluster d'autorité d'approbation	192.168.210.22
Noms du cluster d'autorité d'approbation	vTA Cluster1 (activé) vTA Cluster2 (désactivé)
Fichier d'informations de principal	`C:\vta\principal.json`
Fichier de certificat TPM	`C:\vta\cacert.cer`
Fichier image de base de l'hôte ESXi	`C:\vta\image.tgz`
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User trustedadmin@vsphere.local
-Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster
```

```
Name                 State                Id
----                 -----                --
vTA Cluster1         Enabled              TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled             TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath
C:\vta\principal.json

Name                                          Domain          Type       TrustAuthorityClusterId
----                                          ------          ----       -----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER   TrustAuthorityCluster-domain-
c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                          Domain          Type       TrustAuthorityClusterId
----                                          ------          ----       -----------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER   TrustAuthorityCluster-domain-
c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA
-FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                     Health
-----------------------                 ----                                     ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                            Health
-----------------------                 -------------                            ------
TrustAuthorityCluster-domain-c8         ESXi 7.0.0-0.0.14828939                  Ok
```

Étape suivante

Continuez avec Créer le fournisseur de clés sur le cluster d'autorité d'approbation.

Créer le fournisseur de clés sur le cluster d'autorité d'approbation

Pour que le service de fournisseur de clés se connecte à un fournisseur de clés, vous devez d'abord créer un fournisseur de clés approuvé, puis configurer une configuration d'approbation entre le cluster Autorité d'approbation vSphere et le serveur de clés (KMS). Pour la plupart des serveurs de clés compatibles KMIP, cette configuration implique la configuration de certificats de client et de serveur.

Ce qui était précédemment appelé un cluster KMS dans vSphere 6.7 est désormais appelé fournisseur de clés dans vSphere 7.0. Pour plus d'informations sur les fournisseurs de clés, consultez À propos du service de fournisseur de clés de Autorité d'approbation vSphere.

Dans un environnement de production, il est possible que vous souhaitiez créer plusieurs fournisseurs de clés. En créant plusieurs fournisseurs de clés, vous pouvez choisir la manière dont vous voulez gérer votre déploiement en fonction de l'organisation de l'entreprise, des différentes unités commerciales ou des clients, etc.

Si vous suivez ces tâches dans l'ordre, vous êtes toujours connecté à l'instance de vCenter Server du cluster Autorité d'approbation vSphere .

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créez et activez une clé sur le serveur de clés comme clé principale (auparavant appelée clé maître) pour le fournisseur de clés approuvé. Cette clé encapsule d'autres clés et secrets utilisés par ce fournisseur de clés approuvé. Pour plus d'informations sur la création de clés, consultez la documentation de votre fournisseur de serveur de clés.

Procédure

1. Assurez-vous que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation. Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.
2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3. Pour créer le fournisseur de clés approuvé, exécutez l'applet de commande `New-TrustAuthorityKeyProvider`.

   Par exemple, cette commande utilise `1` pour PrimaryKeyID (précédemment appelé MasterKeyID) et le nom `clkp`. Si vous suivez ces tâches dans l'ordre, vous avez précédemment attribué des informations `Get-TrustAuthorityCluster` à une variable (par exemple, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
   -KmipServerAddress ip_address -KmipServerUsername user -KmipServerPassword password
   ```

PrimaryKeyID est normalement un ID de clé provenant du serveur de clés sous la forme d'un UUID. La valeur de PrimaryKeyID dépend du fournisseur. Consultez la documentation de votre serveur de clés. L'applet de commande `New-TrustAuthorityKeyProvider` peut accepter d'autres options, telles que `KmipServerPort`, `ProxyAddress` et `ProxyPort`. Pour plus d'informations, consultez le système d'aide de `New-TrustAuthorityKeyProvider`.

Note Pour ajouter plusieurs serveurs de clés au fournisseur de clés, utilisez l'appelt de commande `Add-TrustAuthorityKeyProviderServer`.

Les informations du fournisseur de clés s'affichent.

4 Établissez la connexion approuvée pour que le serveur de clés approuve le fournisseur de clés approuvé. Le processus exact dépend des certificats acceptés par le serveur de clés et de la stratégie de votre entreprise. Sélectionnez l'option correspondant à votre serveur et terminez les étapes requises.

Option	Reportez-vous au
Chargement d'un certificat client	Téléchargement du certificat client pour établir une connexion fiable avec le fournisseur de clés approuvé.
Chargement d'un certificat KMS et d'une clé privée	Téléchargez le certificat et la clé privée pour établir une connexion fiable avec le fournisseur de clés approuvé.
Demande de signature du nouveau certificat	Création d'une demande de signature de certificat pour établir une connexion fiable avec un fournisseur de clé approuvé.

5 Terminez la configuration de l'approbation en chargeant un certificat de serveur de clés de telle sorte que le fournisseur de clés approuvé approuve le serveur de clés.

a Attribuez les informations de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` à une variable.

Par exemple :

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Cette variable obtient les fournisseurs de clés approuvés dans le cluster d'autorité d'approbation donné, dans le cas présent, `$vTA`.

Note Si vous disposez de plusieurs fournisseurs de clés approuvés, utilisez des commandes semblables aux suivantes pour sélectionner celle de votre choix :

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

L'utilisation de `Select-Object -Last 1` sélectionne le dernier fournisseur de clés approuvé dans la liste.

b Pour obtenir le certificat de serveur du serveur de clés, exécutez la commande `Get-TrustAuthorityKeyProviderServerCertificate`.

Par exemple :

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers
```

Les informations sur le certificat de serveur s'affichent. Au départ, le certificat n'est pas approuvé, l'état approuvé est donc False. Si plusieurs serveurs de clés sont configurés, une liste des certificats est renvoyée. Vérifiez et ajoutez chaque certificat en suivant les instructions ci-dessous.

c Avant d'approuver le certificat, attribuez les informations `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` à une variable (par exemple, `cert`) et exécutez la commande `$cert.Certificate.ToString()`, puis vérifiez la sortie.

Par exemple :

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

Les informations sur le certificat s'affichent, y compris le sujet, l'émetteur et d'autres informations.

d Pour ajouter le certificat du serveur KMIP au fournisseur de clés approuvé, exécutez `Add-TrustAuthorityKeyProviderServerCertificate`.

Par exemple :

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

Les informations du certificat s'affichent et l'état approuvé est désormais True.

6 Vérifiez l'état du fournisseur de clés.

a Pour actualiser l'état du fournisseur de clés, attribuez à nouveau la variable `$kp`.

Par exemple :

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Note Si vous disposez de plusieurs fournisseurs de clés approuvés, utilisez des commandes semblables aux suivantes pour sélectionner celle de votre choix :

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

L'utilisation de `Select-Object -Last 1` sélectionne le dernier fournisseur de clés approuvé dans la liste.

b Pour obtenir l'état du fournisseur de clés, exécutez la commande `$kp.Status`.

Par exemple :

```
$kp.Status
```

Note L'actualisation de l'état peut prendre quelques minutes. Pour afficher l'état, attribuez à nouveau la variable `$kp` et réexécutez la commande `$kp.Status`.

Un état de santé OK indique que le fournisseur de clés s'exécute correctement.

Résultats

Le fournisseur de clés approuvé a été créé et a établi une relation d'approbation avec le serveur de clés.

Exemple : Créer le fournisseur de clés sur le cluster d'autorité d'approbation

Cet exemple montre comment utiliser PowerCLI pour créer le fournisseur de clés approuvé sur le cluster d'autorité d'approbation. Il suppose que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation en tant qu'administrateur d'autorité d'approbation. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-8. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Variable `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
Variable `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
Instance de vCenter Server pour le cluster d'autorité d'approbation	192.168.210.22
Serveur de clés compatible KMIP	192.168.110.91
Utilisateur du serveur de clés compatible KMIP	vcqekmip
Nom du cluster d'autorité d'approbation	Cluster vTA
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91 -KmipServerUsername vcqekmip
-KmipServerPassword vcqekmip

Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

<Establish a trusted connection between the key provider and the key server.>

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp
```

```
PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California, C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate
$cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

Étape suivante

Continuez avec Exporter les informations du cluster d'autorité d'approbation.

Téléchargement du certificat client pour établir une connexion fiable avec le fournisseur de clés approuvé

Certains fournisseurs de serveurs de clés (KMS) imposent que vous chargiez le certificat client du fournisseur de clés approuvé sur le serveur de clés. Après le téléchargement, le serveur de clés accepte le trafic provenant du fournisseur de clés approuvé.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.

- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.

Procédure

1 Assurez-vous que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation. Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2 (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

3 Attribuez les informations de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` à une variable.

Par exemple :

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

Si vous suivez ces tâches dans l'ordre, vous avez précédemment attribué des informations `Get-TrustAuthorityCluster` à une variable (par exemple, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Cette variable obtient les fournisseurs de clés approuvés dans le cluster d'autorité d'approbation donné, dans le cas présent, `$vTA`.

Note Si vous disposez de plusieurs fournisseurs de clés approuvés, utilisez des commandes semblables aux suivantes pour sélectionner celle de votre choix :

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

L'utilisation de `Select-Object -Last 1` sélectionne le dernier fournisseur de clés approuvé dans la liste.

4 Pour créer le certificat client du fournisseur de clés approuvé, exécutez la commande `New-TrustAuthorityKeyProviderClientCertificate`.

Par exemple :

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

L'empreinte s'affiche.

5 Pour exporter le certificat client du fournisseur de clés, exécutez l'applet de commande `Export-TrustAuthorityKeyProviderClientCertificate`.

Par exemple :

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

Le certificat est exporté vers un fichier.

6 Téléchargez le fichier de certificat sur le serveur de clés.

Reportez-vous à la documentation du serveur de clés pour plus d'informations.

Résultats

Le fournisseur de clés approuvé a établi une relation de confiance avec le serveur de clés.

Téléchargez le certificat et la clé privée pour établir une connexion fiable avec le fournisseur de clés approuvé

Certains fournisseurs de serveur de clés (KMS) nécessitent que vous configuriez le fournisseur de clés approuvé avec le certificat client et la clé privée fournis par le serveur de clés. Après avoir configuré le fournisseur de clés approuvé, le serveur de clés accepte le trafic du fournisseur de clés approuvé.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.
- Demandez un certificat et une clé privée au format PEM auprès du fournisseur de serveurs de clés. Si le certificat est renvoyé dans un format autre que PEM, convertissez-le en PEM. Si la clé privée est protégée par un mot de passe, créez un fichier PEM avec le mot de passe supprimé. Vous pouvez utiliser la commande `openssl` pour les deux opérations. Par exemple :
  - Pour convertir un certificat au format CRT dans le format PEM :

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - Pour convertir un certificat DER dans le format PEM :

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

- Pour supprimer le mot de passe d'une clé privée :

```
openssl rsa –in key.pem –out keynopassword.pem
Enter pass phrase for key.pem:
writing RSA key
```

Procédure

1 Assurez-vous que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation. Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2 (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

```
Disconnect–VIServer –server * –Confirm:$false
Connect–VIServer –server TrustAuthorityCluster_VC_ip_address –User trust_admin_user –Password
'password'
```

3 Attribuez les informations de `Get–TrustAuthorityKeyProvider –TrustAuthorityCluster $vTA` à une variable.

Par exemple :

```
$kp = Get–TrustAuthorityKeyProvider –TrustAuthorityCluster $vTA
```

Si vous suivez ces tâches dans l'ordre, vous avez précédemment attribué des informations `Get–TrustAuthorityCluster` à une variable (par exemple, `$vTA = Get–TrustAuthorityCluster 'vTA Cluster'`).

La variable `$kp` obtient les fournisseurs de clés approuvés dans le cluster d'autorité d'approbation donné, dans le cas présent, `$vTA`.

Note Si vous disposez de plusieurs fournisseurs de clés approuvés, utilisez des commandes semblables aux suivantes pour sélectionner celle de votre choix :

```
Get–TrustAuthorityKeyProvider –TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get–TrustAuthorityKeyProvider –TrustAuthorityCluster $vTA | Select–Object –Last 1
```

L'utilisation de `Select–Object –Last 1` sélectionne le dernier fournisseur de clés approuvé dans la liste.

4 Téléchargez le certificat et la clé privée à l'aide de la commande `Set–TrustAuthorityKeyProviderClientCertificate`.

Par exemple :

```
Set–TrustAuthorityKeyProviderClientCertificate –KeyProvider $kp –CertificateFilePath <path/to/
certfile.pem> –PrivateKeyFilePath <path/to/privatekey.pem>
```

Résultats

Le fournisseur de clés approuvé a établi une relation de confiance avec le serveur de clés.

Création d'une demande de signature de certificat pour établir une connexion fiable avec un fournisseur de clé approuvé

Certains fournisseurs de serveur de clés (KMS) exigent que vous génériez une demande de signature de certificat (CSR) et envoyiez cette CSR au fournisseur de serveur de clés. Le fournisseur de serveur de clés signe la CSR et renvoie le certificat signé.ssfourniseur Après avoir configuré ce certificat signé en tant que certificat client du fournisseur de clés approuvé, le serveur de clés accepte le trafic provenant du fournisseur de clés approuvé.

Cette tâche est un processus en deux étapes. En premier lieu, vous générez la CSR et l'envoyez à votre fournisseur du serveur de clés. Ensuite, vous téléchargez le certificat signé que vous recevez du fournisseur du serveur de clés.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.

Procédure

1. Assurez-vous que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation. Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.
2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3. Attribuez les informations de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` à une variable.

   Par exemple :

   ```
   $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
   ```

   Si vous suivez ces tâches dans l'ordre, vous avez précédemment attribué des informations `Get-TrustAuthorityCluster` à une variable (par exemple, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

Cette variable obtient les fournisseurs de clés approuvés dans le cluster d'autorité d'approbation donné, dans le cas présent, `$vTA`.

Note Si vous disposez de plusieurs fournisseurs de clés approuvés, utilisez des commandes semblables aux suivantes pour sélectionner celle de votre choix :

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

L'utilisation de `Select-Object -Last 1` sélectionne le dernier fournisseur de clés approuvé dans la liste.

4 Pour générer une demande CSR, utilisez l'applet de commande `New-TrustAuthorityKeyProviderClientCertificateCSR`.

Par exemple :

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

La demande CSR s'affiche. Pour obtenir la demande CSR, vous pouvez également utiliser l'applet de commande `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp`.

5 Pour obtenir un certificat signé, soumettez la demande CSR à votre fournisseur du serveur de clés.

Les certificats doivent être au format PEM. Si le certificat est renvoyé dans un format autre que PEM, convertissez-le en PEM à l'aide de la commande `openssl`. Par exemple :

- Pour convertir un certificat au format CRT dans le format PEM :

  ```
  openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
  ```

- Pour convertir un certificat DER dans le format PEM :

  ```
  openssl x509 -inform DER -in clientcert.der -out clientcert.pem
  ```

6 Lorsque vous recevez le certificat signé du fournisseur du serveur de clés, chargez-le vers le serveur de clés en utilisant la cmdlet `Set-TrustAuthorityKeyProviderClientCertificate`.

Par exemple :

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath <path/tp/
certfile.pem>
```

Résultats

Le fournisseur de clés approuvé a établi une relation de confiance avec le serveur de clés.

Exporter les informations du cluster d'autorité d'approbation

Pour que le cluster approuvé se connecte au cluster Autorité d'approbation vSphere , exportez les informations de service du cluster d'autorité d'approbation sous la forme d'un fichier, puis importez celui-ci dans le cluster approuvé. Vous devez vous assurer de protéger la confidentialité de ces fichiers et de les transporter en toute sécurité.

Si vous suivez ces tâches dans l'ordre, vous êtes toujours connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

Note Stockez le fichier d'informations sur le service exporté dans un endroit sûr, au cas où vous devez restaurer la configuration de Autorité d'approbation vSphere .

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.

Procédure

1. Assurez-vous que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation. Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.
2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster d'autorité d'approbation.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3. Pour exporter les informations du service d'attestation et du service de fournisseur de clés du cluster d'autorité d'approbation, exécutez l'applet de commande `Export-TrustAuthorityServicesInfo`.

   Par exemple, cette commande exporte les informations sur le service vers le fichier `clsettings.json`. Si vous effectuez ces tâches dans l'ordre, vous avez précédemment attribué les informations de `Get-TrustAuthorityCluster` à une variable (par exemple, `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

   ```
   Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath C:\vta\clsettings.json
   ```

   Le fichier est créé.

Résultats

Un fichier contenant les informations du cluster d'autorité d'approbation est créé.

Exemple : Exporter les informations du cluster d'autorité d'approbation

Cet exemple montre comment utiliser PowerCLI pour exporter les informations du service de cluster d'autorité d'approbation. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-9. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Variable `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
Instance de vCenter Server pour le cluster d'autorité d'approbation	192.168.210.22
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       10/16/2019   9:59 PM           8177 clsettings.json
```

Étape suivante

Continuez avec Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés.

Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés

Une fois que vous avez importé les informations du cluster Autorité d'approbation vSphere sur le cluster approuvé, les hôtes approuvés démarrent le processus d'attestation avec le cluster d'autorité d'approbation.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.

- Exporter les informations du cluster d'autorité d'approbation.

Procédure

1. Assurez-vous que vous êtes connecté en tant qu'administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster approuvé.

   Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster approuvé.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

   Note Vous pouvez également démarrer une autre session PowerCLI pour vous connecter à l'instance de vCenter Server du cluster approuvé.

3. Vérifiez que l'état du cluster approuvé est Désactivé.

   ```
   Get-TrustedCluster
   ```

   L'état est indiqué comme étant Désactivé.

4. Attribuez les informations de `Get-TrustedCluster` à une variable.

   Par exemple, cette commande attribue des informations pour le cluster `Trusted Cluster` à la variable `$TC`.

   ```
   $TC = Get-TrustedCluster -Name 'Trusted Cluster'
   ```

5. Vérifiez la valeur de la variable en l'affichant.

   Par exemple :

   ```
   $TC
   ```

   Les informations de la commande `Get-TrustedCluster` s'affichent.

6. Pour importer les informations du cluster d'autorité d'approbation dans vCenter Server, exécutez l'applet de commande `Import-TrustAuthorityServicesInfo`.

   Par exemple, cette commande importe les informations sur le service depuis le fichier `clsettings.json` précédemment exporté dans Exporter les informations du cluster d'autorité d'approbation.

   ```
   Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
   ```

Le système répond par une invite de confirmation.

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 Lorsque vous êtes invité à confirmer, appuyez sur Entrée. (La valeur par défaut est **Y**.)

Les informations de service pour les hôtes situés dans le cluster d'autorité d'approbation s'affichent.

8 Pour activer le cluster approuvé, exécutez l'applet de commande `Set-TrustedCluster`.

Par exemple :

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

Le système répond par une invite de confirmation.

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

Si le cluster approuvé n'est pas dans un état sain, le message d'avertissement suivant s'affiche avant le message de confirmation :

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus. This
cmdlet will automatically remediate the TrustedCluster.
```

9 Lorsque vous êtes invité à confirmer, appuyez sur Entrée. (La valeur par défaut est **Y**.)

Le cluster approuvé est activé.

Note Vous pouvez également activer le cluster approuvé en activant le service d'attestation et le service de fournisseur de clés individuellement. Utilisez les commandes `Add-TrustedClusterAttestationServiceInfo` et `Add-TrustedClusterKeyProviderServiceInfo`. Par exemple, les commandes suivantes activent les services un par un pour le cluster `Trusted Cluster` disposant de deux services de fournisseurs de clés et de deux services d'attestation.

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

10 Vérifiez que le service d'attestation et le service de fournisseur de clés sont configurés dans le cluster approuvé.

a Attribuez les informations de `Get-TrustedCluster` à une variable.

Par exemple, cette commande attribue des informations pour le cluster `Trusted Cluster` à la variable `$TC`.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b Vérifiez que le service d'attestation est configuré.

```
$tc.AttestationServiceInfo
```

Les informations du service d'attestation s'affichent.

c Vérifiez que le serveur du fournisseur de clés est configuré.

```
$tc.KeyProviderServiceInfo
```

Les informations du service de fournisseur de clés s'affichent.

Résultats

Les hôtes approuvés ESXi dans le cluster approuvé commencent le processus d'attestation avec le cluster d'autorité d'approbation.

Exemple : Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés

Cet exemple montre comment importer les informations du service de cluster d'autorité d'approbation dans le cluster approuvé. Le tableau suivant montre des exemples de composants et de valeurs qui sont utilisés.

Tableau 9-10. Exemple de configuration de Autorité d'approbation vSphere

Composant	Valeur
Instance de vCenter Server du cluster approuvé	192.168.110.22
Administrateur d'autorité d'approbation	trustedadmin@vsphere.local
Nom du cluster approuvé	Cluster approuvé
Hôtes ESXi dans le cluster d'autorité d'approbation	192.168.210.51 et 192.168.210.52
Variable `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
```

```
192.168.110.22                443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                  State             Id
----                  -----             --
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                  State             Id
----                  -----             --
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

Name                  State             Id
----                  -----             --
Trusted Cluster       Enabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...
```

Étape suivante

Continuez avec Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de vSphere Client ou Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de la ligne de commande.

Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de vSphere Client

Vous pouvez configurer le fournisseur de clés approuvé à l'aide de vSphere Client.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.
- Exporter les informations du cluster d'autorité d'approbation.
- Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur de vCenter Server ou un administrateur disposant privilège **Opérations de chiffrement.Gérer les serveurs de clés**.
3. Sélectionnez l'instance de vCenter Server, puis sélectionnez **Configurer**.
4. Sélectionnez **Fournisseurs de clés** sous **Sécurité**.
5. Sélectionnez **Ajouter des fournisseurs de clés approuvés**.

   Les fournisseurs de clés approuvés disponibles sont affichés avec l'état Connecté.
6. Sélectionnez un fournisseur de clés approuvé et cliquez sur **Ajouter des fournisseurs de clés**.

   Le fournisseur de clés approuvé est indiqué comme étant Approuvé et Connecté. S'il s'agit du premier fournisseur de clés approuvé que vous ajoutez, il est marqué comme étant par défaut.

Résultats

Les hôtes approuvés ESXi peuvent désormais effectuer des opérations de chiffrement, telles que la création de machines virtuelles chiffrées.

Étape suivante

Le chiffrement d'une machine virtuelle avec un fournisseur de clés approuvé ressemble à l'expérience utilisateur de chiffrement des machines virtuelles qui a été donnée pour la première fois dans vSphere 6.5. Voir Chapitre 10 Utiliser le chiffrement dans votre environnement vSphere.

Configurer le fournisseur de clés approuvé pour les hôtes approuvés à l'aide de la ligne de commande

Vous pouvez configurer des fournisseurs de clés approuvés à l'aide de la ligne de commande. Vous pouvez configurer le fournisseur de clés approuvé par défaut pour vCenter Server, ou au niveau du cluster ou du dossier dans la hiérarchie d'objets vCenter.

Conditions préalables

- Activer l'administrateur de l'autorité d'approbation.
- Activer l'état de l'autorité d'approbation.
- Collecter des informations sur les hôtes ESXi et vCenter Server à approuver.
- Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
- Créer le fournisseur de clés sur le cluster d'autorité d'approbation.
- Exporter les informations du cluster d'autorité d'approbation.
- Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés.

Sur le cluster approuvé, vous devez disposer d'un rôle qui comprend le privilège **Opérations de chiffrement.Gérer KMS**.

Procédure

1. Assurez-vous que vous êtes connecté en tant qu'administrateur de vCenter Server du cluster approuvé.

   Par exemple, vous pouvez entrer la commande `$global:defaultviservers` pour afficher tous les serveurs connectés.

2. (Facultatif) Si nécessaire, vous pouvez exécuter les commandes suivantes pour vous assurer que vous êtes connecté à l'instance de vCenter Server du cluster approuvé.

   ```
   Disconnect-VIServer -server * -Confirm:$false
   Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
   ```

3. Obtenez le fournisseur de clés approuvé.

   ```
   Get-KeyProvider
   ```

   Vous pouvez utiliser l'option `-Name` *keyprovider* pour spécifier un fournisseur de clés approuvé unique.

4 Attribuez les informations du fournisseur de clés approuvé `Get-KeyProvider` à une variable.

   Par exemple, cette commande attribue les informations à la variable `$workload_kp`.

```
$workload_kp = Get-KeyProvider
```

   Si vous disposez de plusieurs fournisseurs de clés approuvés, vous pouvez utiliser `Select-Object` pour les sélectionner.

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

5 Enregistrez le fournisseur de clés approuvé.

```
Register-KeyProvider -KeyProvider $workload_kp
```

   Pour enregistrer d'autres fournisseurs de clés approuvés, répétez les étapes 4 et 5.

6 Définissez le fournisseur de clés approuvé par défaut à utiliser.

   a Pour définir le fournisseur de clés par défaut au niveau de vCenter Server, exécutez la commande suivante.

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

   b Pour définir le fournisseur de clés au niveau du cluster, exécutez la commande suivante.

   Par exemple, cette commande définit le fournisseur de clés du cluster `Trusted Cluster`.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

   c Pour définir le fournisseur de clés au niveau du dossier, exécutez la commande suivante.

   Par exemple, cette commande définit le fournisseur de clés du dossier `TC Folder`, qui a été créé sur le centre de données `workLoad`.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

Étape suivante

Le chiffrement d'une machine virtuelle avec un fournisseur de clés approuvé ressemble à l'expérience utilisateur de chiffrement des machines virtuelles qui a été donnée pour la première fois dans vSphere 6.5. Voir Chapitre 10 Utiliser le chiffrement dans votre environnement vSphere.

Gestion de Autorité d'approbation vSphere dans votre environnement vSphere

Après avoir configuré Autorité d'approbation vSphere , vous pouvez effectuer des opérations supplémentaires, telles que l'arrêt et le démarrage de services, l'ajout d'hôtes à des clusters et l'affichage de l'état du cluster d'autorité d'approbation.

Vous pouvez effectuer des tâches à l'aide de vSphere Client, de l'API et des applets de commande PowerCLI. Consultez la documentation *Guide de programmation de vSphere Web Services SDK*, la documentation *VMware PowerCLI* et la documentation *Référence d'applets de commande VMware PowerCLI*.

Démarrer, arrêter et redémarrer les services Autorité d'approbation vSphere

Vous pouvez démarrer, arrêter et redémarrer les services Autorité d'approbation vSphere à l'aide de vSphere Client.

Les services qui constituent Autorité d'approbation vSphere sont le service d'attestation (attestd) et le service de fournisseur de clés (kmxd).

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster vSphere Trust Authority à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur.
3. Accédez à un hôte ESXi dans le cluster d'autorité d'approbation.
4. Cliquez sur **Configurer**, puis sélectionnez **Services** sous **Système**.
5. Localisez le service attestd et le service kmxd.
6. Sélectionnez l'opération **Redémarrer**, **Démarrer** ou **Arrêter**, selon le cas.

Afficher les hôtes de l'autorité d'approbation

Vous pouvez afficher les hôtes Autorité d'approbation vSphere configurés pour un cluster approuvé à l'aide de vSphere Client.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur.
3. Sélectionnez l'instance de vCenter Server.
4. Cliquez sur l'onglet **Configurer** et sélectionnez **Autorité d'approbation** sous **Sécurité**.

   Les hôtes ESXi dans le cluster autorité d'approbation configurés pour le cluster approuvé sont affichés.

Afficher l'état du cluster Autorité d'approbation vSphere

Vous pouvez afficher l'état du cluster Autorité d'approbation vSphere à l'aide de vSphere Client. L'état est activé ou désactivé.

Lorsque l'état du cluster d'autorité d'approbation est activé, les hôtes approuvés dans le cluster approuvé peuvent communiquer avec le service d'attestation et le service de fournisseur de clés.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster d'autorité d'approbation à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur.
3. Sélectionnez le cluster d'autorité d'approbation dans la hiérarchie des objets.
4. Cliquez sur l'onglet **Configurer** et sélectionnez **Cluster d'autorité d'approbation** sous **Autorité d'approbation**.

   L'état s'affiche comme étant activé ou désactivé.

Redémarrer le service d'hôte approuvé

Vous pouvez redémarrer le service qui s'exécute sur vos hôtes approuvés.

Le service, kmxa, s'exécute sur les hôtes ESXi approuvés.

Conditions préalables

L'accès à ESXi Shell doit être activé. Reportez-vous à la section Activer l'accès à ESXi Shell.

Procédure

1. Utilisez SSH ou une autre connexion de console distante pour démarrer une session sur le dispositif approuvé ESXi.
2. Connectez-vous en tant qu'utilisateur racine.
3. Exécutez la commande suivante.

```
/etc/init.d/kmxa restart
```

Ajout et suppression d'hôtes Autorité d'approbation vSphere

Ajoutez et supprimez des hôtes ESXi d'un cluster Autorité d'approbation vSphere à l'aide de scripts fournis par VMware.

Dans vSphere 7.0, vous ajoutez et supprimez les hôtes ESXi d'un cluster Autorité d'approbation vSphere existant ou d'un cluster approuvé à l'aide de scripts fournis par VMware. À partir de vSphere 7.0 Update 1, vous utilisez la fonction Corriger pour ajouter des hôtes ESXi à un cluster approuvé existant. Reportez-vous aux sections Ajouter un hôte à un cluster approuvé avec vSphere Client et Ajouter un hôte à un cluster approuvé avec l'interface de ligne de commande. Dans vSphere 7.0 Update 1, vous devez toujours utiliser des scripts pour ajouter des hôtes ESXi à un cluster d'autorité d'approbation existant. Consultez les articles de la base de connaissances VMware sur https://kb.vmware.com/s/article/77234 et https://kb.vmware.com/s/article/77146.

Ajouter un hôte à un cluster approuvé avec vSphere Client

Vous pouvez ajouter des hôtes ESXi à un cluster approuvé existant à l'aide de vSphere Client.

Une fois que vous avez initialement configuré un cluster approuvé, vous pouvez ajouter d'autres hôtes ESXi. Cependant, lorsque vous ajoutez l'hôte à un cluster approuvé, vous devez effectuer l'étape supplémentaire de correction. Lorsque vous corrigez le cluster approuvé, vous vous assurez que l'état de configuration souhaité correspond à sa configuration appliquée.

Dans la première version de Autorité d'approbation vSphere disponible dans vSphere 7.0, vous exécutez des scripts pour ajouter un hôte à un cluster approuvé existant. À partir de vSphere 7.0 Update 1, vous utilisez la fonctionnalité Corriger pour ajouter un hôte à un cluster approuvé. Dans vSphere 7.0 Update 1, vous devez toujours utiliser des scripts pour ajouter un hôte à un cluster d'autorité d'approbation existant. Reportez-vous à la section Ajout et suppression d'hôtes Autorité d'approbation vSphere .

Conditions préalables

L'instance de vCenter Server du cluster approuvé doit exécuter vSphere 7.0 Update 1 ou version ultérieure.

Si vous ajoutez un hôte ESXi disposant d'une version ESXi différente ou d'un type de matériel TPM différent de celui que vous avez configuré initialement pour le cluster approuvé, des étapes supplémentaires sont requises. Vous devez exporter et importer ces informations dans le cluster Autorité d'approbation vSphere . Reportez-vous aux sections Collecter des informations sur les hôtes ESXi et vCenter Server à approuver et Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.

Privilèges requis : voir les tâches d'ajout d'hôtes dans Privilèges requis pour les tâches courantes.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur d'autorité d'approbation.
3. Accédez à un cluster approuvé.
4. Dans l'onglet **Configurer**, sélectionnez **Configuration > Démarrage rapide**.
5. Cliquez sur **Ajouter** dans la carte **Ajouter des hôtes**.
6. Suivez les invites.
7. Dans l'onglet **Autorité d'approbation**, cliquez sur **Corriger**.
8. Pour vérifier que le cluster approuvé est sain, cliquez sur **Vérifier la santé**.

Ajouter un hôte à un cluster approuvé avec l'interface de ligne de commande

Vous pouvez ajouter des hôtes ESXi à un cluster approuvé existant à l'aide de la ligne de commande.

Une fois que vous avez initialement configuré un cluster approuvé, vous pouvez ajouter d'autres hôtes ESXi. Cependant, lorsque vous ajoutez l'hôte à un cluster approuvé, vous devez effectuer l'étape supplémentaire de correction. Lorsque vous corrigez le cluster approuvé, vous vous assurez que l'état de configuration souhaité correspond à sa configuration appliquée.

Dans la première version de Autorité d'approbation vSphere disponible dans vSphere 7.0, vous exécutez des scripts pour ajouter un hôte à un cluster approuvé existant. À partir de vSphere 7.0 Update 1, vous utilisez la fonctionnalité Corriger pour ajouter un hôte approuvé. Dans vSphere 7.0 Update 1, vous devez toujours utiliser des scripts pour ajouter un hôte à un cluster d'autorité d'approbation existant. Reportez-vous à la section Ajout et suppression d'hôtes Autorité d'approbation vSphere .

Conditions préalables

- L'instance de vCenter Server du cluster approuvé doit exécuter vSphere 7.0 Update 1 ou version ultérieure.
- PowerCLI 12.1.0 ou version ultérieure est requis.
- Privilèges requis : voir les tâches d'ajout d'hôtes dans Privilèges requis pour les tâches courantes.

Procédure

1. Utilisez les étapes normalement exécutées pour ajouter l'hôte ESXi au cluster approuvé.
2. Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu' administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster approuvé.

   ```
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
   ```

3. Pour vérifier l'état du cluster approuvé, exécutez l'applet de commande PowerCLI `Get-TrustedClusterAppliedStatus`.

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster '
   ```

4. Si le cluster approuvé n'est pas sain, exécutez l'applet de commande `Set-TrustedCluster` avec le paramètre `-Remediate`.

   ```
   Set-TrustedCluster -TrustedCluster 'TrustedCluster ' -Remediate
   ```

5. Pour vérifier que le cluster approuvé est sain, exécutez à nouveau l'applet de commande `Get-TrustedClusterAppliedStatus`.

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster '
   ```

Désaffectation d'hôtes approuvés d'un cluster approuvé

Vous pouvez supprimer ou désaffecter des hôtes approuvés d'un cluster approuvé. En fonction du scénario, vous pouvez désaffecter un ou tous les hôtes approuvés d'un cluster approuvé.

Lorsque vous désaffectez un hôte approuvé, la fonction Corriger définit l'état souhaité de l'hôte approuvé sur celui du cluster non approuvé dans lequel il est déplacé. L'hôte approuvé désactivé devient un hôte normal. Le cluster approuvé (à partir duquel l'hôte approuvé a été déplacé) continue de disposer de la configuration de l'état souhaité et fonctionne toujours en tant que cluster approuvé.

Lorsque vous supprimez tous les hôtes approuvés d'un cluster approuvé, vous désaffectez le cluster approuvé. Vous supprimez la configuration de l'état souhaité et la configuration appliquée des hôtes approuvés et du cluster approuvé, puis vous transférez tous les hôtes approuvés vers un cluster non approuvé.

Vous pouvez réutiliser des hôtes approuvés désaffectés dans votre environnement. Par exemple, vous pouvez réutiliser les hôtes dans une capacité d'infrastructure non approuvée ou en tant qu'hôtes Autorité d'approbation vSphere . Vous pouvez utiliser les hôtes désaffectés dans la même instance d evCenter Server ou dans une instance différente de vCenter Server.

Pour plus d'informations sur la configuration et la santé des clusters approuvés, consulte consultez Présentation de la santé et de la correction du cluster approuvé.

Conditions préalables

- L'instance de vCenter Server du cluster approuvé doit exécuter vSphere 7.0 Update 1 ou version ultérieure.
- Si vous utilisez PowerCLI, la version 12.1.0 ou une version ultérieure est requise.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur d'autorité d'approbation.
3. Accédez à un cluster approuvé.

4 Décidez comment désaffecter les hôtes approuvés du cluster approuvé.

Tâche	Étapes
Préserver l'état de configuration souhaité du cluster approuvé et des hôtes approuvés restants	a Mettez les hôtes en mode de maintenance et placez-les dans un nouveau cluster vide (c'est-à-dire que le cluster ne contient pas d'hôtes). b Sortez du mode de maintenance sur les hôtes. c Pour le nouveau cluster vide (pas le cluster approuvé), dans l'onglet **Autorité d'approbation**, cliquez sur **Corriger**. La correction supprime la configuration approuvée des hôtes déplacés. Le cluster approuvé conserve la configuration de l'état souhaité.

Supprimer l'état de configuration souhaité et l'état de configuration appliqué de tous les hôtes approuvés	a Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu' administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster approuvé.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Exécutez l'applet de commande `Set-TrustedCluster`, par exemple :
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster ' -State Disabled`
	La configuration de l'infrastructure approuvée est supprimée de tous les hôtes approuvés et la configuration de l'état souhaité du cluster approuvé est supprimée.
	c Mettez tous les hôtes en mode de maintenance et placez-les dans un autre cluster.
	d Sortez du mode de maintenance sur les hôtes.

5 Pour vérifier que le cluster approuvé est sain, cliquez sur **Vérifier la santé** dans l'onglet **Autorité d'approbation** pour le cluster approuvé.

Étape suivante

Si vous ne prévoyez plus d'attester des versions spécifiques de ESXi ou du matériel TPM à partir des hôtes ESXi désaffectés, mettez à jour la configuration du cluster d'autorité d'approbation pour une sécurité optimale. Consultez l'article de la base de connaissances de VMware à l'adresse https://kb.vmware.com/s/article/77146.

Sauvegarde de la configuration de Autorité d'approbation vSphere

Utilisez les fichiers que vous avez exportés lors de la configuration de Autorité d'approbation vSphere comme sauvegarde de votre autorité d'approbation. Vous pouvez utiliser ces fichiers pour restaurer un déploiement d'autorité d'approbation. Conservez ces fichiers de configuration confidentiels et transportez-les en toute sécurité.

La plupart des informations de configuration et d'état de Autorité d'approbation vSphere sont stockées sur les hôtes ESXi dans la base de données ConfigStore. L'interface de gestion de vCenter Server que vous utilisez pour sauvegarder une instance de vCenter Server ne sauvegarde pas les informations de configuration de Autorité d'approbation vSphere . Si vous

enregistrez et stockez en toute sécurité les fichiers de configuration que vous avez exportés lors de la configuration de votre environnement Autorité d'approbation vSphere , vous disposez des informations nécessaires pour restaurer une configuration de Autorité d'approbation vSphere . Reportez-vous à Collecter des informations sur les hôtes ESXi et vCenter Server à approuver si vous devez générer ces informations.

Modifier la clé principale d'un fournisseur de clés

Vous pouvez modifier la clé principale d'un fournisseur de clés, par exemple, lorsque vous souhaitez la rotation de la clé principale utilisée.

Pour obtenir des conseils sur le cycle de vie des clés, consultez Meilleures pratiques de chiffrement des machines virtuelles.

Conditions préalables

Créez et activez une clé sur le KMS à utiliser comme nouvelle clé principale pour le fournisseur de clés approuvé. Cette clé encapsule d'autres clés et secrets utilisés par ce fournisseur de clés approuvé. Pour plus d'informations sur la création de clés, consultez la documentation de votre fournisseur de KMS.

Procédure

1 Exécutez la commande `Set-TrustAuthorityKeyProvider`.

Par exemple :

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 Vérifiez l'état du fournisseur de clés.

a Attribuez l'information `Get-TrustAuthorityCluster` à une variable.

Par exemple :

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b Attribuez les informations de `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` à une variable.

Par exemple :

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c Vérifiez l'état du fournisseur de clés en exécutant `$kp.Status`.

Par exemple :

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

Un état de santé OK indique que le fournisseur de clés s'exécute correctement.

Résultats

La nouvelle clé principale est utilisée pour les nouvelles opérations de chiffrement. Les données chiffrées avec l'ancienne clé principale sont toujours déchiffrées à l'aide de l'ancienne clé.

Présentation des rapports d'attestation de l'hôte approuvé

Dans Autorité d'approbation vSphere , vCenter Server vérifie et signale l'état d'attestation de l'hôte approuvé. Vous pouvez utiliser vSphere Client pour afficher l'état d'attestation des hôtes approuvés.

Autorité d'approbation vSphere utilise l'attestation à distance pour les hôtes approuvés afin de prouver l'authenticité de leur logiciel démarré. L'attestation vérifie que les hôtes approuvés exécutent un logiciel VMware authentique ou un logiciel de partenaire signé par VMware. L'instance de vCenter Server du cluster approuvé communique avec l'hôte approuvé pour obtenir un rapport d'attestation interne. Le rapport d'attestation spécifie si l'hôte approuvé a attesté ou non avec le service d'attestation exécuté sur le cluster d'autorité d'approbation. Si l'hôte approuvé n'a pas attesté, le rapport d'attestation inclut également un message d'erreur. vSphere Client affiche les états d'attestation suivants pour les hôtes approuvés.

Effectué

L'hôte approuvé a attesté avec un service d'attestation Autorité d'approbation vSphere et le rapport d'attestation interne est accessible par vCenter Server.

Failed

L'hôte approuvé n'a pas pu attester avec un service d'attestation Autorité d'approbation vSphere . Le rapport d'attestation interne de vCenter Server contient l'erreur signalée par le service d'attestation avec lequel l'hôte approuvé a tenté d'attester.

vSphere Client indique également si un hôte a été attesté par Autorité d'approbation vSphere ou par vCenter Server.

Lorsqu'un hôte approuvé n'est pas attesté, les machines virtuelles, y compris les machines virtuelles chiffrées, exécutées sur l'hôte approuvé restent accessibles. Vous ne pouvez pas mettre sous tension des machines virtuelles sur un hôte approuvé non attesté. Cependant, vous pouvez toujours ajouter des machines virtuelles non chiffrées. Lorsqu'un hôte approuvé n'est pas attesté, prenez les mesures nécessaires pour résoudre le problème d'attestation. Pour plus d'informations sur les concepts d'attestation, consultez Flux de processus de l'autorité d'approbation vSphere.

Lorsque vous avez configuré plusieurs hôtes d'autorité d'approbation, plusieurs rapports d'attestation sont potentiellement disponibles sur chaque hôte. Lors de la génération d'un rapport d'état, vSphere Client affiche l'état du premier rapport « attesté » qu'il trouve. S'il n'y a aucun rapport « attesté », vSphere Client affiche l'erreur du premier rapport « non attesté » qu'il trouve.

Même si vous avez configuré plusieurs hôtes d'autorité d'approbation, vSphere Client affiche l'état et éventuellement un message d'erreur, à partir d'un seul rapport d'attestation.

Afficher l'état d'attestation du cluster approuvé

Vous pouvez afficher l'état de l'attestation d'un hôte approuvé à l'aide de vSphere Client.

Conditions préalables

- Les hôtes approuvés et les hôtes Autorité d'approbation vSphere doivent exécuter ESXi 7.0 Update 1 ou version ultérieure.
- Les hôtes de vCenter Server des clusters respectifs doivent exécuter vSphere 7.0 Update 1 ou version ultérieure.

Procédure

1. Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client.
2. Connectez-vous en tant qu'administrateur.

   Vous pouvez vous connecter en tant qu'administrateur d'autorité d'approbation ou administrateur de vSphere.
3. Accédez à un centre de données et cliquez sur l'onglet **Surveiller**.
4. Cliquez sur **Sécurité**.

5 Vérifiez l'état de l'hôte approuvé dans la colonne Attestation et lisez le message qui l'accompagne dans la colonne Message.

Étape suivante

En cas d'erreurs, consultez Résoudre les problèmes d'attestation d'hôte approuvé.

Résoudre les problèmes d'attestation d'hôte approuvé

Les rapports d'attestation de Autorité d'approbation vSphere fournissent un point de départ pour le dépannage des erreurs d'attestation d'hôte approuvé.

Procédure

1 Afficher l'état d'attestation du cluster approuvé.

2 Utilisez le tableau suivant pour dépanner et résoudre les erreurs.

Erreur	Cause et solution
Services d'attestation non configurés.	Les services d'attestation n'ont pas été configurés. Configurez l'hôte approuvé pour utiliser les services d'attestation à l'aide de l'action Corriger. Reportez-vous à la section Corriger un cluster approuvé.
Aucun périphérique TPM2 disponible.	Installez et configurez l'hôte approuvé pour utiliser un module TPM (Trusted Platform Module). Consultez la documentation du fabricant.
Impossible de récupérer la clé publique ou le certificat d'approbation TPM2.	Vérifiez que le module TPM est pris en charge et qu'il dispose d'une clé d'approbation valide. Vous devrez peut-être contacter le support VMware.
Le rapport d'attestation n'est pas disponible.	Il est possible que l'hôte approuvé n'ait pas terminé l'attestation. Patientez quelques minutes, puis revérifiez l'état de l'attestation.
La version du service d'attestation est incompatible avec la demande.	Mettez à jour l'hôte d'autorité d'approbation exécutant le service d'attestation pour vSphere 7.0 Update 1 ou version ultérieure.
Échec de l'attestation, car le démarrage sécurisé n'est pas activé.	Vérifiez que l'hôte approuvé est configuré pour utiliser le démarrage sécurisé. Reportez-vous à la section Démarrage sécurisé UEFI des hôtes ESXi.
L'attestation n'est pas parvenue à identifier la version du logiciel distant.	Importez les informations de l'image de base de l'hôte approuvé dans le service d'attestation. Reportez-vous à la section Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
Échec de l'attestation, car un certificat TPM est requis.	Vérifiez que le module TPM est pris en charge. Vous pouvez également exécuter l'applet de commande PowerCLI suivante pour modifier com.vmware.esx.attestation.tpm2.settings et définir `requireCertificateValidation` sur `false`. `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`

Erreur	Cause et solution
Échec de l'attestation en raison d'un TPM inconnu.	Importez la clé d'approbation TPM dans les services d'attestation. Reportez-vous à la section Importer les informations de l'hôte approuvé dans le cluster d'autorité d'approbation.
Erreur : vapi.send.failed.	Le service kmxa peut ne pas s'exécuter sur l'hôte approuvé ou le service kmxa ne peut pas contacter le service d'attestation. Assurez-vous que le service kmxa a démarré. Vérifiez également que le service d'attestation est en cours d'exécution. Reportez-vous à la section Redémarrer le service d'hôte approuvé.

Vérification et correction de la santé d'un cluster approuvé

Vous pouvez vérifier et valider la santé d'un cluster approuvé. Lorsque des problèmes surviennent avec la santé d'un cluster approuvé, vous pouvez corriger la configuration de ce cluster approuvé.

Présentation de la santé et de la correction du cluster approuvé

Si la configuration d'un cluster approuvé n'est pas saine, vous devez résoudre les incohérences de configuration. Pour ce faire, vous devez corriger le cluster approuvé. Lorsque vous corrigez un cluster approuvé, vous vous assurez que tous les hôtes approuvés dans le cluster approuvé ont la même configuration de confiance.

Un cluster approuvé se compose d'un cluster vCenter Server d'hôtes ESXi approuvés qui sont attestés à distance par le cluster d'autorité d'approbation. Lorsque vous configurez initialement Autorité d'approbation vSphere , vous devez importer les informations des services d'autorité d'approbation de votre cluster d'autorité d'approbation dans le cluster approuvé. Le cluster approuvé utilise cette configuration de composants pour contacter le service de fournisseur de clés et le service d'attestation s'exécutant sur le cluster d'autorité d'approbation. Pour plus d'informations sur la configuration d'un cluster approuvé, consultez Importer les informations du cluster d'autorité d'approbation sur les hôtes approuvés. Après avoir configuré un cluster approuvé, vous pouvez vérifier et corriger sa santé.

Présentation de la santé du cluster approuvé

La vérification de la santé d'un cluster approuvé dépend des éléments suivants.

Configuration de l'état souhaité

La configuration de l'état souhaité est basée sur les informations des services d'autorité d'approbation que vous importez dans le cluster approuvé. La configuration de l'état souhaité est la « source de vérité » du cluster approuvé. Considérez la configuration de l'état souhaité comme ce qui est initialement créé lorsque vous configurez le cluster approuvé.

Configuration appliquée

La configuration appliquée est l'enregistrement des services d'attestation et des services de fournisseur de clés spécifiques pour lesquels vous avez configuré le cluster approuvé. La configuration appliquée est celle à laquelle le cluster approuvé s'exécute actuellement.

Vous pouvez considérer la configuration appliquée comme la configuration « exécution ». La configuration de l'état souhaité doit correspondre à la configuration appliquée. Cependant, si la configuration appliquée est incohérente avec la configuration de l'état souhaité, le cluster approuvé est considéré comme « non sain ». Un cluster approuvé qui n'est pas sain peut subir des performances dégradées ou ne pas fonctionner du tout.

Ce contrôle de santé n'est pas un indicateur de santé globale d'un cluster approuvé ou de l'infrastructure Autorité d'approbation vSphere . Le contrôle de santé compare uniquement la configuration de l'état souhaité du cluster approuvé à la configuration appliquée.

Présentation de la correction de cluster approuvé

La correction est le processus par lequel Autorité d'approbation vSphere résout une configuration incohérente d'un cluster approuvé. La configuration d'un cluster approuvé peut devenir incohérente dans le temps ou en raison d'autres erreurs opérationnelles.

Utilisez la correction de la manière suivante :

- Vérifiez la santé du cluster approuvé.
- Si le cluster approuvé est défectueux, corrigez-le.

Vous pouvez utiliser vSphere Client ou l'interface de ligne de commande pour vérifier la santé du cluster approuvé. Voir Vérifier la santé du cluster approuvé. Vous pouvez également utiliser vSphere Client ou l'interface de ligne de commande pour corriger un cluster approuvé. Reportez-vous à la section Corriger un cluster approuvé.

Note La correction est également le processus approprié à utiliser lorsque vous ajoutez un hôte à un cluster approuvé existant. Reportez-vous aux sections Ajouter un hôte à un cluster approuvé avec vSphere Client et Ajouter un hôte à un cluster approuvé avec l'interface de ligne de commande.

Vérifier la santé du cluster approuvé

Vous pouvez vérifier l'état de santé d'un cluster approuvé à l'aide de vSphere Client ou de la ligne de commande.

Pour plus d'informations, consultez Présentation de la santé et de la correction du cluster approuvé.

Conditions préalables

- L'instance de vCenter Server du cluster approuvé doit exécuter vSphere 7.0 Update 1 ou version ultérieure.
- Si vous utilisez PowerCLI, la version 12.1.0 ou une version ultérieure est requise.

Procédure

1 Vérifiez la santé du cluster approuvé.

Outil	Étapes
vSphere Client	a Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client. b Connectez-vous en tant qu'administrateur d'autorité d'approbation. c Accédez à un cluster approuvé, sélectionnez **Configurer**, puis sélectionnez **Autorité d'approbation**. d Cliquez sur **Vérifier la santé**.

CLI	a Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu' administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster approuvé.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b Exécutez l'applet de commande `Get-TrustedClusterAppliedStatus`, par exemple :
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster '`

2 En cas d'erreurs, consultez Corriger un cluster approuvé.

Corriger un cluster approuvé

Vous pouvez corriger la configuration d'un cluster approuvé à l'aide de vSphere Client ou de la ligne de commande.

Conditions préalables

L'instance de vCenter Server du cluster approuvé doit exécuter vSphere 7.0 Update 1 ou version ultérieure.

Procédure

1 Connectez-vous à l'instance de vCenter Server du cluster approuvé.

Outil	Étapes
vSphere Client	a Connectez-vous à l'instance de vCenter Server du cluster approuvé à l'aide de vSphere Client. b Connectez-vous en tant qu'administrateur d'autorité d'approbation.
CLI	Dans une session PowerCLI, exécutez l'applet de commande `Connect-VIServer` pour vous connecter en tant qu' administrateur de l'autorité d'approbation à l'instance de vCenter Server du cluster approuvé. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2 Corrigez le cluster approuvé, puis revérifiez la santé du cluster approuvé.

Outil	Étapes
vSphere Client	a Accédez à un cluster approuvé. b Sélectionnez **Configurer**, puis sélectionnez **Autorité d'approbation**. c Cliquez sur **Corriger**. d Cliquez sur **Vérifier la santé**.

CLI	a Exécutez l'applet de commande `Set-TrustedCluster` avec le paramètre `-Remediate`, par exemple :
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster ' -Remediate`
	b Exécutez l'applet de commande `Get-TrustedClusterAppliedStatus`, par exemple :
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster '`

Utiliser le chiffrement dans votre environnement vSphere

10

Que vous utilisiez un fournisseur de clés standard, un fournisseur de clés approuvé ou vSphere Native Key Provider, l'utilisation du chiffrement dans votre environnement vSphere nécessite une certaine préparation.

Après avoir configuré votre environnement, vous pouvez utilisez vSphere Client pour créer des machines virtuelles et des disques virtuels chiffrés et chiffrer les machines virtuelles et les disques existants.

Vous pouvez effectuer d'autres tâches à l'aide de l'API et de l'interface de ligne de commande `crypto-util`. Consultez *Guide de programmation de vSphere Web Services SDK* pour obtenir de la documentation sur l'API et l'aide de la ligne de commande `crypto-util` pour plus d'informations sur cet outil.

Créer une stratégie de stockage de chiffrement

Avant de pouvoir créer des machines virtuelles chiffrées, vous devez créer une stratégie de stockage de chiffrement. Vous créez la stratégie de stockage une fois, puis vous l'attribuez à chaque fois que vous chiffrez une machine virtuelle ou un disque virtuel.

Si vous souhaitez utiliser le chiffrement de machine virtuelle avec d'autres filtres d'E/S ou utiliser l'assistant de **création de stratégie de stockage VM** dans vSphere Client, consultez la documentation *Stockage vSphere* pour plus de détails.

Conditions préalables

- Configurez la connexion au certificat KMS.

  Bien qu'il soit possible de créer une stratégie de stockage de chiffrement de machine virtuelle sans connexion existante au certificat KMS, vous ne pouvez pas effectuer de tâche de chiffrement tant qu'une connexion de confiance n'a pas été établie avec le serveur KMS.
- Privilèges requis : **Opérations cryptographiques.Gérer les stratégies de chiffrement**.

Procédure

1. Connectez-vous à vCenter Server en utilisant vSphere Client.
2. Sélectionnez **Accueil**, cliquez sur **Stratégies et profils**, puis cliquez sur **Stratégies de stockage de machine virtuelle**.

3 Cliquez sur **Créer une stratégie de stockage de machine virtuelle**.

4 Spécifiez les valeurs de la stratégie de stockage.

   a Entre un nom de stratégie de stockage et une description facultative, puis cliquez sur **Suivant**.

   b Si vous n'êtes pas familiarisé avec cet assistant, étudiez les informations sur la **Structure de la stratégie**, puis cliquez sur **Suivant**.

   c Cochez la case **Utiliser les règles communes dans la stratégie de stockage de machine virtuelle**.

   d Cliquez sur **Ajouter un composant** et sélectionnez **Chiffrement > Propriétés de chiffrement par défaut**, puis cliquez sur **Suivant**.

   Dans la plupart des cas, les propriétés par défaut sont appropriées. Vous n'aurez besoin d'une stratégie personnalisée que si vous souhaitez associer le chiffrement à d'autres fonctionnalités telles que la mise en cache ou la réplication.

   e Décochez la case **Utiliser les ensembles de règles dans la stratégie de stockage** et cliquez sur **Suivant**.

   f Sur la page **Compatibilité du stockage**, laissez l'option Compatible sélectionnée, sélectionnez une banque de données, puis cliquez sur **Suivant**.

   g Passez vos informations en revue et cliquez sur **Terminer**.

Activer explicitement le mode de chiffrement de l'hôte

Le mode de chiffrement de l'hôte doit être activé si vous souhaitez effectuer des tâches de chiffrement, par exemple pour créer une machine virtuelle chiffrée sur un hôte ESXi. Dans la plupart des cas, le mode de chiffrement de l'hôte est automatiquement activé lorsque vous effectuez une tâche de chiffrement.

L'activation explicite du mode de chiffrement est parfois nécessaire. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.

Conditions préalables

Privilège requis : **Cryptographic operations.Register host**

Procédure

1 Connectez-vous à vCenter Server en utilisant vSphere Client.

2 Accédez à l'hôte ESXi et cliquez sur **Configurer**.

3 Dans Système, cliquez sur **Profil de sécurité**.

4 Cliquez sur **Modifier** dans le panneau Mode de chiffrement de l'hôte.

5 Sélectionnez **Activé** et cliquez sur **OK**.

Désactiver le mode de chiffrement de l'hôte

Le mode de chiffrement d'hôte est automatiquement activé lorsque vous effectuez une tâche de chiffrement, si l'utilisateur dispose des privilèges suffisants pour activer le mode de chiffrement. Une fois le mode de chiffrement de l'hôte activé, tous les vidages de mémoire sont chiffrés afin d'éviter que des informations sensibles ne soient communiquées au personnel d'assistance. Si vous n'utilisez plus le chiffrement des machines virtuelles avec un hôte ESXi, vous pouvez désactiver le mode de chiffrement manuellement ou à l'aide de l'API publique.

Cette tâche décrit la désactivation manuelle du mode de chiffrement de l'hôte. À partir de vSphere 7.0, vous pouvez utiliser l'API pour désactiver le mode de chiffrement de l'hôte. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Procédure

1. Annulez l'enregistrement de toutes les machines virtuelles chiffrées à partir de l'hôte dont vous souhaitez désactiver le mode de chiffrement.
2. Annulez l'enregistrement de l'hôte auprès de vCenter Server.
3. (Facultatif) Si l'hôte est dans un cluster, annulez l'enregistrement des autres hôtes pour lesquels le chiffrement est activé dans ce cluster.
4. Redémarrez tous les hôtes dont l'enregistrement avait été annulé.
5. Enregistrez à nouveau les hôtes auprès de vCenter Server.

Résultats

Le mode de chiffrement de l'hôte est désactivé tant que vous n'ajoutez pas de machines virtuelles chiffrées.

Créer une machine virtuelle chiffrée

Une fois le KMS configuré, vous pouvez créer des machines virtuelles chiffrées.

Cette tâche décrit comment créer une machine virtuelle chiffrée à l'aide de vSphere Client. vSphere Client filtre par stratégies de stockage de chiffrement des machines virtuelles, ce qui facilite la création de machines virtuelles chiffrées.

Note La création d'une machine virtuelle chiffrée est plus rapide et consomme moins de ressources de stockage que le chiffrement d'une machine virtuelle existante. Si possible, chiffrez les machines virtuelles pendant le processus de création.

Conditions préalables

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement ou utilisez l'exemple fourni (Stratégie de chiffrement des machines virtuelles).

- Assurez-vous que la machine virtuelle est hors tension.
- Vérifiez que vous disposez des privilèges requis.
  - **Opérations de chiffrement.Chiffrer un nouvel élément**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Cliquez avec le bouton droit sur l'objet et sélectionnez **Nouvelle machine virtuelle**.
4. Suivez les invites pour créer une machine virtuelle chiffrée.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom unique et un emplacement cible pour la machine virtuelle.
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous avez des privilèges de création de machines virtuelles. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.
Sélectionner le stockage	Cochez la case **Chiffrer cette machine virtuelle**. Les stratégies de stockage de machine virtuelle incluant le chiffrement s'affichent. Sélectionnez une stratégie de stockage de machine virtuelle (l'échantillon groupé est la stratégie de chiffrement de VM), puis sélectionnez une banque de données compatible.
Sélectionner une compatibilité	Sélectionnez la compatibilité. Vous ne pouvez faire migrer une machine virtuelle chiffrée que sur les hôtes compatibles avec ESXi 6.5 ou une version plus récente.
Sélectionner un système d'exploitation client	Sélectionnez le système d'exploitation invité sur lequel vous prévoyez d'installer ultérieurement la machine virtuelle.
Personnalisation du matériel	Personnalisez le matériel. Par exemple, changez la taille du disque ou le CPU. (Facultatif) Sélectionnez l'onglet **Options de VM** et développez **Chiffrement**. Sélectionnez les disques à exclure du chiffrement. Lorsque vous désélectionnez un disque, seuls Accueil VM Home et les autres disques sélectionnés sont chiffrés. Tout nouveau disque dur que vous ajoutez est chiffré. Vous pouvez modifier la stratégie de stockage de certains disques par la suite, si nécessaire.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Cloner une machine virtuelle chiffrée

Lors du clonage d'une machine virtuelle chiffrée, le clone est chiffré avec les mêmes clés. Pour modifier les clés du clone, procédez à un rechiffrement du clone au moyen de l'API. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Vous pouvez effectuer les opérations suivantes lors du clonage.

- Créer une machine virtuelle chiffrée à partir d'une machine virtuelle ou d'un modèle de machine virtuelle non chiffré.
- Créer une machine virtuelle non chiffrée à partir d'une machine virtuelle ou d'un modèle de machine virtuelle chiffré.
- Rechiffrer la machine virtuelle de destination avec différentes clés parmi celles de la machine virtuelle source.

Vous pouvez créer un clone instantané de machine virtuelle à partir d'une machine virtuelle chiffrée avec l'inconvénient que le clone instantané partage la même clé avec la machine virtuelle source. Vous ne pouvez pas rechiffrer les clés sur la machine virtuelle source ou le clone instantané de machine virtuelle. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Conditions préalables

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement ou utilisez l'exemple fourni (Stratégie de chiffrement des machines virtuelles).
- Privilèges requis :
  - **Opérations de chiffrement.Cloner**
  - **Opérations de chiffrement.Chiffrer**
  - **Opérations de chiffrement.Déchiffrer**
  - **Opérations de chiffrement.Rechiffrer**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également disposer de privilèges **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1. Accédez à la machine virtuelle dans l'inventaire de vSphere Client.

2 Pour créer un clone d'une machine chiffrée, cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **Cloner > Cloner une Machine virtuelle** et suivez les invites.

Option	Action
Sélectionner un nom et un dossier	Indiquez le nom et l'emplacement cible du clone.
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous avez des privilèges de création de machines virtuelles. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.
Sélectionner le stockage	Effectuez une sélection dans le menu **Sélectionner un format de disque virtuel** et sélectionnez une banque de données. Vous pouvez modifier la stratégie de stockage dans le cadre de l'opération de clonage. Par exemple, si vous choisissez de basculer d'une stratégie de chiffrement à une stratégie de non-chiffrement, cela aura pour effet de déchiffrer les disques.
Sélectionner les options du clone	Sélectionnez des options de clone, comme abordé dans la documentation de *Administration d'une machine virtuelle vSphere*.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

3 (Facultatif) Modifiez les clés de la machine virtuelle clonée.

Par défaut, la machine virtuelle clonée est créée avec les mêmes clés que son parent. Il est recommandé de modifier les clés de la machine virtuelle clonée pour vous assurer que plusieurs machines virtuelles ne disposent pas des mêmes clés.

a Décidez d'un rechiffrement superficiel ou approfondi.

Pour utiliser un autre clé DEK et KEK, effectuez un rechiffrement approfondi de la machine virtuelle clonée. Pour utiliser une clé KEK différente, effectuez un rechiffrement superficiel de la machine virtuelle clonée. Pour un rechiffrement approfondi, vous devez mettre hors tension la machine virtuelle. Vous pouvez effectuer une opération de rechiffrement superficielle alors que la machine virtuelle est sous tension et si des snapshots sont présents sur la machine virtuelle. Le rechiffrement superficiel d'une machine virtuelle chiffrée avec des snapshots n'est autorisé que sur une seule branche de snapshot (chaîne de disques). Plusieurs branches de snapshot ne sont pas prises en charge. Si le rechiffrement superficiel échoue avant la mise à jour de tous les liens de la chaîne avec la nouvelle clé KEK, vous pouvez toujours accéder à la machine virtuelle chiffrée si vous disposez de l'ancienne et de la nouvelle clé KEK.

b Effectuez un rechiffrement du clone à l'aide de l'API. Reportez-vous à la section *Guide de programmation de vSphere Web Services SDK*.

Chiffrer une machine virtuelle ou un disque virtuel existant

Vous pouvez chiffrer une machine ou un disque virtuel existant en modifiant sa stratégie de stockage. Vous ne pouvez chiffrer les disques virtuels que pour les machines virtuelles qui sont elles-mêmes chiffrées.

Cette tâche décrit comment chiffrer une machine virtuelle ou un disque virtuel existant à l'aide de vSphere Client.

Chiffrement des machines virtuelles dans vSphere Client (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_encrypt)

Conditions préalables

- Établissez une connexion de confiance avec le serveur KMS et sélectionnez un serveur KMS par défaut.
- Créez une stratégie de stockage de chiffrement ou utilisez l'exemple fourni (Stratégie de chiffrement des machines virtuelles).
- Assurez-vous que la machine virtuelle est hors tension.
- Vérifiez que vous disposez des privilèges requis.
  - **Opérations de chiffrement.Chiffrer un nouvel élément**
  - Si le mode de chiffrement de l'hôte n'est pas Activé, vous devez également **Opérations de chiffrement.Enregistrer un hôte**.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle à modifier et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

   Vous pouvez définir la stratégie de stockage des fichiers de machines virtuelles, représentée par Accueil VM, ainsi que la stratégie de stockage des disques virtuels.
3. Modifiez la stratégie de stockage.
   - Pour chiffrer la machine virtuelle et ses disques durs, sélectionnez une stratégie de stockage de chiffrement et cliquez sur **OK**.
   - Pour chiffrer la machine virtuelle sans chiffrer les disques virtuels, activez **Configurer par disque**, sélectionnez la stratégie de stockage de chiffrement pour Accueil VM et les autres stratégies de stockage des disques virtuels, puis cliquez sur **OK**.

   Vous ne pouvez pas chiffrer le disque virtuel d'une machine virtuelle non chiffrée.
4. Si vous préférez, vous pouvez chiffrer la machine virtuelle, ou la machine virtuelle et les disques, dans le menu **Modifier les paramètres** dans vSphere Client.
   a. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
   b. Sélectionnez l'onglet **Options de VM** et ouvrez **Chiffrement**. Choisissez une stratégie de chiffrement. Si vous désélectionnez tous les disques, seul l'accueil de VM est chiffré.
   c. Cliquez sur **OK**.

Déchiffrer une machine ou un disque virtuel

Vous pouvez déchiffrer une machine virtuelle, ses disques ou les deux, en modifiant la stratégie de stockage.

Cette tâche décrit comment déchiffrer une machine virtuelle chiffrée à l'aide de vSphere Client.

Toutes les machines virtuelles chiffrées nécessitent le paramètre vMotion chiffré. Pendant le processus de déchiffrement des machines virtuelles, le paramètre vMotion chiffré demeure. Vous devez modifier ce paramètre de façon explicite, afin que l'option vMotion chiffré ne soit plus utilisée.

Cette tâche explique comment procéder au déchiffrement au moyen des stratégies de stockage. Avec les disques virtuels, vous pouvez également procéder au déchiffrement depuis le menu **Modifier les paramètres**.

Conditions préalables

- La machine virtuelle doit être chiffrée.
- La machine virtuelle doit être hors tension ou en mode de maintenance.
- Privilèges requis : **Opérations de chiffrement.Déchiffrer**

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle à modifier et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

   Vous pouvez définir la stratégie de stockage des fichiers de machines virtuelles, représentée par Accueil VM, ainsi que la stratégie de stockage des disques virtuels.
3. Sélectionnez une stratégie de stockage.
   - Pour déchiffrer la machine virtuelle et ses disques durs, désactivez **Configurer par disque**, sélectionnez une stratégie de stockage dans le menu déroulant et cliquez sur **OK**.
   - Pour déchiffrer un disque virtuel, mais pas la machine virtuelle, activez **Configurer par disque**, sélectionnez la stratégie de stockage de chiffrement pour Accueil VM et d'autres stratégies de stockage pour les disques virtuels et cliquez sur **OK**.

   Vous ne pouvez pas déchiffrer la machine virtuelle et laisser le disque dur chiffré.
4. Si vous préférez, vous pouvez utiliser vSphere Client pour déchiffrer la machine virtuelle et les disques dans le menu **Modifier les paramètres**.
   a. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
   b. Sélectionnez l'onglet **Options de VM** et développez **Chiffrement**.
   c. Pour déchiffrer la machine virtuelle et ses disques durs, choisissez **Aucun** dans le menu déroulant **Chiffrement de machine virtuelle**.

d Pour déchiffrer un disque virtuel, mais pas la machine virtuelle, désélectionnez le disque.

e Cliquez sur **OK**.

5 (Facultatif) Vous pouvez modifier le paramètre vMotion chiffré.

a Cliquez avec le bouton droit sur la machine virtuelle et cliquez sur **Modifier les paramètres**.

b Cliquez sur **Options VM** et ouvrez la section **Chiffrement**.

c Définissez la valeur de **vMotion chiffré**.

Modifier la stratégie de chiffrement des disques virtuels

Lorsque vous créez une machine virtuelle chiffrée depuis vSphere Client, vous pouvez choisir les disques virtuels à chiffrer parmi ceux que vous ajoutez pendant le processus de création. Vous pouvez déchiffrer des disques virtuels avec l'option **Modifier les stratégies de stockage VM**.

Note Une machine virtuelle chiffrée peut comporter des disques virtuels qui ne sont pas chiffrés. Cependant, une machine virtuelle chiffrée ne peut pas avoir de disques virtuels chiffrés.

Reportez-vous à la section Chiffrement des disques virtuels.

Cette tâche explique comment modifier la stratégie de chiffrement au moyen des stratégies de stockage. Vous pouvez également utiliser le menu **Modifier les paramètres** pour effectuer cette modification.

Conditions préalables

- Vous devez avoir le privilège **Opérations de chiffrement.Gérer les stratégies de chiffrement**.
- Assurez-vous que la machine virtuelle est hors tension.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Client.

2 Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Stratégies de VM > Modifier les stratégies de stockage VM**.

3 Modifier la stratégie de stockage.

- Pour modifier la stratégie de stockage pour la machine virtuelle et ses disques durs, sélectionnez une stratégie de stockage de chiffrement et cliquez sur **OK**.
- Pour chiffrer la machine virtuelle sans chiffrer les disques virtuels, activez **Configurer par disque**, sélectionnez la stratégie de stockage de chiffrement pour Accueil VM et les autres stratégies de stockage des disques virtuels, puis cliquez sur **OK**.

Vous ne pouvez pas chiffrer le disque virtuel d'une machine virtuelle non chiffrée.

4 Si vous préférez, vous pouvez modifier la stratégie de stockage dans le menu **Modifier les paramètres**.

   a Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

   b Cliquez sur l'onglet **Matériel virtuel**, développez un disque dur et sélectionnez une stratégie de chiffrement dans le menu déroulant.

   c Cliquez sur **OK**.

Résoudre les problèmes de clés manquantes

Dans certaines circonstances, l'hôte ESXi ne peut pas obtenir la clé (KEK) pour une machine virtuelle chiffrée ou un disque virtuel chiffré depuis vCenter Server. Dans ce cas, vous pouvez toujours annuler l'enregistrement ou recharger la machine virtuelle. Cependant, vous ne pouvez pas effectuer d'autres opérations de machine virtuelle comme la suppression de la machine virtuelle ou la mise sous tension de la machine virtuelle. Une alarme vCenter Server vous informe lorsqu'une machine virtuelle chiffrée est dans un état verrouillé. Vous pouvez déverrouiller une machine virtuelle chiffrée, verrouillée à l'aide de vSphere Client, après avoir pris les mesures nécessaires pour rendre les clés requises disponibles sur le cluster KMS.

Si la clé de la machine virtuelle n'est pas disponible, l'état de la machine virtuelle s'affiche comme étant non valide. La machine virtuelle ne peut pas se mettre sous tension. Si la clé de la machine virtuelle est disponible, mais qu'une clé pour un disque chiffré n'est pas disponible, l'état de la machine virtuelle ne s'affiche pas comme étant non valide. Toutefois, la machine virtuelle ne peut pas être mise sous tension et l'erreur suivante se produit :

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

Note La procédure suivante illustre les situations pouvant entraîner le verrouillage d'une machine virtuelle, le déclenchement des alarmes et des journaux d'événements correspondants s'affichant et ce qu'il convient de faire dans chaque cas.

Procédure

1 Si le problème provient de la connexion entre le système vCenter Server et le cluster KMS, une alarme de machine virtuelle est générée et un message d'erreur s'affiche dans le journal des événements .

   Vous devez rechercher manuellement les clés dans le fournisseur de clés et rétablir la connexion au cluster KMS. Lorsque le cluster KMS et les clés deviennent disponibles, déverrouillez les machines virtuelles verrouillées. Reportez-vous à la section Déverrouiller les machines virtuelles verrouillées. Vous pouvez également redémarrer l'hôte et réenregistrer la machine virtuelle afin de la déverrouiller après la restauration de la connexion.

Notez que la perte de connexion au cluster KMS ne verrouille pas automatiquement la machine virtuelle. La machine virtuelle passe à l'état verrouillé uniquement si les conditions suivantes sont réunies :

- La clé n'est pas disponible sur l'hôte ESXi.
- vCenter Server ne peut pas récupérer les clés dans le cluster KMS.

Après chaque redémarrage, un hôte ESXi doit pouvoir atteindre vCenter Server. vCenter Server demande la clé avec l'ID correspondant au cluster KMS et la rend disponible pour ESXi.

Si, après la restauration de la connexion avec le fournisseur de clés, la machine virtuelle reste verrouillée, reportez-vous à la section Déverrouiller les machines virtuelles verrouillées.

2 Si la connexion est restaurée, enregistrez la machine virtuelle. Si la connexion est restaurée et qu'une erreur se produit lorsque vous tentez d'enregistrer la machine virtuelle, vérifiez que vous disposez du privilège **Opérations de chiffrement.Enregistrer les VM** pour le système vCenter Server.

Ce privilège n'est pas requis pour la mise sous tension d'une machine virtuelle chiffrée si la clé est disponible. Ce privilège est requis pour l'enregistrement de la machine virtuelle si la clé doit être récupérée.

3 Si la clé n'est plus disponible sur le cluster KMS, une alarme de machine virtuelle est générée et un message d'erreur s'affiche dans le journal des événements .

Demandez à l'administrateur KMS de restaurer la clé. Un problème de clé inactive peut se produire si vous mettez sous tension une machine virtuelle qui a été supprimée de l'inventaire et qui n'a pas été enregistrée depuis longtemps. Cela se produit également si vous redémarrez l'hôte ESXi et que KMS n'est pas disponible.

a Récupérez l'ID de la clé en utilisant Managed Object Browser (MOB) ou vSphere API.

Récupérez l'`keyId` de `VirtualMachine.config.keyId.keyId`.

b Demandez à l'administrateur KMS de réactiver la clé qui est associée à cet ID de clé.

c Après la restauration de la clé, reportez-vous à la section Déverrouiller les machines virtuelles verrouillées.

Si la clé peut être restaurée sur KMS, vCenter Server la récupère et la transmet à l'hôte ESXi dès que celui-ci en a besoin.

4 Si KMS est accessible et que l'hôte ESXi est mis sous tension, mais que le système vCenter Server n'est pas disponible, suivez ces étapes pour déverrouiller les machines virtuelles.

   a Restaurez le système vCenter Server ou définissez un autre système vCenter Server, puis établissez une relation de confiance avec le cluster KMS.

   Vous devez utiliser le même nom de fournisseur de clés, mais l'adresse IP du cluster KMS peut être différente.

   b Réenregistrez toutes les machines virtuelles qui sont verrouillées.

   La nouvelle instance de vCenter Server récupère les clés de KMS et les machines virtuelles sont déverrouillées.

5 Si les clés sont manquantes uniquement sur l'hôte ESXi, une alarme de machine virtuelle est générée et le message suivant s'affiche dans le journal des événements :

   `La machine virtuelle est verrouillée, car il manque des clés sur l'hôte.`

   Le système vCenter Server peut récupérer les clés manquantes dans le fournisseur de clés. Aucune récupération manuelle des clés n'est requise. Reportez-vous à la section Déverrouiller les machines virtuelles verrouillées.

Déverrouiller les machines virtuelles verrouillées

Une alarme vCenter Server vous informe lorsqu'une machine virtuelle chiffrée est dans un état verrouillé. Vous pouvez déverrouiller une machine virtuelle chiffrée verrouillée à l'aide de vSphere Client (client basé sur HTML5) après avoir pris les mesures nécessaires pour rendre les clés requises disponibles sur le serveur KMS.

Conditions préalables

- Vérifiez que vous disposez des privilèges requis : **Opérations de chiffrementEnregistrer la VM**
- D'autres privilèges peuvent être requis pour des tâches facultatives, telles que l'activation du chiffrement de l'hôte.
- Avant de déverrouiller une machine virtuelle verrouillée, dépannez la cause du verrouillage et essayez de corriger le problème manuellement. Reportez-vous à la section Résoudre les problèmes de clés manquantes.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Client.

2 Accédez à l'onglet **Résumé** de la machine virtuelle.

   Lorsqu'une machine virtuelle est verrouillée, l'alarme Machine virtuelle verrouillée s'affiche.

3 Décidez si vous souhaitez accepter l'alarme ou réinitialiser l'alarme sur le vert, mais ne déverrouillez pas maintenant la machine virtuelle.

   Lorsque vous cliquez sur **Accepter** ou **Réinitialiser sur le vert**, l'alarme disparaît, mais la machine virtuelle reste verrouillée jusqu'à ce que vous la déverrouillez.

4 Accédez à l'onglet **Surveiller** de la machine virtuelle et cliquez sur **Événements** pour obtenir des informations supplémentaires sur la raison pour laquelle la machine virtuelle est verrouillée.

5 Effectuez le dépannage suggéré avant de déverrouiller la machine virtuelle.

6 Accédez à l'onglet **Résumé** de la machine virtuelle et cliquez sur **Déverrouiller la machine virtuelle**, sous la console de machine virtuelle.

   Un message s'affiche, indiquant que les données de la clé de chiffrement sont transmises à l'hôte.

7 Cliquez sur **Yes**.

Résoudre les problèmes du mode de chiffrement de l'hôte ESXi

Dans certaines circonstances, le mode de chiffrement de l'hôte ESXi peut se retrouver désactivé.

Un hôte ESXi nécessite que le mode de chiffrement de l'hôte soit activé s'il contient des machines virtuelles chiffrées. Si l'hôte détecte qu'il manque sa clé d'hôte ou si le fournisseur de clés n'est pas disponible, l'hôte peut échouer à activer le mode de chiffrement. vCenter Server génère une alarme lorsque le mode de chiffrement de l'hôte ne peut pas être activé.

Procédure

1 Si le problème provient de la connexion entre le système vCenter Server et le fournisseur de clés, une alarme est générée et un message d'erreur s'affiche dans le journal des événements .

   Vous devez rechercher manuellement les clés dans le fournisseur de clés et rétablir la connexion au fournisseur de clés.

2 Si des clés sont manquantes, une alarme est générée et un message d'erreur s'affiche dans le journal des événements.

   Vous devez récupérer manuellement les clés manquantes dans le fournisseur de clés.

Étape suivante

Si, après la restauration de la connexion au fournisseur de clés ou la récupération manuelle des clés dans le fournisseur de clés, le mode de chiffrement de l'hôte reste désactivé, réactivez-le. Reportez-vous à la section Réactiver le mode de chiffrement de l'hôte ESXi.

Réactiver le mode de chiffrement de l'hôte ESXi

À partir de vSphere 6.7, une alarme vCenter Server vous avertit lorsque le mode de chiffrement d'un hôte ESXi est désactivé. Vous pouvez réactiver le mode de chiffrement de l'hôte s'il a été désactivé.

Conditions préalables

- Vérifiez que vous disposez des privilèges requis : **Opérations de chiffrement.Enregistrer l'hôte**
- Avant de réactiver le nouveau mode de chiffrement, résolvez la cause du problème et essayez de corriger celui-ci manuellement.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Accédez à l'onglet **Résumé** de l'hôte ESXi.

   Lorsque le mode de chiffrement est désactivé, l'alarme L'hôte requiert l'activation du mode de chiffrement s'affiche.
3. Choisissez si vous souhaitez accepter l'alarme, ou réinitialisez celle-ci sur le vert, mais ne réactivez pas le mode de chiffrement de l'hôte maintenant.

   Lorsque vous cliquez sur **Accepter** ou **Réinitialiser sur le vert**, l'alarme s'arrête, mais le mode de chiffrement de l'hôte reste désactivé jusqu'à ce que vous le réactiviez.
4. Accédez à l'onglet **Surveiller** de l'hôte ESXi et cliquez sur **Événements** pour obtenir plus d'informations sur la raison pour laquelle le mode de chiffrement est désactivé.

   Effectuez le dépannage suggéré avant de réactiver le mode de chiffrement.
5. Sous l'onglet **Résumé**, cliquez sur **Activer le mode de chiffrement de l'hôte** pour réactiver le chiffrement de l'hôte.

   Un message s'affiche, indiquant que les données de la clé de chiffrement sont transmises à l'hôte.
6. Cliquez sur **Yes**.

Définir le seuil d'expiration du certificat du serveur KMS

Par défaut, vCenter Server vous informe 30 jours avant l'expiration des certificats de votre serveur de gestion des clés (KMS, Key Management Server). Vous pouvez modifier cette valeur par défaut.

Les certificats KMS ont une date d'expiration. Lorsque le seuil de la date d'expiration est atteint, une alarme vous en informe.

vCenter Server et les fournisseurs de clés échangent deux types de certificats : serveur et client. Le magasin VMware Endpoint Certificate Store (VECS) sur le système vCenter Server stocke les certificats de serveur et un certificat de client par le fournisseur de clés. Comme il y a deux types de certificats, deux alarmes existent : une pour chaque type de certificat (client et serveur).

Procédure

1. Connectez-vous à un système vCenter Server à l'aide de vSphere Client.
2. Sélectionnez le système vCenter Server dans la hiérarchie des objets.
3. Cliquez sur **Configurer**.
4. Sous **Paramètres**, cliquez sur **Paramètres avancés**, puis cliquez sur **Modifier les paramètres**.
5. Cliquez sur l'icône **Filtre** et entrez `vpxd.kmscert.threshold` ou faites défiler jusqu'au paramètre de configuration.
6. Entrez une valeur en jours, puis cliquez sur **Enregistrer**.

Chiffrement de machines virtuelles vSphere et vidages mémoire

Si votre environnement utilise le chiffrement de machines virtuelles vSphere et si une erreur se produit sur l'hôte ESXi, le vidage mémoire qui en résulte est chiffré pour protéger les données clients. Les vidages mémoire qui sont inclus dans le module vm-support sont également chiffrés.

Note Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la politique de votre organisation en matière de sécurité et de confidentialité lorsque vous gérez des vidages mémoire.

Vidages mémoire sur hôtes ESXi

Lorsqu'un hôte ESXi, un monde utilisateur ou une machine virtuelle échoue, un vidage de mémoire est généré, et l'hôte redémarre. Si le mode de chiffrement est activé sur l'hôte ESXi, le vidage de mémoire est chiffré à l'aide d'une clé qui se trouve dans le cache de la clé ESXi. Cette clé provient du KMS. Pour plus d'informations, reportez-vous à Méthodologie utilisée par le chiffrement de machine virtuelle vSphere pour protéger votre environnement.

Lorsqu'un hôte ESXi est « sécurisé » au niveau du chiffrement et qu'un vidage de mémoire est généré, un événement est créé. L'événement indique qu'un vidage de mémoire s'est produit avec les informations suivantes : nom de monde, heures de déclenchement, ID de clé utilisé pour chiffrer le vidage de mémoire et nom du fichier de vidage de mémoire. Vous pouvez afficher l'événement dans la visionneuse d'événements sous **Tâches et événements** pour vCenter Server.

Le tableau suivant affiche les clés de chiffrement utilisées pour chaque type de vidage de mémoire, par version de vSphere.

Tableau 10-1. Clés de chiffrement de vidage de mémoire

Type de vidage de mémoire	Clé de chiffrement (ESXi 6.5)	Clé de chiffrement (ESXi 6.7 et versions ultérieures)
Noyau ESXi	Clé de l'hôte	Clé de l'hôte
Monde utilisateur (hostd)	Clé de l'hôte	Clé de l'hôte
Machine virtuelle chiffrée	Clé de l'hôte	Clé de machine virtuelle

Ce que vous pouvez faire après le redémarrage d'un hôte ESXi dépend de plusieurs facteurs.

- Dans la plupart des cas, vCenter Server récupère la clé de l'hôte à partir du KMS et tente de transmettre la clé à l'hôte ESXi après le redémarrage. Si l'opération réussit, vous pouvez générer le module vm-support et vous pouvez déchiffrer ou rechiffrer le vidage mémoire. Reportez-vous à la section Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré.
- Si vCenter Server ne peut pas se connecter à l'hôte ESXi, vous devriez pouvoir récupérer la clé du KMS. Reportez-vous à la section Résoudre les problèmes de clés manquantes.
- Si l'hôte a utilisé une clé personnalisée et que cette clé diffère de la clé que vCenter Server transmet à l'hôte, vous ne pouvez pas manipuler le vidage mémoire. Évitez d'utiliser des clés personnalisées.

Vidages mémoire et modules vm-support

Lorsque vous contactez le support technique de VMware pour une erreur grave, votre représentant du support vous demande généralement de générer un module vm-support. Le module inclut des fichiers journaux et d'autres informations, notamment les vidages mémoire. Si votre représentant du support ne parvient pas à résoudre les problèmes en examinant les fichiers journaux et les autres informations, il peut vous demander de déchiffrer les vidages mémoire et de lui transmettre les informations pertinentes. Pour protéger les informations sensibles comme les clés, respectez la politique de votre organisation en matière de sécurité et de confidentialité. Reportez-vous à la section Collecter un module vm-support pour un hôte ESXi qui utilise le chiffrement.

Vidages mémoire sur systèmes vCenter Server

Un vidage mémoire sur un système vCenter Server n'est pas chiffré. vCenter Server contient déjà des informations potentiellement sensibles. Assurez-vous au minimum que le vCenter Server est protégé. Reportez-vous à la section Chapitre 4 Sécurisation des systèmes vCenter Server. Il peut également s'avérer utile de désactiver les vidages mémoire pour le système vCenter Server. Les autres informations contenues dans les fichiers journaux peuvent aider à déterminer le problème.

Collecter un module vm-support pour un hôte ESXi qui utilise le chiffrement

Si le mode de chiffrement de l'hôte est activé pour l'hôte ESXi, tout vidage de mémoire intervenant dans le module `vm-support` est chiffré. Vous pouvez collecter le module auprès de

vSphere Client. Vous pouvez également spécifier un mot de passe si vous prévoyez de déchiffrer le vidage de mémoire à une date ultérieure.

Le module `vm-support` inclut des fichiers journaux, des fichiers de vidage de mémoire, etc.

Conditions préalables

Informez votre représentant de l'assistance technique que le mode de chiffrement de l'hôte est activé pour l'hôte ESXi. Votre représentant de l'assistance technique vous demandera peut-être de déchiffrer les vidages de mémoire et d'extraire les informations appropriées.

Note Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la politique de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés des hôtes.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Cliquez sur **Hôtes et clusters**, puis cliquez avec le bouton droit de la souris sur l'hôte ESXi.
3. Sélectionnez l'option **Exporter les journaux système**.
4. Dans la boîte de dialogue, sélectionnez l'option **Mot de passe pour les vidages de mémoire chiffrés**, puis indiquez un mot de passe et confirmez-le.
5. Pour les autres options, conservez les paramètres par défaut ou effectuez des modifications si l'assistance technique VMware vous y invite, puis cliquez sur **Exportation des journaux**.
6. Indiquez l'emplacement du fichier.
7. Si votre représentant de l'assistance technique vous a demandé de déchiffrer le vidage de mémoire dans le module `vm-support`, connectez-vous à n'importe quel hôte ESXi et appliquez la procédure suivante.
   a. Connectez-vous à l'ESXi, puis au répertoire dans lequel se trouve le module `vm-support`.

      Le nom de fichier est de type esx.date_et_heure.tgz.

   b. Assurez-vous que le répertoire dispose de suffisamment d'espace pour le module, le module décompressé et le module recompressé, ou déplacez le module.

   c. Procédez à l'extraction du module dans le répertoire local.

      ```
      vm-support -x *.tgz .
      ```

      La hiérarchie de fichiers qui en résulte peut contenir des fichiers de vidage de mémoire pour l'hôte ESXi, en général dans `/var/core`. Elle peut contenir plusieurs fichiers de vidage de mémoire pour des machines virtuelles.

d Déchiffrez individuellement chaque fichier de vidage de mémoire chiffré.

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file est le fichier de clé d'incident se trouvant au niveau supérieur du répertoire.

encryptedZdump est le nom du fichier de vidage de mémoire chiffré.

decryptedZdump est le nom du fichier généré par la commande. Rendez le nom semblable à celui du fichier *encryptedZdump*.

e Fournissez le mot de passe que vous avez spécifié lors de la création du module `vm-support`.

f Supprimez les vidages de mémoire chiffrés et compressez à nouveau le module.

```
vm-support --reconstruct
```

8 Supprimez tout fichier contenant des informations confidentielles.

Déchiffrer ou chiffrer à nouveau un vidage de mémoire chiffré

Vous pouvez déchiffrer, ou chiffrer à nouveau, un vidage de mémoire chiffré sur votre hôte ESXi à l'aide de l'interface de ligne de commande `crypto-util`.

Vous pouvez vous-même déchiffrer et examiner les vidages de mémoire dans le module vm-support. Les vidages de mémoire peuvent contenir des informations sensibles. Suivez la stratégie de votre organisation en matière de sécurité et de confidentialité pour protéger les informations sensibles comme les clés.

Pour plus de détails sur le rechiffrement d'un vidage de mémoire et sur d'autres fonctionnalités de `crypto-util`, consultez l'aide de la ligne de commande.

Note `crypto-util` est destinée à des utilisateurs expérimentés.

Conditions préalables

La clé ayant servi à chiffrer le vidage de mémoire doit être disponible sur l'hôte ESXi qui a généré le vidage de mémoire.

Procédure

1 Connectez-vous directement à l'hôte ESXi sur lequel le vidage de mémoire s'est produit.

Si l'hôte ESXi est en mode de verrouillage, ou si l'accès SSH est désactivé, vous devrez peut-être commencer par activer l'accès.

2 Déterminez si le vidage de mémoire est chiffré.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope describe vmmcores.ve`
fichier zdump	`crypto-util envelope describe --offset 4096 zdumpFile`

3 Déchiffrez le vidage de mémoire; selon son type.

Option	Description
Surveiller le vidage de mémoire	`crypto-util envelope extract vmmcores.ve vmmcores`
fichier zdump	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

Activer ou désactiver la persistance de clé sur un hôte ESXi

Vous devez activer la persistance de clé sur un hôte ESXi. Elle n'est pas activée par défaut.

Pour des informations conceptuelles sur la persistance de clé, voir Présentation de la persistance des clés.

Conditions préalables

Conditions requises pour activer la persistance de clé :

- ESXi 7.0 mise à jour 2 ou supérieur
- Hôte ESXi installé avec TPM 2.0
- A accès à l'ensemble de commandes ESXCLI. Vous pouvez exécuter des commandes ESXCLI à distance ou les exécuter dans le ESXi Shell.

Pour plus de sécurité, le TPM peut également utiliser une stratégie de scellement pour empêcher la falsification lors du démarrage de l'hôte ESXi. Reportez-vous à la section Présentation des stratégies de scellement TPM.

Procédure

1 Utilisez SSH ou une autre connexion de console à distance pour démarrer une session sur l'hôte ESXi.

2 Connectez-vous en tant qu'utilisateur racine.

3 Activez ou désactivez la persistance de clé.

a Pour activer la persistance de clé :

```
esxcli system security keypersistence enable
```

b Pour désactiver la persistance de clé :

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

Sécurisation des machines virtuelles avec le TPM

11

Avec la fonctionnalité vTPM (Virtual Trusted Platform Module), vous pouvez ajouter un cryptoprocesseur virtuel TPM 2.0 à une machine virtuelle.

Un vTPM est une représentation logicielle d'une puce TPM 2.0 (Trusted Platform Module) physique. Un vTPM agit comme n'importe quel autre périphérique virtuel. Vous pouvez ajouter un vTPM à une machine virtuelle de la même manière que vous ajoutez des CPU virtuels, de la mémoire, des contrôleurs de disque ou des contrôleurs réseau. Un vTPM ne nécessite pas de puce TPM matérielle.

Ce chapitre contient les rubriques suivantes :

- Présentation du vTPM (Virtual Trusted Platform Module)
- Créer une machine virtuelle avec un vTPM (Virtual Trusted Platform Module)
- Activer le module de plate-forme sécurisée virtuel pour une machine virtuelle existante
- Supprimer le module de plate-forme sécurisée virtuel d'une machine virtuelle
- Identifier les machines virtuelles compatibles vTPM (Virtual Trusted Platform Module)
- Afficher les certificats des périphériques Virtual Trusted Platform Module
- Exporter et remplacer les certificats des périphériques Virtual Trusted Platform Module

Présentation du vTPM (Virtual Trusted Platform Module)

Un vTPM (Virtual Trusted Platform Module) est une représentation logicielle d'une puce TPM 2.0 (Trusted Platform Module) physique. Un vTPM agit comme n'importe quel autre périphérique virtuel.

Présentation des vTPM

Les vTPM fournissent des fonctions de sécurité basées sur le matériel, telles que la génération de nombres aléatoires, l'attestation, la génération de clés, etc. Lors de l'ajout à une machine virtuelle, un vTPM permet au système d'exploitation invité de créer et de stocker des clés privées. Ces clés ne sont pas exposées au système d'exploitation invité. Par conséquent, cela réduit la surface d'attaque de la machine virtuelle. En règle générale, si le système d'exploitation invité est compromis, les données secrètes qui s'y trouvent le sont également, mais l'activation

d'un vTPM réduit considérablement ce risque. Ces clés peuvent être utilisées uniquement par le système d'exploitation invité pour le chiffrement ou la signature. Avec un vTPM attaché, un tiers peut attester à distance (valider) de l'identité du microprogramme et du système d'exploitation invité.

Vous pouvez ajouter un vTPM aussi bien à une nouvelle machine virtuelle qu'à une machine virtuelle existante. Un vTPM varie en fonction du chiffrement de la machine virtuelle pour protéger les données de TPM stratégiques. Lorsque vous configurez un vTPM, les fichiers de la machine virtuelle sont chiffrés, mais pas les disques. Vous pouvez choisir d'ajouter le chiffrement de manière explicite pour la machine virtuelle et ses disques.

Lorsque vous sauvegardez une machine virtuelle activée avec un vTPM, la sauvegarde doit inclure toutes les données de machine virtuelle, y compris le fichier `*.nvram`. Si votre sauvegarde n'inclut pas le fichier `*.nvram`, vous ne pouvez pas restaurer une machine virtuelle avec un vTPM. De plus, étant donné que les fichiers de base de machine virtuelle d'une machine virtuelle activée avec un vTPM sont chiffrés, assurez-vous que les clés de chiffrement sont disponibles au moment de la restauration.

Un vTPM ne nécessite pas qu'une puce TPM 2.0 (Trusted Platform Module) physique soit présente sur l'hôte ESXi. Cependant, si vous souhaitez effectuer une attestation d'hôte, une entité externe, telle qu'une puce physique TPM 2.0, est requise. Reportez-vous à la section Sécurisation des hôtes ESXi avec un module de plate-forme sécurisée.

Note Par défaut, aucune stratégie de stockage n'est associée à une machine virtuelle qui a été activée avec un vTPM. Seuls les fichiers de machine virtuelle (Accueil VM) sont chiffrés. Si vous préférez, vous pouvez choisir d'ajouter le chiffrement explicite de la machine virtuelle et de ses disques, mais les fichiers de la machine virtuelle peuvent être déjà chiffrés.

Configuration requise pour un vTPM

Pour utiliser un vTPM, votre environnement vSphere doit répondre aux exigences suivantes :

- Configuration requise pour la machine virtuelle :
  - Micrologiciel EFI
  - Matériel version 14 ou ultérieure
- Configuration requise pour le composant :
  - vCenter Server 6.7 ou version ultérieure pour les machines virtuelles Windows, vCenter Server 7.0 Update 2 pour les machines virtuelles Linux.
  - Chiffrement de la machine virtuelle (pour chiffrer les fichiers de base de la machine virtuelle).
  - Fournisseur de clés configuré pour vCenter Server. Reportez-vous à la section Comparaison des fournisseurs de clés vSphere.
- Prise en charge du système d'exploitation invité :
  - Linux

- Windows Server 2008 et versions ultérieures
- Windows 7 et versions ultérieures

Différences entre un TPM matériel et un TPM virtuel

Vous utilisez un TPM (Trusted Platform Module) matériel afin de fournir un stockage sécurisé pour des informations d'identification ou des clés. Un vTPM offre les mêmes fonctions qu'un TPM, mais il fournit des capacités de coprocesseur cryptographique dans le logiciel. Un vTPM utilise le fichier `.nvram` (chiffré à l'aide du chiffrement de machine virtuelle) comme son espace de stockage sécurisé.

Un TPM matériel inclut une clé préchargée appelée Paire de clés de type EK. La paire de clés de type EK est composée d'une clé privée et d'une clé publique. La paire de clés de type EK fournit une identité unique au TPM. Pour un vTPM, cette clé est fournie par VMware Certificate Authority (VMCA) ou par une autorité de certification (CA) tierce. Après que le vTPM utilise une clé, celle-ci n'est généralement pas modifiée, car cela invalide des informations sensibles stockées dans le vTPM. Le vTPM ne contacte l'autorité de certification tierce à aucun moment.

Créer une machine virtuelle avec un vTPM (Virtual Trusted Platform Module)

Vous pouvez ajouter un vTPM (Virtual Trusted Platform Module) lorsque vous créez une machine virtuelle pour fournir une sécurité renforcée au système d'exploitation invité. Vous devez créer un fournisseur de clés avant de pouvoir ajouter un vTPM.

Le TPM virtuel de VMware est compatible avec TPM 2.0 et permet de créer une puce virtuelle compatible TPM pour la machine virtuelle et le système d'exploitation invité qu'elle héberge.

Conditions préalables

- Assurez-vous que votre environnement vSphere est configuré avec un fournisseur de clés. Pour plus d'informations, reportez-vous aux éléments suivants :
  - Configuration de Autorité d'approbation vSphere
  - Chapitre 7 Configuration et gestion d’un fournisseur de clés standard
  - Chapitre 8 Configuration et gestion de vSphere Native Key Provider
- Le système d'exploitation invité que vous utilisez peut être Windows Server 2008 et versions ultérieures, Windows 7 et versions ultérieures ou Linux.
- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être ESXi 6.7 ou version ultérieure (système d'exploitation invité Windows) ou 7.0 Update 2 (système d'exploitation invité Linux).
- La machine virtuelle doit utiliser le microprogramme EFI.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Cliquez avec le bouton droit sur l'objet, sélectionnez **Nouvelle machine virtuelle** et suivez les invites pour créer une machine virtuelle.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom et un emplacement cible
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous disposez des privilèges de création de machines virtuelles. Reportez-vous à la section Conditions préalables et privilèges requis pour les tâches de chiffrement.
Sélectionner le stockage	Sélectionnez une banque de données compatible.
Sélectionner une compatibilité	Vous devez sélectionner **ESXi 6.7 et versions ultérieures** pour le système d'exploitation invité Windows ou **ESXi 7.0 U2** et versions ultérieures pour le système d'exploitation invité Linux.
Sélectionner un système d'exploitation client	Sélectionnez Windows ou Linux pour l'utiliser comme système d'exploitation invité.
Personnalisation du matériel	Cliquez sur **Ajouter un périphérique** et sélectionnez **Trusted Platform Module**. Vous pouvez personnaliser le matériel. Par exemple, changez la taille du disque ou le CPU.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Résultats

La machine virtuelle avec vTPM activé s'affiche dans votre inventaire comme spécifié.

Activer le module de plate-forme sécurisée virtuel pour une machine virtuelle existante

Vous pouvez ajouter un vTPM (Virtual Trusted Platform Module) à une machine virtuelle existante pour mettre en œuvre une sécurité renforcée pour le système d'exploitation invité. Vous devez créer un fournisseur de clés avant de pouvoir ajouter un vTPM.

Le TPM virtuel de VMware est compatible avec TPM 2.0 et permet de créer une puce virtuelle compatible TPM pour la machine virtuelle et le SE invité qu'elle héberge.

Conditions préalables

- Assurez-vous que votre environnement vSphere est configuré pour un fournisseur de clés. Pour plus d'informations, reportez-vous aux éléments suivants :
  - Configuration de Autorité d'approbation vSphere

- Chapitre 7 Configuration et gestion d'un fournisseur de clés standard
- Chapitre 8 Configuration et gestion de vSphere Native Key Provider

- Le système d'exploitation invité que vous utilisez peut être Windows Server 2008 et versions ultérieures, Windows 7 et versions ultérieures ou Linux.
- Vérifiez si la machine virtuelle est désactivée.
- Les hôtes ESXi en cours d'exécution dans votre environnement doivent être ESXi 6.7 ou version ultérieure (système d'exploitation invité Windows) ou 7.0 Update 2 (système d'exploitation invité Linux).
- La machine virtuelle doit utiliser le microprogramme EFI.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.
3. Dans la boîte de dialogue **Modifier les paramètres**, cliquez sur **Ajouter un périphérique** et sélectionnez **Trusted Platform Module**.
4. Cliquez sur **OK**.

   L'onglet **Résumé** de la machine virtuelle inclut désormais le vTPM dans le volet **Matériel VM**.

Supprimer le module de plate-forme sécurisée virtuel d'une machine virtuelle

Vous pouvez supprimer la sécurité vTPM (Virtual Trusted Platform Module) d'une machine virtuelle.

Lors de la suppression d'un périphérique vTPM, toutes les informations chiffrées sur la machine virtuelle deviennent irrécupérables. Avant de supprimer un vTPM d'une machine virtuelle, désactivez toutes les applications dans le système d'exploitation invité utilisant le vTPM, telles que BitLocker. Dans le cas contraire, la machine virtuelle peut ne pas démarrer. En outre, vous ne pouvez pas supprimer un vTPM d'une machine virtuelle qui contient des snapshots.

Conditions préalables

Assurez-vous que la machine virtuelle est hors tension.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle dans l'inventaire que vous voulez modifier, puis sélectionnez **Modifier les paramètres**.
3. Dans la boîte de dialogue **Modifier les paramètres**, sélectionnez l'onglet **Matériel virtuel**, puis localisez l'entrée Trusted Platform Module.

4 Déplacez le curseur sur le périphérique et cliquez sur l'icône **Supprimer**.

   Cette icône apparaît uniquement pour le matériel virtuel que vous pouvez supprimer en toute sécurité.

5 Cliquez sur **Supprimer** pour confirmer la suppression du périphérique.

   Le périphérique vTPM est marqué pour suppression.

6 Cliquez sur **OK**.

   Vérifiez que l'entrée Virtual Trusted Platform Module ne figure plus dans l'onglet **Résumé** de la machine virtuelle, dans le volet **Matériel VM**.

Identifier les machines virtuelles compatibles vTPM (Virtual Trusted Platform Module)

Vous pouvez identifier les machines virtuelles qui sont activées pour l'utilisation d'un vTPM (Virtual Trusted Platform Module).

Vous pouvez générer une liste de toutes les machines virtuelles de votre inventaire, indiquant le nom de la machine virtuelle, le système d'exploitation et l'état de vTPM. Vous pouvez également exporter cette liste vers un fichier CSV pour l'utiliser dans des audits de conformité.

Procédure

1 Connectez-vous à vCenter Server à l'aide de vSphere Client.

2 Sélectionnez une instance de vCenter Server, un hôte ou un cluster.

3 Cliquez sur l'onglet **VM**, puis sur **Machines virtuelles**.

4 Cliquez sur la barre de menus d'une colonne de machine virtuelle, sélectionnez **Afficher/Masquer les colonnes**, puis **TPM**.

   La colonne TPM affiche Présent pour toutes les machines virtuelles sur lesquelles TPM est activé. Les machines virtuelles sans TPM sont répertoriées comme Pas présent.

5 Vous pouvez exporter le contenu d'une vue de liste d'inventaires vers un fichier CSV.

   a Cliquez sur **Exporter** dans le coin inférieur droit d'une vue de liste.

      La boîte de dialogue Exporter le contenu de la liste s'affiche et présente les options disponibles pour l'exportation vers le fichier CSV.

   b Décidez d'exporter vers le fichier CSV toutes les lignes ou seulement la sélection de lignes actuelle.

   c Parmi les options disponibles, sélectionnez les colonnes que vous souhaitez inclure au fichier CSV.

   d Cliquez sur **Exporter**.

      Le fichier CSV est généré et disponible au téléchargement.

Afficher les certificats des périphériques Virtual Trusted Platform Module

Les périphériques vTPM (Virtual Trusted Platform Module) sont préconfigurés avec des certificats par défaut, que vous pouvez examiner.

Conditions préalables

Pour cela, vous devez disposer d'une machine virtuelle compatible vTPM dans votre environnement.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Cliquez sur **VM**, puis sur **Machines virtuelles**.
4. Sélectionnez la machine virtuelle vTPM dont vous souhaitez afficher les informations de certificat.

   Si nécessaire, cliquez sur la barre de menus d'une colonne de machine virtuelle, sélectionnez **Afficher/Masquer les colonnes** et sélectionnez **TPM** pour afficher les machines virtuelles avec un TPM « Présent ».
5. Cliquez sur l'onglet **Configurer**.
6. Sous **TPM**, sélectionnez **Certificats**.
7. Sélectionnez le certificat et affichez ses informations.
8. (Facultatif) Pour exporter les informations du certificat, cliquez sur **Exporter**.

   Le certificat est enregistré sur le disque.

Étape suivante

Vous pouvez remplacer le certificat par défaut par un certificat émis par une autorité de certification tierce. Reportez-vous à la section Exporter et remplacer les certificats des périphériques Virtual Trusted Platform Module.

Exporter et remplacer les certificats des périphériques Virtual Trusted Platform Module

Vous pouvez remplacer le certificat par défaut fourni avec un périphérique vTPM (Virtual Trusted Platform Module).

Conditions préalables

Pour cela, vous devez disposer d'une machine virtuelle compatible vTPM dans votre environnement.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Sélectionnez la machine virtuelle compatible vTPM dans l'inventaire pour laquelle vous souhaitez remplacer les informations de certificat.
4. Cliquez sur l'onglet **Configurer**.
5. Sous **TPM**, sélectionnez **Demandes de signature**.
6. Sélectionnez un certificat.
7. Pour exporter les informations du certificat, cliquez sur **Exporter**.

   Le certificat est enregistré sur le disque.
8. Obtenez un certificat émis par une autorité de certification tierce pour la demande de signature de certificat que vous avez exportée.

   Vous pouvez utiliser n'importe quelle autorité de certification dont vous disposez dans votre environnement informatique.
9. Remplacez le certificat existant lorsque vous disposez du nouveau certificat.
   a. Cliquez avec le bouton droit dans l'inventaire sur la machine virtuelle pour laquelle vous voulez remplacer le certificat, puis sélectionnez **Modifier les paramètres**.
   b. Dans la boîte de dialogue **Modifier les paramètres**, développez **Périphériques de sécurité**, puis **Module de plate-forme sécurisée (TPM)**.

      Les certificats apparaissent.
   c. Cliquez sur **Remplacer** pour le certificat que vous souhaitez remplacer.

      La boîte de dialogue de **Téléchargement de fichier** s'ouvre.
   d. Sur votre machine locale, recherchez le nouveau certificat et téléchargez-le.

      Le nouveau certificat remplace le certificat par défaut fourni avec le périphérique vTPM.
   e. Le nom du certificat est mis à jour dans l'onglet **Résumé** de la machine virtuelle, sous la liste **Module de plate-forme sécurisée (TPM) virtuel**.

Sécurisation des systèmes d'exploitation invités Windows avec la sécurité basée sur la virtualisation

12

À partir de vSphere 6.7, vous pouvez activer la sécurité basée sur la virtualisation de Microsoft sur les systèmes d'exploitation invités Windows pris en charge.

La sécurité basée sur la virtualisation de Microsoft, fonctionnalité des systèmes d'exploitation Windows 10 et Windows Server 2016, utilise la virtualisation matérielle et logicielle afin d'améliorer la sécurité système en créant un sous-système spécialisé restreint par l'hyperviseur et isolé.

La sécurité basée sur la virtualisation de Microsoft vous autorise à utiliser les fonctionnalités de sécurité Windows suivantes pour renforcer votre système et isoler les clés système et les données secrètes de l'utilisateur contre tout risque de compromission :

- Protection des informations d'identification : vise à isoler et à renforcer la protection des clés système et des données secrètes de l'utilisateur contre la compromission.
- Protection du périphérique : fournit un ensemble de fonctionnalités conçues pour empêcher conjointement les programmes malveillants de s'exécuter sur un système Windows et de les éliminer.
- Intégrité du code configurable : garantit que seul un code approuvé s'exécute à partir du chargeur de démarrage.

Pour plus d'informations, consultez la rubrique sur la sécurité basée sur la virtualisation de dans la documentation Microsoft.

Après avoir activé la sécurité basée sur la virtualisation pour une machine virtuelle via vCenter Server, activez la sécurité basée sur la virtualisation au sein du système d'exploitation invité Windows.

Ce chapitre contient les rubriques suivantes :

- Recommandations sur la sécurité basée sur la virtualisation
- Activer la sécurité basée sur la virtualisation sur une machine virtuelle
- Activer la sécurité basée sur la virtualisation sur une machine virtuelle existante
- Activer la sécurité basée sur la virtualisation sur le système d'exploitation invité

- Désactiver la sécurité basée sur la virtualisation
- Identifier les machines virtuelles sur lesquelles la sécurité basée sur la virtualisation est activée

Recommandations sur la sécurité basée sur la virtualisation

Suivez les recommandations en matière de sécurité basée sur la virtualisation afin d'optimiser la sécurité et la facilité de gestion de votre environnement de système d'exploitation invité Windows.

Évitez les problèmes en suivant ces recommandations.

Matériel de sécurité basée sur la virtualisation

Utilisez le matériel suivant pour VBS :

- Intel
  - CPU Haswell ou versions ultérieures. Pour des performances optimales, utilisez la CPU Skylake-EP ou versions ultérieures.
  - Le CPU Ivy Bridge est acceptable.
  - Le CPU Sandy Bridge peut causer un ralentissement des performances.
- AMD
  - CPU de la série Zen 2 (Rome) ou version ultérieure.
  - Les CPU d'une version antérieure peuvent ralentir les performances.

Les atténuations de la vulnérabilité Exception de vérification de la machine sur la taille de page Modifier le CPU Intel peuvent avoir une incidence négative sur les performances du système d'exploitation invité lorsque VBS est utilisé. Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/76050.

Compatibilité du système d'exploitation invité Windows

VBS est pris en charge pour les machines virtuelles Windows 10, Windows Server 2016 et versions ultérieures, bien que les versions 1607 et 1703 de Windows Server 2016 requièrent des correctifs. Consultez la documentation Microsoft pour connaître la ESXi compatibilité matérielle de l'hôte. L'utilisation de CPU Intel pour VBS nécessite vSphere 6.7 ou version ultérieure et la version matérielle 14.

Sous AMD, VBS est pris en charge sur les machines virtuelles Windows 10, version 1809 et Windows 2019 et versions ultérieures. L'utilisation de CPU AMD pour VBS nécessite vSphere 7.0 Update 2 ou version ultérieure et la version matérielle 18.

Initialement, Windows 10 nécessitait que vous activiez Hyper-V pour VBS. L'activation d'Hyper-V n'est pas requise pour Windows 10. Il en va de même pour Windows Server 2016 et versions ultérieures. Pour plus d'informations, consultez la documentation Microsoft actuelle et les *Notes de mise à jour VMware vSphere*.

Fonctionnalités de VMware non pris en charge sur la sécurité basée sur la virtualisation

Les fonctionnalités suivantes ne sont pas prises en charge dans une machine virtuelle lorsque la sécurité basée sur la virtualisation est activée :

- Tolérance aux pannes
- Relais PCI
- Ajout à chaud de CPU ou de mémoire

Installation et mise à niveau de mises en garde avec la sécurité basée sur la virtualisation

Avant de configurer la sécurité basée sur la virtualisation, vous devez comprendre les mises en garde suivantes de l'installation et mise à niveau :

- Les nouvelles machines virtuelles configurées pour Windows 10 et Windows Server 2016 sur des versions matérielles virtuelles antérieures à la version 14 sont créées avec le BIOS hérité par défaut. Vous devez réinstaller le système d'exploitation invité après le changement du type de microprogramme de la machine virtuelle à partir du BIOS hérité sur l'UEFI.
- Si vous prévoyez de migrer vos machines virtuelles depuis les versions précédentes de vSphere vers vSphere 6.7 ou versions ultérieures et activer la sécurité basée sur la virtualisation sur vos machines virtuelles, utilisez l'UEFI pour éviter d'avoir à réinstaller le système d'exploitation.

Activer la sécurité basée sur la virtualisation sur une machine virtuelle

Vous pouvez activer la sécurité basée sur la virtualisation de Microsoft (VBS) pour les systèmes d'exploitation invités Windows pris en charge en même temps que vous créez une machine virtuelle.

L'activation de VBS est un processus qui implique d'abord l'activation de VBS dans la machine virtuelle, puis l'activation de VBS dans le SE invité de Windows.

Conditions préalables

Reportez-vous à la section Recommandations sur la sécurité basée sur la virtualisation pour découvrir les CPU acceptables.

L'utilisation de CPU Intel pour VBS nécessite vSphere 6.7 ou version ultérieure. Créez une machine virtuelle qui utilise la version matérielle 14 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits)
- Windows Server 2016 (64 bits)

- Windows Server 2019 (64 bits)

L'utilisation de CPU AMD pour VBS nécessite vSphere 7.0 Update 2 ou version ultérieure. Créez une machine virtuelle qui utilise la version matérielle 18 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits), version 1809
- Windows Server 2019 (64 bits)

Avant d'activer VBS, assurez-vous d'installer les derniers correctifs pour Windows 10, version 1809 et Windows Server 2019.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez un objet dans l'inventaire qui est un objet parent valide d'une machine virtuelle, par exemple un hôte ESXi ou un cluster.
3. Cliquez avec le bouton droit sur l'objet, sélectionnez **Nouvelle machine virtuelle** et suivez les invites pour créer une machine virtuelle.

Option	Action
Sélectionner un type de création	Créez une machine virtuelle.
Sélectionner un nom et un dossier	Spécifiez un nom et un emplacement cible
Sélectionner une ressource de calcul	Spécifiez un objet pour lequel vous disposez des privilèges de création de machines virtuelles.
Sélectionner le stockage	Dans la stratégie de stockage VM, sélectionnez la stratégie de stockage. Sélectionnez une banque de données compatible.
Sélectionner une compatibilité	CPU Intel : assurez-vous qu'**ESXi 6.7 et versions ultérieures** est sélectionné. CPU AMD : assurez-vous qu'**ESXi 7.0 U2 et versions ultérieures** est sélectionné.
Sélectionner un système d'exploitation invité	CPU Intel : sélectionnez Windows 10 (64 bits), Windows Server 2016 (64 bits) ou Windows Server 2019 (64 bits). CPU AMD : sélectionnez Windows 10 (64 bits) ou Windows Server 2019 (64 bits). Cochez la case **Activer la sécurité basée sur la virtualisation de Windows**.
Personnalisation du matériel	Personnalisez le matériel. Par exemple, changez la taille du disque ou le CPU.
Prêt à terminer	Passez vos informations en revue et cliquez sur **Terminer**.

Résultats

Une fois que la machine virtuelle est créée, confirmez que son onglet **Résumé** affiche « VBS true » dans la description du système d'exploitation invité.

Étape suivante

Reportez-vous à la section Activer la sécurité basée sur la virtualisation sur le système d'exploitation invité.

Activer la sécurité basée sur la virtualisation sur une machine virtuelle existante

Vous pouvez activer la sécurité basée sur la virtualisation de Microsoft (VBS) sur des machines virtuelles existantes pour les systèmes d'exploitation invités Windows pris en charge.

L'activation de VBS est un processus qui implique d'abord l'activation de VBS dans la machine virtuelle, puis l'activation de VBS dans le SE invité.

Note Les nouvelles machines virtuelles configurées pour Windows 10, Windows Serveur 2016 et Windows Server 2019 sur des versions matérielles antérieures à la version 14 sont créées avec le BIOS hérité par défaut. Si vous modifiez le type de microprogramme de la machine virtuelle à partir du BIOS hérité vers l'interface UEFI, vous devez réinstaller le système d'exploitation invité.

Conditions préalables

Reportez-vous à la section Recommandations sur la sécurité basée sur la virtualisation pour découvrir les CPU acceptables.

L'utilisation de CPU Intel pour VBS nécessite vSphere 6.7 ou version ultérieure. La machine virtuelle doit avoir été créée en utilisant la version matérielle 14 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits)
- Windows Server 2016 (64 bits)
- Windows Server 2019 (64 bits)

L'utilisation de CPU AMD pour VBS nécessite vSphere 7.0 Update 2 ou version ultérieure. La machine virtuelle doit avoir été créée en utilisant la version matérielle 18 ou une version ultérieure et l'un des systèmes d'exploitation invités pris en charge suivants :

- Windows 10 (64 bits), version 1809
- Windows Server 2019 (64 bits)

Avant d'activer VBS, assurez-vous d'installer les derniers correctifs pour Windows 10, version 1809 et Windows Server 2019.

Procédure

1. Dans vSphere Client, accédez à la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Cliquez sur l'onglet **Options VM**.

4 Décochez la case **Activer** pour la sécurité basée sur la virtualisation.

5 Cliquez sur **OK**.

Résultats

Confirmez que l'onglet **Résumé** de la machine virtuelle affiche « VBS true » dans la description du système d'exploitation invité.

Étape suivante

Reportez-vous à la section Activer la sécurité basée sur la virtualisation sur le système d'exploitation invité.

Activer la sécurité basée sur la virtualisation sur le système d'exploitation invité

Vous pouvez activer la sécurité basée sur la virtualisation de Microsoft (VBS) pour les systèmes d'exploitation invités Windows pris en charge.

Vous activez VBS à partir du système d'exploitation invité de Windows. Windows configure et applique VBS via une stratégie GPO (Group Policy Object). La stratégie GPO vous donne la possibilité de désactiver puis d'activer les différents services, tels que le démarrage sécurisé, la protection du périphérique et la protection des informations d'identification qu'offre VBS. Certaines versions de Windows nécessitent également de procéder à l'activation de la plate-forme Hyper-V.

Pour plus de détails, consultez la documentation de Microsoft sur le déploiement de la protection du périphérique pour activer la sécurité basée sur la virtualisation.

Conditions préalables

- Assurez-vous que la sécurité basée sur la virtualisation a été activée sur la machine virtuelle.

Procédure

1 Dans Microsoft Windows, modifiez la stratégie de groupe pour activer VBS et choisir d'autres options de sécurité liées à VBS.

2 (Facultatif) Pour les versions de Microsoft Windows antérieures à Redstone 4, dans le panneau de contrôle des fonctionnalités Windows, activez la plate-forme Hyper-V.

3 Redémarrez le système d'exploitation invité.

Désactiver la sécurité basée sur la virtualisation

Si vous n'utilisez plus la sécurité basée sur la virtualisation (VBS) avec une machine virtuelle, vous pouvez désactiver VBS. Lorsque vous désactivez VBS pour la machine virtuelle, les options de Windows VBS restent inchangées, mais peuvent provoquer des problèmes de performance.

Avant de désactiver VBS sur la machine virtuelle, désactivez les options VBS au sein de Windows.

Conditions préalables

Assurez-vous que la machine virtuelle est hors tension.

Procédure

1. Dans vSphere Client, accédez à la machine virtuelle activée par VBS.

   Reportez-vous à la section Identifier les machines virtuelles sur lesquelles la sécurité basée sur la virtualisation est activée pour vous aider à localiser les machines virtuelles activées par VBS.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Cliquez sur **Options VM**.
4. Décochez la case **Activer** pour la sécurité basée sur la virtualisation.

   Un message vous rappelle de désactiver VBS dans le SE invité.
5. Cliquez sur **OK**.
6. Vérifiez que l'onglet **Résumé** de la machine virtuelle n'affiche plus « VBS true » dans la description du système d'exploitation invité.

Identifier les machines virtuelles sur lesquelles la sécurité basée sur la virtualisation est activée

Vous pouvez déterminer les machines virtuelles pour lesquelles la sécurité basée sur la virtualisation est activée, pour des raisons de conformité et de génération de rapports.

Procédure

1. Connectez-vous à vCenter Server à l'aide de vSphere Client.
2. Sélectionnez une instance vCenter Server, un centre de données ou un hôte dans l'inventaire.
3. Cliquez sur l'onglet **VM**, puis sur **Machines virtuelles**.
4. Dans la liste des machines virtuelles, cliquez sur la flèche vers le bas dans un en-tête de colonne pour afficher ou masquer les colonnes, puis activez la case à cocher **VBS**.

   La colonne **VBS** s'affiche.
5. Recherchez l'attribut Présent dans la colonne **VBS**.

Sécurisation de la mise en réseau vSphere

13

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 vSphere standard
- Protection des commutateurs standard et VLAN
- Sécuriser les vSphere Distributed Switches et les groupes de ports distribués
- Sécurisation des machines virtuelles avec des VLAN
- Création de plusieurs réseaux sur un hôte ESXi
- Sécurité du protocole Internet
- Garantir une configuration SNMP appropriée
- 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 grand 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.

Les pare-feu basés sur l'hôte peuvent ralentir les performances. Équilibrez vos besoins en sécurité par rapport à vos objectifs de performances avant d'installer des pare-feu basés sur l'hôte sur des machines virtuelles situées à un autre emplacement 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 à la suivante. La segmentation permet de prévenir diverses menaces, notamment la falsification de la réponse ARP (ARP spoofing). Dans le cas de la falsification de la réponse ARP, un pirate manipule la table ARP pour remapper les adresses IP et MAC afin d'accéder au trafic réseau vers et depuis 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.

Une planification rigoureuse de la segmentation réduit les chances de transmissions de paquets entre les zones de machines virtuelles. La segmentation évite ainsi les intrusions 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 avec une des deux approches suivantes.

- 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 après la création des segments initiaux. Cette approche est moins sujette à une configuration incorrecte.
- Configurez des réseaux locaux virtuels (VLAN) pour protéger votre réseau. Les VLAN fournissent presque tous les avantages de sécurité inhérents dans l'implémentation de réseaux physiquement séparés sans surcharge de matériel. Elles peuvent vous économiser les coûts de déploiement et de maintenance de périphériques supplémentaires, de câblage, etc. Reportez-vous à la section Sécurisation des machines virtuelles avec des VLAN.

Prévention de l'accès non autorisé

Les exigences en matière de sécurité des machines virtuelles sont souvent identiques à celles des machines physiques.

- Si un 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.
- Une machine virtuelle est susceptible d'être attaquée par d'autres machines virtuelles, même si vous ne la connectez pas au réseau physique.

Les machines virtuelles sont isolées les unes des autres. Une machine virtuelle ne peut pas lire ou écrire dans la mémoire d'une autre machine virtuelle, accéder à ses données, utiliser ses applications, etc. Cependant, au sein du réseau, une machine virtuelle ou un groupe de machines virtuelles peut malgré tout être la cible d'un accès non autorisé à partir d'autres machines virtuelles. Protégez vos machines virtuelles contre ces accès non autorisés.

Pour plus d'informations sur la protection des machines virtuelles, consultez le document NIST intitulé « Secure Virtual Network Configuration for Virtual Machine (VM) Protection » (Configuration sécurisée d'un réseau virtuel pour la protection des machines virtuelles) à l'adresse :

https://csrc.nist.gov/publications/detail/sp/800-125b/final

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 obtenir la liste de tous les ports et protocoles pris en charge dans les produits VMware, y compris vSphere et vSAN, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/. Vous pouvez rechercher des ports selon le produit VMware, créer une liste personnalisée de ports et imprimer ou enregistrer des listes de ports.

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.

Des pare-feu doivent être présents aux points d'entrée. Un pare-feu peut être situé entre les clients et vCenter Server ou vCenter Server et les clients peuvent être situés derrière un pare-feu.

Pour obtenir la liste de tous les ports et protocoles pris en charge dans les produits VMware, y compris vSphere et vSAN, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/. Vous pouvez rechercher des ports selon le produit VMware, créer une liste personnalisée de ports et imprimer ou enregistrer des listes de ports.

Les réseaux configurés avec vCenter Server peuvent recevoir les communications par le biais de vSphere Client, de l'interface utilisateur des autres clients ou des clients qui utilisent vSphere API. 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 donnés 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 aux autres points d'accès dans le réseau, en fonction de l'utilisation du réseau et du niveau de sécurité requis par les clients. Sélectionnez les emplacements de vos pare-feu en fonction des risques de sécurité pour la configuration de votre réseau. Les emplacements de pare-feu suivants sont généralement utilisés.

- Entre vSphere 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 Client, entre vSphere Client et l'hôte ESXi. Cette connexion s'ajoute à la connexion entre vSphere 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 que vous prévoyez de migrer des machines virtuelles entre elles, ouvrez les ports dans les pare-feu qui séparent l'hôte source des hôtes cibles.
- Entre les hôtes ESXi et le stockage réseau tel que le stockage NFS ou iSCSI. Ces ports ne sont pas spécifiques à VMware. Configurez-les en fonction des spécifications de votre réseau.

Connexion à vCenter Server via un pare-feu

Ouvrez le port TCP 443 dans le pare-feu pour permettre à vCenter Server de recevoir des données.

Par défaut, vCenter Server utilise le port TCP 443 pour surveiller les 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. 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.

Connexion des hôtes ESXi via des pare-feu

Si vous avez un pare-feu entre vos hôtes ESXi et vCenter Server, assurez-vous que 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 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.

Pare-feu pour les configurations sans vCenter Server

Si votre environnement n'inclut pas vCenter Server, les clients peuvent se connecter directement au réseau ESXi.

Vous pouvez vous connecter à un hôte ESXi autonome de différentes manières.

- VMware Host Client
- Interface ESXCLI
- vSphere Web Services SDK ou vSphere Automation SDK
- Des clients tiers

Les exigences de pare-feu pour les hôtes autonomes sont similaires aux exigences lorsque vCenter Server est présent.

- Utilisez un pare-feu pour protéger votre couche ESXi ou, en fonction de votre configuration, vos clients et la 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. L'attribution de licence étant résidente dans ESXi, un License Server distinct avec un pare-feu n'est pas nécessaire.

Vous pouvez configurer les ports du pare-feu à l'aide d'ESXCLI ou VMware Host Client. Reportez-vous à la section *Gestion individuelle des hôtes vSphere - VMware Host Client*.

Connexion à la console de 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 Client ou directement à l'hôte ESXi depuis VMware Host Client.

Connexion à une console de machine virtuelle basée sur une interface de navigation au moyen vSphere Client

Lorsque vous vous connectez avec vSphere 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 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 Client à accéder à vCenter Server par le port 443.
- Le pare-feu doit autoriser vCenter Server à accéder à ESXi par le port 902.

Connexion à VMware Remote Console via vSphere Client

Si vous utilisez vSphere Client et que vous vous connectez à VMware Remote Console (VMRC), l'accès suivant doit être possible :

- Le pare-feu doit autoriser vSphere Client à accéder à vCenter Server par le port 443.
- Le pare-feu doit permettre à VMRC d'accéder à vCenter Server sur le port 443 et d'accéder à l'hôte ESXi sur le port 902 pour les versions VMRC antérieures à la version 11.0, et le port 443 pour VMRC version 11.0 et versions ultérieures. Pour plus d'informations sur les conditions requises pour VMRC version 11.0 et le port ESXi, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/76672.

Connexion aux hôtes ESXi directement avec VMware Host Client

Vous pouvez utiliser la console de machine virtuelle VMware Host Client si vous vous connectez directement à un hôte ESXi.

Note N'utilisez pas VMware Host Client pour vous connecter directement aux hôtes gérés par un système vCenter Server. Si vous apportez des modifications à ces hôtes depuis VMware Host Client, votre environnement devient instable.

Le pare-feu doit autoriser l'accès à l'hôte ESXi sur les ports 443 et 902.

VMware Host Client utilise le port 902 pour fournir une connexion aux 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

Le groupe de ports VMkernel ou le groupe de ports de machine virtuelle sur un commutateur standard dispose d'une stratégie de sécurité configurable. 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.

À l'instar des adaptateurs réseau physiques, les adaptateurs réseau de machine virtuelle peuvent emprunter l'identité d'une autre machine virtuelle. L'emprunt d'identité est un risque de sécurité.

- Une machine virtuelle peut envoyer des trames qui semblent provenir d'une autre machine de sorte à pouvoir recevoir des trames réseau destinées à cette machine.
- Un adaptateur réseau de machine virtuelle peut être configuré afin de recevoir des trames destinées à d'autres machines.

Lorsque vous ajoutez un groupe de ports VMkernel ou 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. Le système d'exploitation invité qui pourrait tenter d'emprunter l'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, reportez-vous à la section sur la stratégie de sécurité de la publication *Mise en réseau vSphere*. Cette section explique :

- Comment les adaptateurs réseau de machine virtuelle contrôlent les transmissions ;
- La manière dont les attaques sont contrées à ce niveau.

Sécuriser les commutateurs vSphere standard

Vous pouvez sécuriser le trafic de commutation standard contre les attaques de couche 2 en limitant certains modes d'adresses MAC des adaptateurs réseau de machine virtuelle.

Chaque adaptateur réseau de 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 d'un adaptateur réseau de 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. Un système d'exploitation peut donc emprunter l'identité d'un adaptateur réseau que le réseau récepteur autorise et planifier des attaques malveillantes sur les périphériques dans un réseau.

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 :

- Modifications d'adresse MAC (reportez-vous à Modifications d'adresse MAC)
- Mode Proximité (reportez-vous à Fonctionnement en mode promiscuité)
- 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 Client. Reportez-vous à la documentation *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.

Pour plus d'informations sur la configuration de l'adaptateur de machine virtuelle pour le mode promiscuité, reportez-vous à la section sur la configuration de la stratégie de sécurité d'un commutateur vSphere Standard ou d'un groupe de ports standard dans la documentation de *Mise en réseau vSphere*.

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.

Protection des commutateurs standard et VLAN

Les commutateurs standard VMware assurent une protection contre certaines menaces pour la sécurité du VLAN. En raison de la manière dont certains commutateurs standard sont conçus, ils protègent les VLAN contre un grand nombre d'attaques, dont un grand nombre implique le VLAN hopping.

Disposer de cette protection ne garantit pas que la configuration de vos machines virtuelles n'est pas vulnérable à d'autres types d'attaques. Par exemple, les commutateurs standard ne protègent pas le réseau physique contre ces attaques : ils protègent uniquement le réseau virtuel.

Les commutateurs standard et les VLAN peuvent protéger des types d'attaques suivants.

Saturation MAC

Saturation d'un commutateur avec des paquets contenant des adresses MAC balisées comme provenant de sources différentes. De nombreux commutateurs utilisent une table de mémoire adressable par contenu pour détecter et stocker l'adresse source de chaque paquet. Lorsque la table est pleine, le commutateur peut passer dans un état totalement ouvert dans lequel chaque paquet entrant est diffusé sur tous les ports, permettant à l'attaquant de voir tout le trafic du commutateur. Cet état peut provoquer une fuite des paquets sur les VLAN.

Bien que les commutateurs standard de VMware stockent la table d'adresses MAC, ils n'obtiennent pas les adresses MAC du trafic observable et ne sont pas vulnérables à ce type d'attaque.

Attaques 802.1q et de balisage ISL

Force un commutateur à rediriger des cadres d'un VLAN à un autre en amenant le commutateur à agir comme un tronçon et à diffuser le trafic aux autres VLAN.

Les commutateurs standard de VMware n'effectuent pas la jonction dynamique requise pour ce type d'attaque et ne sont pas par conséquent vulnérables.

Attaques à double encapsulation

Survient lorsqu'un attaquant crée un paquet à double encapsulation dans lequel l'identifiant de VLAN dans la balise interne est différent de l'identifiant de VLAN dans la balise externe.

Pour des raisons de compatibilité descendante, les VLAN natifs ôtent la balise externe des paquets transmis sauf s'ils sont configurés pour ne pas le faire. Lorsque le commutateur d'un VLAN natif ôte la balise externe, seule la balise interne reste et cette balise interne achemine le paquet à un VLAN différent de celui identifié par la balise externe maintenant manquante.

Les commutateurs standard de VMware rejettent les cadres à double encapsulation qu'une machine virtuelle tente d'envoyer sur un port configuré pour un VLAN spécifique. Par conséquent, ils ne sont pas vulnérables à ce type d'attaque.

Attaques de force brute multidiffusion

Implique l'envoi d'un grand nombre de cadres multidiffusion à un VLAN connu presque simultanément pour surcharger le commutateur afin qu'il autorise par erreur la diffusion de certains cadres sur d'autres VLAN.

Les commutateurs standard de VMware ne permettent pas aux cadres de quitter leur domaine de diffusion correspondant (VLAN) et ne sont pas vulnérables à ce type d'attaque.

Attaques l'arbre recouvrant

Spanning-Tree Protocol (STP) cible, qui est utilisé pour contrôler le pontage entre des parties du LAN. L'attaquant envoie des paquets Bridge Protocol Data Unit (BPDU) qui tentent de modifier la topologie du réseau, en se définissant comme le pont racine. En tant que pont racine, l'attaquant peut renifler le contenu des cadres transmis.

Les commutateurs standard de VMware ne prennent pas en charge STP et ne sont pas vulnérables à ce type d'attaque.

Attaques à trame aléatoire

Implique l'envoi d'un grand nombre de paquets dans lesquels les adresses de source et de destination restent identiques, mais dans lesquels les zones sont modifiées aléatoirement en longueur, type ou contenu. L'objectif de cette attaque est de forcer les paquets à être réacheminés par erreur vers un VLAN différent.

Les commutateurs standard de VMware ne sont pas vulnérables à ce type d'attaque.

Comme de nouvelles menaces de sécurité continuent à se développer, ne considérez pas cela comme une liste exhaustive des attaques. Vérifiez régulièrement les ressources de sécurité de VMware sur le Web pour en savoir plus sur la sécurité, les alertes de sécurité récentes et les tactiques de sécurité de VMware.

Sécuriser les vSphere Distributed Switches et les groupes de ports distribués

Les administrateurs disposent de plusieurs options pour sécuriser des vSphere Distributed Switches dans leur environnement vSphere.

Les règles qui s'appliquent aux VLAN dans un vSphere Distributed Switch sont identiques à celles qui s'appliquent pour un commutateur standard. Pour plus d'informations, consultez Protection des commutateurs standard et VLAN.

Procédure

1. Pour les groupes de ports distribués avec liaison statique, désactivez la fonction Extension automatique.

   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 des ID de VLAN ne sont pas correctement suivis, une réutilisation erronée de ces derniers risque de générer un trafic inattendu. 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 une zone de texte pour le nom du commutateur. Ce libellé sert de descripteur fonctionnel du commutateur, tout comme le 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 libeller le commutateur comme étant interne pour indiquer qu'il est réservé au réseau interne sur le commutateur virtuel privé d'une machine virtuelle. Aucun trafic ne transite par les 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 :

   - Modifications d'adresse MAC (reportez-vous à Modifications d'adresse MAC)

- Mode Proximité (reportez-vous à Fonctionnement en mode promiscuité)
- 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*.

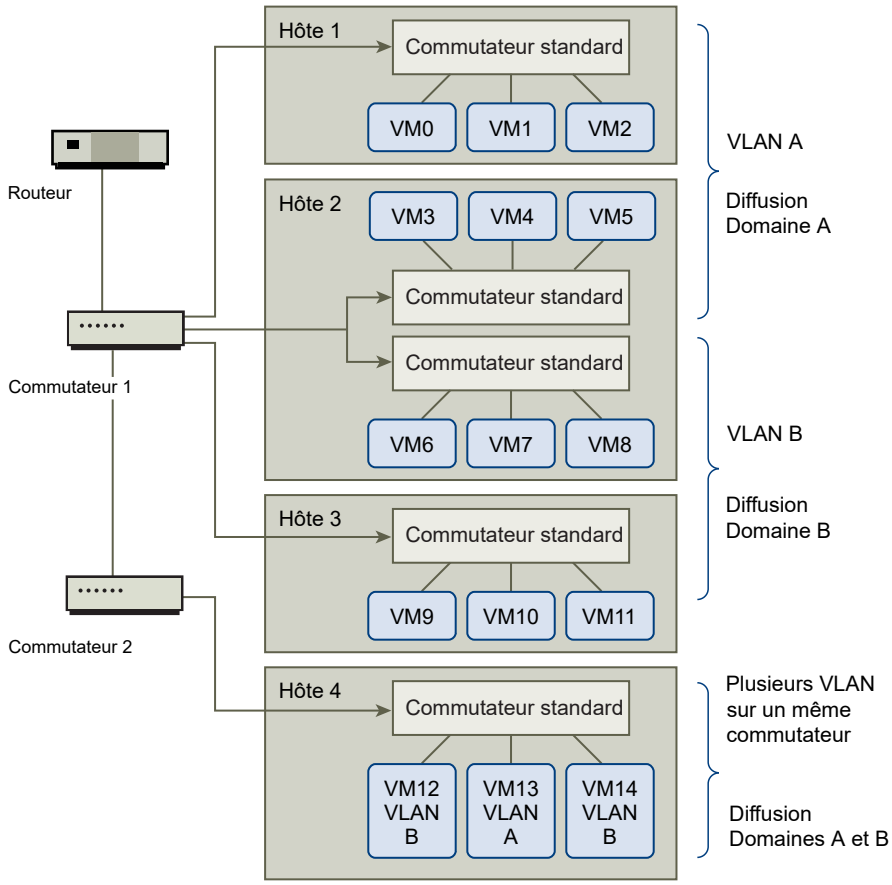
Sécurisation des machines virtuelles avec des VLAN

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 13-1. 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**.

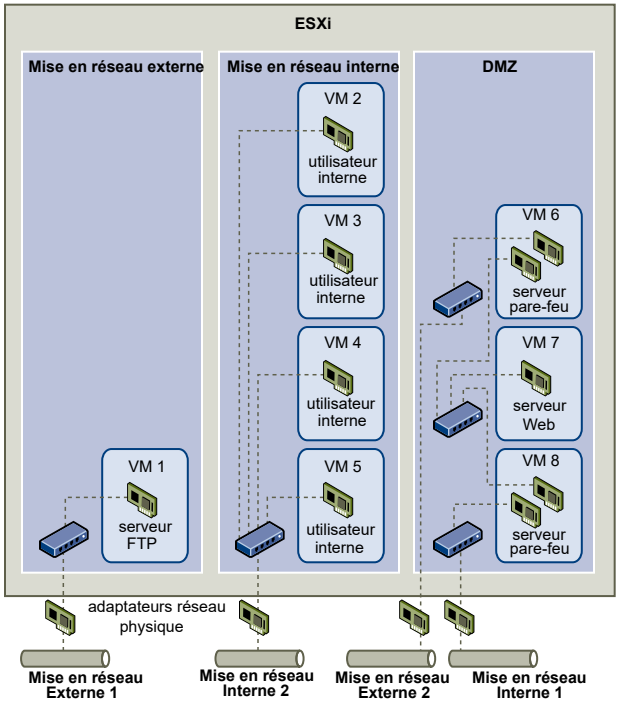
   Sur un commutateur standard, vous pouvez configurer le mode de mise en réseau VLAN au niveau du commutateur ou du groupe de ports, et sur un commutateur distribué au niveau du groupe de ports distribués ou du port.

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.

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 13-2. 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 distinctes de machines virtuelles : sur le serveur FTP, dans les machines virtuelles internes 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. La société utilise le réseau externe 2 pour prendre en charge les serveurs Web que les services marketing et financiers utilisent pour héberger le site Web d'entreprise et d'autres fonctionnalités Web destinées à des utilisateurs externes. Le réseau interne 1 est utilisé par le service marketing pour publier son contenu sur le site Web de l'entreprise, pour proposer 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 se connectent 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 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 `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 à l'aide de la commande `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
`--sa-source=` ***source address***	Requis. Spécifiez l'adresse source.
`--sa-destination=` ***destination address***	Requis. Spécifiez l'adresse de destination.
`--sa-mode=` ***mode***	Requis. Spécifiez le mode, soit `transport` ou `tunnel`.
`--sa-spi=` ***security parameter index***	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.
`--encryption-algorithm=` ***encryption algorithm***	Requis. Spécifiez l'algorithme de chiffrement à l'aide d'un des paramètres suivants. ■ `3des-cbc` ■ `aes128-cbc` ■ `null` (n'assure aucun chiffrage)
`--encryption-key=` ***encryption key***	Requise 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=` ***authentication algorithm***	Requis. Spécifiez l'algorithme d'authentification, soit `hmac-sha1` ou `hmac-sha2-256`.
`--integrity-key=` ***authentication key***	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=`***name***	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 0x697076367265616479 6c6f676f3364657363626f757432
--integrity-algorithm hmac-sha1
```

```
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

Supprimer une association de sécurité IPsec

Vous pouvez supprimer une association de sécurité à l'aide de la commande 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 ajouter une stratégie de sécurité disponible à l'aide de la commande ESXCLI.

Procédure

- Dans 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 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=` ***source address***	Requis. Spécifiez l'adresse IP source et la longueur du préfixe.
`--sp-destination=` ***destination address***	Requis. Spécifiez l'adresse de destination et la longueur du préfixe.

Option	Description
--source-port= ***port***	Requis. Spécifiez le port source. Le port source doit être un nombre compris entre 0 et 65 535.
--destination-port= ***port***	Requis. Spécifiez le port de destination. Le port source doit être un nombre compris entre 0 et 65 535.
--upper-layer-protocol= ***protocol***	Spécifiez le protocole de couche supérieure à l'aide d'un des paramètres suivants. ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
--flow-direction= ***direction***	Spécifiez la direction dans laquelle vous souhaitez surveiller le trafic à l'aide de `in` ou `out`.
--action= ***action***	Définissez l'action à prendre lorsque le trafic avec les paramètres spécifiés est rencontré à l'aide des paramètres suivants. ■ `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= ***mode***	Spécifiez le mode, soit `tunnel` ou `transport`.
--sa-name=*security association name*	Requis. Indiquez le nom de l'association de sécurité pour la règle de sécurité à utiliser.
--sp-name=*name*	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=sa1
--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 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.

SNMP doit être configuré sur chaque hôte ESXi. Vous pouvez utiliser ESXCLI, PowerCLI ou vSphere Web Services SDK pour la configuration.

Pour obtenir des informations sur la configuration de SNMP 3, consultez la documentation *Surveillance et performances de vSphere*. Pour plus d'informations sur les options de la commande `esxcli system snmp`, consultez *Référence d'ESXCLI*.

Procédure

1. Exécutez la commande suivante pour déterminer si SNMP est utilisé.

   ```
   esxcli system snmp get
   ```

2. Pour activer SNMP, exécutez la commande suivante.

   ```
   esxcli system snmp set --enable true
   ```

3. Pour désactiver SNMP, exécutez la commande suivante.

   ```
   esxcli system snmp set --disable true
   ```

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.

- Le protocole STP (Spanning Tree Protocol) détecte les boucles et les empêche de former la topologie réseau. Les commutateurs virtuels VMware empêchent les boucles d'une autre manière, mais ne prennent pas en charge le protocole STP directement. Lorsque des modifications de topologie réseau se produisent, un certain temps est nécessaire (30 à 50 secondes) au réseau pour réapprendre la topologie. Pendant ce temps, aucun trafic ne peut être transmis. Pour éviter ces problèmes, les fournisseurs de réseaux ont créé des fonctionnalités pour activer les ports de commutateur afin de poursuivre le transfert du trafic. Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/1003804. Consultez la documentation de votre fournisseur de réseau pour connaître les configurations de réseau et de matériel de mise en réseau appropriées.
- Assurez-vous que le trafic NetFlow 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. Ces informations augmentent le risque d'affichage et de capture d'informations sensibles en transit par des pirates. 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. Donnez aux administrateurs réseau des autorisations pour tous les composants du réseau virtuel, mais pas d'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 sont souvent configurés avec un VLAN natif et ce VLAN natif est souvent VLAN 1 par défaut. ESXi ne dispose pas d'un 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. Cela 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 qui sont spécifiées en tant que VLAN 1 sont balisées avec un 1. Par conséquent, le trafic de l'hôte ESXi destiné au VLAN natif n'est pas routé correctement, car il est balisé avec un 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. Lorsque des remplacements sont activés, vous pouvez utiliser des paramètres de sécurité qui sont différents pour la machine virtuelle et le niveau des groupes 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 l'ensemble du 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 par leur arrivée.

Adoption de pratiques d'isolation réseau

Les pratiques d'isolation réseau améliorent 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 standard commun. Le trafic de production (VM) peut partager le commutateur standard si le groupe de ports de gestion vSphere du VLAN n'est pas utilisé par les machines virtuelles de production.

Vérifiez que le segment de réseau n'est pas routé, à l'exception des réseaux dans lesquels se trouvent d'autres entités de gestion. Le routage d'un segment de réseau peut sembler pertinent pour vSphere Replication. Assurez-vous notamment que le trafic des machines virtuelles de production ne peut pas être routé vers ce réseau.

Contrôlez strictement l'accès à la fonctionnalité de gestion 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, rendez obligatoire l'utilisation d'un VPN pour la connexion des administrateurs au réseau de gestion. N'autorisez l'accès au réseau de gestion qu'aux administrateurs approuvés.
- Configurez des zones de passage 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 généralement non chiffré. Toute personne ayant accès à ce réseau peut afficher le trafic de stockage IP. 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.

Utilisez un VLAN dédié sur un commutateur standard commun pour le groupe de ports vMotion. Le trafic de production (VM) peut utiliser le même commutateur standard si le groupe de ports vMotion du VLAN n'est pas utilisé par les machines virtuelles de production.

Isoler le trafic vSAN

Lors de la configuration de votre réseau vSAN, isolez le trafic vSAN sur son propre segment de réseau de couche 2. Vous pouvez effectuer cette isolation en utilisant des commutateurs ou des ports dédiés, ou en utilisant un VLAN.

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

Ne configurez pas votre hôte pour envoyer des informations sur le réseau à une machine virtuelle, sauf si vous utilisez des produits qui utilisent vSphere Network Appliance API (DvFilter). Si vSphere Network Appliance API 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. Accédez à l'hôte dans l'inventaire de vSphere Client.
2. Cliquez sur **Configurer**.
3. Dans Système, cliquez sur **Paramètres système avancés**.
4. 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 la zone de texte Filtre pour afficher tous les paramètres associés.

5 Vérifiez le paramètre.

- Si vous n'utilisez pas les paramètres DvFilter, assurez-vous que la valeur est vide.
- Si vous utilisez les paramètres DvFilter, assurez-vous que la valeur du paramètre est correcte. La valeur doit correspondre à celle que le produit faisant appel à DvFilter utilise.

Meilleures pratiques concernant plusieurs composants vSphere

14

Certaines meilleures pratiques en matière de sécurité, telles que la configuration de PTP ou NTP dans votre environnement, affectent plusieurs composants vSphere. Tenez compte des recommandations suivantes lorsque vous configurez votre environnement.

Reportez-vous à Chapitre 3 Sécurisation des hôtes ESXi et à Chapitre 5 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 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 physiques de votre réseau vSphere ne sont pas synchronisées, les certificats SSL et les jetons SAML, qui sont sensibles au temps, risquent de ne pas être reconnus comme étant valides dans les communications entre les machines 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 `vmware-vpxd` de vCenter Server.

Des incohérences de temps dans vSphere peuvent entraîner l'échec du premier démarrage sur différents services, selon l'heure de l'environnement et la synchronisation actuelle de l'heure. Des problèmes se produisent généralement lorsque l'hôte ESXi cible pour vCenter Server de destination n'est pas synchronisé avec les serveurs NTP ou PTP. De même, des problèmes peuvent survenir si le vCenter Server de destination migre vers un hôte ESXi paramétré avec une heure différente en raison du DRS entièrement automatisé.

Pour éviter les problèmes de synchronisation, assurez-vous que les éléments suivants soient corrects avant l'installation, la migration ou la mise à niveau de vCenter Server.

- L'hôte ESXi cible sur lequel l'instance de destination de vCenter Server doit être déployée est synchronisé avec les serveurs NTP ou PTP.
- L'hôte ESXi qui exécute vCenter Server source est synchronisé avec les serveurs NTP ou PTP.
- Lors de la mise à niveau ou la migration de vSphere 6.5 ou 6.7 vers vSphere 7.0, si le dispositif vCenter Server Appliance est connecté à une instance externe de Platform Services Controller, assurez-vous que l'hôte ESXi qui exécute l'instance externe de Platform Services Controller est synchronisé avec les serveurs NTP ou PTP.
- Si vous effectuez la mise à niveau ou la migration de vSphere 6.5 ou 6.7 vers vSphere 7.0, vérifiez que le dispositif vCenter Server ou vCenter Server source et l'instance externe de Platform Services Controller sont configurés avec l'heure correcte.
- Lorsque vous mettez à niveau une instance de vCenter Server 6.5 ou 6.7 avec une instance externe de Platform Services Controller vers vSphere 7.0, le processus de mise à niveau est converti en instance de vCenter Server avec une instance intégrée de Platform Services Controller.

Assurez-vous que toute machine hôte Windows sur laquelle vCenter Server s'exécute est synchronisée avec le serveur NTP (Network Time Server). Consultez l'article de la base de connaissances VMware accessible à l'adresse https://kb.vmware.com/s/article/1318.

Pour synchroniser les horloges ESXi avec un serveur NTP ou un serveur PTP, vous pouvez utiliser VMware Host Client. Pour plus d'informations sur la modification de la configuration de l'heure d'un hôte ESXi, reportez-vous à *Gestion des hôtes uniques vSphere - VMware Host Client*.

Pour savoir comment modifier les paramètres de synchronisation de l'heure pour vCenter Server, reportez-vous à la section « Configurer les paramètres du fuseau horaire et de synchronisation de l'heure du système » dans *Configuration de vCenter Server*.

Pour découvrir comment modifier la configuration de l'heure pour un hôte en utilisant vSphere Client, reportez-vous à la section « Modification de la configuration de l'heure pour un hôte » dans *Gestion de vCenter Server et des hôtes*.

- Synchroniser les horloges ESXi avec un serveur de temps réseau

  Avant d'installer vCenter Server, assurez-vous que les horloges de toutes les machines sur votre réseau vSphere sont synchronisées.
- Configuration des paramètres de synchronisation horaire dans vCenter Server

  Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server après le déploiement.

Synchroniser les horloges ESXi avec un serveur de temps réseau

Avant d'installer vCenter Server, assurez-vous que les horloges de toutes les machines sur votre réseau vSphere sont synchronisées.

Cette tâche explique comment configurer NTP depuis VMware Host Client.

Procédure

1. Démarrez VMware Host Client et connectez-vous à l'hôte ESXi.
2. Cliquez sur **Gérer**.
3. Sous **Système**, cliquez sur **Heure et date**, puis sur **Modifier les paramètres**.
4. Sélectionnez **Utiliser le protocole de temps du réseau (activer le client NTP)**.
5. Dans la zone de texte Serveurs NTP, saisissez l'adresse IP ou le nom de domaine complet d'un ou de plusieurs serveurs NTP avec lequel effectuer la synchronisation.
6. Dans le menu déroulant **Stratégie de démarrage du service NTP**, sélectionnez **Démarrer et arrêter avec hôte**.
7. Cliquez sur **Enregistrer**.

   L'hôte se synchronise avec le serveur NTP.

Configuration des paramètres de synchronisation horaire dans vCenter Server

Vous pouvez modifier les paramètres de synchronisation horaire dans vCenter Server après le déploiement.

Lorsque vous déployez vCenter Server, 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 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 du système 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. Si vous décidez d'utiliser le logiciel natif de synchronisation horaire, la synchronisation horaire régulière de VMware Tools dans vCenter Server est désactivée, et l'inverse.

Utiliser la synchronisation de l'heure de VMware Tools

Vous pouvez configurer vCenter Server 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

Pour configurer vCenter Server de manière à utiliser une synchronisation de l'heure basée sur NTP, vous devez ajouter les serveurs NTP à la configuration vCenter Server.

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 en exécutant la commande suivante `ntp.set`.

   ```
   ntp.set --servers IP-addresses-or-host-names
   ```

   Dans cette commande, *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 serveurs NTP actuels (le cas échéant) et ajoute les nouveaux 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 remplace les serveurs NTP actuels dans la configuration NTP par les nouveaux serveurs NTP que vous spécifiez.

3. (Facultatif) Pour vérifier que vous avez correctement appliqué les nouveaux paramètres de configuration NTP, exécutez la commande suivante.

   ```
   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.

4 (Facultatif) Pour vérifier si le serveur NTP est accessible, exécutez la commande suivante.

```
ntp.test --servers IP-addresses-or-host-names
```

La commande renvoie l'état des serveurs NTP.

Étape suivante

Si la synchronisation NTP est désactivée, vous pouvez configurer les paramètres de synchronisation de l'heure de vCenter Server de façon à la baser sur un serveur NTP. Reportez-vous à la section Synchroniser l'heure dans vCenter Server avec un serveur NTP.

Synchroniser l'heure dans vCenter Server avec un serveur NTP

Vous pouvez configurer les paramètres de synchronisation de l'heure dans vCenter Server 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. Reportez-vous à la section Ajouter ou remplacer les serveurs NTP dans la configuration de vCenter Server.

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 vSAN*.

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 des mesures pour réduire les risques de sécurité.

iSCSI prend en charge l'accès aux périphériques SCSI et l'échange de données à l'aide du protocole TCP/IP sur un port réseau plutôt que via une connexion directe à un périphérique SCSI. Une transaction iSCSI encapsule les blocs de données SCSI brutes dans des enregistrements iSCSI et transmet les données au périphérique ou à l'utilisateur demandeur.

Les SAN iSCSI permettent une utilisation efficace de l'infrastructure Ethernet existante afin de fournir aux hôtes un accès aux ressources de stockage qu'ils peuvent partager dynamiquement. Les SAN iSCSI sont une solution de stockage économique pour les environnements qui s'appuient sur un pool de stockage commun 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 associés aux hôtes et à celles des iSCSI configurés directement via l'hôte.

Sécurisation des périphériques iSCSI

Pour sécuriser des périphériques iSCSI, exigez que l'hôte ESXi (l'initiateur) puisse s'authentifier auprès du périphérique iSCSI (la cible), à chaque fois que l'hôte tente d'accéder aux données sur le LUN cible.

L'authentification garantit que l'initiateur a le droit d'accéder à une cible. Vous accordez ce droit lorsque vous configurez l'authentification sur le périphérique iSCSI.

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 le secrets CHAP sont uniques. Configurez un secret d'authentification mutuel différent pour chaque hôte. Si possible, configurez un secret pour chaque client qui soit différent de celui de l'hôte ESXi. Les secrets uniques garantissent qu'un pirate ne pourra pas créer un autre hôte arbitraire et s'authentifier auprès du périphérique de stockage, même si un hôte est compromis. Lorsqu'il existe un secret partagé, 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 de Kerberos pour NFS 4.1

Avec NFS version 4.1, ESXi prend en charge le mécanisme d'authentification Kerberos.

Le mécanisme Kerberos RPCSEC_GSS est un service d'authentification. Il permet à un client NFS 4.1 installé sur ESXi de justifier son identité à un serveur NFS, préalablement au montage d'un partage NFS. Grâce au chiffrement, la sécurité Kerberos permet de travailler sur une connexion réseau non sécurisée.

La mise en œuvre ESXi de Kerberos pour NFS 4.1 fournit deux modèles de sécurité, krb5 et krb5i, qui offrent deux niveaux de sécurité différents.

- Kerberos pour l'authentification uniquement (krb5) prend en charge la vérification de l'identité.
- Kerberos pour l'authentification et l'intégrité des données (krb5i), en plus de la vérification de l'identité, fournit des services d'intégrité des données. Ces services permettent de protéger le trafic NFS contre la falsification en vérifiant les modifications potentielles des paquets de données.

Kerberos prend en charge des algorithmes de chiffrement qui empêchent les utilisateurs non autorisés d'obtenir l'accès au trafic NFS. Le client NFS 4.1 sur ESXi tente d'utiliser l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 pour accéder à un partage sur le serveur NAS. Avant d'utiliser vos banques de données NFS 4.1, assurez-vous que l'algorithme AES256-CTS-HMAC-SHA1-96 ou AES128-CTS-HMAC-SHA1-96 est activé sur le serveur NAS.

Le tableau suivant compare les niveaux de sécurité Kerberos pris en charge par ESXi.

Tableau 14-1. Types de sécurité Kerberos

		ESXi 6.0	ESXi 6.5 et versions ultérieures
Kerberos pour l'authentification uniquement (krb5)	Total de contrôle d'intégrité pour l'en-tête RPC	Oui avec DES	Oui avec AES
	Total de contrôle d'intégrité pour les données RPC	Non	Non
Kerberos pour l'authentification et l'intégrité des données (krb5i)	Total de contrôle d'intégrité pour l'en-tête RPC	Pas de krb5i	Oui avec AES
	Total de contrôle d'intégrité pour les données RPC		Oui avec AES

Lorsque vous utilisez l'authentification Kerberos, les considérations suivantes s'appliquent :

- ESXi utilise Kerberos avec le domaine Active Directory.
- En tant qu'administrateur de vSphere, vous devez spécifier les informations d'identification Active Directory requises pour octroyer l'accès aux banques de données Kerberos NFS 4.1 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. Pour automatiser le processus d'attribution, définissez l'utilisateur dans un profil d'hôte et appliquez le profil à tous les hôtes ESXi.
- Vous ne pouvez pas utiliser deux mécanismes de sécurité, AUTH_SYS et Kerberos, pour la même banque de données NFS 4.1 partagée par plusieurs hôtes.

Pour des instructions détaillées, reportez-vous à la documentation *Stockage vSphere*.

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.

Par défaut, la possibilité d'envoyer des données de performance relatives à l'hôte à une machine virtuelle est désactivée. Ce paramétrage par défaut empêche une machine virtuelle d'obtenir des informations détaillées sur l'hôte physique. Si une faille de sécurité se produit sur la machine virtuelle, le paramètre rend les données de l'hôte indisponibles à l'attaquant.

Note La procédure suivante illustre le processus. Vous pouvez utiliser les commandes ESXCLI ou VMware PowerCLI pour effectuer cette tâche simultanément sur tous les hôtes.

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 Client

Pour empêcher des intrus d'utiliser une session inactive, configurez des délais d'expiration pour ESXi Shell et vSphere Client.

Délai d'expiration d'ESXi Shell

Pour ESXi Shell, vous pouvez configurer les délais d'expiration suivants pour vSphere 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. Les modifications n'ont pas d'incidence sur les sessions existantes.

Délai d'expiration d'vSphere Client

Par défaut, les sessions vSphere 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 configuration de TLS

15

vSphere active uniquement TLS par défaut. TLS 1.0 et TLS 1.1 sont désactivés par défaut. Si vous effectuez une nouvelle installation, une mise à niveau ou une migration, vSphere désactive TLS 1.0 et 1.1. Vous pouvez utiliser l'utilitaire TLS Configurator pour activer temporairement les versions antérieures du protocole sur les systèmes vSphere. Vous pouvez ensuite désactiver les anciennes versions moins sécurisées, une fois que toutes les connexions utilisent TLS 1.2.

Tenez compte de votre environnement avant d'effectuer une reconfiguration. Selon les exigences de votre environnement et les versions de logiciel, vous devrez peut-être réactiver TLS 1.0 et TLS 1.1, en plus de TLS 1.2, afin de maintenir l'interopérabilité. Pour les produits VMware, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/s/article/2145796 pour obtenir la liste des produits VMware qui prennent en charge le protocole TLS 1.2. Pour l'intégration à des produits tiers, consultez la documentation de votre fournisseur. L'utilitaire TLS Configurator fonctionne avec vSphere 7.0 et versions antérieures, notamment les versions 6.7, 6.5 et 6.0.

Ce chapitre contient les rubriques suivantes :

- Ports prenant en charge la désactivation des versions TLS
- Activation ou désactivation des versions de TLS dans vSphere
- Effectuer une sauvegarde manuelle facultative
- Activer ou désactiver les versions TLS sur les systèmes vCenter Server
- Activer ou désactiver les versions de TLS sur les hôtes ESXi
- Analyser vCenter Server pour les protocoles TLS activés
- Restaurer les modifications de l'utilitaire de configuration TLS

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 et ESXi. Vous pouvez désactiver TLS 1.0, ou TLS 1.0 et TLS 1.1.

À partir de vSphere 7.0, vCenter Server exécute deux services de proxy inverse :

- Service de proxy inverse de VMware, `rhttpproxy`.
- Envoy

Envoy est un dispositif Edge et un proxy de service Open Source. Envoy est propriétaire du port 443 et toutes les demandes vCenter Server entrantes sont acheminées via Envoy. Dans vSphere 7.0, `rhttpproxy` sert de serveur de gestion de configuration pour Envoy. Par conséquent, la configuration TLS est appliquée à `rhttpproxy`, qui à son tour envoie la configuration à Envoy.

vCenter Server et ESXi utilisent des ports pouvant être activés ou désactivés pour les protocoles TLS. L'option `scan` de l'utilitaire de configuration TLS affiche les versions TLS activées pour chaque service. Reportez-vous à la section Analyser vCenter Server pour les protocoles TLS activés.

Pour obtenir la liste de tous les ports et protocoles pris en charge dans les produits VMware, y compris vSphere et vSAN, reportez-vous à la section Outil Ports et protocoles de VMware™ à l'adresse https://ports.vmware.com/. Vous pouvez rechercher des ports selon le produit VMware, créer une liste personnalisée de ports et imprimer ou enregistrer des listes de ports.

Notes et mises en garde

- La version vSphere 6.7 était la version finale de vCenter Server pour Windows. Consultez la documentation *Sécurité vSphere* pour la version 6.7 du produit afin d'obtenir plus d'informations sur la reconfiguration de TLS pour les ports Update Manager sur vCenter Server pour Windows.
- Vous pouvez utiliser TLS 1.2 pour chiffrer la connexion entre l'instance de vCenter Server et un serveur Microsoft SQL Server externe. Vous ne pouvez pas utiliser une connexion TLS 1.2 unique pour la base de données Oracle externe. Consultez l'article de la base de connaissances de VMware à l'adresse https://kb.vmware.com/kb/2149745.
- Pour vSphere 6.7 et les versions antérieures, 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*.
- Si vous modifiez les protocoles TLS, vous devez redémarrer l'hôte ESXi pour appliquer les modifications. Vous devez redémarrer l'hôte, même si vous appliquez les modifications via la configuration du cluster à l'aide des profils d'hôte. Vous pouvez choisir de redémarrer l'hôte immédiatement ou de reporter le redémarrage à un moment plus commode.

Activation ou 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.

vSphere Lifecycle Manager est toujours inclus dans le système vCenter Server et le script met à jour le port correspondant.

1 Exécutez l'utilitaire TLS Configurator sur vCenter Server.

2 Exécutez l'utilitaire TLS Configurator 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.

Conditions préalables

Vous avez deux possibilités pour utiliser TLS dans votre environnement.

- Désactivez TLS 1.0, et activez TLS 1.1 et TLS 1.2.
- Désactivez TLS 1.0, et TLS 1.1 et activez TLS 1.2.

Effectuer une sauvegarde manuelle facultative

L'utilitaire de configuration TLS effectue une sauvegarde à chaque fois que le script modifie vCenter Server. Si vous avez besoin d'effectuer une sauvegarde dans un répertoire spécifique, vous pouvez effectuer une sauvegarde manuelle.

La sauvegarde de la configuration ESXi n'est pas prise en charge.

Pour vCenter Server, le répertoire par défaut est `/tmp/`*`yearmonthday`*`T`*`time`*.

Procédure

1 Modifiez le répertoire en `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`..

2 Pour effectuer une sauvegarde dans un répertoire spécifique, exécutez la commande suivante.

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

3 Vérifiez que la sauvegarde s'est effectuée correctement.

Une sauvegarde réussie ressemble à l'exemple suivant. L'ordre des services affiché peut être différent à chaque fois que vous exécutez la commande `reconfigureVc backup`, en raison du mode d'exécution de celle-ci.

```
vCenter Transport Layer Security reconfigurator, version=7.0.0, build=15518531
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================ Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20200206T183550
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmcam
Backing up: vmware-stsd
Backing up: vmdird
Backing up: vmware-sps
```

```
Backing up: vmware-rhttpproxy
Backing up: vami-lighttp
Backing up: vmware-updatemgr
Backing up: rsyslog
```

4 (Facultatif) Si vous devez par la suite effectuer une restauration, exécutez la commande suivante.

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

Activer ou désactiver les versions TLS sur les systèmes vCenter Server

Vous pouvez utiliser l'utilitaire de configuration de TLS pour activer ou désactiver les versions de TLS sur les systèmes vCenter Server. Dans le cadre de ce processus, vous pouvez désactiver TLS 1.0 et activer TLS 1.1 et TLS 1.2. Vous pouvez également désactiver TLS 1.0 et TLS 1.1 et activer 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 avec le nom d'utilisateur et le mot de passe pour administrator@vsphere.local, ou en tant qu'un autre membre du groupe d'administrateurs de vCenter Single Sign-On qui peut exécuter des scripts.

2 Accédez au répertoire dans lequel se trouve le script.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 Exécutez la commande en fonction 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.

  ```
  directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2
  ```

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2, exécutez la commande suivante.

  ```
  directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
  ```

4 Si votre environnement inclut d'autres systèmes vCenter Server, répétez le processus sur chaque système vCenter Server.

5 Répétez cette configuration sur chaque hôte ESXi.

Activer ou désactiver les versions de TLS sur les hôtes ESXi

Vous pouvez utiliser l'utilitaire de configuration de TLS pour activer ou désactiver les versions de TLS sur un hôte ESXi. Dans le cadre de ce processus, vous pouvez désactiver TLS 1.0 et activer TLS 1.1 et TLS 1.2. Vous pouvez également désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2.

Pour les hôtes ESXi, utilisez un utilitaire différent que pour les autres composants de votre environnement vSphere. L'utilitaire est spécifique à cette version et ne peut pas être utilisé pour une version précédente.

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.

Cette procédure explique comment effectuer cette tâche sur un hôte unique. Vous pouvez écrire un script pour configurer plusieurs hôtes.

Procédure

1. Connectez-vous au système vCenter Server avec le nom d'utilisateur et le mot de passe de l'utilisateur vCenter Single Sign-On vCenter qui peut exécuter des scripts.
2. Accédez au répertoire dans lequel se trouve le script.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator
   ```

3. Sur un hôte qui fait partie 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.

     ```
     ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2
     ```

   - 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.

     ```
     ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
     ```

4 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.

```
./reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.1 TLSv1.2
```

Note Pour reconfigurer un hôte ESXi autonome (ne faisant pas partie d'un système vCenter Server), utilisez l'option `ESXiHost –h` *HOST* `–u` *ESXi_USER*. Pour l'option *HOST*, vous pouvez spécifier l'adresse IP ou le nom de domaine complet d'un hôte ESXi unique, ou une liste d'adresses IP d'hôte ou de noms de domaine complets. Par exemple, pour activer TLS 1.1 et TLS 1.2 sur deux hôtes ESXi :

```
reconfigureEsx ESXiHost –h 198.51.100.2 198.51.100.3 –u root –p TLSv1.1 TLSv1.2
```

- Pour désactiver TLS 1.0 et TLS 1.1 et activer uniquement TLS 1.2 sur un hôte individuel, exécutez la commande suivante.

```
./reconfigureEsx vCenterHost –h ESXi_Host_Name –u Administrative_User –p TLSv1.2
```

5 Redémarrez l'hôte ESXi pour terminer les modifications du protocole TLS.

Analyser vCenter Server pour les protocoles TLS activés

Après avoir activé ou désactivé les versions TLS sur vCenter Server, vous pouvez utiliser l'utilitaire de configuration de TLS pour afficher vos modifications.

L'option `scan` de l'utilitaire de configuration TLS affiche les versions TLS activées pour chaque service.

Procédure

1 Connectez-vous au système vCenter Server.

a Connectez-vous au dispositif à l'aide de SSH en tant qu'utilisateur avec des privilèges pour exécuter des scripts.

b Si l'interpréteur de commandes de dépistage n'est pas actuellement activé, exécutez les commandes suivantes.

```
shell.set --enabled true
shell
```

2 Accédez au répertoire `VcTlsReconfigurator`.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 Pour afficher les services pour lesquels TLS est activé et les ports utilisés, exécutez la commande suivante.

```
reconfigureVc scan
```

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.

Conditions préalables

Avant de restaurer les modifications, utilisez l'interface de gestion de vCenter Server pour effectuer une sauvegarde de vCenter Server.

Procédure

1 Connectez-vous à l'instance de vCenter Server sur laquelle vous souhaitez restaurer les modifications en tant qu'utilisateur disposant de privilèges d'exécution de scripts.

2 Si le shell de dépistage n'est pas actuellement activé, exécutez les commandes suivantes.

```
shell.set --enabled true
shell
```

3 Accédez au répertoire `VcTlsReconfigurator`.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

4 Examinez la sauvegarde précédente.

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
```

Le résultat est semblable à l'exemple suivant.

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

5 Exécutez la commande suivante pour effectuer une restauration.

```
reconfigureVc restore -d Chemin_répertoire_étape_précédente
```

Le résultat est semblable à l'exemple suivant.

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

6 Répétez la procédure sur toutes les autres instances de vCenter Server.

Privilèges définis

16

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.

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 d'opérations de chiffrement
- Privilèges du groupe dvPort
- Privilèges de Distributed Switch
- Privilèges de centre de données
- Privilèges de banque de données
- Privilèges de cluster de banques de données
- Privilèges de gestionnaire d'agent ESX
- Privilèges d'extension
- Privilèges de fournisseur de statistiques externes
- Privilèges de dossier

- Privilèges globaux
- Privilèges de fournisseur de mises à jour de santé
- 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 de vSphere with Tanzu
- 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 VcTrusts/VcIdentity
- Privilèges d'administrateur d'infrastructure approuvée
- Privilèges de vApp
- Privilèges VcIdentityProviders
- Privilèges de configuration de VMware vSphere Lifecycle Manager
- Privilèges de perspectives de santé ESXi de VMware vSphere Lifecycle Manager
- Privilèges généraux de VMware vSphere Lifecycle Manager
- Privilèges de compatibilité matérielle de VMware vSphere Lifecycle Manager
- Privilèges d'images de VMware vSphere Lifecycle Manager
- Privilèges de correction d'image de VMware vSphere Lifecycle Manager
- Privilèges de paramètres de VMware vSphere Lifecycle Manager
- Privilèges de gestion des lignes de base de VMware vSphere Lifecycle Manager
- Privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager

- Privilèges Télécharger les fichiers de VMware vSphere Lifecycle Manager
- 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 vServices
- Privilèges de balisage vSphere

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 16-1. 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

Tableau 16-1. Privilèges d'alarmes (suite)

Nom de privilège	Description	Requis sur
Alarmes.Supprimer une alarme	Permet la suppression d'une alarme.	Objet sur lequel une alarme est définie
Alarmes.Définir un état d'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. Voir *Installation et configuration de 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 16-2. 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
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. Pour obtenir plus d'informations sur la gestion des certificats vCenter Server, reportez-vous à la section Privilèges requis pour les opérations de gestion des certificats dans la documentation *Authentification 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 16-3. Privilèges de certificats d'hôte

Nom de privilège	Description	Requis sur
Certificats.Gérer des 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 16-4. 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 un abonnement pour une bibliothèque publiée	Permet la création d'un abonnement 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 une bibliothèque abonnée	Autorise la création de bibliothèques abonnées.	vCenter Server

Tableau 16-4. Privilèges de bibliothèque de contenu (suite)

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Supprimer un élément de 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 une bibliothèque locale	Autorise la suppression d'une bibliothèque locale.	Bibliothèque
Bibliothèque de contenu.Supprimer une bibliothèque abonnée	Autorise la suppression d'une bibliothèque abonnée.	Bibliothèque
Bibliothèque de contenu.Supprimer l'abonnement d'une bibliothèque publiée	Permet la suppression d'un abonnement à une bibliothèque.	Bibliothèque
Bibliothèque de contenu.Télécharger des fichiers	Autorise le téléchargement de fichiers de la bibliothèque de contenu.	Bibliothèque
Bibliothèque de contenu.Expulser un 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 une 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 un 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 par défaut pour l'administrateur de bibliothèque de contenu. 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
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

Tableau 16-4. Privilèges de bibliothèque de contenu (suite)

Nom de privilège	Description	Requis sur
Bibliothèque de contenu.Publier un élément de bibliothèque auprès de ses abonnés	Permet la publication d'éléments de bibliothèque aux abonnés.	Bibliothèque. Configurez cette autorisation pour qu'elle se propage à tous les éléments de la bibliothèque.
Bibliothèque de contenu.Publier une bibliothèque auprès de ses abonnés	Permet la publication des bibliothèques aux abonnés.	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 Client n'est associé à ce privilège.	Bibliothèque
Bibliothèque de contenu.Mettre à jour les 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 16-4. 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.Mettre à jour l'abonnement d'une bibliothèque publiée	Permet les mises à jour des paramètres d'abonnement. Les utilisateurs peuvent mettre à jour les paramètres, tels que la spécification de l'instance de vCenter Server de la bibliothèque abonnée et le placement de ses éléments de modèle de machine virtuelle.	Bibliothèque
Bibliothèque de contenu.Afficher les paramètres de configuration	Vous autorise à afficher les paramètres de configuration. Aucun élément d'interface utilisateur de vSphere Client n'est associé à ce privilège.	Bibliothèque

Privilèges d'opérations de chiffrement

Les privilèges d'opérations de chiffrement contrôlent qui peut effectuer quel type d'opération de chiffrement, et sur quel type d'objet.

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 16-5. Privilèges d'opérations de chiffrement

Nom de privilège	Description	Requis sur
Opérations de chiffrement.Accès direct	Permet aux utilisateurs d'accéder aux ressources chiffrées. Les utilisateurs peuvent exporter des machines virtuelles, disposer d'un accès NFC aux machines virtuelles et ouvrir une session de console sur une machine virtuelle chiffrée.	Machine virtuelle, hôte ou banque de données
Opérations de chiffrement.Ajouter un disque	Permet aux utilisateurs d'ajouter un disque à une machine virtuelle chiffrée.	Machine virtuelle
Opérations de chiffrement.Cloner	Permet aux utilisateurs de cloner une machine virtuelle chiffrée.	Machine virtuelle
Opérations de chiffrement.Déchiffrer	Permet aux utilisateurs de déchiffrer une machine virtuelle ou un disque.	Machine virtuelle
Opérations de chiffrement.Chiffrer	Permet aux utilisateurs de chiffrer une machine virtuelle ou un disque de machine virtuelle.	Machine virtuelle

Tableau 16-5. Privilèges d'opérations de chiffrement (suite)

Nom de privilège	Description	Requis sur
Opérations de chiffrement.Chiffrer un nouvel élément	Permet aux utilisateurs de chiffrer une machine virtuelle ou un disque lors de sa création.	Dossier de machine virtuelle
Opérations de chiffrement.Gérer des stratégies de chiffrement	Permet aux utilisateurs de gérer les stratégies de stockage des machines virtuelles avec des filtres d'E/S de chiffrement. Par défaut, les machines virtuelles qui utilisent la stratégie de stockage de chiffrement n'utilisent pas d'autres stratégies de stockage.	Dossier racine de vCenter Server
Opérations de chiffrement.Gérer KMS	Permet aux utilisateurs de gérer le serveur de gestion des clés (KMS) du système vCenter Server. Les tâches de gestion incluent l'ajout et la suppression d'instances de serveur de gestion des clés et l'établissement d'une relation de confiance avec ce serveur.	Système vCenter Server
Opérations de chiffrement.Gérer des clés	Permet aux utilisateurs d'effectuer des opérations de gestion des clés. Ces opérations ne sont pas prises en charge à partir du dispositif vSphere Client mais peuvent être effectuées en utilisant `crypto-util` ou l'API.	Dossier racine de vCenter Server
Opérations de chiffrement.Migrer	Permet aux utilisateurs de migrer une machine virtuelle vers un hôte ESXi différent. Prend en charge la migration avec ou sans vMotion et Storage vMotion. Prend en charge la migration vers une autre instance de vCenter Server.	Machine virtuelle
Opérations de chiffrement.Rechiffrer	Permet aux utilisateurs de rechiffrer les machines virtuelles ou les disques avec une clé différente. Ce privilège est requis pour les opérations de rechiffrement importantes et superficielles.	Machine virtuelle
Opérations de chiffrement.Enregistrer une VM	Permet aux utilisateurs d'enregistrer une machine virtuelle auprès d'un hôte ESXi.	Dossier de machine virtuelle

Tableau 16-5. Privilèges d'opérations de chiffrement (suite)

Nom de privilège	Description	Requis sur
Opérations de chiffrement.Enregistrer un hôte	Permet aux utilisateurs d'activer le chiffrement sur un hôte. Vous pouvez activer le chiffrement sur un hôte explicitement, ou le processus de création de machine virtuelle peut l'activer.	Dossier hôte pour les hôtes autonomes, cluster des hôtes dans le cluster
Opérations de chiffrement.Lire les informations sur le serveur de clés	Permet aux utilisateurs de lister les vSphere Native Key Providers sur le vCenter Server et sur les hôtes. Permet également aux utilisateurs d'obtenir les informations sur le vSphere Native Key Provider.	vCenter Server ou hôte

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 16-6. 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 de portée	Permet de définir la portée d'un groupe de ports virtuels distribués.	Groupes de ports virtuels

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 16-7. Privilèges de vSphere Distributed Switch

Nom de privilège	Description	Requis sur
Distributed Switch.Créer	Autorise la création d'une instance de Distributed Switch.	Centres de données, dossiers réseau
Distributed Switch.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
Distributed Switch.Opération de l'hôte	Autorise le changement des membres hôtes d'une instance de Distributed Switch.	Distributed switches
Distributed Switch.Modifier	Autorise la modification de la configuration d'une instance de Distributed Switch.	Distributed switches
Distributed Switch.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
Distributed Switch.Opération de stratégie	Autorise la modification de la règle d'un vSphere Distributed Switch.	Distributed switches
Distributed Switch .Opération de configuration de port	Autorise la modification de la configuration d'un port dans un vSphere Distributed Switch.	Distributed switches
Distributed Switch.Opération de définition de port	Autorise la modification des paramètres d'un port dans un vSphere Distributed Switch.	Distributed switches
Distributed Switch.Opération VSPAN	Autorise la modification de la configuration VSPAN d'un vSphere Distributed Switch.	Distributed switches

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 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 16-8. 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 d'un profil de protocole réseau	Permet de configurer le profil réseau d'un centre de données.	Centre de données
Centre de données.Interroger une allocation de pool de requêtes IP	Permet la configuration d'un pool d'adresses IP.	Centre de données
Centre de données.Reconfigurer 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
Centre de données.Supprimer centre de données	Permet de supprimer un centre de données. Pour pouvoir exécuter cette opération, vous devez disposer de ce privilège 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 16-9. 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
Banque de données.Renommer une banque de données	Permet de renommer une banque de données.	Centres de données
Banque de données.Mettre à jour des 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 des métadonnées de 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 16-10. 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 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 16-11. Gestionnaire d'agent ESX

Nom de privilège	Description	Requis sur
ESX Agent Manager.Configuration	Permet de déployer une machine virtuelle d'agent sur un hôte ou un cluster.	Machines virtuelles
ESX Agent Manager.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
ESX Agent View.Afficher	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 16-12. Privilèges d'extension

Nom de privilège	Description	Requis sur
Extension.Enregistrer une extension	Permet d'enregistrer une extension (plug-in).	Instance racine de vCenter Server
Extension.Annuler l'enregistrement d'une extension	Permet d'annuler l'enregistrement d'une extension (plug-in).	Instance racine de vCenter Server
Extension.Mettre à jour une extension	Permet de mettre à jour une extension (plug-in).	Instance racine de vCenter Server

Privilèges de fournisseur de statistiques externes

Les privilèges de fournisseur de statistiques externes contrôlent la capacité de notifier vCenter Server des statistiques DRS (Distributed Resource Scheduler) proactif.

Ces privilèges s'appliquent uniquement à une API interne à VMware.

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 16-13. 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 16-14. 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.	Instance racine de 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.	Instance racine de 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.	Instance racine de vCenter Server
Global.Désactiver des méthodes	Permet à des serveurs d'extensions de vCenter Server de désactiver des opérations sur des objets gérés par vCenter Server.	Instance racine de vCenter Server
Global.Activer des méthodes	Permet aux serveurs d'extensions vCenter Server d'activer certaines opérations sur des objets gérés par vCenter Server.	Instance racine de vCenter Server
Global.Balise globale	Permet l'ajout ou la suppression de balises globales.	Hôte racine ou instance racine de vCenter Server
Global.Santé	Permet l'affichage de l'état de fonctionnement de composants de vCenter Server.	Instance racine de vCenter Server
Global.Licences	Permet l'affichage de licences installées, ainsi que l'ajout ou la suppression de licences.	Hôte racine ou instance racine de 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.	Instance racine de vCenter Server
Global.Proxy	Permet l'accès à une interface interne pour ajouter ou supprimer des points finaux à ou depuis un proxy.	Instance racine de vCenter Server
Global.Action de script	Permet de planifier une action de script conjointement à une alarme.	Tout objet
Global.Gestionnaires de services	Permet l'utilisation de la commande `resxtop` dans ESXCLI.	Hôte racine ou instance racine de vCenter Server
Global.Définir un attribut personnalisé	Permet de visualiser, créer ou supprimer des attributs personnalisés pour un objet géré.	Tout objet

Tableau 16-14. Privilèges globaux (suite)

Nom de privilège	Description	Requis sur
Global.Paramètres	Permet la lecture ou la modification de paramètres de configuration d'exécution de vCenter Server.	Instance racine de vCenter Server
Global.Balise système	Permet l'ajout ou la suppression de balises système.	Instance racine de vCenter Server

Privilèges de fournisseur de mises à jour de santé

Les privilèges de fournisseur de mise à jour de santé contrôlent la capacité des fournisseurs de matériel de notifier vCenter Server des événements HA proactive.

Ces privilèges s'appliquent uniquement à une API interne à VMware.

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 16-15. 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 16-16. 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

Tableau 16-16. Privilèges de configuration d'hôte (suite)

Nom de privilège	Description	Requis sur
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 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.Microprogramme	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 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 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
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 16-17. 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 cluster	Permet de créer un cluster.	Dossiers d'hôte
Hôte.Inventaire.Modifier 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
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'hôte contrôlent les actions effectuées lorsque VMware Host 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 16-18. 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.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

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 16-19. 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 16-20. Privilèges de profil d'hôte

Nom de privilège	Description	Requis sur
Profil d'hôte.Effacer	Permet d'effacer les informations liées au profil.	Instance racine de vCenter Server
Profil d'hôte.Créer	Permet la création d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Supprimer	Permet la suppression d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Modifier	Permet la modification d'un profil d'hôte.	Instance racine de vCenter Server
Profil d'hôte.Exporter	Permet l'exportation d'un profil d'hôte	Instance racine de vCenter Server
Profil d'hôte.Afficher	Permet l'affichage d'un profil d'hôte.	Instance racine de vCenter Server

Privilèges de vSphere with Tanzu

Les privilèges des espaces de noms contrôlent les utilisateurs autorisés à créer et gérer des espaces de noms VMware vSphere® with VMware Tanzu™.

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 16-21. Privilèges des espaces de noms

Nom de privilège	Description	Requis sur
Espaces de noms.Modifier la configuration à l'échelle du cluster	Permet de modifier la configuration à l'échelle du cluster et d'activer et désactiver les espaces de noms du cluster.	Clusters
Espaces de noms.Modifier la configuration de l'espace de noms	Permet de modifier les options de configuration de l'espace de noms, telles que l'allocation des ressources et les autorisations des utilisateurs.	Clusters

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 16-22. Privilèges de réseau

Nom de privilège	Description	Requis sur
Réseau.Attribuer 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 16-23. 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.	Instance racine de 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 16-24. 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 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.Réattribuer 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 16-25. Privilèges de stockage basé sur le profil

Nom de privilège	Description	Requis sur
Stockage basé sur le profil.Mise à jour du stockage basé 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.	Instance racine de vCenter Server
Stockage basé sur le profil.Vue du stockage basé sur le profil	Permet d'afficher les capacités de stockage et les profils de stockage définis.	Instance racine de 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 16-26. 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.	Instance racine de vCenter Server
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 16-27. 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 une tâche	Permet de reconfigurer les propriétés de tâche planifiée.	Tout objet
Tâche planifiée.Supprimer une 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 16-28. Privilèges de session

Nom de privilège	Description	Requis sur
Sessions.Emprunter l'identité d'un utilisateur	Permet d'emprunter l'identité d'un autre utilisateur. Cette capacité est utilisée par des extensions.	Instance racine de vCenter Server
Sessions.Message	Permet de définir le message global de connexion.	Instance racine de vCenter Server
Sessions.Valider une session	Permet de vérifier la validité de la session.	Instance racine de 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.	Instance racine de 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. À partir de vSphere 6.0, les vues de stockage sont abandonnées et ces privilèges ne s'y appliquent plus.

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 16-29. Privilèges de vues de stockage

Nom de privilège	Description	Requis sur
Vues de stockage.Configurer un service	Permet aux utilisateurs ayant des privilèges d'utiliser tous les API du service de surveillance du stockage. Utilisez **Vues de stockage.Afficher** pour les privilèges des API en lecture seule du service de surveillance du stockage.	Instance racine de vCenter Server
Vues de stockage.Afficher	Permet aux utilisateurs ayant des privilèges d'utiliser les API en lecture seule du service de surveillance du stockage.	Instance racine de 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 16-30. 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 Client n'est associé à ce privilège.	Instance racine de vCenter Server
Tâches.Mettre à jour une tâche	Permet à une extension de mettre à jour une tâche définie par l'utilisateur. Aucun élément d'interface utilisateur de vSphere Client n'est associé à ce privilège.	Instance racine de vCenter Server

Privilèges Transfer Service

Les privilèges Transfer Service sont internes à VMware. N'utilisez pas ces privilèges.

Privilèges VcTrusts/VcIdentity

Les privilèges VcTrusts/VcIdentity contrôlent l'accès à diverses API et fonctionnalités internes liées à la confiance entre les systèmes vCenter Server.

Tableau 16-31. Privilèges VcTrusts/VcIdentity

Nom de privilège	Description	Requis sur
VcTrusts/VcIdentity.Créer/Mettre à jour/Supprimer (privilèges d'administrateur)	Autorise un accès complet au niveau administratif à diverses API et fonctionnalités internes liées à la confiance entre les systèmes vCenter Server.	S.O.
VcTrusts/VcIdentity.Créer/Mettre à jour/Supprimer (sous les Privilèges d'administrateur)	Autorise un accès administratif réduit à diverses API et fonctionnalités internes liées à la confiance entre les systèmes vCenter Server. Ce privilège limite la création/mise à jour/suppression de VcTrusts/VcIdentity afin que l'utilisateur ne puisse pas transférer des privilèges non-administrateur.	S.O.

Privilèges d'administrateur d'infrastructure approuvée

Les privilèges d'administrateur d'infrastructure approuvée configurent et gèrent un déploiement de Autorité d'approbation vSphere .

Ces privilèges déterminent qui peut effectuer des tâches de configuration et de gestion pour un déploiement de Autorité d'approbation vSphere . Pour plus d'informations sur les rôles d'autorité d'approbation et le groupe TrustedAdmins, consultez Conditions préalables et privilèges requis pour l'autorité d'approbation vSphere.

Tableau 16-32. Privilèges d'administrateur d'infrastructure approuvée

Nom de privilège	Description	Requis sur
Administrateur d'infrastructure approuvée.Configurer l'approbation du serveur de clés	Permet de gérer les fournisseurs de clés du service de fournisseur de clés.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Configurer les certificats TPM de l'hôte d'autorité d'approbation	Permet la création et la modification des paramètres du service d'attestation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Configurer les métadonnées de l'hôte d'autorité d'approbation	Permet de modifier les images de base à attester par le service d'attestation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Configurer l'attestation SSO	Permet de modifier les hôtes qui peuvent être approuvés par les hôtes d'autorité d'approbation.	Instance racine de vCenter Server

Tableau 16-32. Privilèges d'administrateur d'infrastructure approuvée (suite)

Nom de privilège	Description	Requis sur
Administrateur d'infrastructure approuvée.Configurer la stratégie de conversion de jeton	Permet de configurer la stratégie de conversion de jeton.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Répertorier les hôtes d'infrastructure approuvée	Permet de lire des informations sur les hôtes approuvés et les hôtes d'autorité d'approbation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Répertorier les informations sur le STS	Permet d'exporter les détails de l'hôte approuvé afin qu'ils puissent être importés dans le cluster d'autorité d'approbation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Gérer les hôtes d'infrastructure approuvée	Permet de modifier les informations sur les hôtes approuvés et les hôtes d'autorité d'approbation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Lire l'approbation du serveur de clés	Permet de lire les fournisseurs de clés du service de fournisseur de clés.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Lire l'attestation SSO	Permet de lire les hôtes qui peuvent être approuvés par les hôtes d'autorité d'approbation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Récupérer les certificats d'hôte de l'autorité d'approbation TPM	Permet de lire les paramètres du service d'attestation.	Instance racine de vCenter Server
Administrateur d'infrastructure approuvée.Récupérer les métadonnées de l'hôte de l'autorité d'approbation	Permet de lire les images de base qui peuvent être attestées par le service d'attestation.	Instance racine de vCenter Server

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 16-33. 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.Attribuer un pool de ressources	Permet d'attribuer un pool de ressources à un vApp.	vApp
vApp.Attribuer 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.Exporter	Permet d'exporter un vApp à partir de vSphere.	vApp
vApp.Importer	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 un 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
vApp.Configuration d'une application de vApp	Permet de modifier la structure interne d'un vApp, telle que l'information produit et les propriétés.	vApp
vApp.Configuration d'une instance de vApp	Permet de modifier la configuration d'une instance de vApp, telle que les stratégies.	vApp

Tableau 16-33. Privilèges de vApp (suite)

Nom de privilège	Description	Requis sur
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 Client n'est associé à ce privilège.	vApp
vApp.Configuration des ressources de 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 VcIdentityProviders

Les privilèges VcIdentityProviders contrôlent l'accès à l'API VcIdentityProviders.

Tableau 16-34. Privilèges VcIdentityProviders

Nom de privilège	Description	Requis sur
VcIdentityProviders.Créer	Autorise l'accès en création seule à l'API VcIdentityProviders (fournisseurs d'identité vCenter Server).	S.O.
VcIdentityProviders.Gérer	Autorise l'accès en écriture au niveau administratif (créer, lire, mettre à jour, supprimer) à l'API VcIdentityProviders (fournisseurs d'identité vCenter Server).	S.O.
VcIdentityProviders.Lire	Autorise l'accès en lecture à l'API VcIdentityProviders (fournisseurs d'identité vCenter Server).	S.O.

Privilèges de configuration de VMware vSphere Lifecycle Manager

Les privilèges de configuration de VMware vSphere Lifecycle Manager contrôlent la capacité de configuration du service vSphere Lifecycle Manager.

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 16-35. Privilèges de configuration de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Configurer.Configurer le service	Permet la configuration du service vSphere Lifecycle Manager et de la tâche planifiée de téléchargement des correctifs.	Instance racine de vCenter Server

Privilèges de perspectives de santé ESXi de VMware vSphere Lifecycle Manager

Les privilèges de perspective de santé de VMware vSphere Lifecycle Manager ESXi contrôlent la capacité de vérification de la santé des hôtes et des clusters ESXi.

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 16-36. Privilèges de perspectives de santé ESXi de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Perspectives de santé d'ESXi.Lire	Permet d'interroger la santé des hôtes et des clusters ESXi.	Hôtes Clusters
VMware vSphere Lifecycle Manager.Perspectives de santé d'ESXi.Écrire	S.O.	S.O.

Privilèges généraux de VMware vSphere Lifecycle Manager

Les privilèges généraux de VMware vSphere Lifecycle Manager contrôlent la capacité de lecture et d'écriture des ressources de Lifecyle Manager.

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 16-37. Privilèges généraux de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges généraux.Lire	Permet de lire les ressources de vSphere Lifecycle Manager. Ce privilège est requis pour obtenir des informations sur la tâche.	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges généraux.Écrire	Permet d'écrire les ressources de vSphere Lifecycle Manager. Ce privilège est requis pour annuler une tâche de vSphere Lifecycle Manager.	Instance racine de vCenter Server

Privilèges de compatibilité matérielle de VMware vSphere Lifecycle Manager

Les privilèges de compatibilité matérielle de VMware vSphere Lifecycle Manager contrôlent la capacité de détection et de résolution des problèmes potentiels de compatibilité matérielle.

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 16-38. Privilèges de compatibilité matérielle de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges de compatibilité matérielle.Accès à la compatibilité matérielle	Permet l'accession aux données de compatibilité matérielle et la résolution des problèmes potentiels de compatibilité matérielle.	Hôtes

Privilèges d'images de VMware vSphere Lifecycle Manager

Les privilèges d'images de VMware vSphere Lifecycle Manager contrôlent la capacité de gestion des images.

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 16-39. Privilèges d'images de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges d'image.Lire	Permet la lecture d'images de vSphere Lifecycle Manager. Ce privilège est requis pour : ■ Répertorier tous les brouillons d'un cluster ■ Obtenir plus d'informations sur un brouillon ■ Effectuer une analyse sur un brouillon ■ Valider un brouillon ■ Récupérer le contenu d'un brouillon ■ Calculer la liste des composants effectifs ■ Afficher le contenu du document d'état souhaité actuel ■ Démarrer une analyse sur un cluster ■ Obtenir le résultat de la conformité ■ Obtenir une recommandation ■ Exporter l'état souhaité actuel en tant que dépôt, fichier JSON ou image ISO	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges d'image.Écrire	Permet la gestion des images de vSphere Lifecycle Manager. Ce privilège est requis pour : ■ Créer, supprimer ou valider un brouillon ■ Importer l'état souhaité ■ Générer des recommandations ■ Définir ou supprimer différentes parties d'un brouillon	Instance racine de vCenter Server

Privilèges de correction d'image de VMware vSphere Lifecycle Manager

Les privilèges d'images de VMware vSphere Lifecycle Manager contrôlent la capacité de correction des images.

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 16-40. Privilèges de correction d'image de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges de correction d'image.Lire	Permet d'effectuer la vérification préalable de la correction.	Clusters
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges de correction d'image.Écrire	Permet d'effectuer la correction.	Clusters

Privilèges de paramètres de VMware vSphere Lifecycle Manager

Les privilèges de paramètres de VMware vSphere Lifecycle Manager contrôlent la capacité de gestion des dépôts et des stratégies de correction.

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 16-41. Privilèges de paramètres de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges relatifs aux paramètres.Lire	Permet la lecture de dépôts et de stratégies de correction de vSphere Lifecycle Manager.	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager : privilèges relatifs aux paramètres.Écrire	Permet l'écriture de dépôts et de stratégies de correction de vSphere Lifecycle Manager.	Instance racine de vCenter Server

Privilèges de gestion des lignes de base de VMware vSphere Lifecycle Manager

Les privilèges de gestion des lignes de base de VMware vSphere Lifecycle Manager contrôlent la capacité de gestion des lignes de base et des groupes de lignes de base.

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 16-42. Privilèges de gestion des lignes de base de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Gérer les lignes de base.Attacher une ligne de base	Permet l'attachement de lignes de base et de groupes de lignes de base à des objets dans l'inventaire vSphere.	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Gérer les lignes de base.Gérer une ligne de base	Permet la création, la modification ou la suppression de lignes de base et de groupes de lignes de base.	Instance racine de vCenter Server

Privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager

Les privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager contrôlent la capacité d'affichage, d'analyse et de correction des correctifs, extensions ou mises à niveau applicables.

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 16-43. Privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Gérer les correctifs et les mises à niveau.Corriger pour appliquer les correctifs, les extensions et les mises à niveau	Permet la correction de machines virtuelles et d'hôtes en vue d'appliquer des correctifs, des extensions ou des mises à niveau lors de l'utilisation de lignes de base. Ce privilège permet également d'afficher l'état de conformité.	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Gérer les correctifs et les mises à niveau.Rechercher les correctifs, les extensions et les mises à niveau applicables	Permet l'analyse de machines virtuelles et d'hôtes pour rechercher des correctifs, des extensions ou des mises à niveau applicables lors de l'utilisation de lignes de base.	Instance racine de vCenter Server

Tableau 16-43. Privilèges Gérer les correctifs et les mises à niveau de VMware vSphere Lifecycle Manager (suite)

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Gérer les correctifs et les mises à niveau.Transférer les correctifs et les extensions	Permet le transfert de correctifs ou d'extensions vers des hôtes ESXi lors de l'utilisation de lignes de base. Ce privilège permet également d'afficher l'état de conformité des hôtes ESXi.	Instance racine de vCenter Server
VMware vSphere Lifecycle Manager.Gérer les correctifs et les mises à niveau.Afficher l'état de conformité	Permet l'affichage d'informations de conformité de ligne de base pour un objet dans l'inventaire vSphere.	Instance racine de vCenter Server

Privilèges Télécharger les fichiers de VMware vSphere Lifecycle Manager

Les privilèges Télécharger les fichiers de VMware vSphere Lifecycle Manager contrôlent la capacité d'importation des mises à jour dans le dépôt de vSphere Lifecycle Manager.

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 16-44. Privilèges Télécharger les fichiers de VMware vSphere Lifecycle Manager

Nom de privilège	Description	Requis sur
VMware vSphere Lifecycle Manager.Télécharger un fichier.Télécharger un fichier	Permet le chargement de fichiers ISO de mise à niveau et de bundles de correctifs hors ligne.	Instance racine de vCenter Server

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 16-45. Privilèges de configuration de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Acquérir un bail de disque	Permet des opérations de bail de disque pour une machine virtuelle.	Machines virtuelles
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.Configuration avancée	Permet l'ajout ou la modification de paramètres avancés dans le fichier de configuration de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Modifier le nombre de CPU	Permet de changer le nombre de CPU virtuels.	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	Permet de modifier les paramètres généraux d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Modifier le placement du fichier d'échange	Permet de changer la règle de placement du fichier d'échange d'une machine virtuelle.	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 le périphérique USB hôte	Permet d'attacher à une machine virtuelle un périphérique USB hébergé sur hôte.	Machines virtuelles
Machine virtuelle.Configuration.Configurer le 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

Tableau 16-45. Privilèges de configuration de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
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.Afficher 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.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 des fichiers sans propriétaire	Permet d'interroger des fichiers sans propriétaire.	Machines virtuelles
Machine virtuelle.Configuration.Recharger à partir du chemin d'accès	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 des informations d'invité	Permet de modifier les informations du système d'exploitation invité d'une machine virtuelle	Machines virtuelles
Machine virtuelle.Configuration.Définir une annotation	Permet d'ajouter ou de modifier une annotation de machine virtuelle.	Machines virtuelles
Machine virtuelle.Configuration.Basculer le suivi des changements de disques	Permet l'activation ou la désactivation du suivi des modifications des disques de la machine virtuelle.	Machines virtuelles

Tableau 16-45. Privilèges de configuration de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Configuration.Basculer le parent de déviation	Permet l'activation ou la désactivation d'un parent vmfork.	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 applications 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 de l'API vSphere Web 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.

Tableau 16-46. Opérations de système invité d'une machine virtuelle

Nom de privilège	Description	Pertinent sur l'objet
Machine virtuelle.Systèmes invités.Modification d'alias d'un système invité	Autorise les opérations d'invité d'une machine virtuelle impliquant la modification de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Systèmes invités.Requête d'alias d'un système invité	Autorise les opérations d'invité d'une machine virtuelle impliquant l'interrogation de l'alias de la machine virtuelle.	Machines virtuelles
Machine virtuelle.Systèmes invités.Modifications d'un système 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 Client n'est associé à ce privilège.	Machines virtuelles

Tableau 16-46. Opérations de système invité d'une machine virtuelle (suite)

Nom de privilège	Description	Pertinent sur l'objet
Machine virtuelle.Systèmes invités.Exécution du programme d'un système invité	Autorise les opérations de système invité d'une machine virtuelle impliquant l'exécution d'une application dans la machine virtuelle. Aucun élément d'interface utilisateur de vSphere Client n'est associé à ce privilège.	Machines virtuelles
Machine virtuelle.Systèmes invités.Requêtes d'un système 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 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 16-47. 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 machine virtuelle	Permet d'exécuter des opérations de sauvegarde sur des machines virtuelles.	Machines virtuelles
Machine virtuelle.Interaction.Configurer un support sur CD	Permet de configurer un DVD virtuel ou un lecteur de CD-ROM.	Machines virtuelles

Tableau 16-47. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Configurer un support sur disquette	Permet de configurer un périphérique de disquettes 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
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 à un périphérique	Permet de modifier l'état connecté des périphériques virtuels déconnectables d'une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction .Glisser-déplacer	Permet le glisser-déplacer de fichiers entre une machine virtuelle et un client distant.	Machines virtuelles
Machine virtuelle.Interaction.Gestion par VIX API d'un 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
Machine virtuelle.Interaction .Interrompre ou reprendre	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
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

Tableau 16-47. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
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
Machine virtuelle.Interaction.Session d'enregistrement sur machine virtuelle	Permet d'enregistrer une session sur une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Session de relecture sur 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 redémarre le système d'exploitation invité.	Machines virtuelles
Machine virtuelle .Interaction .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
Machine virtuelle .Interaction .Interrompre Fault Tolerance	Permet la suspension de Fault Tolerance pour une machine virtuelle.	Machines virtuelles
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
Machine virtuelle.Interaction.Désactiver Fault Tolerance	Permet de mettre hors tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles

Tableau 16-47. Interaction de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
Machine virtuelle.Interaction.Activer Fault Tolerance	Permet de mettre sous tension Fault Tolerance pour une machine virtuelle.	Machines virtuelles
Machine virtuelle.Interaction.Installation de 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 16-48. Privilèges d'inventaire de machine virtuelle

Nom de privilège	Description	Requis sur
Machine virtuelle .Inventaire.Créer à partir d'un modèle existant	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.Enregistrer	Permet d'ajouter une machine virtuelle existante à vCenter Server ou à un inventaire d'hôtes.	Clusters, hôtes, dossiers de machine virtuelle

Tableau 16-48. Privilèges d'inventaire de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
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 16-49. 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 fichier	Permet d'effectuer des opérations sur des fichiers associés à une machine virtuelle, y compris les fichiers vmx, les disques, les journaux et les nvram.	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 instance racine de vCenter Server
Machine virtuelle.Provisionnement.Autoriser le téléchargement de fichiers de machine virtuelle	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 instance racine de vCenter Server

Tableau 16-49. Privilèges de provisionnement de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
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.Déployer 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.	Instance racine de vCenter Server
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 des tâches 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.

Tableau 16-50. Privilèges de configuration de services de machine virtuelle

Nom de privilège	Description
Machine virtuelle.Configuration de service.Autoriser les notifications	Permet la génération et la consommation de notifications sur l'état des services.
Machine virtuelle.Configuration de service.Autoriser l'interrogation des 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 16-51. 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

Tableau 16-51. Privilèges d'état de machine virtuelle (suite)

Nom de privilège	Description	Requis sur
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.Restaurer un 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 16-52. 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 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 16-53. 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 jour la dépendance	Permet des mises à jour d'une dépendance pour configurer le nom ou la description.	vApp et machines virtuelles

Privilèges de balisage vSphere

Les privilèges de balisage vSphere 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 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 16-54. Privilèges de balisage vSphere

Nom de privilège	Description	Requis sur
Balisage vSphere.Attribuer une balise vSphere ou en annuler l'attribution	Permet d'attribuer ou non une balise pour un objet dans l'inventaire vCenter Server.	Tout objet
Balisage vSphere.Attribuer une balise vSphere ou en annuler l'attribution sur un objet	Permet aux objets d'avoir des balises attribuées ou non attribuées. Utilisez ce privilège pour limiter les objets auxquels les utilisateurs peuvent attribuer des balises ou annuler l'attribution de balises.	Tout objet
Balisage vSphere.Créer une balise vSphere	Permet de créer une balise.	Tout objet
Balisage vSphere.Créer une catégorie de balises vSphere	Permet de créer une catégorie de balise.	Tout objet
Balisage vSphere.Supprimer une balise vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Balisage vSphere.Supprimer une catégorie de balises vSphere	Permet de supprimer une catégorie de balise.	Tout objet
Balisage vSphere.Modifier une balise vSphere	Permet de modifier une balise.	Tout objet
Balisage vSphere.Modifier une catégorie de balises vSphere	Permet la modification d'une catégorie de balise.	Tout objet

Tableau 16-54. Privilèges de balisage vSphere (suite)

Nom de privilège	Description	Requis sur
Balisage vSphere.Modifier le champ Utilisé par une catégorie	Permet la modification du champ UsedBy pour une catégorie de balise.	Tout objet
Balisage vSphere.Modifier le champ Utilisé par une balise	Permet la modification du champ UsedBy pour une balise.	Tout objet

Présentation de la sécurisation renforcée et de la conformité dans vSphere

17

Les organisations veulent garantir la sécurité de leurs données en réduisant les risques de vol de données, de cyber-attaque ou d'accès non autorisé. Les organisations doivent également souvent se conformer à diverses réglementations, des normes gouvernementales aux normes privées, telles que le NIST (National Institute of Standards and Technology) et DISA STIG (Defense Information Systems Agency Security Technical Implementation Guides). Pour garantir que votre environnement vSphere est conforme à ces normes, il faut comprendre un large ensemble d'éléments à prendre en compte, notamment les personnes, les processus et les technologies.

Une présentation de haut niveau des rubriques de sécurité et de conformité nécessitant un examen approfondi aide à planifier votre stratégie de conformité. Vous pouvez également tirer parti d'autres ressources de conformité sur le site Web VMware.

Ce chapitre contient les rubriques suivantes :

- Sécurité ou conformité dans l'environnement vSphere
- Présentation du guide de configuration de sécurité vSphere
- À propos de l'Institut national des normes et de la technologie (NIST, National Institute of Standards and Technology)
- À propos des directives STIG DISA
- À propos du cycle de développement de sécurité de VMware
- Journalisation d'audit
- Présentation des prochaines étapes de sécurité de conformité
- vCenter Server et FIPS

Sécurité ou conformité dans l'environnement vSphere

Les termes sécurité et conformité sont souvent utilisés de manière interchangeable. Cependant, ce sont des concepts uniques et distincts.

La sécurité, souvent considérée comme la sécurité des informations, est généralement définie comme un ensemble de contrôles techniques, physiques et administratifs que vous mettez en œuvre pour assurer la confidentialité, l'intégrité et la disponibilité. Par exemple, vous sécurisez un hôte en définissant les comptes autorisant une connexion et par quels moyens (SSH, console directe, etc.). En revanche, la conformité est un ensemble de conditions nécessaires pour répondre aux contrôles minimaux établis par différentes structures réglementaires qui fournissent une assistance limitée sur n'importe quel type de technologie, de fournisseur ou de configuration. Par exemple, l'industrie PCI (Payment Card Industry) a établi des directives de sécurité pour aider les organisations à protéger de manière proactive les données des comptes clients.

La sécurité réduit le risque de vol de données, de cyberattaques ou d'accès non autorisé, alors que la conformité est la preuve qu'un contrôle de la sécurité est en place, généralement dans un cadre temporel défini. La sécurité est principalement définie dans les décisions de conception et exprimée dans les configurations de la technologie. La conformité se concentre sur le mappage de la corrélation entre les contrôles de sécurité et les exigences spécifiques. Un mappage de conformité fournit une vue centralisée pour répertorier de nombreux contrôles de sécurité requis. Ces contrôles sont décrits de façon plus détaillée en incluant des citations de conformité respectives de chaque contrôle de sécurité, tels que régis par un domaine, par exemple NIST, PCI, FedRAMP, HIPAA, etc.

Les programmes de cyber-sécurité et de conformité effectifs reposent sur trois piliers : les personnes, les processus et les technologies. Une idée fausse généralement répandue veut que la technologie puisse à elle seule répondre à tous vos besoins en matière de cybersécurité. La technologie joue un rôle crucial dans le développement et l'exécution d'un programme de sécurité des informations. Cependant, la technologie sans processus et procédures, connaissances et formation, crée une vulnérabilité au sein de votre organisation.

Lors de la définition de vos stratégies de sécurité et de conformité, gardez les éléments suivants à l'esprit :

- Les personnes ont besoin de connaissances et de formation générales, tandis que le personnel informatique a besoin d'une formation spécifique.
- Le processus définit comment les activités, les rôles et la documentation de votre organisation contribuent à atténuer les risques. Les processus ne sont efficaces que si les personnes les appliquent correctement.
- La technologie peut être utilisée pour prévenir ou réduire l'impact des risques de cyber-sécurité dans votre organisation. La technologie à utiliser dépend du niveau d'acceptation du risque de votre organisation.

VMware fournit des kits de conformité qui contiennent à la fois un guide d'audit et un guide d'applicabilité du produit, ce qui permet de faire le lien entre les obligations réglementaires et de conformité et les guides de mise en œuvre. Pour plus d'informations, consultez https://core.vmware.com/compliance.

Glossaire des termes relatifs à la conformité

La conformité introduit des termes et des définitions spécifiques importants à comprendre.

Tableau 17-1. Conditions de conformité

Terme	Définition
CJIS	Services d'information sur la justice pénale (Criminal Justice Information Services). Dans le contexte de la conformité, les services CJIS produisent une stratégie de sécurité établissant comment la justice pénale au niveau local, de l'état et fédéral, ainsi que les forces de l'ordre prennent des mesures de sécurité visant à protéger des informations sensibles telles que les empreintes digitales et les antécédents criminels.
STIG DISA	Defense Information Systems Agency Security Technical Implementation Guide. DISA (Defense Information Systems Agency) est l'entité responsable de la gestion de la position en matière de sécurité de l'infrastructure informatique du Ministère de la Défense (DoD). DISA accomplit cette tâche en développant et en utilisant des Guides de mise en œuvre techniques de sécurité ou « STIG ».
FedRAMP	Federal Risk and Authorization Management Program. FedRAMP est un programme à l'échelle du gouvernement qui fournit une approche normalisée de l'évaluation de la sécurité, l'autorisation et la surveillance continue des produits et des services cloud.
HIPAA	Health Insurance Portability and Accountability Act. Adoptée au congrès en 1996, la loi HIPAA produit des effets suivants : ■ Donne à des millions de travailleurs américains et à leurs familles la possibilité de transférer et de maintenir une couverture d'assurance-maladie lorsqu'ils changent d'employeur ou perdent leur emploi ■ Réduit les fraudes et abus en matière de soins de santé ■ Impose des normes globales en matière d'informations relatives aux soins de santé, notamment pour la facturation électronique et autres processus ■ Nécessite la protection et le traitement confidentiel des informations de santé protégées Le dernier point est le plus important pour la documentation de la *sécurité vSphere*.
NCCoE	National Cybersecurity Center of Excellence. NCCoE est une organisation gouvernementale américaine qui produit et partage publiquement des solutions aux problèmes de sécurité que les entreprises américaines rencontrent. Le centre forme regroupe des spécialistes issus d'entreprises technologiques de cyber-sécurité, d'autres agences fédérales et d'universités afin de résoudre chaque problème.

Tableau 17-1. Conditions de conformité (suite)

Terme	Définition
NIST	National Institute of Standards and Technology. Fondée en 1901, NIST est une agence fédérale non réglementaire faisant parti du Département du Commerce des États-Unis. L'une des missions du NIST est de promouvoir l'innovation et la compétitivité industrielle en faisant progresser les sciences, les normes et les technologies de mesure de manière à favoriser la sécurité économique et améliorer notre qualité de vie.
PAG	Product Applicability Guide. Document qui fournit des directives générales aux organisations pour les aider à choisir des solutions leur permettant de répondre aux exigences de conformité leur étant imposées.
PCI DSS	Payment Card Industry Data Security Standard. Ensemble de normes de sécurité visant à garantir que toutes les entreprises qui acceptent, traitent, stockent ou transmettent des informations de carte de crédit maintiennent un environnement sécurisé.
Solutions de conformité VVD/VCF	VMware Validated Design/VMware Cloud Foundation. Les conceptions validées VMware fournissent des Blueprints complets et ayant fait l'objet de tests intensifs, permettant de construire et d'exploiter un centre de données défini par le logiciel. Les solutions de conformité VVD/VCF permettent aux clients de répondre aux exigences de conformité de nombreuses réglementations gouvernementales et industrielles.

Présentation du guide de configuration de sécurité vSphere

VMware crée des Guides de sécurisation renforcée qui fournissent des recommandations sur le déploiement et l'exploitation des produits VMware de manière sécurisée. Pour vSphere, ce guide est appelé *Guide de configuration de la sécurité vSphere* (nommé auparavant *Guide de sécurisation renforcée*).

Le *Guide de configuration de la sécurité vSphere* contient des recommandations en matière de sécurité pour vSphere. Le *Guide de configuration de la sécurité vSphere* n'est pas directement relié aux directives ou aux cadres réglementaires, il ne s'agit donc pas d'un guide de conformité. En outre, le *Guide de configuration de la sécurité vSphere* n'est pas destiné à être utilisé comme liste de contrôle de la sécurité. La sécurité doit toujours être vue comme un compromis. Lorsque vous implémentez des contrôles de sécurité, vous pouvez avoir une incidence négative sur l'utilisation, les performances ou d'autres tâches opérationnelles. Examinez attentivement vos charges de travail, vos modèles d'utilisation, votre structure organisationnelle, etc. avant d'apporter des modifications à la sécurité, quel que soit le conseil fourni par VMware ou d'autres sources du secteur. Si votre organisation est soumise à des exigences de conformité réglementaire, consultez Sécurité ou conformité dans l'environnement vSphere ou visitez le

site Web https://core.vmware.com/compliance. Ce site contient des kits de conformité et des guides d'audit de produit pour aider les administrateurs vSphere et les auditeurs réglementaires à sécuriser et à attester l'infrastructure virtuelle pour différents cadres réglementaires, tels que NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001, etc.

Le *Guide de configuration de la sécurité vSphere* ne traite pas la sécurisation des éléments suivants :

- Logiciel s'exécutant dans la machine virtuelle, tel que le système d'exploitation invité et les applications
- Trafic en cours d'exécution via les réseaux de machine virtuelle
- Sécurité des produits de modules complémentaires

Le *Guide de configuration de la sécurité vSphere* n'est pas destiné à être utilisé comme un outil de « conformité ». Le *Guide de configuration de la sécurité vSphere* vous permet de prendre les mesures initiales d'une mise en conformité, mais ne garantit pas par lui-même la conformité de votre déploiement. Pour plus d'informations sur la conformité, reportez-vous à Sécurité ou conformité dans l'environnement vSphere.

Lecture du Guide de configuration de la sécurité vSphere

Le *Guide de configuration de la sécurité vSphere* est une feuille de calcul contenant des directives de sécurité pour vous aider à modifier votre configuration de sécurité vSphere. Ces recommandations sont regroupées en onglets en fonction des composants affectés, avec une partie ou l'ensemble des colonnes suivantes.

Tableau 17-2. Colonnes de la feuille de calcul du Guide de configuration de la sécurité vSphere

En-tête de colonne	Description
ID de directive	ID unique en deux parties faisant référence à une configuration de sécurité ou une recommandation de sécurisation renforcée. La première partie indique le composant, défini comme suit : ■ ESXi : hôtes ESXi ■ VM : machines virtuelles ■ vNetwork : commutateurs virtuels
Description	Une brève description de la recommandation particulier.
Discussion	Description de la vulnérabilité correspondant à une recommandation particulière.
Paramètre de configuration	Fournit le paramètre de configuration applicable ou le nom de fichier, le cas échéant.

Tableau 17-2. Colonnes de la feuille de calcul du Guide de configuration de la sécurité vSphere (suite)

En-tête de colonne	Description
Valeur souhaitée	État ou valeur souhaité de la recommandation. Voici les valeurs possibles : ■ S.O. ■ Site spécifique ■ False ■ Vrai ■ Activé ■ Désactivé ■ Pas présent ou False
Valeur par défaut	Valeur par défaut définie par vSphere.
La valeur souhaitée est-elle la valeur par défaut ?	Indique si le paramètre de sécurité est la configuration par défaut du produit.
Action nécessaire	Type d'action à prendre sur la recommandation particulière. Les actions comprennent : ■ Mettre à jour ■ Audit uniquement ■ Modifier ■ Ajouter ■ Supprimer
Emplacement du paramètre dans vSphere Client	Étapes de vérification de la valeur à l'aide de vSphere Client.
Impact fonctionnel négatif en cas de modification de la valeur par défaut ?	Description, le cas échéant, d'un impact négatif potentiel découlant de l'utilisation de la recommandation de sécurité.
Évaluation de la commande PowerCLI	Étapes de vérification de la valeur à l'aide de PowerCLI.
Exemple de correction de la commande PowerCLI	Étapes de configuration (correction) de la valeur à l'aide de PowerCLI.
Correction de la commande de vCLI	Étapes de configuration (correction) de la valeur à l'aide des commandes vCLI.
Évaluation de la commande PowerCLI	Étapes de vérification de la valeur à l'aide des commandes PowerCLI.
Correction de la commande PowerCLI	Étapes de configuration (correction) de la valeur à l'aide des commandes PowerCLI.
Capable de définir à l'aide du profil d'hôte	Si le paramètre est possible en utilisant des profils d'hôte (s'applique uniquement aux directives de ESXi).
Sécurisation renforcée	Si TRUE, la directive n'a qu'une seule implémentation pour être conforme. Si FALSE, vous pouvez assurer la mise en œuvre de la directive avec plusieurs paramètres de configuration. Le paramètre réel est souvent spécifique du site.
Paramètre spécifique du site	Si TRUE, le paramètre pour être conforme avec la directive dépend des règles ou des normes qui sont spécifiques de ce déploiement vSphere.
Paramètre d'audit	Si TRUE, la valeur du paramètre répertoriée devra éventuellement être modifiée pour répondre aux règles spécifiques du site.

Note Ces colonnes peuvent changer au fil du temps si nécessaire. Par exemple, les ajouts récents incluent les colonnes ID STIG DISA, Sécurisation renforcée et le Paramètre spécifique du site. Consultez https://blogs.vmware.com pour des annonces sur les mises à jour au *Guide de configuration de la sécurité vSphere*.

N'appliquez pas aveuglément les directives du *Guide de configuration de la sécurité vSphere* à votre environnement. Prenez plutôt le temps d'évaluer chaque paramètre et de prendre une décision éclairée quant à son application éventuelle. Au minimum, vous pouvez utiliser les instructions fournies dans les colonnes Évaluation pour vérifier la sécurité de votre déploiement.

Le *Guide de la configuration de la sécurité vSphere* est une aide pour la mise en œuvre de la conformité dans votre déploiement. Lorsqu'il est utilisé avec les directives DISA (Defense Information Systems Agency) et autres directives de conformité, le *Guide de la configuration de la sécurité vSphere* vous permet de mapper les contrôles de sécurité vSphere au type de conformité correspondant à chaque directive.

À propos de l'Institut national des normes et de la technologie (NIST, National Institute of Standards and Technology)

L'Institut national des normes et de la technologie (NIST) est un organisme public non réglementaire qui développe des technologies, des mesures, des normes et des directives. La conformité aux directives et aux normes NIST est devenue une priorité supérieure dans de nombreux secteurs aujourd'hui.

L'Institut national des normes et de la technologie (NIST) a été fondé en 1901 et fait désormais partie du Département du Commerce des États-Unis. NIST est un des plus anciens laboratoires de sciences physiques du pays. Aujourd'hui, les mesures du NIST prennent en charge les plus petites technologies jusqu'aux plus grandes, ainsi que les créations humaines les plus complexes, des dispositifs à l'échelle nanométrique jusqu'aux gratte-ciel et réseaux de communication mondiaux résistant aux tremblements de terre.

FISMA (Federal Information Security Management Act) est une loi fédérale des États-Unis adoptée en 2002 contraignant les agences fédérales à développer, documenter et mettre en œuvre un programme de sécurité et de protection des informations. NIST joue un rôle important dans la mise en œuvre FISMA par la production de normes et directives de sécurité clés (par exemple, les séries FIPS 199, FIPS 200 et SP 800).

Les organisations gouvernementales et privées utilisent NIST 800-53 pour sécuriser des systèmes d'informations. Les contrôles de sécurité et de confidentialité sont essentiels pour protéger contre diverses menaces les opérations des organisations (notamment les missions, les fonctions, l'image de marque et la réputation), les ressources et les effectifs des organisations. Ces menaces incluent notamment les cyber-attaques malveillantes, les catastrophe naturelles,

les incidents structurels et les erreurs humaines. VMware a fait appel à un partenaire d'audit tiers afin d'évaluer les produits et les solutions VMware par rapport au catalogue de contrôle NIST 800-53. Pour plus d'informations, visitez la page Web de NIST à l'adresse https://www.nist.gov/cyberframework.

À propos des directives STIG DISA

DISA (Defense Information Systems Agency) développe et publie des Guides de mise en œuvre technique de la sécurité ou « STIG ». Les STIG DISA fournissent des conseils techniques pour renforcer la sécurité des systèmes et réduire les menaces.

DISA (Defense Information Systems Agency) est l'agence de prise en charge de combat du Département de la Défense des États-Unis (DoD) chargée de gérer la position en matière de sécurité du réseau DODIN (DOD Information Network). L'agence DISA accomplit notamment cette tâche en développant et en diffusant les Guides de mise en œuvre technique de la sécurité ou STIG, et en délégant leur mise en œuvre. En bref, les STIG sont des guides portables basés sur des normes pour renforcer la sécurité des systèmes. Les STIG sont obligatoires pour les systèmes informatiques DoD des États-Unis et, en tant que tels, fournissent une ligne de base certifiée et sécurisée pour les entités hors DoD pour mesurer leur niveau de sécurité.

Les fournisseurs tels que VMware envoient des conseils de sécurisation renforcée suggérés à l'agence DISA à des fins d'évaluation, en fonction des protocoles et des commentaires de la DISA. Une fois ce processus terminé, le STIG officiel est publié sur le site Web de l'organisation DISA sur la page https://public.cyber.mil/stigs/. VMware fournit des lignes de base de sécurité et des conseils de sécurisation renforcée pour vSphere dans le cadre du *Guide de configuration de la sécurité de vSphere*. Reportez-vous à la section https://core.vmware.com/security.

À propos du cycle de développement de sécurité de VMware

Le programme SDL (Security Development Lifecycle) de VMware identifie et réduit les risques de sécurité pendant la phase de développement de produits logiciels VMware. VMware exploite également le centre de réponse de sécurité VMware (VSRC) pour effectuer l'analyse et la correction de problèmes de sécurité logicielle dans les produits VMware.

SDL est la méthodologie de développement logiciel que le groupe vSECR (VMware Security Engineering, Communication, and Response) et les groupes de développement de produits VMware utilisent pour aider à identifier et atténuer les problèmes de sécurité. Pour plus d'informations sur le cycle de vie développement de sécurité VMware, reportez-vous à la page Web à l'adresse https://www.vmware.com/security/sdl.html.

VSRC collabore avec les clients et la communauté de recherche de sécurité pour résoudre les problèmes de sécurité et fournir aux clients des informations de sécurité en temps opportun. Pour plus d'informations sur le centre de réponse de sécurité VMware, reportez-vous à la page Web à l'adresse https://www.vmware.com/security/vsrc.html.

Journalisation d'audit

La journalisation d'audit du trafic réseau, des alertes de conformité, de l'activité du pare-feu, des modifications du système d'exploitation et des activités de provisionnement est considérée comme une meilleure pratique pour maintenir la sécurité de tout environnement informatique. En outre, la journalisation est une exigence spécifique de nombreuses réglementations et normes.

L'une des premières mesures à prendre pour assurer le suivi des modifications apportées à votre infrastructure consiste à effectuer un audit de votre environnement. Par défaut, vSphere inclut des outils qui vous permettent d'afficher et de suivre les modifications. Par exemple, vous pouvez utiliser l'onglet Tâches et événements de vSphere Client sur tout objet de votre hiérarchie vSphere pour voir les modifications ayant été apportées. Vous pouvez également utiliser PowerCLI pour récupérer les événements et les tâches. En outre, vRealize Log Insight permet la journalisation d'audit pour prendre en charge la collecte et la conservation d'importants événements système. En outre, de nombreux outils de tiers permettent d'effectuer l'audit de vCenter.

Les fichiers journaux peuvent fournir une piste d'audit pour aider à déterminer qui ou quoi accède à un hôte, une machine virtuelle, etc. Pour plus d'informations, consultez Emplacements des fichiers journaux ESXi .

Événements d'audit Single Sign-On

Les événements d'audit Single Sign-On (SSO) sont des enregistrements d'actions système ou utilisateur pour l'accès aux services SSO.

Lorsqu'un utilisateur se connecte à vCenter Server via Single Sign-On, ou apporte des modifications qui affectent SSO, les événements d'audit suivants sont consignés dans le fichier journal d'audit SSO :

- **Tentatives de connexion et de déconnexion :** événements liés aux opérations de connexion et de déconnexion ayant échoué et réussi.
- **Modification de privilège :** événement de modification d'un rôle ou d'autorisations d'utilisateur.
- **Modification de compte :** événement de modification des informations relatives à un compte d'utilisateur, par exemple, nom d'utilisateur, mot de passe ou informations de compte supplémentaires.
- **Modification de la sécurité :** événement de modification d'une configuration, d'un paramètre ou d'une stratégie de sécurité.
- **Compte activé ou désactivé :** événement marquant l'activation ou la désactivation d'un compte.
- **Source d'identité :** événement d'ajout, de suppression ou de modification d'une source d'identité.

Dans vSphere Client, les données d'événement sont affichées dans l'onglet **Surveiller**. Consultez la documentation de *Surveillance et performances de vSphere*.

Les données d'événement d'audit SSO incluent les détails suivants :

- Horodatage de l'événement.
- Utilisateur ayant effectué l'action.
- Description de l'événement.
- Gravité de l'événement.
- Adresse IP du client utilisée pour se connecter à vCenter Server, le cas échéant.

Présentation de journal des événements d'audit SSO

Le processus Single Sign-On vSphere écrit des événements d'audit dans le fichier `audit_events.log` dans le répertoire `/var/log/audit/sso-events/`.

Attention Ne modifiez jamais manuellement le fichier `audit_events.log`, car cela peut provoquer l'échec de la journalisation d'audit.

Tenez compte des observations suivantes lorsque vous travaillez avec le fichier `audit_events.log` :

- Le fichier journal est archivé dès qu'il atteint une taille de 50 Mo.
- Un maximum de 10 fichiers d'archive est conservé. Si la limite est atteinte, le fichier le plus ancien est supprimé de la création d'une nouvelle archive.
- Les fichiers d'archive sont nommés `audit_events-<index>.log.gz`, où l'index est un nombre compris entre 1 et 10. La première archive créée est index 1 et cet index augmente à chaque archive suivante.
- Les événements les plus anciens se trouvent dans l'index d'archive 1. Le fichier indexé le plus élevé correspond à la dernière archive.

Présentation des prochaines étapes de sécurité de conformité

La conduite d'une évaluation de sécurité est la première étape de présentation des vulnérabilités dans votre infrastructure. Une évaluation de sécurité fait partie d'un audit de sécurité, elle analyse à la fois les systèmes et les pratiques, notamment en matière de conformité de sécurité.

Une évaluation de sécurité correspond généralement à l'analyse de l'infrastructure physique de votre organisation (pare-feux, réseaux, matériel, etc.) pour identifier les vulnérabilités et les failles. Une évaluation de la sécurité n'est pas identique à un audit de sécurité. Un audit de la sécurité inclut non seulement une révision de l'infrastructure physique mais les autres aspects, tels que la stratégie et les procédures d'exploitation standard, notamment la conformité de la sécurité. Une fois que vous disposez de l'audit, vous pouvez décider des étapes requises pour résoudre les problèmes du système.

Vous pouvez vous poser ces questions d'ordre générales lors de la préparation d'un audit de sécurité :

1 Notre organisation respecte-t-elle une réglementation de conformité ? Si oui, laquelle ou lesquelles ?

2 Quel est notre intervalle d'audit ?

3 Quel est notre intervalle interne d'autoévaluation ?

4 Avons-nous accès aux résultats d'audit précédents et les avons-nous consultés ?

5 Avons-nous recours à une société d'audit tierce pour nous aider à préparer un audit ? Dans ce cas, quel est leur niveau de maîtrise de la virtualisation ?

6 Exécutons-nous des analyses de vulnérabilité sur les systèmes et les applications ? Quand et à quelle fréquence ?

7 Quelles sont nos stratégies internes en matière de cyber-sécurité ?

8 La journalisation d'audit est-elle configurée conformément à vos besoins ? Reportez-vous à la section Journalisation d'audit.

En l'absence de directives spécifiques précisant où il convient de commencer, vous pouvez passer directement à la sécurisation de votre environnement vSphere :

- Maintenir votre environnement à jour avec les derniers correctifs logiciels et microprogrammes
- Assurer une bonne gestion des mot de passe et l'intégrité de tous les comptes
- Passer en revue les recommandations de sécurité du fournisseur approuvé
- Faire référence aux Guides de Configuration de sécurité VMware (voir Présentation du guide de configuration de sécurité vSphere)
- Utiliser les directives disponibles et éprouvées d'infrastructures de stratégies telles que NIST, ISO, etc.
- Suivre les instructions d'infrastructures de conformité réglementaire telles que PCI, DISA et FedRAMP

vCenter Server et FIPS

À partir de vSphere 7.0 Update 2, vous pouvez activer le chiffrement validé par FIPS sur le périphérique vCenter Server Appliance.

La norme FIPS 140-2 est une norme gouvernementale des États-Unis et du Canada qui spécifie les exigences de sécurité pour les modules de chiffrement. vSphere utilise des modules de chiffrement validés par FIPS pour qu'ils soient compatibles à ceux spécifiés par la norme FIPS 140-2. L'objectif de la prise en charge de vSphere FIPS est de faciliter les activités de conformité et de sécurité dans divers environnements régulés.

À partir de vSphere 6.7, ESXi et vCenter Server utilisent le chiffrement validé par FIPS pour protéger les interfaces de gestion et l'autorité de certification de VMware (VMCA).

vSphere 7.0 Update 2 ajoute un chiffrement validé par FIPS supplémentaire à vCenter Server Appliance. Par défaut, cette option de validation FIPS est désactivée.

Note vSphere favorise la compatibilité sur FIPS, certains composants doivent donc prendre en compte divers éléments. Reportez-vous à la section Considérations lors de l'utilisation de FIPS.

Activer et désactiver FIPS sur le vCenter Server Appliance

Vous pouvez activer ou désactiver la cryptographie validée par FIPS sur le vCenter Server Appliance à l'aide de demandes HTTP.

Vous pouvez utiliser différentes méthodes pour exécuter des demandes HTTP. Cette tâche indique comment utiliser le centre de développeurs dans le vSphere Client pour activer et désactiver FIPS sur le vCenter Server Appliance. Consultez *Guide de programmation de VMware vCenter Server Management* pour plus d'informations sur l'utilisation des API pour travailler avec les vCenter Server Appliance.

Procédure

1. Connectez-vous au système vCenter Server en utilisant vSphere Client.
2. Dans le menu, sélectionnez **Centre de développement**.
3. Cliquez sur **Explorateur d'API**.
4. Dans le menu déroulant **Sélectionnez l'API**, sélectionnez **Dispositif**.
5. Faites défiler les catégories vers le bas et développez **system/security/global_fips**.
6. Développez **GET** et cliquez sur **Exécuter** sous **Essayer**.

   Vous pouvez voir le paramètre actuel sous **Réponse**.
7. Modifiez le paramètre .
   a. Pour activer FIPS, développez **PUT**, entrez ce qui suit dans le `request_body`, puis cliquez sur **Exécuter**.

   ```
   {
   "enabled":true
   }
   ```

   b. Pour désactiver FIPS, développez **PUT**, entrez ce qui suit dans le `request_body`, puis cliquez sur **Exécuter**.

   ```
   {
   "enabled":false
   }
   ```

Résultats

Le vCenter Server Appliance redémarre après que vous avez activé ou désactivé FIPS.

Considérations lors de l'utilisation de FIPS

Lors de l'activation de FIPS sur vCenter Server Appliance, certains composants présentent actuellement des contraintes fonctionnelles.

Aucune différence ne doit être notée après l'activation de FIPS sur vCenter Server, mais il convient toutefois de prendre en compte certains éléments.

Tableau 17-3. Considérations relatives à FIPS

Produit ou composant	Considération	Solution
VMware Directory Service	Certains composants hérités de VMware Directory Service (vmdir) utilisent la fonction de hachage cryptographique SHA-1 pour les signatures numériques, que FIPS 140-2 ne prend pas en charge.	Aucun actuellement.
Python	Dans certains cas, Python utilise sa fonctionnalité cryptographique intégrée au lieu d'OpenSSL. Par exemple, lorsque Python exécute un algorithme cryptographique, mais que pour une raison quelconque OpenSSl échoue, Python passe à son implémentation interne pour ces algorithmes.	Aucun actuellement. **Note** VMware ne peut pas effectuer de certification FIPS pour les algorithmes internes de Python.
Single Sign-On vSphere	Lorsque vous activez FIPS, vCenter Server prend uniquement en charge les modules cryptographiques pour l'authentification fédérée. Par conséquent, RSA SecureID et certaines cartes CAC ne fonctionnent plus.	Utilisez l'authentification fédérée. Consultez la documentation sur l'*Authentification vSphere* pour obtenir plus de détails.
Plug-ins d'interface utilisateur vSphere Client non-VMware et de partenaires	Ces plug-ins peuvent ne pas fonctionner si FIPS est activé.	Mettez à niveau les plug-ins pour qu'ils utilisent des bibliothèques de chiffrement conformes. Consultez « Préparation des plug-ins locaux pour la conformité FIPS » dans https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance.