

# vSphere のセキュリティ

Update 2

変更日：2022 年 4 月 27 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
〒108-0023 東京都港区芝浦 3-1-1  
田町ステーションタワー N 18 階  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2009-2022 VMware, Inc. All rights reserved. 著作権および商標情報。

# 目次

vSphere セキュリティについて 13

更新情報 15

## 1 vSphere 環境のセキュリティ 17

ESXi ハイパーバイザーのセキュリティ強化 17

vCenter Server システムおよび関連付けられているサービスのセキュリティ強化 19

仮想マシンのセキュリティ 20

仮想ネットワーク レイヤーの保護 21

vSphere 環境のパスワード 22

セキュリティのベスト プラクティスおよびリソース 24

## 2 vCenter Single Sign-On による vSphere 認証 26

vCenter Single Sign-On について 27

vCenter Single Sign-On によって環境を保護する方法 27

vCenter Single Sign-On コンポーネント 29

vCenter Single Sign-On がインストールに与える影響 30

vCenter Single Sign-On がアップグレードに与える影響 31

vSphere での vCenter Single Sign-On の使用 33

vsphere.local ドメイン内のグループ 35

vCenter Server のパスワード要件とロックアウト動作 37

vCenter Single Sign-On アイデンティティ ソースの構成 38

vCenter Single Sign-On による vCenter Server の ID ソース 38

vCenter Single Sign-On 用のデフォルト ドメインの設定 40

vCenter Single Sign-On アイデンティティ ソースの追加 40

Active Directory アイデンティティ ソースの設定 42

Active Directory LDAP Server および OpenLDAP Server アイデンティティ ソースの設定 43

vCenter Single Sign-On アイデンティティ ソースの編集 44

vCenter Single Sign-On アイデンティティ ソースの削除 45

Windows セッション認証での vCenter Single Sign-On の使用 45

vCenter Server 2 要素認証 46

vCenter Single Sign-On のスマート カード認証の構成 47

コマンド ラインを使用したスマート カード認証の設定 48

Platform Services Controller Web インターフェイスを使用したスマート カード認証の管理 51

スマート カード認証の失効ポリシーの設定 54

RSA SecurID 認証の設定 55

ログイン バナーの管理 58

別のサービス プロバイダの ID プロバイダとして vCenter Single Sign-On を使用する 58

SAML サービス プロバイダの追加	59
Security Token Service (STS)	60
アプライアンスでの新しい STS 署名証明書の生成	61
vCenter Server Windows 環境での新しい STS 署名証明書の生成	62
Security Token Service 証明書の更新	64
LDAPS SSL 証明書の有効期限日の判断	65
vCenter Single Sign-On ポリシーの管理	66
vCenter Single Sign-On のパスワード ポリシーの編集	66
vCenter Single Sign-On のロックアウト ポリシーの編集	67
vCenter Single Sign-On のトークン ポリシーの編集	68
vCenter Single Sign-On ユーザーおよびグループの管理	69
vCenter Single Sign-On ユーザーの追加	70
vCenter Single Sign-On ユーザーの無効化および有効化	71
vCenter Single Sign-On ユーザーの削除	71
vCenter Single Sign-On ユーザーの編集	72
vCenter Single Sign-On グループの追加	72
vCenter Single Sign-On グループへのメンバーの追加	73
vCenter Single Sign-On グループからのメンバーの削除	74
vCenter Single Sign-On ソリューション ユーザーの削除	74
vCenter Single Sign-On パスワードの変更	75
vCenter Single Sign-On のセキュリティのベスト プラクティス	76
vCenter Single Sign-On のトラブルシューティング	76
Lookup Service エラーの原因の特定	76
Active Directory ドメイン認証を使用してログインできない	78
ユーザー アカウントがロックされているために vCenter Server ログインが失敗する	79
VMware ディレクトリ サービスのレプリケーションに時間がかかることがある	80

### 3 vSphere セキュリティ証明書 81

異なるソリューション パスの証明書の要件	82
証明書管理の概要	85
証明書の置き換えの概要	87
vSphere 6.0 で証明書が使用される場合	90
VMCA および VMware コア ID サービス	92
VMware Endpoint 証明書ストアの概要	92
証明書の失効の管理	94
大規模なデプロイでの証明書の置き換え	94
Platform Services Controller Web インターフェイスを使用した証明書の管理	96
Platform Services Controller Web インターフェイスからの証明書ストアの探索	97
Platform Services Controller Web インターフェイスからの新しい VMCA 署名付き証明書への証明書の置き換え	98
Platform Services Controller Web インターフェイスから VMware 認証局 (VMCA) を中間 CA にする	99

Platform Services Controller からカスタム証明書を使用するためのシステムの設定	101
vSphere Certificate Manager による証明書署名要求の生成 (カスタム証明書)	101
証明書ストアへの信頼できるルート証明書の追加	103
Platform Services Controller からのカスタム証明書の追加	103
vSphere Certificate Manager ユーティリティによる証明書の管理	105
古い証明書の再発行による、最後に実行された操作の取り消し	106
すべての証明書のリセット	106
新しい VMCA ルート証明書の再生成およびすべての証明書の置き換え	106
VMCA を中間認証局にする (Certificate Manager)	107
vSphere Certificate Manager で CSR を生成し、ルート証明書 (中間認証局) を用意する	107
VMCA ルート証明書をカスタム署名証明書で置き換え、すべての証明書で置き換える	109
VMCA 証明書によるマシン SSL 証明書の置き換え (中間 CA)	110
VMCA 証明書によるソリューション ユーザー証明書の置き換え (中間 CA)	112
カスタム証明書によるすべての証明書の置き換え (Certificate Manager)	112
vSphere Certificate Manager による証明書署名要求の生成 (カスタム証明書)	112
カスタム証明書によるマシン SSL 証明書の置き換え	114
カスタム証明書によるソリューション ユーザー証明書の置き換え	115
証明書の手動での置き換え	116
サービスの起動および停止について	116
新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え	117
新規の VMCA 署名付きルート証明書の生成	118
VMCA 署名付き証明書によるマシン SSL 証明書の置き換え	120
新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え	123
混合モード環境での VMware ディレクトリ サービス証明書の置き換え	128
中間認証局としての VMCA の使用	129
ルート証明書の置き換え (中間 CA)	130
マシン SSL 証明書の置き換え (中間 CA)	132
ソリューション ユーザー証明書の置き換え (中間 CA)	136
VMware ディレクトリ サービス証明書の置き換え	141
混合モード環境での VMware ディレクトリ サービス証明書の置き換え	142
vSphere でのサードパーティ証明書の使用	143
証明書の要求およびカスタム ルート証明書のインポート	144
カスタム証明書によるマシン SSL 証明書の置き換え	146
カスタム証明書によるソリューション ユーザー証明書の置き換え	148
VMware ディレクトリ サービス証明書の置き換え	149
混合モード環境での VMware ディレクトリ サービス証明書の置き換え	150
CLI コマンドによる証明書とサービスの管理	151
証明書管理の操作に必要な権限	152
certool 構成の変更	153
certool 初期化コマンド リファレンス	154
certool 管理コマンド リファレンス	157

- vecs-cli コマンド リファレンス 159
- dir-cli コマンド リファレンス 163
- vSphere Web Client での vCenter 証明書の表示 168
- vCenter 証明書の有効期限の警告に対するしきい値の設定 169

## 4 vSphere のアクセス許可とユーザー管理タスク 170

- vSphere での認可について 171
- vCenter Server のアクセス許可モデルについて 171
- 権限の階層的な継承 173
- 複数の権限の設定 175
  - 例 1: 複数の権限の継承 176
  - 例 2: 子の権限による親の権限のオーバーライド 176
  - 例 3: ユーザー ロールによるグループ ロールのオーバーライド 177
- vCenter コンポーネントの権限の管理 178
  - インベントリ オブジェクトへのアクセス許可の追加 178
  - 権限の変更 179
  - 権限の削除 180
  - 権限の検証設定の変更 180
- グローバル権限 181
  - グローバル権限の追加 182
  - タグ オブジェクトに対する権限 182
- ロールを使用した権限の割り当て 184
  - vCenter Server システム ロール 185
  - カスタム ロールの作成 186
  - ロールのクローン作成 186
  - ロールの編集 187
- ロールと権限のベスト プラクティス 187
- 一般的なタスクに必要な権限 188

## 5 ESXi ホストのセキュリティ強化 191

- ホストの構成設定を管理するスクリプトの使用 192
- ホスト プロファイルを使用した ESXi ホストの構成 193
- ESXi のセキュリティに関する一般的推奨事項 194
  - ESXi のパスワードとアカウントのロックアウト 195
  - ESXi ネットワーク セキュリティに関する推奨事項 197
  - 管理対象オブジェクト ブラウザ (MOB) の無効化 198
  - 許可されている (SSH) キーの無効化 198
- ESXi ホストの証明書管理 199
  - ホストのアップグレードと証明書 201
  - ESXi 証明書のデフォルト設定 202
  - 複数の ESXi ホストの証明書有効期限情報の表示 203

単一 ESXi ホストの証明書の詳細の表示	203
ESXi 証明書の更新	204
証明書のデフォルト設定の変更	205
証明書モードの切り替えについて	205
証明書モードの変更	207
ESXi SSL 証明書とキーの置き換え	208
ESXi 証明書署名要求の要件	209
ESXi Shell からのデフォルトの証明書とキーの置き換え	209
vifs コマンドを使用したデフォルトの証明書と鍵の置き換え	210
HTTPS PUT を使用したデフォルトの証明書の置き換え	211
vCenter Server TRUSTED_ROOTS ストア（カスタム証明書）の更新	211
Auto Deploy でのカスタム証明書の使用	212
ESXi 証明書とキー ファイルのリストア	214
セキュリティ プロファイルによるホストのカスタマイズ	214
ESXi ファイアウォールの構成	215
ESXi ファイアウォール設定の管理	215
ESXi ホストで許可される IP アドレスの追加	216
ESXi ホストの送受信ファイアウォール ポート	217
NFS クライアント ファイアウォールの動作	219
ESXi ESXCLI ファイアウォールのコマンド	220
セキュリティ プロファイルによる ESXi サービスのカスタマイズ	221
セキュリティ プロファイルでのサービスの有効化または無効化	222
ロックダウン モード	223
ロックダウン モードの動作	225
vSphere Web Client を使用したロックダウン モードの有効化	226
vSphere Web Client を使用したロックダウン モードの無効化	227
ダイレクト コンソール ユーザー インターフェイスからの通常ロックダウン モードの有効化または無効化	228
ロックダウン モードでのアクセス権を持つアカウントの指定	228
ホストと VIB の許容レベルの確認	230
ESXi への権限の割り当て	231
ルート ユーザーの権限	232
vpxuser の権限	233
DCUI ユーザーの権限	233
Active Directory を使用した ESXi ユーザーの管理	233
vSphere Authentication Proxy のインストールまたはアップグレード	234
Active Directory を使用するためのホストの構成	235
ディレクトリ サービス ドメインへのホストの追加	236
ディレクトリ サービス設定の表示	237
vSphere Authentication Proxy の使用	237
vSphere Authentication Proxy のインストールまたはアップグレード	237
vSphere Authentication Proxy を認証に使用しようホストを構成	239

vSphere Authentication Proxy の設定	240
vSphere Authentication Proxy 証明書のエクスポート	240
ESXi へのプロキシ サーバ証明書のインポート	241
vSphere Authentication Proxy を使用した、ドメインへのホストの追加	242
ESXi ホスト用認証プロキシ証明書の置き換え	242
ESXi のセキュリティのベスト プラクティス	243
PCI および PCIe デバイスおよび ESXi	244
ESXi のスマート カード認証の構成	244
スマート カード認証を有効化	245
スマート カード認証の無効化	245
接続問題発生時のユーザー認証情報の認証	246
ロックダウン モードでのスマート カード認証の使用	246
ESXi SSH キー	246
SSH セキュリティ	247
vifs コマンドを使用した SSH 鍵のアップロード	247
HTTPS の PUT を使用した SSH 鍵のアップロード	248
ESXi Shell の使用	249
vSphere Web Client を使用した ESXi Shell へのアクセスの有効化	250
vSphere Web Client での ESXi Shell 可用性のタイムアウトの作成	250
vSphere Web Client でのアイドル ESXi Shell セッションのタイムアウトの作成	251
ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用した ESXi Shell へのアクセスの有効化	251
ダイレクト コンソール ユーザー インターフェイスでの ESXi Shell 可用性のタイムアウトの作成	252
アイドル ESXi Shell セッションのタイムアウトの作成	253
トラブルシューティングのために ESXi Shell にログイン	253
ESXi Web プロキシの設定の変更	254
vSphere Auto Deploy のセキュリティの考慮事項	254
ESXi ログ ファイルの管理	255
ESXi ホストでの syslog の構成	255
ESXi ログ ファイルの場所	257
フォールト トレランス ログ記録トラフィックのセキュリティ強化	257

## 6 vCenter Server システムのセキュリティ 258

vCenter Server のセキュリティのベスト プラクティス	258
vCenter Server アクセス コントロールのベスト プラクティス	258
vCenter Server パスワード ポリシーの設定	260
vCenter Server Windows ホストの保護	260
期限が切れたかまたは失効した証明書とログを失敗したインストールから削除	261
vCenter Server ネットワーク接続の制限	261
Linux クライアントの使用制限の検討	262
インストール済みプラグインの確認	262
vCenter Server Appliance のセキュリティのベスト プラクティス	263



レガシー ESXi ホストのサムプリントの検証	263
ネットワーク ファイル コピーによる SSL 証明書検証が有効かどうかの確認	264
vCenter Server の TCP および UDP ポート	265
CIM ベースのハードウェア監視ツールのアクセス制御	266

## 7 仮想マシンのセキュリティ 268

仮想マシンから VMX ファイルへの情報メッセージの制限	268
仮想ディスクの圧縮の防止	269
仮想マシンのセキュリティのベスト プラクティス	269
仮想マシンの全般的な保護	270
仮想マシンをデプロイするためのテンプレートの使用	271
仮想マシン コンソールの使用の最小化	271
仮想マシンのリソースの引き継ぎの防止	271
仮想マシン内の不必要な機能の無効化	272
不要なハードウェア デバイスの削除	272
未使用の表示機能の無効化	273
非公開機能の無効化	274
HGFS ファイル転送の無効化	275
ゲスト OS システムとリモート コンソール間のコピー アンド ペースト操作の無効化	275
クリップボードにコピーされた機密データの漏えい制限	276
ユーザーによる仮想マシン内のコマンドの実行を制限	276
仮想マシンのユーザーまたはプロセスによるデバイスの切断防止	277
ゲスト OS の可変メモリ制限の変更	278
ゲスト OS のプロセスによるホストへの構成メッセージの送信防止	278
独立型の読み取り専用ディスクの使用の回避	279

## 8 vSphere ネットワークのセキュリティ強化 280

vSphere ネットワーク セキュリティの概要	280
ファイアウォールによるネットワークのセキュリティ強化	282
vCenter Server を使用した構成でのファイアウォール	282
ファイアウォールを介した vCenter Server への接続	283
vCenter Server を使用しない構成でのファイアウォール	283
ファイアウォールを介した ESXi ホストの接続	284
ファイアウォールを介した仮想マシン コンソールへの接続	284
物理スイッチのセキュリティ強化	285
セキュリティ ポリシーによる標準スイッチ ポートのセキュリティ強化	286
vSphere 標準スイッチのセキュリティ強化	286
MAC アドレス変更	287
偽装転送	287
無差別モード操作	288
vSphere 分散スイッチおよび分散ポート グループのセキュリティ強化	288

VLAN を使用した仮想マシンのセキュリティ強化	289
VLAN のセキュリティの考慮事項	290
VLAN のセキュリティ強化	291
単一の ESXi ホストでのネットワーク DMZ の作成	291
単一の ESXi ホスト内での複数のネットワークの作成	293
インターネット プロトコル セキュリティ	295
使用可能なセキュリティ アソシエーションの一覧表示	295
IPsec セキュリティ アソシエーションの追加	295
IPsec セキュリティ アソシエーションの削除	296
使用可能な IPsec セキュリティ ポリシーの一覧表示	297
IPsec セキュリティ ポリシーの作成	297
IPsec セキュリティ ポリシーの削除	298
SNMP 構成が適切であることの確認	298
必要なときにのみ vSphere Network Appliance API で仮想スイッチを使用	299
vSphere ネットワークのセキュリティのベスト プラクティス	299
ネットワークのセキュリティに関する一般的推奨事項	300
ネットワーク コンポーネントのラベル付け	301
vSphere VLAN 環境の文書化と確認	301
徹底したネットワーク隔離プラクティスの採用	302

## 9 複数の vSphere コンポーネントが関係するベスト プラクティス 304

vSphere ネットワーク上の時計の同期	304
ネットワーク タイム サーバによる ESXi の時計の同期	304
vCenter Server Appliance の時刻同期設定の構成	305
VMware Tools の時刻同期の使用	305
vCenter Server Appliance 構成内の NTP サーバの追加または置換	306
vCenter Server Appliance と NTP サーバとの時刻同期	307
ストレージのセキュリティのベスト プラクティス	307
iSCSI ストレージのセキュリティ	307
iSCSI デバイスのセキュリティ強化	308
iSCSI SAN の保護	308
SAN リソースのマスキングおよびゾーニング	309
NFS 4.1 用 Kerberos 認証情報の使用	309
ホストのパフォーマンス データのゲストへの送信が無効化されていることを確認する	310
ESXi Shell および vSphere Web Client のタイムアウトの設定	310

## 10 TLS 再構成ユーティリティでの TLS プロトコル構成の管理 312

TLS バージョンの無効化をサポートするポート	312
vSphere での TLS バージョンの無効化	314
TLS 構成ユーティリティのインストール	314
オプションの手動バックアップの実行	316

vCenter Server システムでの TLS バージョンの無効化	317
ESXi ホストでの TLS バージョンの無効化	318
Platform Services Controller システムでの TLS バージョンの無効化	319
TLS 構成の変更を元に戻す	321
vSphere Update Manager での TLS バージョンの無効化	322
Update Manager ポート 9087 の以前の TLS バージョンを無効にする	323
Update Manager ポート 8084 での以前の TLS バージョンの無効化	324
Update Manager ポート 9087 での無効な TLS バージョンの再有効化	324
Update Manager ポート 8084 での無効な TLS バージョンの再有効化	325

## 11 事前定義された権限 326

アラーム権限	327
Auto Deploy およびイメージ プロファイルの権限	328
証明書権限	329
コンテンツ ライブラリの権限	330
データセンター権限	331
データストアの権限	332
データストア クラスターの権限	333
Distributed Switch の権限	333
ESX Agent Manager の権限	334
拡張機能権限	335
フォルダの権限	335
グローバル権限	335
ホスト CIM 権限	336
ホスト構成権限	337
ホスト インベントリ	338
ホストのローカル操作権限	339
ホスト vSphere レプリケーションの権限	339
ホスト プロファイル権限	340
Inventory Service プロバイダの権限	340
Inventory Service のタグ付けの権限	340
ネットワーク権限	341
パフォーマンス権限	342
特権	342
プロファイル駆動型のストレージの権限	343
リソース権限	343
スケジュール設定タスクの権限	344
セッションの権限	344
ストレージ ビュー権限	345
タスクの権限	345
転送サービス権限	345

VRM ポリシー権限	346
仮想マシンの構成の権限	346
仮想マシン ゲストの操作権限	347
仮想マシン相互作用の権限	348
仮想マシンのインベントリ権限	356
仮想マシンのプロビジョニングの権限	357
仮想マシンのサービス構成権限	358
仮想マシンのスナップショット管理の権限	358
仮想マシンの vSphere Replication 権限	359
dvPort グループの権限	359
vApp 権限	360
vService の権限	361

# vSphere セキュリティについて

vSphere セキュリティでは、VMware® vCenter® Server および VMware ESXi を運用する vSphere® 環境のセキュリティについて説明します。

また、vSphere 環境の保護に役立つセキュリティ機能と、攻撃から環境を守る方法について解説します。

また、vSphere 環境の保護に役立つセキュリティ機能と、攻撃から環境を守る方法について解説します。

表 1-1. vSphere セキュリティ の概要

トピック	コンテンツの概要
vCenter Single Sign-On による認証	<ul style="list-style-type: none"><li>■ vCenter Single Sign-On の機能とサービス。</li><li>■ ID ソースの追加と管理。</li><li>■ vCenter Single Sign-On のポリシー。</li><li>■ ユーザーとグループ。</li></ul>
権限とユーザーの管理	<ul style="list-style-type: none"><li>■ 権限モデル（ロール、グループ、オブジェクト）</li><li>■ カスタム ロールの作成</li><li>■ 権限の設定</li><li>■ グローバル権限の管理</li></ul>
証明書の管理	<ul style="list-style-type: none"><li>■ ESXi 証明書の管理</li><li>■ vCenter Server および関連サービスの証明書の管理。<ul style="list-style-type: none"><li>■ ユーザー インターフェイスを使用した証明書の管理。</li><li>■ Certificate Manager ユーティリティを使用した証明書の管理。</li><li>■ CLI を使用した証明書の手動管理（例を含む）。</li></ul></li></ul>
ホストのセキュリティ機能	<ul style="list-style-type: none"><li>■ ロックダウン モードおよびその他のセキュリティ プロファイル機能</li><li>■ ホストのスマート カード認証</li><li>■ vSphere Authentication Proxy</li></ul>
セキュリティのベスト プラクティスおよび強化	<p>VMware のセキュリティ エキスパートが提案するベスト プラクティスと推奨事項</p> <ul style="list-style-type: none"><li>■ vCenter Server のセキュリティ。</li><li>■ ホストのセキュリティ。</li><li>■ 仮想マシンのセキュリティ。</li><li>■ ネットワークのセキュリティ。</li></ul>
vSphere の権限	今回のリリースでサポートされる vSphere のすべての権限

## 関連ドキュメント

このドキュメント以外に、VMware は vSphere の各リリースに対応する『堅牢化ガイド』(<http://www.vmware.com/security/hardening-guides.html>) を公開しています。セキュリティ強化ガイドは、潜在的なセキュリティ問題が記載されたスプレッドシートです。ここには、それぞれの問題が 3 種類のリスク プロファイルのどれに該当するかが明記されています。この『vSphere セキュリティ』では、リスク プロファイル 1（最高機密を扱う行政機関などの最高レベルのセキュリティ環境）の情報は記載されていません。

## 対象読者

記載されている情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を対象としています。

# 更新情報

『vSphere セキュリティ』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere セキュリティ』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2022 年 4 月 27 日	■ <a href="#">ストレージ ビュー</a> 権限へのマイナー更新。
2021 年 11 月 05 日	■ <a href="#">ESXi のセキュリティのベスト プラクティス</a> へのマイナー更新。 ■ <a href="#">ESXi ホストでの TLS バージョンの無効化</a> : vCenter Server にログインすることを記述するように修正。
2020 年 8 月 14 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。 ■ <a href="#">仮想マシンのセキュリティ</a> へのマイナー更新。
2017 年 10 月 4 日	■ <a href="#">証明書モードの切り替えについて</a> で、ホストをメンテナンス モードに切り替えてから切断してもモードの切り替えは実行されることを記述。ホストを削除する必要はありません。
JA-001949-07	■ <a href="#">異なるソリューション バスの証明書の要件</a> : 証明書の要件を詳しく説明する新しいトピックを追加。詳しい情報が少なかった古いトピックは削除されました。 ■ <a href="#">10 章 TLS 再構成ユーティリティでの TLS プロトコル構成の管理</a> : 新しい章を追加。
JP-001949-06	■ <a href="#">コマンド ラインを使用したスマート カード認証の設定</a> : コンマ区切りのリストにスペースを使用できないことを明記。 ■ <a href="#">コマンド ラインを使用したスマート カード認証の設定</a> : スクリプトの場所を追加。 ■ <a href="#">カスタム証明書によるソリューション ユーザー証明書の置き換え</a> : 完全な証明書チェーンが必要であることを明記。 ■ <a href="#">複数の権限の設定</a> : 導入時の問題を修正。
JP-001949-05	■ <a href="#">権限の検証設定の変更</a> : 検証と検証期間に関する情報を追加。
JP-001949-04	■ <a href="#">ネットワーク ファイル コピーによる SSL 証明書検証が有効かどうかの確認</a> : パラメータ名の誤りを修正。 ■ <a href="#">CLI コマンドによる証明書とサービスの管理</a> : Windows での service-control コマンドの場所に関する情報を追加。
JP-001949-03	■ <a href="#">タグ オブジェクトに対する権限</a> : タグの権限に関する情報を追加。 ■ <a href="#">vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する</a> : 証明書の順序に関する記述を改訂。
JP-001949-02	■ <a href="#">2 章 vCenter Single Sign-On による vSphere 認証</a> : vSphere Client を使用したログインに関する注意事項を追加。 ■ <a href="#">Active Directory アイデンティティ ソースの設定</a> : 内容を明確化。システムは Active Directory 名に参加している必要があり、ドメイン名は DNS を介して解決できる必要があります。

リビジョン	説明
JP-001949-01	<ul style="list-style-type: none"> <li>■ vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する：証明書の順序を修正。</li> <li>■ ESXi のパスワードとアカウントのロックアウトを更新。パスフレーズはデフォルトでは有効になっていません。</li> <li>■ コマンド ラインを使用したスマート カード認証の設定：アプライアンス シェルにアクセスするための手順を修正。</li> <li>■ vCenter Single Sign-On パスワードの変更：内容を修正。パスワードの有効期限が切れた場合は、管理者に連絡する必要があります。</li> <li>■ ホストの構成設定を管理するスクリプトの使用：PowerCLI スクリプトを更新。</li> <li>■ vCenter Single Sign-On がインストールに与える影響内の vCenter Server インスタンス数に関する情報を更新。</li> <li>■ コマンド ラインを使用したスマート カード認証の設定、Platform Services Controller Web インターフェイスを使用したスマート カード認証の管理、RSA SecurID 認証の設定：内容を更新。</li> <li>■ vCenter Server の TCP および UDP ポート：内容を修正。たとえば、ポート 903 とポート 5900 ~ 5964 は、vCenter Server システム上ではなくホスト上で使用され、9090 など他のいくつかのポートは内部でのみ使用されます。</li> <li>■ vifs コマンドを使用した SSH 鍵のアップロード：DSA 鍵に関する情報を削除。</li> <li>■ Security Token Service (STS)：新しい STS 署名証明書を生成するための手順を追加。</li> </ul>
JP-001949-00	初期リリース。



# vSphere 環境のセキュリティ

# 1

vSphere 環境のコンポーネントは、証明書、認可、各 ESXi でのファイアウォール、アクセス制限などのいくつかの機能により、初期状態からセキュリティで保護されています。デフォルトのセットアップは、vCenter オブジェクトでアクセス許可を設定する、ファイアウォールのポートを開く、デフォルトの証明書を変更するなど、多くの方法で変更することができます。これにより、vCenter Server システム、ESXi ホスト、および仮想マシンをセキュリティで保護する際の柔軟性が最大限に高められています。

注意を要する vSphere のさまざまな分野の大まかな概要を把握しておく、セキュリティ戦略を計画するのに役立ちます。VMware Web サイトにある他の vSphere セキュリティ リソースも有用です。

この章には、次のトピックが含まれています。

- [ESXi ハイパーバイザーのセキュリティ強化](#)
- [vCenter Server システムおよび関連付けられているサービスのセキュリティ強化](#)
- [仮想マシンのセキュリティ](#)
- [仮想ネットワーク レイヤーの保護](#)
- [vSphere 環境のパスワード](#)
- [セキュリティのベスト プラクティスおよびリソース](#)

## ESXi ハイパーバイザーのセキュリティ強化

ESXi ハイパーバイザーは、初期状態でセキュリティ強化されています。さらに ESXi ホストを保護するには、ロックダウン モードや他の組み込み機能を使用できます。参照ホストを設定し、そのホストのホスト プロファイルに基づいてすべてのホストに変更を加える場合、またはスクリプトによる管理を実行する場合は、変更がすべてのホストに確実に適用されるようにして使用環境をさらに保護することができます。

このガイドで詳しく説明されている次の機能を使用して、vCenter Server によって管理される ESXi ホストの保護機能を強化します。『Security of the VMware vSphere Hypervisor』ホワイト ペーパーも参照してください。

### ESXi アクセスの制限

デフォルトでは、ESXi Shell サービスと SSH サービスは実行されておらず、ルート ユーザーのみがダイレクト コンソール ユーザー インターフェイス (DCUI) にログインできます。ESXi または SSH アクセスを有効化する場合、タイムアウトを設定して不正アクセスのリスクを制限することができます。

ESXi ホストにアクセスできるユーザーには、ホストを管理するためのアクセス許可が必要です。ホスト オブジェクトでのアクセス許可は、ホストを管理する vCenter Server から設定します。

### 名前付きユーザーと最小限の権限の使用

多くのタスクは、デフォルトでルート ユーザーが実行できます。管理者がルート ユーザー アカウントを使用して ESXi ホストにログインできるようにする代わりに、vCenter Server のアクセス許可管理インターフェイスから、異なるホスト構成権限を異なる名前付きユーザーに適用することができます。vSphere Web Client から、カスタム ロールを作成し、そのロールに権限を割り当て、そのロールを名前付きユーザーと ESXi ホスト オブジェクトに関連付けることができます。

単一ホスト シナリオでは、ユーザーを直接に管理します。『vSphere Client による vSphere 管理』ドキュメントを参照してください。

### 開いている ESXi ファイアウォール ポートの数の最小化

ESXi ホストのファイアウォール ポートは、デフォルトで、対応するサービスを開始するときのみ開かれます。vSphere Web Client、または ESXCLI コマンドや PowerCLI コマンドを使用して、ファイアウォール ポートのステータスを確認および管理できます。

[ESXi ファイアウォールの構成](#) を参照してください。

### ESXi ホスト管理の自動化

多くの場合、同じデータセンター内の異なるホストが同期されていることが重要なため、スクリプトによるインストールか vSphere Auto Deploy を使用してホストをプロビジョニングします。ホストはスクリプトを使用して管理できます。スクリプトによる管理の代わりに、ホスト プロファイルを使用することもできます。参照ホストを設定し、ホスト プロファイルをエクスポートし、そのプロファイルをホストに適用します。ホスト プロファイルは、直接適用するか、Auto Deploy によるプロビジョニングの一部として適用できます。

vSphere Auto Deploy の詳細については、[ホストの構成設定を管理するスクリプトの使用](#)および『vSphere のインストールとセットアップ』を参照してください。

### ロックダウン モードの利用

ロックダウン モードの場合、ESXi ホストには、デフォルトで vCenter Server を介してのみアクセスできます。vSphere 6.0 以降では、厳密なロックダウン モードか通常ロックダウン モードを選択することができ、例外ユーザーを定義して、バックアップ エージェントなどのサービス アカウントへの直接アクセスを許可することができます。

[ロックダウン モード](#) を参照してください。

### VIB パッケージの整合性の確認

各 VIB パッケージには許容レベルが関連付けられています。VIB は、許容レベルがホストの許容レベル以上の場合にのみ、ESXi ホストに追加することができます。CommunitySupported VIB または PartnerSupported VIB は、ホストの許容レベルを明示的に変更しない限り、ホストに追加することができます。

[ホストと VIB の許容レベルの確認](#) を参照してください。

### ESXi 証明書の管理

vSphere 6.0 以降では、VMware 認証局 (VMCA) により、VMCA をデフォルトでルート認証局とする署名証明書を使用して、各 ESXi ホストをプロビジョニングします。企業ポリシーで規定されている場合は、既存の証明書を、サードパーティ CA によって署名された証明書で置き換えることができます。

を参照してください。 [ESXi ホストの証明書管理](#)

## スマート カード認証

vSphere 6.0 以降、ESXi では、ユーザー名とパスワード認証に代わるオプションとしてスマート カード認証がサポートされます。

[ESXi のスマート カード認証の構成](#) を参照してください。

## ESXi アカウントのロックアウト

vSphere 6.0 以降では、SSH 経由および vSphere Web Services SDK 経由のアクセスで、アカウントのロックがサポートされるようになりました。ダイレクト コンソール インターフェイス (DCUI) と ESXi Shell では、アカウント ロックアウトはサポートされていません。デフォルトでは、アカウントがロックされるまでに、最大 10 回のログイン試行の失敗が許可されています。アカウントはデフォルトで 2 分後にロック解除されます。

[ESXi のパスワードとアカウントのロックアウト](#) を参照してください。

スタンドアロン ホストのセキュリティの考慮事項は類似していますが、管理タスクは若干異なります。『vSphere Client による vSphere 管理』ドキュメントを参照してください。

# vCenter Server システムおよび関連付けられているサービスのセキュリティ強化

vCenter Server システムおよび関連付けられているサービスは、vCenter Single Sign-On による認証と、vCenter Server アクセス許可モデルを使用した認可によって保護されます。デフォルトの動作を変更できます。また使用中の環境へのアクセスを保護するための追加的な手順を取ることもできます。

vSphere 環境を保護するときは、vCenter Server インスタンスに関連付けられているすべてのサービスが保護される必要があることを考慮します。一部の環境では、いくつかの vCenter Server インスタンスと 1 つ以上の Platform Services Controller インスタンスを保護する場合があります。

## すべての vCenter ホスト マシンを強化する

vCenter 環境を保護するための最初の手順は、vCenter Server または関連付けられているサービスが動作する各マシンを強化することです。物理マシンであれ仮想マシンであれ、同様のことを考慮する必要があります。必ず、オペレーティング システムに最新のセキュリティ パッチをインストールし、業界標準のベスト プラクティスに従ってホスト マシンを保護してください。

## vCenter 証明書モデルについて

VMware Certificate Authority は、デフォルトでは、各 ESXi ホスト、環境内の各マシン、および VMCA 署名付き証明書を持つ各ソリューション ユーザーをプロビジョニングします。環境の動作のための設定は不要ですが、企業ポリシーの必要性に応じて、デフォルトの動作を変更できます。3 章 [vSphere セキュリティ証明書](#) を参照してください。

さらに保護を強化する場合は、有効期限切れの証明書、失効した証明書、および失敗したインストールを必ず明示的に削除してください。

## vCenter Single Sign-On の構成

vCenter Server および関連付けられているサービスは、vCenter Single Sign-On 認証フレームワークによって保護されます。初めてソフトウェアをインストールするときに、administrator@vsphere.local ユーザーのパスワードを指定すると、そのドメインのみがアイデンティティ ソースとして使用できます。その他のアイデンティティ ソース（Active Directory または LDAP）を追加して、デフォルトのアイデンティティ ソースを設定できます。今後は、アイデンティティ ソースを認証できるユーザーが、オブジェクトの表示やタスクの実行を行うことができます（そのような権限がある場合）。2 章 [vCenter Single Sign-On による vSphere 認証](#) を参照してください。

## ユーザーまたはグループへのロールの割り当て

適切にログインするために、オブジェクトに付与した各アクセス許可を、名前付きユーザーまたはグループと、事前定義のロールまたはカスタム ロールに関連付けます。vSphere 6.0 のアクセス許可モデルは、ユーザーまたはグループを認可する複数の方法を備え、柔軟性が非常に高くなっています。[vSphere での認可について](#) および [一般的なタスクに必要な権限](#) を参照してください。

管理者権限と管理者ロールの使用を、必ず制限してください。可能な場合は、匿名の管理者ユーザーは使用しないでください。

## NTP の設定

環境内の各ノードに NTP を設定します。証明書インフラストラクチャは、正確なタイム スタンプを必要とし、ノードが同期されない場合は適切に機能しません。

[vSphere ネットワーク上の時計の同期](#) を参照してください。

# 仮想マシンのセキュリティ

仮想マシンを保護するには、ゲスト OS に継続的にパッチを適用し、物理マシンと同じように使用環境を保護します。不要な機能を無効にして、仮想マシン コンソールの使用を最小限に抑え、ベスト プラクティスを実行することを検討してください。

## ゲスト OS の保護

ゲスト OS を保護するには、最新のパッチを使用し、適切な場合はアンチスパイウェアやアンチマルウェア アプリケーションも使用するようにします。ゲスト OS ベンダーのドキュメントや、書籍またはインターネットで入手できる、そのオペレーティング システムに関するその他の情報を参照してください。

## 不要な機能の無効化

不要な機能が無効になっていて、潜在的な攻撃ポイントが最小限に抑えられていることを確認します。使用頻度の少ない機能が多くがデフォルトで無効になっています。不要なハードウェアを削除し、仮想マシンとリモート コンソール間の Host-Guest FileSystem (HGFS) やコピー アンド ペーストなどの特定の機能を無効にします。

[仮想マシン内の不必要な機能の無効化](#) を参照してください。

## テンプレートおよびスクリプトによる管理の使用

仮想マシン テンプレートを使用すると、要件に合わせてオペレーティング システムを設定し、同じ設定でその他の仮想マシンを作成できます。

初期導入後に仮想マシンの設定を変更する場合、PowerCLI などのスクリプトを使用することを検討してください。このドキュメントでは、GUI を使用してタスクを実行する方法について説明します。使用中の環境の一貫性を維持するには、GUI ではなくスクリプトの使用を検討してください。大規模環境の場合、仮想マシンをフォルダにグループ化してスクリプトを最適化できます。

テンプレートの詳細については、[仮想マシンをデプロイするためのテンプレートの使用](#)および『vSphere 仮想マシン管理』を参照してください。PowerCLI の詳細については、VMware PowerCLI のドキュメントを参照してください。

## 仮想マシン コンソールの使用の最小化

仮想マシン コンソールには、物理サーバで行う監視と同じように、仮想マシンで監視を行う機能があります。仮想マシン コンソールにアクセスできるユーザーは、仮想マシンの電源管理とリムーバブル デバイスの接続制御にアクセスできます。そのため、仮想マシン コンソールへのアクセスは、仮想マシンに対する悪意のある攻撃を許してしまう可能性があります。

## 仮想ネットワーク レイヤーの保護

仮想ネットワーク レイヤーには、仮想ネットワーク アダプタ、仮想スイッチ、分散仮想スイッチ、ポートおよびポート グループが含まれます。ESXi は、仮想ネットワーク レイヤーに依存し、仮想マシンとそのユーザー間の通信をサポートします。また、ESXi は仮想ネットワーク レイヤーを使用して、iSCSI SAN、NAS ストレージなどと通信します。

vSphere には、安全なネットワーク インフラストラクチャに必要なすべての機能が備わっています。仮想スイッチ、分散仮想スイッチ、仮想ネットワーク アダプタなどのインフラストラクチャの各要素を個別に保護できます。また、次のガイドラインを考慮してください。詳細については、[8 章 vSphere ネットワークのセキュリティ強化](#)を参照してください。

### ネットワーク トラフィックの隔離

ESXi 環境の保護には、ネットワーク トラフィックの隔離が不可欠です。それぞれのネットワークで、さまざまなアクセスおよび隔離レベルが必要です。管理ネットワークは、クライアントのトラフィック、コマンドライン インターフェイス (CLI) または API トラフィック、およびサードパーティ製のソフトウェア トラフィックを通常のトラフィックから隔離します。このネットワークは、システム管理者、ネットワーク管理者、およびセキュリティ管理者のみがアクセスできるようにする必要があります。

[ESXi ネットワーク セキュリティに関する推奨事項](#) を参照してください。

### ファイアウォールを使用した仮想ネットワーク要素の保護

ファイアウォール ポートを開閉して、仮想ネットワークの各要素を個別に保護できます。ファイアウォール ルールを使用すれば、サービスと対応するファイアウォールを関連付け、サービスのステータスに応じて ESXi ファイアウォールを開閉できます。

[ESXi ファイアウォールの構成](#) を参照してください。

## ネットワーク セキュリティ ポリシーの検討

ネットワーク セキュリティ ポリシーにより、MAC アドレスのなりすましや望ましくないポート スキャンからトラフィックを保護することができます。標準スイッチおよび Distributed Switch のセキュリティ ポリシーは、ネットワーク プロトコル スタックのレイヤー 2（データ リンク レイヤー）に実装されます。セキュリティ ポリシーの 3 つの要素は、無差別モード、MAC アドレス変更、および偽装転送です。

手順については、『vSphere ネットワーク』ドキュメントを参照してください。

## 仮想マシン ネットワークの保護

仮想マシン ネットワークのセキュリティを強化するのに使用する方法は、インストールされているゲスト OS の種類、仮想マシンを信頼できる環境で操作するかどうか、また、その他のさまざまな要因によって異なります。仮想スイッチおよび分散仮想スイッチは、ファイアウォールのインストールなどの他の一般的なセキュリティ機能と一緒に使用すると、十分な防御を提供します。

[8 章 vSphere ネットワークのセキュリティ強化](#) を参照してください。

## 使用環境を保護する VLAN の検討

ESXi は、IEEE 802.1q VLAN をサポートしています。これは、仮想マシン ネットワークまたはストレージ構成の保護強化に使用できます。VLAN では物理ネットワークをセグメント化し、同じ物理ネットワーク上の 2 台のマシンが同じ VLAN 上にないかぎり、相互にパケットを送受信できないようにできます。

[VLAN を使用した仮想マシンのセキュリティ強化](#) を参照してください。

## 仮想化ストレージへの接続の保護

仮想マシンは、オペレーティング システム ファイル、プログラム ファイル、およびその他のデータを仮想ディスクに格納します。仮想マシンは、各仮想ディスクを SCSI コントローラに接続された SCSI ドライブとして認識します。仮想マシンは、ストレージの詳細から隔離され、仮想ディスクが存在する LUN に関する情報にはアクセスできません。

仮想マシン ファイル システム (VMFS) は、仮想ボリュームを ESXi ホストに提供する分散ファイル システムおよびボリューム マネージャです。ストレージへの接続の保護はユーザーが行います。たとえば、iSCSI ストレージを使用している場合、CHAP および相互 CHAP（会社のポリシーで求められる場合）を使用するように vSphere Web Client または CLI で環境を設定できます。

[ストレージのセキュリティのベスト プラクティス](#) を参照してください。

## IPSec の使用の評価

ESXi では、IPSec over IPv6 がサポートされています。IPSec over IPv4 は使用できません。

[インターネット プロトコル セキュリティ](#) を参照してください。

また、使用環境のネットワーク レイヤーの保護に VMware NSX for vSphere が適しているかどうかを評価します。

## vSphere 環境のパスワード

vSphere 環境のパスワードの制限、ロックアウト、および有効期限は、ユーザーがターゲットとするシステム、ユーザーの種類、およびポリシーの設定方法によって決まります。



## ESXi のパスワード

ESXi パスワードの制限は、Linux PAM モジュール `pam_passwdqc` によって決まります。 [ESXi のパスワードとアカウントのロックアウト](#) を参照してください。

## vCenter Server サービスとその他の vCenter サービスのパスワード

vCenter Single Sign-On で、vCenter Server サービスとその他の vCenter サービスにログインするすべてのユーザーに対する認証を管理します。パスワードの制限、ロックアウト、および有効期限は、ユーザーのドメインとそのユーザーがどのようなユーザーかによって決まります。

### administrator@vsphere.local

administrator@vsphere.local ユーザー（インストール中に別のドメインを選択した場合は、administrator@mydomain ユーザー）のパスワードには、有効期限がなく、ロックアウト ポリシーの対象にはなりません。その他の点について、このパスワードは vCenter Single Sign-On パスワード ポリシーに設定されている制限に従う必要があります。 [vCenter Single Sign-On のパスワード ポリシーの編集](#) を参照してください。

このユーザーのパスワードを忘れた場合は、パスワードのリセットに関する情報を VMware ナレッジ ベースで検索してください。

### その他の vsphere.local ユーザー

その他の vsphere.local ユーザー、または、インストール中に指定したローカル ドメインのユーザーは、vCenter Single Sign-On のパスワード ポリシーとロックアウト ポリシーに設定された制限に従う必要があります。 [vCenter Single Sign-On のパスワード ポリシーの編集](#) および [vCenter Single Sign-On のロックアウト ポリシーの編集](#) を参照してください。これらのユーザーのパスワードの有効期限は、デフォルトでは 90 日後に切れますが、パスワード ポリシーの一環として管理者はこの期限を変更できます。

ユーザーが自分の vsphere.local パスワードを忘れた場合は、管理者ユーザーが `dir-cli` コマンドを使用してパスワードをリセットできます。

### その他のユーザー

その他すべてのユーザーのパスワードの制限、ロックアウト、および有効期限は、ユーザーが認証できるドメイン（アイデンティティ ソース）によって決まります。

vCenter Single Sign-On では、1 つのデフォルト アイデンティティ ソースがサポートされ、ユーザーは自分のユーザー名のみを使用して vSphere Client にログインできます。ドメインによってパスワード パラメータが決定されます。デフォルト以外のドメインのユーザーとしてログインする場合は、`user@domain` または `domain\user` のように指定して、ドメイン名を含めることができます。この場合も、ドメイン パスワード パラメータが適用されます。

## vCenter Server Appliance ダイレクト コンソール ユーザー インターフェイス ユーザーのパスワード

vCenter Server Appliance は事前に構成された Linux ベースの仮想マシンであり、Linux 上で vCenter Server サービスおよび関連サービスを実行するために最適化されています。

vCenter Server Appliance をデプロイするときに、アプライアンスの Linux オペレーティング システムのルート ユーザーのパスワードと、administrator@vsphere.local ユーザーのパスワードを指定します。ダイレクト コンソール ユーザー インターフェイスから、ルート ユーザーのパスワードの変更と、その他の vCenter Server Appliance ローカル ユーザー管理タスクを実行できます。vCenter Server Appliance の構成 を参照してください。

## セキュリティのベスト プラクティスおよびリソース

ベスト プラクティスに従うと、ESXi および vCenter Server は、仮想化を行っていない環境と同等またはそれ以上のセキュリティを実現できます。

このマニュアルでは、vSphere インフラストラクチャのさまざまなコンポーネントに関するベスト プラクティスについて説明しています。

表 1-1. セキュリティのベスト プラクティス

vSphere コンポーネント	リソース
ESXi ホスト	<a href="#">ESXi のセキュリティのベスト プラクティス</a>
vCenter Server システム	<a href="#">vCenter Server のセキュリティのベスト プラクティス</a>
仮想マシン	<a href="#">仮想マシンのセキュリティのベスト プラクティス</a>
vSphere ネットワーク	<a href="#">vSphere ネットワークのセキュリティのベスト プラクティス</a>

このマニュアルは、セキュアな環境を実現するために必要な情報源の 1 つに過ぎません。

VMware セキュリティ リソース（セキュリティ関連の警告やダウンロードを含む）は次の Web サイトで入手できます。

表 1-2. Web 上のヴィエムウェア セキュリティ リソース

テクニカル ノート	リソース
VMware のセキュリティ ポリシー、最新バージョンのセキュリティ アラート、セキュリティ ダウンロード、セキュリティ トピックを中心とした説明	<a href="http://www.vmware.com/go/security">http://www.vmware.com/go/security</a>
企業セキュリティ対策ポリシー	<a href="http://www.vmware.com/support/policies/security_response.html">http://www.vmware.com/support/policies/security_response.html</a> 当社は、お客様がセキュアな環境を維持するために尽力します。セキュリティ上の問題は迅速に解決します。ヴィエムウェア セキュリティ対策ポリシーでは、当社製品において起こりうる脆弱性を解決するための、当社の取り組みを文書化しています。



表 1-2. Web 上のヴィエムウェア セキュリティ リソース（続き）

テクニカル ノート	リソース
サードパーティのソフトウェア サポート ポリシー	<a href="http://www.vmware.com/support/policies/">http://www.vmware.com/support/policies/</a> VMware 製品では、さまざまなストレージ システム、バックアップ エージェントなどのソフトウェア エージェント、システム管理エージェントなどをサポートしています。ESXi をサポートするエージェント、ツール、およびその他のソフトウェアのリストについては、 <a href="http://www.vmware.com/vmtn/resources/">http://www.vmware.com/vmtn/resources/</a> で ESXi の互換性ガイドを参照してください。 業界には、当社が検証しきれない多くの製品や構成が提供されています。互換性ガイドに製品や構成がリストされていない場合、テクニカル サポートは、お客様の問題解決のお手伝いを致しますが、その製品または構成が使用可能かどうかは保証できません。常に、サポートされていない製品や構成のセキュリティ リスクについては注意して評価してください。
コンプライアンスとセキュリティ標準、および仮想化とコンプライアンスに関するパートナーのソリューションと詳細なコンテンツ	<a href="http://www.vmware.com/go/compliance">http://www.vmware.com/go/compliance</a>
異なるバージョンの vSphere コンポーネントの、CCEVS や FIPS のようなセキュリティ認証と検証についての情報。	<a href="https://www.vmware.com/support/support-resources/certifications.html">https://www.vmware.com/support/support-resources/certifications.html</a>
異なるバージョンの vSphere とその他の VMware 製品の堅牢化ガイド。	<a href="https://www.vmware.com/support/support-resources/hardening-guides.html">https://www.vmware.com/support/support-resources/hardening-guides.html</a>
『Security of the VMware vSphere Hypervisor』ホワイト ペーパー	<a href="http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf">http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf</a>

# vCenter Single Sign-On による vSphere 認証

## 2

vCenter Single Sign-On は認証ブローカーおよびセキュリティ トークン交換インフラストラクチャです。ユーザーまたはソリューション ユーザーが vCenter Single Sign-On の認証を受けることができる場合、そのユーザーは SAML トークンを受信します。その後、ユーザーは SAML トークンを使用して vCenter Server サービスの認証を受けることができます。次に、ユーザーは権限のあるアクションを実行できます。

すべての通信でトラフィックが暗号化され、認証されたユーザーのみが権限のあるアクションを実行できるため、環境の安全が確保されます。

vSphere 6.0 以降では、vCenter Single Sign-On は Platform Services Controller に含まれています。Platform Services Controller には、vCenter Server および vCenter Server コンポーネントをサポートする共有サービスが用意されています。vCenter Single Sign-On、VMware 認証局、ライセンス サービス、および Lookup Service などが共有サービスになります。Platform Services Controller の詳細については、『vSphere のインストールとセットアップ』を参照してください。

最初のハンドシェイクでは、ユーザーはユーザー名とパスワード、ソリューション ユーザーは証明書を使用して認証を行います。ソリューション ユーザー証明書の置き換えの詳細については、[3 章 vSphere セキュリティ証明書](#)を参照してください。

ユーザーが vCenter Single Sign-On で認証できるようになると、そのユーザーに特定のタスクの実行を認可できます。通常、vCenter Server 権限を割り当てますが、vSphere には他のアクセス許可モデルも用意されています。[vSphere での認可について](#)を参照してください。

---

**注：** vCenter Server インスタンスに対し、Active Directory ユーザーが vSphere Client から SSPI でログインできるようにするには、vCenter Server インスタンスを Active Directory ドメインに参加させる必要があります。外部 Platform Services Controller を使用した vCenter Server Appliance を Active Directory ドメインに参加させる方法については、VMware のナレッジベースの記事 (<http://kb.vmware.com/kb/2118543>) を参照してください。

---

この章には、次のトピックが含まれています。

- [vCenter Single Sign-On について](#)
- [vCenter Single Sign-On アイデンティティ ソースの構成](#)
- [vCenter Server 2 要素認証](#)
- [別のサービス プロバイダの ID プロバイダとして vCenter Single Sign-On を使用する](#)
- [Security Token Service \(STS\)](#)
- [vCenter Single Sign-On ポリシーの管理](#)

- vCenter Single Sign-On ユーザーおよびグループの管理
- vCenter Single Sign-On のセキュリティのベスト プラクティス
- vCenter Single Sign-On のトラブルシューティング

## vCenter Single Sign-On について

vCenter Single Sign-On を効果的に管理するには、基盤となるアーキテクチャと、それがインストールとアップグレードにどのように影響するかについて理解する必要があります。



vCenter Single Sign-On 6.0 ドメインとサイト

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

## vCenter Single Sign-On によって環境を保護する方法

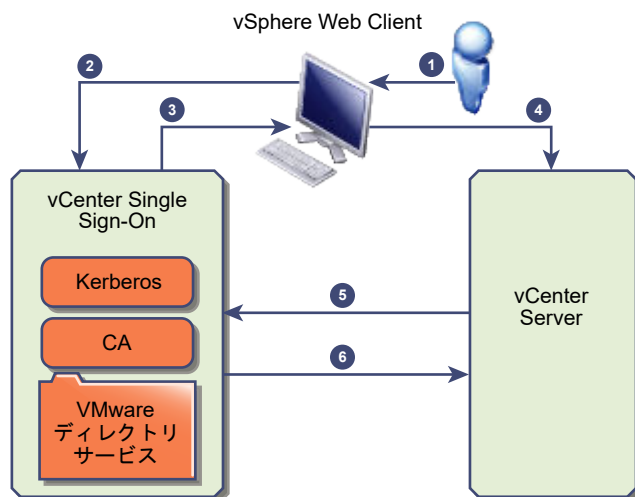
vCenter Single Sign-On では、ユーザーが各コンポーネントで個別に認証を行うのではなく、セキュアなトークンメカニズムを介して、vSphere コンポーネントが相互に通信できるようにします。

vCenter Single Sign-On は、STS (Security Token Service)、安全なトラフィック用の SSL、Active Directory または OpenLDAP によるユーザー（人）の認証、証明書によるソリューション ユーザーの認証を組み合わせで使用します。

### ユーザー（人）の vCenter Single Sign-On ハンドシェイク

次の図に、ユーザー（人）のハンドシェイクを示します。

図 2-1. ユーザー（人）の vCenter Single Sign-On ハンドシェイク



- 1 ユーザーは、vCenter Server システムや別の vCenter サービスにアクセスするためのユーザー名とパスワードで、vSphere Web Client にログインします。

また、ユーザーはパスワードなしでログインして、[Windows セッション認証を使用してください] チェックボックスにチェックを付けることができます。

- 2 vSphere Web Client は、ログイン情報を vCenter Single Sign-On サービスに渡します。このサービスにより、vSphere Web Client の SAML トークンがチェックされます。vSphere Web Client に有効なトークンがある場合、vCenter Single Sign-On により、ユーザーが構成済み ID ソース（Active Directory など）に存在するかどうかチェックされます。
  - ユーザー名のみが使用されている場合は、vCenter Single Sign-On によってデフォルト ドメイン内がチェックされます。
  - ドメイン名がユーザー名に含まれている場合（*DOMAIN/user1* または *user1@DOMAIN*）、vCenter Single Sign-On によってそのドメインがチェックされます。
- 3 ユーザーがアイデンティティ ソースの認証を受けることができる場合、そのユーザーを vSphere Web Client に示すトークンが vCenter Single Sign-On によって返されます。
- 4 vSphere Web Client はトークンを vCenter Server システムに渡します。
- 5 vCenter Server は、トークンが有効で期限切れになっていないことを、vCenter Single Sign-On サーバでチェックします。
- 6 vCenter Single Sign-On サーバにより、トークンが vCenter Server システムに返され、vCenter Server 認可フレームワークを利用してユーザーのアクセスを許可します。

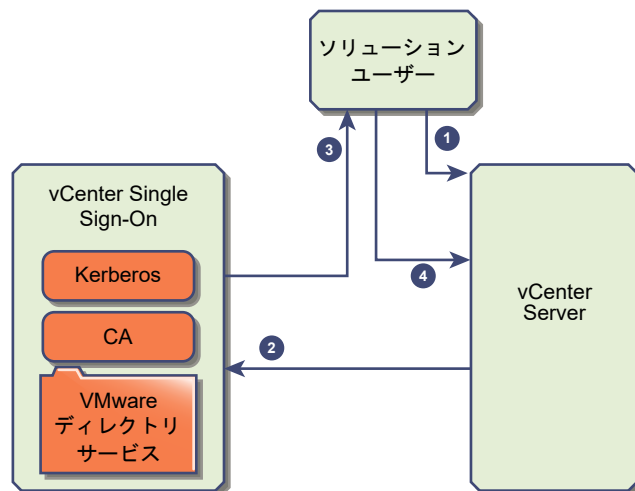
これで、ユーザーは認証を受けて、自分のロールに権限があるすべてのオブジェクトを表示および変更できます。

**注：** まず、各ユーザーにアクセスなしロールが割り当てられます。vCenter Server の管理者は、ユーザーがログインできるように少なくとも読み取り専用ロールを割り当てる必要があります。[インベントリ オブジェクトへのアクセス許可の追加](#) を参照してください。

## ソリューション ユーザーの vCenter Single Sign-On ハンドシェイク

ソリューション ユーザーは、vCenter Server インフラストラクチャで使用するサービスのセット（vCenter Server や vCenter Server の拡張機能など）です。VMware の拡張機能や、場合によってはサードパーティ製拡張機能も vCenter Single Sign-On の認証を受けることができます。

図 2-2. ソリューション ユーザーの vCenter Single Sign-On ハンドシェイク



ソリューション ユーザーの場合、やりとりは、次のように行われます。

- 1 ソリューション ユーザーが vCenter サービスに接続しようとします。
- 2 ソリューション ユーザーは vCenter Single Sign-On にリダイレクトされます。ソリューション ユーザーが vCenter Single Sign-On を初めて使用する場合、有効な証明書を提供する必要があります。
- 3 証明書が有効であれば、vCenter Single Sign-On は SAML トークン（ベアラ トークン）をソリューション ユーザーに割り当てます。このトークンは、vCenter Single Sign-On によって署名されます。
- 4 ソリューション ユーザーは vCenter Single Sign-On にリダイレクトされ、そのアクセス許可に基づいてタスクを実行できます。
- 5 次にソリューション ユーザーが認証を受ける必要があるときは、SAML トークンを使用して vCenter Server にログインできます。

デフォルトでは、起動時に VMCA からソリューション ユーザーに証明書がプロビジョニングされるため、このハンドシェイクは自動的に行われます。会社のポリシーで、サードパーティ CA 署名付き証明書が求められる場合、ソリューション ユーザー証明書をサードパーティ CA 署名付き証明書に置き換えることができます。これらの証明書が有効であれば、vCenter Single Sign-On は SAML トークンをソリューション ユーザーに割り当てます。

[vSphere でのサードパーティ証明書の使用](#) を参照してください。

## vCenter Single Sign-On コンポーネント

vCenter Single Sign-On には、Security Token Service (STS)、管理サーバ、vCenter Lookup Service、および VMware ディレクトリ サービス (vmdir) が含まれています。VMware ディレクトリ サービスは、証明書管理でも使用されます。

インストール時に各コンポーネントは、組み込みデプロイの一部として、または Platform Services Controller の一部としてデプロイされます。

### STS (Security Token Service)

STS サービスは、Security Assertion Markup Language (SAML) トークンを発行します。これらのセキュリティ トークンは、vCenter Single Sign-On によってサポートされている ID ソースのタイプの 1 つで、ユーザーの ID を表します。SAML トークンを使用すると、vCenter Single Sign-On で正常に認証されたユーザーおよびプログラムは、vCenter Single Sign-On がサポートしている任意の vCenter サービスを、サービスごとに認証を受けずに何度でも利用できます。

vCenter Single Sign-On サービスは、署名証明書ですべてのトークンに署名し、そのトークン署名証明書をディスクに保存します。サービス自体の証明書もディスクに保存されます。

### 管理サーバ

管理サーバにより、ユーザーは vCenter Single Sign-On の管理者権限で vCenter Single Sign-On サーバの構成や、vSphere Web Client からユーザーとグループの管理を行うことができます。初期設定では administrator@your\_domain\_name のユーザーのみにこの権限が付与されます。vSphere 5.5 では、administrator@vsphere.local のユーザーに管理者権限が付与されていました。vSphere 6.0 では、新しい Platform Services Controller を使用して vCenter Server をインストールするときや vCenter Server Appliance をデプロイするときに vSphere ドメインを変更できます。このドメイン名に Microsoft Active Directory や OpenLDAP のドメイン名を使用しないでください。

## VMware Directory Service (vmdir)

VMware Directory Service (vmdir) は、インストール時に指定したドメインに関連付けられ、組み込みの各デプロイおよび各 Platform Services Controller に含まれます。このサービスは、LDAP ディレクトリをポート 389 で使用できるようにするマルチテナントのピアレプリケート ディレクトリ サービスです。このサービスでは、vSphere 5.5 以前のシステムとの後方互換性のためにポート 11711 を引き続き使用します。

使用している環境に Platform Services Controller の複数のインスタンスが含まれている場合、1 つの vmdir インスタンスで更新された vmdir の内容は、他のすべての vmdir インスタンスに伝達されます。

vSphere 6.0 以降、VMware Directory Service では、vCenter Single Sign-On の情報だけでなく、証明書情報も格納されます。

## ID 管理サービス

ID ソースおよび STS 認証要求を処理します。

## vCenter Single Sign-On がインストールに与える影響

バージョン 5.1 以降、vSphere には、vCenter Server 管理インフラストラクチャの一部として vCenter Single Sign-On サービスが含まれています。この変更は vCenter Server のインストールに影響します。

vSphere ソフトウェアのコンポーネントは安全なトークン交換メカニズムを使用して相互に通信し、他のすべてのユーザーも vCenter Single Sign-On によって認証するため、vCenter Single Sign-On による認証で vSphere の安全性が強化されます。

vSphere 6.0 以降、vCenter Single Sign-On は、組み込みデプロイに含まれているか、Platform Services Controller の一部になっています。Platform Services Controller には、vCenter Single Sign-On、VMware Certificate Authority、VMware Lookup Service、およびライセンス サービスなど、vSphere のコンポーネント間の通信に必要なすべてのサービスが組み込まれています。

インストールの順序は重要です。

## 最初のインストール

インストールを分散させる場合は、vCenter Server をインストールするか、vCenter Server Appliance をデプロイする前に、Platform Services Controller をインストールする必要があります。組み込みデプロイの場合は、自動的に正しい順序でインストールされます。

## 後続のインストール

4 つ前後の vCenter Server インスタンスまでは、1 つの Platform Services Controller によって vSphere 環境全体にサービスを提供できます。新しい vCenter Server インスタンスは、同じ Platform Services Controller に接続することができます。vCenter Server インスタンスの数が 4 つ前後より多くなる場合は、パフォーマンスを向上させるために追加の Platform Services Controller をインストールできます。各 Platform Services Controller 上の vCenter Single Sign-On サービスは、認証データを他のすべてのインスタンスと同期します。正確な数は、vCenter Server インスタンスの使用程度およびその他の要因によって決まります。

## vCenter Single Sign-On がアップグレードに与える影響

シンプル インストール環境を vCenter Server 6 の組み込みデプロイにアップグレードする場合、アップグレードはシームレスになります。カスタム インストールをアップグレードする場合、vCenter Single Sign-On サービスは、アップグレード後に Platform Services Controller の一部になります。アップグレード後に vCenter Server にログインできるユーザーは、アップグレード前のバージョンとデプロイ構成によって異なります。

アップグレードの一環として、vsphere.local の代わりに別の vCenter Single Sign-On ドメイン名を使用するように定義できます。

### アップグレード パス

アップグレードの結果は、選択したインストール オプションおよびアップグレード先のデプロイ モデルによって異なります。

表 2-1. アップグレード パス

ソース	結果
vSphere 5.5 以前のシンプル インストール	Platform Services Controller が組み込まれた vCenter Server。
vSphere 5.5 以前のカスタム インストール	<p>vCenter Single Sign-On が vCenter Server とは異なるノードにあった場合、外部 Platform Services Controller を使用する環境になります。</p> <p>vCenter Single Sign-On が vCenter Server と同じノードにあった場合で、他のサービスが別のノードにある場合、組み込み Platform Services Controller を使用する環境になります。</p> <p>カスタム インストールに複数のレプリケーション vCenter Single Sign-On サーバが含まれていた場合、複数のレプリケーション Platform Services Controller インスタンスを使用する環境になります。</p>

### シンプル インストールのアップグレード後にログイン可能なユーザー

シンプル インストール オプションを使用してプロビジョニングされた環境をアップグレードする場合、常に組み込みの Platform Services Controller を使用するインストールになります。ログインを許可されるユーザーは、ソースの環境が vCenter Single Sign-On を含むかどうかにより異なります。

表 2-2. シンプル インストール環境のアップグレード後のログイン権限

ソースのバージョン	ログイン アクセス権限	メモ
vSphere 5.0	ローカル オペレーティング システム ユーザー administrator@vsphere.local	ユーザー ストアの変更により、インストール中に vSphere インベントリ階層のルート フォルダの管理者情報を求められることがあります。  以前のインストールで Active Directory をサポートしていた場合は、その Active Directory ドメインを ID ソースとして追加できます。
vSphere 5.1	ローカル オペレーティング システム ユーザー administrator@vsphere.local Admin@SystemDomain	vSphere 5.5 からは、vCenter Single Sign-On では 1 つのデフォルトの ID ソースのみをサポートします。  デフォルトの ID ソースは設定可能です。  デフォルト以外のドメインのユーザーは、ログイン時にドメインを指定できます ( <i>DOMAIN\user</i> または <i>user@DOMAIN</i> )。
vSphere 5.5	administrator@vsphere.local またはアップグレード中に指定したドメインの管理者。  すべての ID ソースのすべてのユーザーが以前と同様にログインできます。	

vCenter Single Sign-On を含まない vSphere 5.0 から vCenter Single Sign-On を含むバージョンにアップグレードする場合、ローカル オペレーティング システム ユーザーの重要度は、Active Directory などのディレクトリ サービスのユーザーよりもかなり低くなります。このため、ローカル オペレーティング システム ユーザーを認証済みユーザーにしておくことができない場合や、望ましくない場合もあります。

## カスタム インストールのアップグレード後にログイン可能なユーザー

カスタム インストール オプションを使用してプロビジョニングした環境をアップグレードする場合、結果は最初の選択によって異なります。

- vCenter Single Sign-On が vCenter Server システムと同じノードにあった場合、結果は組み込み Platform Services Controller を使用するインストールになります。
- vCenter Single Sign-On が vCenter Server システムとは別のノードにあった場合、結果は外部 Platform Services Controller を使用するインストールになります。
- vSphere 5.0 からアップグレードする場合、アップグレード プロセスの一環として、外部または組み込みの Platform Services Controller を選択できます。

アップグレード後のログイン権限は、いくつかの要因により異なります。



表 2-3. カスタム インストール環境のアップグレード後のログイン権限

ソースのバージョン	ログイン アクセス権限	メモ
vSphere 5.0	<p>vCenter Single Sign-On は、Platform Services Controller がインストールされたマシンのローカル オペレーティング システムのユーザーを認識しますが、vCenter Server がインストールされたマシンについては認識しません。</p> <p><b>注：</b> 特に統合された環境では、管理にローカル オペレーティング システムのユーザーを使用することはお勧めしません。</p> <p>administrator@vsphere.local は、管理者ユーザーとして、vCenter Single Sign-On および各 vCenter Server インスタンスにログインすることができます。</p>	<p>5.0 のインストールが Active Directory ユーザーをサポートしていた場合、これらのユーザーはアップグレード後はアクセス権がなくなります。ID ソースとして Active Directory ドメインを追加できます。</p>
vSphere 5.1 または vSphere 5.5	<p>vCenter Single Sign-On は、Platform Services Controller がインストールされたマシンのローカル オペレーティング システムのユーザーを認識しますが、vCenter Server がインストールされたマシンについては認識しません。</p> <p><b>注：</b> 特に統合された環境では、管理にローカル オペレーティング システムのユーザーを使用することはお勧めしません。</p> <p>administrator@vsphere.local は、管理者ユーザーとして、vCenter Single Sign-On および各 vCenter Server インスタンスにログインできます。</p> <p>vSphere 5.1 からのアップグレードでは、Admin@SystemDomain は administrator@vsphere.local と同じ権限を持ちます。</p>	<p>vSphere 5.5 からは、vCenter Single Sign-On では 1 つのデフォルトの ID ソースのみをサポートします。デフォルトの ID ソースは設定可能です。</p> <p>デフォルト以外のドメインのユーザーは、ログイン時にドメインを指定できます (DOMAIN\user または user@DOMAIN)。</p>

## vSphere での vCenter Single Sign-On の使用

ユーザーが vSphere コンポーネントにログインするとき、または、vCenter Server のソリューション ユーザーが別の vCenter Server サービスにアクセスするときに、vCenter Single Sign-On は認証を実施します。ユーザーは、vCenter Single Sign-On によって認証され、vSphere オブジェクトを操作するために必要な権限を持っている必要があります。

vCenter Single Sign-On では、ソリューション ユーザーとその他のユーザーの両方が認証されます。

- ソリューション ユーザーは、vSphere 環境内の一連のサービスを表します。インストールの際、VMCA はデフォルトで、各ソリューション ユーザーに証明書を割り当てます。ソリューション ユーザーは、その証明書を使用して vCenter Single Sign-On への認証を行います。vCenter Single Sign-On は、ソリューション ユーザーに SAML トークンを提供し、その後、ソリューション ユーザーは、環境内の他のサービスと連携することが可能になります。
- 他のユーザーが、たとえば、vSphere Web Client から環境内にログインしてきた場合、vCenter Single Sign-On によって、ユーザー名とパスワードが求められます。その認証情報を持つユーザーが対応するアイデンティティ ソース内に見つかった場合、vCenter Single Sign-On はそのユーザーに SAML トークンを割り当てます。これで、このユーザーは、再び認証を求められることなく、環境内の他のサービスにアクセスできます。

ユーザーが表示できるオブジェクトと実行できる内容は、通常、vCenter Server の権限設定で決まります。vCenter Server 管理者は、vCenter Single Sign-On からではなく vSphere Web Client の [管理] - [権限] インターフェイスから権限を割り当てます。4 章 [vSphere のアクセス許可とユーザー管理タスク](#) を参照してください。

## vCenter Single Sign-On ユーザーと vCenter Server ユーザー

vSphere Web Client を使用することにより、ユーザーは vSphere Web Client のログイン ページで認証情報を入力して vCenter Single Sign-On に対して認証を行います。vCenter Server への接続後、認証済みユーザーは、ロールによって権限が与えられているすべての vCenter Server インスタンスまたは他の vSphere オブジェクトを表示することができます。それ以降の認証は不要です。4 章 [vSphere のアクセス許可とユーザー管理タスク](#) を参照してください。

インストール後、administrator@vsphere.local ユーザーは、vCenter Single Sign-On と vCenter Server の両方に対する管理者アクセス権を持ちます。そのユーザーは、次に vCenter Single Sign-On ドメイン (vsphere.local) で、ID ソースを追加してデフォルトの ID ソースを設定し、ユーザーとグループを管理できます。

vCenter Single Sign-On への認証を行うすべてのユーザーは、パスワードの有効期限が切れていても、パスワードを知っている限り、自分のパスワードをリセットできます。 [vCenter Single Sign-On パスワードの変更](#) を参照してください。パスワードを忘れたユーザーのパスワードは、vCenter Single Sign-On の管理者のみがリセットできます。

## vCenter Single Sign-On 管理者ユーザー

vCenter Single Sign-On 管理インターフェイスには、vSphere Web Client からアクセスできます。

vCenter Single Sign-On を構成し、vCenter Single Sign-On ユーザーとグループを管理するには、administrator@vsphere.local ユーザーまたは vCenter Single Sign-On 管理者グループのユーザーが vSphere Web Client にログインする必要があります。認証時、そのユーザーは vSphere Web Client から vCenter Single Sign-On 管理インターフェイスにアクセスして、アイデンティティ ソースとデフォルトのドメインを管理し、パスワード ポリシーを指定し、他の管理タスクを実行することができます。 [vCenter Single Sign-On アイデンティティ ソースの構成](#) を参照してください。

---

**注：** administrator@vsphere.local ユーザーの名前は変更できません。セキュリティを高めるには、vsphere.local ドメインに追加で名前付きユーザーを作成し、管理者権限を割り当てることを検討します。その後、administrator@vsphere.local の使用を停止できます。

---

## 別のバージョンの vSphere での認証

バージョン 5.0 以前の vCenter Server システムに接続している場合、vCenter Server はそのユーザーを Active Directory ドメインまたはローカル オペレーティング システムのユーザーのリストと突き合わせて、認証を行います。vCenter Server 以降では、vCenter Single Sign-On を通じてユーザー認証を行います。

---

**注：** vSphere Web Client を使用してバージョン 5.0 以前の vCenter Server を管理することはできません。vCenter Server をバージョン 5.1 以降にアップグレードしてください。

---

## ESXi ユーザー

ESXi は vCenter Single Sign-On に統合されていません。ESXi ホストを Active Directory ドメインに明示的に追加します。[Active Directory を使用するためのホストの構成](#)を参照してください。

vSphere Client、vCLI、または PowerCLI で、ローカル ESXi ユーザーを作成することができます。vCenter Server は ESXi ローカルユーザーを認識せず、ESXi は vCenter Server ユーザーを認識しません。

---

**注：** 可能な場合は、vCenter Server を介して ESXi ホストの権限を管理します。

---

## vCenter Server コンポーネントへのログイン方法

ユーザーが vSphere Web Client から vCenter Server システムにログインする場合、ログイン動作はユーザーがデフォルト ドメイン（つまり、デフォルトのアイデンティティ ソースとして設定されているドメイン）に所属しているかどうかによって異なります。

- デフォルト ドメインに所属しているユーザーはユーザー名とパスワードでログインできます。
- vCenter Single Sign-On にアイデンティティ ソースとして追加されているがデフォルト ドメイン以外のドメインに所属しているユーザーは、vCenter Server にログインできますが、次のいずれかの方法でドメインを指定する必要があります。
  - ドメイン名を前に含める。たとえば MYDOMAIN\user1
  - ドメインを含める。たとえば、user1@mydomain.com
- vCenter Single Sign-On アイデンティティ ソースでないドメインに所属しているユーザーは vCenter Server にはログインできません。vCenter Single Sign-On に追加したドメインがドメイン階層の一部である場合、Active Directory は階層内の他のドメインのユーザーが認証されているかどうかを判断します。

---

**注：** 環境に Active Directory 階層が含まれる場合は、サポートされる設定とサポートされない設定の詳細を、[VMware ナレッジベースの記事 KB 2064250](#) で確認してください。

---

## vsphere.local ドメイン内のグループ

vsphere.local ドメインには、いくつかの事前定義されたグループがあります。それらのグループのいずれかにユーザーを割り当て、対応するアクションを実行できるようにします。

vCenter Server 階層のすべてのオブジェクトには、ユーザーおよびロールとオブジェクトをペアにすることにより、アクセス許可が割り当てられています。たとえば、リソース プールを選択し、対応するロールを割り当てることによってユーザーのグループにそのリソース プールに対する読み取り権限を付与できます。

vCenter Server によって直接管理されることのない一部のサービスの場合、権限は、vCenter Single Sign-On グループの 1 つに対するメンバーシップによって決まります。たとえば、管理者グループのメンバー ユーザーは、vCenter Single Sign-On を管理できます。CAAdmins グループのメンバー ユーザーは VMware Certificate Authority を管理ことができ、License Service.Administrators グループのユーザーはライセンスを管理できます。

vsphere.local には次のグループが事前定義されています。

**注：** これらのグループの多くは、vsphere.local に対して内部になっているか、ユーザーに高レベルの管理権限を付与します。リスクについて慎重に考慮した後にのみ、これらのグループのいずれかにユーザーを追加してください。

**注：** vsphere.local ドメイン内の事前定義されたグループはいずれも削除しないでください。いずれかを削除すると、認証または証明書のプロビジョニングに関連するエラーが発生することがあります。

表 2-4. vsphere.local ドメイン内のグループ

権限	説明
ユーザー	vsphere.local ドメインのユーザー。
SolutionUsers	ソリューション ユーザー グループの vCenter サービス。各ソリューション ユーザーは、証明書により vCenter Single Sign-On に対して個別に認証します。デフォルトでは、VMCA が証明書を使用してソリューション ユーザーをプロビジョニングします。このグループには、メンバーを明示的に追加しないでください。
CAAdmins	CAAdmins グループのメンバーには、VMCA の管理権限があります。通常、これらのグループにメンバーを追加することは推奨されません。
DCAdmins	DCAdmins グループのメンバーは、VMware ディレクトリ サービスでドメイン コントローラ管理者のアクションを実行できます。 <b>注：</b> ドメイン コントローラは、直接管理しないでください。代わりに、vmdir CLI または vSphere Web Client を使用して対応するタスクを実行してください。
SystemConfiguration.BashShellAdministrators	このグループは、vCenter Server Appliance のデプロイの場合にのみ使用できます。 このグループのユーザーは、BASH シェルへのアクセスを有効化および無効化することができます。SSH を使用して vCenter Server Appliance に接続するユーザーは、デフォルトで、制約されたシェルのコマンドにのみアクセスできます。このグループのユーザーは、BASH シェルにアクセスできます。
ActAsUsers	Act-As ユーザーのメンバーは、vCenter Single Sign-On から ActAs トークンを取得できます。
ExternalIPDUsers	このグループは、vSphere では使用されません。このグループは、VMware vCloud Air に関連して必要になります。
SystemConfiguration.Administrators	SystemConfiguration.Administrators グループのメンバーは、vSphere Web Client でシステム構成を表示および管理できます。これらのユーザーは、サービスを表示、起動、および再起動し、サービスのトラブルシューティングを行い、使用可能なノードを表示し、それらのノードを管理することができます。
DCClients	このグループは、管理ノードに VMware ディレクトリ サービス内のデータへのアクセスを許可するために内部で使われます。 <b>注：</b> このグループは変更しないでください。変更を加えると、証明書インフラストラクチャが侵害される可能性があります。
ComponentManager.Administrators	ComponentManager.Administrators グループのメンバーは、サービスを登録または登録解除するコンポーネント マネージャ API を呼び出す（つまり、サービスを変更する）ことができます。このグループのメンバーシップは、サービスでの読み取りアクセスでは不要です。

表 2-4. vsphere.local ドメイン内のグループ（続き）

権限	説明
LicenseService.Administrators	LicenseService.Administrators のメンバーには、すべてのライセンス関連データに対する完全な書き込みアクセス権限が付与されており、ライセンス サービスで登録されているすべての製品資産のシリアル キーを追加、削除、割り当て、および割り当て解除することができます。
管理者	VMware ディレクトリ サービス (vmdir) の管理者。このグループのメンバーは、vCenter Single Sign-On の管理タスクを実行できます。通常、このグループにメンバーを追加することは推奨されません。

## vCenter Server のパスワード要件とロックアウト動作

環境を管理するには、vCenter Single Sign-On のパスワード ポリシー、vCenter Server のパスワード、およびロックアウト動作について理解しておく必要があります。

### vCenter Single Sign-On の管理者パスワード

administrator@vsphere.local のパスワードは、次の要件を満たしている必要があります。

- 8 文字以上
- 小文字が 1 文字以上
- 数字が 1 文字以上
- 特殊文字が 1 文字以上

administrator@vsphere.local のパスワードを 20 文字より長くすることはできません。表示される ASCII 文字のみを使用できます。つまり、スペース文字などは使用できません。

### vCenter Server のパスワード

vCenter Server では、Active Directory、OpenLDAP、または vCenter Single Sign-On サーバのローカルオペレーティング システムなど、構成された ID ソースや、vCenter Single Sign-On によってパスワード要件が指示されます（非推奨）。

### ロックアウト動作

連続した失敗の数が事前設定された回数に達すると、ユーザーはロックアウトされます。デフォルトでは、3 分間に連続して 5 回失敗するとユーザーはロックアウトされ、5 分後にロックアウトは自動的に解除されます。これらのデフォルト設定は、ロックアウト ポリシーを使用して変更できます。[vCenter Single Sign-On のロックアウト ポリシーの編集](#) を参照してください。

vSphere 6.0 以降、システム ドメイン管理者（デフォルトでは administrator@vsphere.local）はロックアウト ポリシーの影響を受けません。

ユーザーは誰でも、`dir-cli password change` コマンドを使用して自分のパスワードを変更できます。ユーザーがパスワードを忘れた場合、管理者は、`dir-cli password reset` コマンドを使用してパスワードをリセットすることができます。

ESXi ローカル ユーザーのパスワードの詳細については、[ESXi のパスワードとアカウントのロックアウト](#)を参照してください。

## vCenter Single Sign-On アイデンティティ ソースの構成

ユーザーがログインすると、vCenter Single Sign-On はデフォルトのアイデンティティ ソースで、そのユーザーが認証可能かどうかを確認します。アイデンティティ ソースは、追加および削除ができるほか、デフォルト設定を変更できます。

vSphere Web Client から vCenter Single Sign-On を構成します。vCenter Single Sign-On を構成するには、vCenter Single Sign-On 管理者権限が必要です。vCenter Single Sign-On 管理者権限があることは、vCenter Server または ESXi の管理者ロールが割り当てられていることとは異なります。デフォルトでは、administrator@vsphere.local ユーザーのみに、新しいインストールの vCenter Single Sign-On サーバにおける管理者権限が割り当てられます。

### ■ vCenter Single Sign-On による vCenter Server の ID ソース

アイデンティティ ソースを使用して、vCenter Single Sign-On に 1 つ以上のドメインを添付できます。ドメインは vCenter Single Sign-On サーバがユーザー認証に使用できるユーザーまたはグループのリポジトリです。

### ■ vCenter Single Sign-On 用のデフォルト ドメインの設定

vCenter Single Sign-On の各 ID ソースは、ドメインと関連付けられています。vCenter Single Sign-On は、ドメイン名なしでログインするユーザーの認証にデフォルトのドメインを使用します。デフォルト以外のドメインに所属するユーザーはログイン時にドメイン名を含む必要があります。

### ■ vCenter Single Sign-On アイデンティティ ソースの追加

ユーザーは、vCenter Single Sign-On アイデンティティ ソースとして追加されたドメインに所属している場合に限り、vCenter Server にログインできます。vCenter Single Sign-On 管理者ユーザーは、vSphere Web Client からアイデンティティ ソースを追加できます。

### ■ vCenter Single Sign-On アイデンティティ ソースの編集

vSphere ユーザーは ID ソースで定義されています。vCenter Single Sign-On に関連付けられている ID ソースの詳細を編集できます。

### ■ vCenter Single Sign-On アイデンティティ ソースの削除

vSphere ユーザーは ID ソースで定義されています。登録された ID ソースのリストから ID ソースを削除できます。

### ■ Windows セッション認証での vCenter Single Sign-On の使用

vCenter Single Sign-On で Windows セッション認証 (SSPI) を使用できます。ログイン ページのチェックボックスを使用できるようにするには、クライアント統合プラグインをインストールする必要があります。

## vCenter Single Sign-On による vCenter Server の ID ソース

アイデンティティ ソースを使用して、vCenter Single Sign-On に 1 つ以上のドメインを添付できます。ドメインは vCenter Single Sign-On サーバがユーザー認証に使用できるユーザーまたはグループのリポジトリです。

ID ソースは、ユーザーおよびグループ データの集合体です。ユーザーおよびグループのデータは、Active Directory、OpenLDAP、またはローカルで vCenter Single Sign-On がインストールされたマシンのオペレーティング システムに格納されます。



インストールが完了すると、vCenter Single Sign-On のすべてのインスタンスに *your\_domain\_name* のアイデンティティ ソース (vsphere.local など) があります。このアイデンティティ ソースは vCenter Single Sign-On の内部のもので、vCenter Single Sign-On 管理者は、アイデンティティ ソースを追加したり、デフォルトのアイデンティティ ソースを設定したり、vsphere.local アイデンティティ ソースのユーザーおよびグループを作成したりできます。

## ID ソースのタイプ

バージョン 5.1 より前の vCenter Server バージョンは、Active Directory およびローカル オペレーティング システムのユーザーをユーザー リポジトリとしてサポートしていました。このため、ローカル オペレーティング システムのユーザーは常に vCenter Server システムから認証可能でした。vCenter Server バージョン 5.1 およびバージョン 5.5 では、認証に vCenter Single Sign-On を使用します。vCenter Single Sign-On 5.1 がサポートしているアイデンティティソースのリストについては、vSphere 5.1 のドキュメントを参照してください。

vCenter Single Sign-On 5.5 は以下のタイプのユーザー リポジトリをアイデンティティ ソースとしてサポートしていますが、デフォルトでサポートするアイデンティティ ソースは 1 つだけです。

- Active Directory バージョン 2003 以降。vSphere Web Client では、[Active Directory (統合 Windows 認証)] として表示されます。vCenter Single Sign-On では単一の Active Directory ドメインをアイデンティティ ソースとして指定できます。ドメインは、子ドメインを持たせたり、フォレスト ルート ドメインにしたりできます。VMware のナレッジベースの記事 [2064250](#) に、vCenter Single Sign-On でサポートされている Microsoft Active Directory の信頼関係についての解説があります。
- LDAP を用いた Active Directory。vCenter Single Sign-On は LDAP を用いた Active Directory の複数のアイデンティティ ソースをサポートします。このアイデンティティ ソース タイプは、vSphere 5.1 とともに含まれる vCenter Single Sign-On サービスとの互換性のために含まれています。vSphere Web Client に [LDAP サーバとしての Active Directory] として表示されます。
- OpenLDAP バージョン 2.4 以降。vCenter Single Sign-On は複数の OpenLDAP アイデンティティ ソースをサポートします。vSphere Web Client では、[OpenLDAP] として表示されます。
- ローカル オペレーティング システム ユーザー。ローカル オペレーティング システム ユーザーは、vCenter Single Sign-On サーバが実行されているオペレーティング システムのローカル ユーザーです。ローカル オペレーティング システムのアイデンティティ ソースは、基本的な vCenter Single Sign-On サーバの展開にのみ使用でき、複数の vCenter Single Sign-On インスタンスを用いた展開では使用できません。1 つのローカル オペレーティング システム アイデンティティ ソースのみが許可されます。vSphere Web Client では、[localos] として表示されます。

---

**注：** Platform Services Controller が vCenter Server システムと異なるマシン上に存在する場合は、ローカル オペレーティング システムのユーザーを使用しないでください。組み込みデプロイでローカル オペレーティング システムのユーザーを使用するのは理にかなっていませんが、お勧めしません。

---

- vCenter Single Sign-On のシステム ユーザー。vCenter Single Sign-On のインストール時に、vsphere.local という名前のただ 1 つのシステム アイデンティティ ソースが作成されます。vSphere Web Client では、[vsphere.local] として表示されます。

---

**注：** いかなる場合でも、デフォルトのドメインが 1 つだけ存在します。ユーザーがデフォルト以外のドメインからログインした場合、このユーザーが正常に認証されるためにはドメイン名 (*DOMAIN/user*) を追加する必要があります。

---

vCenter Single Sign-On のアイデンティティ ソースは vCenter Single Sign-On 管理者ユーザーが管理します。

アイデンティティ ソースは vCenter Single Sign-On サーバ インスタンスに追加できます。リモートのアイデンティティ ソースは、Active Directory および OpenLDAP のサーバ実装に限定されます。

## vCenter Single Sign-On 用のデフォルト ドメインの設定

vCenter Single Sign-On の各 ID ソースは、ドメインと関連付けられています。vCenter Single Sign-On は、ドメイン名なしでログインするユーザーの認証にデフォルトのドメインを使用します。デフォルト以外のドメインに所属するユーザーはログイン時にドメイン名を含む必要があります。

ユーザーが vSphere Web Client から vCenter Server システムにログインする場合、ログイン動作はユーザーがデフォルト ドメイン（つまり、デフォルトのアイデンティティ ソースとして設定されているドメイン）に所属しているかどうかによって異なります。

- デフォルト ドメインに所属しているユーザーはユーザー名とパスワードでログインできます。
- vCenter Single Sign-On にアイデンティティ ソースとして追加されているがデフォルト ドメイン以外のドメインに所属しているユーザーは、vCenter Server にログインできますが、次のいずれかの方法でドメインを指定する必要があります。
  - ドメイン名を前に含める。たとえば MYDOMAIN\user1
  - ドメインを含める。たとえば、user1@mydomain.com
- vCenter Single Sign-On アイデンティティ ソースでないドメインに所属しているユーザーは vCenter Server にはログインできません。vCenter Single Sign-On に追加したドメインがドメイン階層の一部である場合、Active Directory は階層内の他のドメインのユーザーが認証されているかどうかを判断します。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
  - 3 [ID ソース] タブで、ID ソースを選択して [デフォルト ドメインとして設定] アイコンをクリックします。
- ドメイン表示では、デフォルトのドメインのドメイン列に（デフォルト）と表示されます。

## vCenter Single Sign-On アイデンティティ ソースの追加

ユーザーは、vCenter Single Sign-On アイデンティティ ソースとして追加されたドメインに所属している場合に限り、vCenter Server にログインできます。vCenter Single Sign-On 管理者ユーザーは、vSphere Web Client からアイデンティティ ソースを追加できます。



アイデンティティ ソースとして、ネイティブの Active Directory（統合 Windows 認証）ドメインまたは OpenLDAP ディレクトリ サービスを使用できます。後方互換を維持するため、LDAP サーバとして Active Directory を利用できます。 [vCenter Single Sign-On による vCenter Server の ID ソース](#)を参照してください。

インストールの直後に、次のデフォルトのアイデンティティ ソースとユーザーが利用できるようになります。

## localos

すべてのローカル オペレーティング システム ユーザー。アップグレードする場合、すでに認証されているユーザーはアップグレード後も引き続き認証されます。Platform Services Controller を使用している環境で localos アイデンティティ ソースを使用しても意味がありません。

## vsphere.local

vCenter Single Sign-On の内部ユーザーを含みます。

### 前提条件

アイデンティティ ソースとして追加するドメインは、vCenter Single Sign-On を実行しているマシンで使用できるようにする必要があります。vCenter Server Appliance を使用している場合、vCenter Server Appliance の構成 のドキュメントを参照してください。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [アイデンティティ ソース] タブで、[アイデンティティ ソースの追加] アイコンをクリックします。
- 4 アイデンティティ ソースのタイプを選択し、アイデンティティ ソースの設定を入力します。

オプション	説明
<b>Active Directory (統合 Windows 認証)</b>	ネイティブの Active Directory 実装にこのオプションを使用します。このオプションを使用する場合は、vCenter Single Sign-On サービスが稼働しているマシンが Active Directory ドメインに属している必要があります。 <a href="#">Active Directory アイデンティティ ソースの設定</a> を参照してください。
<b>LDAP サーバとしての Active Directory</b>	このオプションは後方互換性用に使用できます。ドメイン コントローラと他の情報を指定する必要があります。 <a href="#">Active Directory LDAP Server および OpenLDAP Server アイデンティティ ソースの設定</a> を参照してください。

オプション	説明
OpenLDAP	OpenLDAP ID ソースにこのオプションを使用します。 <a href="#">Active Directory LDAP Server および OpenLDAP Server アイデンティティ ソースの設定</a> を参照してください。
LocalOS	ID ソースとしてローカル オペレーティング システムを追加する場合に、このオプションを使用します。ローカル オペレーティング システムの名前の入力のみが求められます。このオプションを選択すると、指定されたマシン上のすべてのユーザーは、それらのユーザーが別のドメインに含まれていなくても、vCenter Single Sign-On で認識されるようになります。

**注：** ユーザー アカウントがロックされているか無効である場合は、Active Directory ドメイン内の認証とグループ、およびユーザー検索が失敗します。ユーザー アカウントは、ユーザーとグループの OU への読み取り専用アクセス権を持ち、ユーザーとグループの属性を読み取ることができる必要があります。これは、認証権限についてのデフォルトの Active Directory ドメイン構成です。特別なサービス ユーザーを使用することを推奨します。

- LDAP サーバとしての Active Directory または OpenLDAP アイデンティティ ソースを設定した場合は、[テスト接続] をクリックして、アイデンティティ ソースに接続できることを確認します。
- [OK] をクリックします。

#### 次のステップ

アイデンティティ ソースが追加されると、すべてのユーザーは認証可能になりますが、アクセスなしロールが付与されます。vCenter Server の権限の変更権限を持つユーザーは、ユーザーまたはユーザーのグループに、vCenter Server にログインしてオブジェクトの表示と管理を実行できる権限を割り当てることができます。『vSphere セキュリティ』ドキュメントを参照してください。

## Active Directory アイデンティティ ソースの設定

[Active Directory (統合 Windows 認証)] アイデンティティ ソースのタイプを選択する場合、ローカル マシン アカウントをサービス プリンシパル名 (SPN) として使用するか、または SPN を明示的に指定できます。このオプションは、vCenter Single Sign-On サーバが Active Directory ドメインに参加している場合にのみ使用できます。

#### Active Directory アイデンティティ ソース使用の前提条件

Active Directory アイデンティティ ソースが利用可能な場合にのみ、これを使用するように vCenter Single Sign-On を設定できます。

- Windows 環境に vCenter Server をインストールする場合、その Windows マシンを Active Directory ドメインに追加します。
- vCenter Server Appliance の場合、『vCenter Server Appliance の構成』ドキュメントの手順を実行してください。

**注：** Active Directory (統合 Windows 認証) は、Active Directory ドメイン フォレストのルートに常に使用します。Active Directory フォレスト内の子ドメインを使用して統合 Windows 認証アイデンティティ ソースを構成する方法については、VMware ナレッジ ベースの記事 [KB2070433](#) を参照してください。

設定を迅速に行うには、[マシン アカウントを使用] を選択します。vCenter Single Sign-On が稼動するローカルマシンの名前を変更予定の場合は、SPN を明示的に指定することをお勧めします。

**注：** vSphere 5.5 の場合、SPN を指定しても vCenter Single Sign-On はマシン アカウントを使用します。VMware ナレッジベースの記事 [KB2087978](#) を参照してください。

表 2-5. アイデンティティ ソース設定の追加

テキスト ボックス	説明
[ドメイン名]	mydomain.com のような完全修飾ドメイン名 (FQDN)。IP アドレスは指定しないでください。このドメイン名は、vCenter Server システムによって DNS 解決が可能である必要があります。vCenter Server Appliance を使用している場合は、ネットワーク設定でこの情報を使用して DNS サーバ設定を更新します。
[マシン アカウントを使用]	ローカル マシン アカウントを SPN として使用する場合は、このオプションを選択します。このオプションを選択する場合は、ドメイン名のみを指定します。マシン名を変更する場合は、このオプションを選択しないでください。
[サービス プリンシパル名 (SPN) を使用]	ローカル マシン名を変更する場合は、このオプションを選択します。SPN、アイデンティティ ソースで認証できるユーザー、およびそのユーザーのパスワードを指定する必要があります。
[サービス プリンシパル名 (SPN)]	Kerberos による Active Directory サービスの特定を支援する SNP。STS/example.com のように、名前にドメインを含めます。SPN はドメイン全体で一意である必要があります。setspn -S を実行して、重複した名前が作成されていないことを確認します。setspn の情報については、Microsoft のドキュメントを参照してください。
[ユーザー プリンシパル名 (UPN)] [パスワード]	このアイデンティティ ソースで認証できるユーザー名とパスワード。jchin@mydomain.com のように、メール アドレスの形式を使用します。ユーザー プリンシパル名は、Active Directory サービス インターフェイス エディタ (ADSI エディタ) で検証できます。

## Active Directory LDAP Server および OpenLDAP Server アイデンティティ ソースの設定

LDAP Server アイデンティティ ソースとしての Active Directory は、後方互換性を確保するために用意されています。Active Directory (統合 Windows 認証) オプションは、入力の要求が少ないセットアップで使えます。OpenLDAP Server アイデンティティ ソースは、OpenLDAP を使用する環境で使えます。

OpenLDAP のアイデンティティ ソースを構成する場合は、当社のナレッジ ベース記事 [2064977](#) で追加要件を確認してください。

表 2-6. LDAP サーバとしての Active Directory および OpenLDAP の設定

フィールド	説明
名前	アイデンティティ ソースの名前。
ユーザーのベース DN	ユーザーのベース識別名。

表 2-6. LDAP サーバとしての Active Directory および OpenLDAP の設定（続き）

フィールド	説明
ドメイン名	ドメインの FQDN（example.com など）。このフィールドには IP アドレスを入力しないでください。
ドメイン エイリアス	Active Directory のアイデンティティ ソースの場合、ドメインの NetBIOS 名。SSPI 認証を使用する場合は、アイデンティティ ソースの別名として Active Directory ドメインの NetBIOS 名を追加します。  OpenLDAP のアイデンティティ ソースの場合、別名を指定しないと、大文字で表記されたドメイン名が追加されます。
グループのベース DN	グループのベース識別名。
プライマリ サーバの URL	ドメインのプライマリ ドメイン コントローラ LDAP サーバ。 ldap://hostname:port or ldaps://hostname:port 形式を使用します。通常のポートは、ldap: 接続では 389、ldaps: 接続では 636 です。Active Directory のマルチドメイン コントローラ デプロイの場合、通常のポートは ldap: 接続では 3268、ldaps: 接続では 3269 です。  プライマリまたはセカンダリ LDAP の URL に ldaps:// を使用する場合は、Active Directory サーバの LDAPS エンドポイントに対する信頼を確立する証明書が必要です。
セカンダリ サーバの URL	フェイルオーバーに使用されるセカンダリ ドメイン コントローラ LDAP サーバのアドレス。
証明書の選択	Active Directory LDAP Server または OpenLDAP Server のアイデンティティ ソースで LDAPS を使用する場合は、[証明書の選択] ボタンは、URL フィールドに「ldaps://」と入力した後に有効になります。セカンダリ URL は不要です。
ユーザー名	ユーザーおよびグループの BaseDN に対して、最低限の読み取り専用アクセス権を持つドメイン内のユーザーの ID。
パスワード	[ユーザー名] で指定したユーザーのパスワード。

## vCenter Single Sign-On アイデンティティ ソースの編集

vSphere ユーザーは ID ソースで定義されています。vCenter Single Sign-On に関連付けられている ID ソースの詳細を編集できます。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [ID ソース] タブをクリックします。
- 4 テーブルの ID ソースを右クリックし、[ID ソースの編集]を選択します。

- 5 ID ソースの設定を編集します。使用できるオプションは選択した ID ソースのタイプによって異なります。

オプション	説明
Active Directory (統合 Windows 認証)	ネイティブの Active Directory 実装にこのオプションを使用します。このオプションを使用する場合は、vCenter Single Sign-On サービスが稼働しているマシンが Active Directory ドメインに属している必要があります。 <a href="#">Active Directory アイデンティティ ソースの設定</a> を参照してください。
LDAP サーバとしての Active Directory	このオプションは後方互換性用に使用できます。ドメイン コントローラと他の情報を指定する必要があります。 <a href="#">Active Directory LDAP Server</a> および <a href="#">OpenLDAP Server アイデンティティ ソースの設定</a> を参照してください。
OpenLDAP	OpenLDAP ID ソースにこのオプションを使用します。 <a href="#">Active Directory LDAP Server</a> および <a href="#">OpenLDAP Server アイデンティティ ソースの設定</a> を参照してください。
LocalOS	ID ソースとしてローカル オペレーティング システムを追加する場合に、このオプションを使用します。ローカル オペレーティング システムの名前の入力のみが求められます。このオプションを選択すると、指定されたマシン上のすべてのユーザーは、それらのユーザーが別のドメインに含まれていなくても、vCenter Single Sign-On で認識されるようになります。

- 6 [テスト接続] をクリックして、ID ソースに接続できることを確認します。

- 7 [OK] をクリックします。

## vCenter Single Sign-On アイデンティティ ソースの削除

vSphere ユーザーは ID ソースで定義されています。登録された ID ソースのリストから ID ソースを削除できます。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [ID ソース] タブで、ID ソースを選択して[ID ソースの削除]アイコンをクリックします。
- 4 確認を求められたら[はい]をクリックします。

## Windows セッション認証での vCenter Single Sign-On の使用

vCenter Single Sign-On で Windows セッション認証 (SSPI) を使用できます。ログイン ページのチェックボックスを使用できるようにするには、クライアント統合プラグインをインストールする必要があります。

SSPI を使用すると、現在マシンにログインしているユーザーのログインを迅速に行えるようになります。

### 前提条件

Windows ドメインが適切に設定されている必要があります。当社のナレッジ ベースの記事 [2064250](#) を参照してください。

## 手順

- 1 vSphere Web Client ログイン ページに移動します。
- 2 [Windows セッション認証を使用してください] チェック ボックスを使用できない場合は、ログイン ページの下部にある [クライアント統合プラグインのダウンロード] をクリックします。
- 3 証明書エラーの発生やポップアップ ブロッカーの実行によって、ブラウザでインストールがブロックされた場合は、ブラウザのヘルプの指示に従って、問題を解決してください。
- 4 他のブラウザを閉じるように要求された場合は閉じます。

インストール後に、すべてのブラウザでプラグインが利用できるようになります。ブラウザで要求された場合は、個々のセッションまたはすべてのセッションでプラグインを許可することが必要になる可能性があります。

- 5 ブラウザを終了して再起動します。

再起動後、[Windows セッション認証を使用してください] チェック ボックスを選択できます。

## vCenter Server 2 要素認証

vCenter Single Sign-On では、vCenter Single Sign-On で認識されているアイデンティティ ソース内のユーザ名およびパスワードを使用した認証、または Active Directory アイデンティティ ソースの Windows セッション認証を使用した認証が可能です。また、vSphere 6.0 Update 2 以降では、スマート カード (UPN ベースの Common Access Card (CAC)) を使用して、または RSA SecureID トークンを使用して認証を行うことができます。

## 2 要素認証方法

2 要素認証方法は、一般的に行政機関および大規模企業で利用されます。

### Common Access Card (CAC) 認証

CAC 認証を使用すると、ログインしているコンピュータの USB ドライブに物理カードを接続しているユーザーにのみアクセスが許可されます。公開鍵基盤 (PKI) を展開し、認証局が発行する唯一のクライアント証明書としてスマート カード証明書を設定している場合は、スマート カード証明書のみがユーザーに提示されます。ユーザーが証明書を選択すると、PIN を入力するよう求められます。物理カードおよび PIN (証明書と一致するもの) の両方を持っているユーザーのみがログインできます。

### RSA SecureID 認証

RSA SecureID 認証の場合は、正しく構成された RSA 認証マネージャが環境内に含まれている必要があります。Platform Services Controller が RSA サーバを指すように構成されており、RSA SecureID 認証が有効である場合、ユーザーはユーザー名およびトークンを使用してログインできます。

---

**注：** vCenter Single Sign-On では、ネイティブの SecureID のみがサポートされており、RADIUS 認証はサポートされていません。

---

## デフォルト以外の認証方法の指定

管理者は、[]Platform Services Controller Web インターフェイスから、または `sso-config` スクリプト (Windows では `sso-config.bat`、およびアプライアンスでは `sso-config.sh`) を使用して設定を実行できます。

- Common Access Card 認証の場合、`sso-config` スクリプトを使用して Web ブラウザを設定し、Platform Services Controller Web インターフェイスから、または `sso-config` を使用して vCenter Single Sign-On の設定を実行できます。設定には、CAC 認証の有効化、証明書失効ポリシーの構成、およびログイン バナーの設定が含まれます。
- RSA SecureID の場合、`sso-config` スクリプトを使用してドメインの RSA 認証マネージャを構成し、RSA トークン認証を有効にします。有効になっている場合、Platform Services Controller Web インターフェイスに認証方法が表示されますが、Web インターフェイスから RSA SecureID 認証を構成することはできません。

## 異なる認証方法の組み合わせ

`sso-config` を使用することで、各認証方法を個別に有効または無効にできます。たとえば、2 要素認証方法の 1 つをテストしながら、最初にユーザー名およびパスワードによる認証を有効にしておき、その後に 1 つの認証方法のみを有効にする場合に利用できます。

## vCenter Single Sign-On のスマート カード認証の構成

ユーザーが vSphere Web Client から vCenter Server または関連する Platform Services Controller に接続する場合、スマート カード認証を行うように環境を設定することができます。

### スマート カード認証ログイン

スマート カードは、集積回路チップが埋め込まれた小さなプラスチック製カードです。多くの政府機関および大規模企業では、Common Access Card (CAC) などのスマート カードを使用して、システムのセキュリティ向上やセキュリティ規制への準拠を実現しています。Common Access Card は、各マシンにスマート カード リーダーを搭載した環境で使用します。一般的に、マシンには Common Access Card を管理するスマート カード ハードウェア ドライバが事前にインストールされています。

vCenter Single Sign-On のスマート カード認証を構成すると、vCenter Server または Platform Services Controller システムにログインするユーザーは、スマート カードと PIN を組み合わせて認証を行うように要求されます。

- 1 ユーザーがスマート カードをスマート カード リーダーに挿入すると、vCenter Single Sign-On はカード上の証明書を読み取ります。



- 2 vCenter Single Sign-On は、ユーザーに証明書の選択とその証明書の PIN の入力を求めます。
- 3 また、スマート カード上の証明書が既存のものかどうか、さらに PIN が正しいかどうかを確認します。失効チェックが有効な場合、vCenter Single Sign-On は証明書が失効しているかどうかを確認します。
- 4 証明書が既存のものであり、失効していなければ、ユーザーが認証され、権限を与えられたタスクを実行することができます。

**注：** 通常、テスト環境の場合は、ユーザー名とパスワードによる認証を有効にしても問題ありません。テスト終了後、ユーザー名とパスワードによる認証を無効にして、スマート カード認証を有効にします。その後、vSphere Client ではスマート カード ログインのみを許可します。Platform Services Controller ディレクトリにログインしてユーザー名とパスワードを再度有効にできるのは、マシン上で root 権限または管理者権限を持つユーザーのみです。

## コマンド ラインを使用したスマート カード認証の設定

sso-config ユーティリティを使用して、コマンド ラインからスマート カード認証を設定できます。このユーティリティは、すべてのスマート カード設定タスクをサポートしています。

コマンド ラインからスマート カード認証を設定するときには、必ず最初に sso-config コマンドを使用して、Platform Services Controller を設定します。その後で、Platform Services Controller Web インターフェイスを使用して、他のタスクを実行します。

- 1 ユーザーのログイン時に Web ブラウザがスマート カード証明書の送信を要求するよう、Platform Services Controller を設定します。
- 2 認証ポリシーを設定します。sso-config スクリプトまたは Platform Services Controller Web インターフェイスを使用して、ポリシーを設定できます。サポートされている認証タイプおよび失効の設定は VMware Directory Service に保存され、vCenter Single Sign-On ドメインのすべての Platform Services Controller インスタンスにわたってレプリケートされます。

スマート カード認証が有効で、その他の認証方法が無効な場合、ユーザーはスマート カード認証を使用してログインする必要があります。

vSphere Web Client からのログインが機能しない場合、およびユーザー名とパスワードによる認証が無効な場合、root または管理者ユーザーは、Platform Services Controller コマンド ラインから次のコマンドを実行することで、ユーザー名とパスワードによる認証を再度有効にできます。この例は Windows 向けのものです。Linux の場合は、sso-config.sh を使用します。

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

sso-config スクリプトは次の場所にあります。

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

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



## 前提条件

- 環境内で Platform Services Controller バージョン 6.0 Update 2 以降、および vCenter Server バージョン 6.0 以降を使用していることを確認します。バージョン 5.5 のノードをバージョン 6.0 にアップグレードします。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応するユーザー プリンシパル名 (UPN)。
  - クライアント認証は、証明書の「アプリケーション ポリシー」または「拡張キーの使用」フィールドで指定されている必要があります。指定されていない場合、証明書がブラウザに表示されません。
- Platform Services Controller Web インターフェイスの証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザによる認証は試行されません。
- Active Directory アイデンティティ ソースを構成し、vCenter Single Sign-On に アイデンティティ ソースとして追加します。
- vCenter Server 管理者ロールを、Active Directory アイデンティティ ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、Active Directory グループに参加し、vCenter Server 管理者権限が付与されることで認証が可能になります。administrator@vsphere.local ユーザーは、スマート カード認証を実行できません。
- Platform Services Controller の高可用性ソリューションを環境内で使用する場合、スマート カード認証を設定する前に、すべての高可用性の構成を完了する必要があります。VMware のナレッジベースの記事 [KB2112085](#) (Windows) または [KB2113315](#) (vCenter Server Appliance) を参照してください。

## 手順

- 1 証明書を取得し、sso-config ユーティリティで表示可能なフォルダにその証明書をコピーします。

オプション	説明
Windows	Platform Services Controller Windows 環境にログインし、WinSCP または類似のユーティリティを使用してファイルをコピーします。
アプライアンス	<ol style="list-style-type: none"> <li>a 直接または SSH を使用してアプライアンス コンソールにログインします。</li> <li>b アプライアンス シェルを次のように有効にします。               <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </li> <li>c WinSCP または類似のユーティリティを使用して、証明書を Platform Services Controller 上の /usr/lib/vmware-sso/vmware-sts/conf にコピーします。</li> <li>d 必要に応じて、アプライアンス シェルを次のように無効にします。               <pre>chsh -s "bin/appliancesh" root</pre> </li> </ol>

- 2 各 Platform Services Controller ノードで sso-config CLI を使用して、スマート カード認証を設定します。

- a sso-config スクリプトが配置されているディレクトリに移動します。

オプション	説明
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
アプライアンス	/opt/vmware/bin

- b 次のコマンドを実行します。

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

例：

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

- c 仮想マシンまたは物理マシンを再起動します。

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

- 3 VMware Directory Service (vmdir) のスマート カード認証を有効にするには、次のコマンドを実行します。

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

例：

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

複数の証明書を指定する場合、証明書間のスペースは許可されません。

- 4 他の認証方法をすべて無効にするには、次のコマンドを実行します。

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

これらのコマンドにより、必要に応じて各種の認証方法を有効または無効にすることができます。

- 5 (オプション) 証明書ポリシーの許可リストを設定するには、次のコマンドを実行します。

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

複数のポリシーを指定するには、次のようにコンマでポリシーを区切ります。

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

この許可リストには、証明書の証明書ポリシー拡張で許可されているポリシーのオブジェクト ID を指定します。X509 証明書では、証明書ポリシー拡張を使用できます。

- 6 (オプション) 設定情報をリストで表示するには、次のコマンドを実行します。

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

## Platform Services Controller Web インターフェイスを使用したスマート カード認証の管理

Platform Services Controller Web インターフェイスから、スマート カード認証の有効と無効の切り替え、ログイン バナーのカスタマイズ、失効ポリシーの設定を行うことができます。

コマンドラインからスマート カード認証を設定するときには、必ず最初に `sso-config` コマンドを使用して、Platform Services Controller を設定します。その後で、Platform Services Controller Web インターフェイスを使用して、他のタスクを実行します。

- 1 ユーザーのログイン時に Web ブラウザがスマート カード証明書の送信を要求するよう、Platform Services Controller を設定します。
- 2 認証ポリシーを設定します。`sso-config` スクリプトまたは Platform Services Controller Web インターフェイスを使用して、ポリシーを設定できます。サポートされている認証タイプおよび失効の設定は VMware Directory Service に保存され、vCenter Single Sign-On ドメインのすべての Platform Services Controller インスタンスにわたってレプリケートされます。

スマート カード認証が有効で、その他の認証方法が無効な場合、ユーザーはスマート カード認証を使用してログインする必要があります。

vSphere Web Client からのログインが機能しない場合、およびユーザー名とパスワードによる認証が無効な場合、root または管理者ユーザーは、Platform Services Controller コマンドラインから次のコマンドを実行することで、ユーザー名とパスワードによる認証を再度有効にできます。この例は Windows 向けのものです。Linux の場合は、`sso-config.sh` を使用します。

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

### 前提条件

- 環境内で Platform Services Controller バージョン 6.0 Update 2 以降、および vCenter Server バージョン 6.0 以降を使用していることを確認します。バージョン 5.5 のノードをバージョン 6.0 にアップグレードします。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応するユーザー プリンシパル名 (UPN)。

- クライアント認証は、証明書の「アプリケーション ポリシー」または「拡張キーの使用」フィールドで指定されている必要があります。指定されていない場合、証明書がブラウザに表示されません。
- Platform Services Controller Web インターフェイスの証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザによる認証は試行されません。
- Active Directory アイデンティティ ソースを構成し、vCenter Single Sign-On に アイデンティティ ソースとして追加します。
- vCenter Server 管理者ロールを、Active Directory アイデンティティ ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、Active Directory グループに参加し、vCenter Server 管理者権限が付与されることで認証が可能になります。administrator@vsphere.local ユーザーは、スマート カード認証を実行できません。
- Platform Services Controller の高可用性ソリューションを環境内で使用する場合、スマート カード認証を設定する前に、すべての高可用性の構成を完了する必要があります。VMware のナレッジベースの記事 [KB2112085](#) (Windows) または [KB2113315](#) (vCenter Server Appliance) を参照してください。

#### 手順

- 1 証明書を取得し、sso-config ユーティリティで表示可能なフォルダにその証明書をコピーします。

オプション	説明
Windows	Platform Services Controller Windows 環境にログインし、WinSCP または類似のユーティリティを使用してファイルをコピーします。
アプライアンス	<ol style="list-style-type: none"> <li>a 直接または SSH を使用してアプライアンス コンソールにログインします。</li> <li>b アプライアンス シェルを次のように有効にします。 <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </div> </li> <li>c WinSCP または類似のユーティリティを使用して、証明書を Platform Services Controller 上の /usr/lib/vmware-sso/vmware-sts/conf にコピーします。</li> <li>d 必要に応じて、アプライアンス シェルを次のように無効にします。 <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>chsh -s "bin/appliancesh" root</pre> </div> </li> </ol>

- 2 各 Platform Services Controller ノードで sso-config CLI を使用して、スマート カード認証を設定します。

- a sso-config スクリプトが配置されているディレクトリに移動します。

オプション	説明
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
アプライアンス	/opt/vmware/bin

- b 次のコマンドを実行します。

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

例：

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

複数の証明書をコンマで区切って入力できますが、コンマの後にスペースは入れないでください。

- c 仮想マシンまたは物理マシンを再起動します。

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

- 3 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 4 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 5 [シングル サインオン] - [構成] を参照します。
- 6 [スマート カードの構成] をクリックし、[信頼できる CA 証明書] タブを選択します。
- 7 信頼できる証明書を 1 つ以上追加するには、[証明書の追加] をクリックし、[参照] をクリックします。次に信頼できる CA からのすべての証明書を選択し、[OK] をクリックします。
- 8 認証の構成を指定するには、[認証の設定] の横にある [編集] をクリックし、認証方法の選択または選択解除を行います。

Web インターフェイスから、RSA SecurID 認証の有効と無効の切り替えはできません。ただし、RSA SecurID をコマンド ラインで有効にしている場合は、そのステータスが Web インターフェイスに表示されません。

## スマート カード認証の失効ポリシーの設定

証明書の失効チェックは、カスタマイズできます。また、失効した証明書の情報について、vCenter Single Sign-On の参照先を指定できます。

Platform Services Controller Web インターフェイスまたは `sso-config` スクリプトを使用して動作をカスタマイズできます。認証局が何をサポートするかによって、設定が異なる場合があります。

- 失効チェックが無効になっている場合、vCenter Single Sign-On では証明書失効リスト (CRL) またはオンライン証明書状態プロトコル (OCSP) の設定はすべて無視されます。
- 失効チェックが有効になっている場合、推奨される設定は PKI の設定により異なります。

### OCSP のみ

発行元の認証局で OCSP レスポンダがサポートされている場合、OCSP が有効になり、CRL の代替利用はできなくなります。

### CRL のみ

発行元の認証局で OCSP がサポートされていない場合、CRL チェックが有効になり、OCSP チェックが無効になります。

### OCSP と CRL の両方の利用

発行元の認証局で OCSP レスポンダと CRL の両方がサポートされている場合、vCenter Single Sign-On によって OCSP レスポンダが最初にチェックされます。レスポンダによって不明なステータスが返されるか、使用可能でない場合は、vCenter Single Sign-On によって CRL がチェックされます。この場合、OCSP チェックおよび CRL チェックの両方が有効になり、OCSP に問題がある場合、代わりに CRL を利用できるようになります。

- 失効チェックが有効な場合、上級ユーザーは次の追加設定を指定できます。

### OCSP URL

vCenter Single Sign-On は、デフォルトで、検証されている証明書内で定義される OCSP レスポンダの場所を確認します。Authority Information Access 拡張が証明書内に含まれていない場合や、OCSP レスポンダが環境に存在しない場合は、明示的に場所を指定してオーバーライドできます。

### 証明書の CRL を使用

vCenter Single Sign-On は、デフォルトで、検証されている証明書内で定義される CRL の場所を確認します。CRL Distribution Point 拡張領域が含まれていない場合、または、デフォルト設定をオーバーライドする場合は、このオプションを無効化します。

### CRL の場所

[証明書の CRL を使用] を無効にし、CRL が配置されている場所（ファイルまたは HTTP URL）を指定する場合は、このプロパティを使用します。

また、証明書ポリシーを追加することで、vCenter Single Sign-On が受け入れる証明書をさらに制限できます。

## 前提条件

- 環境内で Platform Services Controller バージョン 6.0 Update 2 以降、および vCenter Server バージョン 6.0 以降を使用していることを確認します。バージョン 5.5 のノードをバージョン 6.0 にアップグレードします。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応するユーザー プリンシパル名 (UPN)。
  - クライアント認証は、証明書の「アプリケーション ポリシー」または「拡張キーの使用」フィールドで指定されている必要があります。指定されていない場合、証明書がブラウザに表示されません。
- Platform Services Controller Web インターフェイスの証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザによる認証は試行されません。
- Active Directory アイデンティティ ソースを構成し、vCenter Single Sign-On に アイデンティティ ソースとして追加します。
- vCenter Server 管理者ロールを、Active Directory アイデンティティ ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、Active Directory グループに参加し、vCenter Server 管理者権限が付与されることで認証が可能になります。administrator@vsphere.local ユーザーは、スマート カード認証を実行できません。
- Platform Services Controller 高可用性ソリューションを環境内で使用する場合、スマート カード認証を設定する前に、すべての高可用性の構成を完了する必要があります。VMware のナレッジベースの記事 [2113085](#) (Windows) または [2113315](#) (vCenter Server Appliance) を参照してください。

## 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 [シングル サインオン] - [構成] を参照します。
- 4 [証明書失効の設定] をクリックし、失効チェックを有効または無効にします。
- 5 環境内で証明書ポリシーが有効になっている場合、[承認された証明書ポリシー] ペインにポリシーを追加できます。

## RSA SecurID 認証の設定

パスワードの代わりに、RSA SecurID 認証トークンを使用してユーザーによるログインを要求するように環境を設定できます。SecurID の設定はコマンド ラインからのみサポートされています。

詳細については、[RSA SecurID の設定](#)に関する 2 つの vSphere ブログ投稿を参照してください。

**注：** RSA 認証マネージャでは、ユーザー ID が ASCII 文字（1 ～ 255 文字）を使用する一意の識別子である必要があります。アンパサンド (&)、パーセント (%), より大きい (>)、より小さい (<)、一重引用符 (') の文字は使用できません。

#### 前提条件

- 環境内で Platform Services Controller バージョン 6.0 Update 2 以降、および vCenter Server バージョン 6.0 以降を使用していることを確認します。バージョン 5.5 のノードをバージョン 6.0 にアップグレードします。
- 環境内に正しく構成された RSA 認証マネージャが配備され、ユーザーに RSA トークンが提供されていることを確認します。RSA 認証マネージャのバージョン 8.0 以降が必要です。
- RSA マネージャが使用するアイデンティティ ソースが、vCenter Single Sign-On に追加されていることを確認します。[vCenter Single Sign-On アイデンティティ ソースの追加](#)を参照してください。
- RSA 認証マネージャのシステムが Platform Services Controller ホスト名を解決でき、Platform Services Controller システムが RSA 認証マネージャのホスト名を解決できることを確認します。
- [アクセス] - [認証エージェント] - [構成ファイルを生成] を選択して、sdconf.rec ファイルを RSA マネージャからエクスポートします。生成された AM\_Config.zip ファイルを解凍し、sdconf.rec ファイルを見つけます。
- sdconf.rec ファイルを Platform Services Controller ノードにコピーします。

#### 手順

- 1 sso-config スクリプトが配置されているディレクトリに移動します。

オプション	説明
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
アプライアンス	/opt/vmware/bin

- 2 RSA SecureID 認証を有効にするには、次のコマンドを実行します。

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

*tenantName* は、vCenter Single Sign-On ドメインの名前であり、デフォルトで vsphere.local になっています。

- 3 (オプション) その他の認証方法を無効にするには、次のコマンドを実行します。

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



- 4 クライアント サイトのテナントが RSA サイトを使用するように環境を設定するには、次のコマンドを実行します。

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

例：

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

次のオプションを指定できます。

オプション	説明
<b>siteID</b>	オプションの Platform Services Controller サイト ID。Platform Services Controller は、サイトあたり 1 つの RSA 認証マネージャ インスタンスまたはクラスタをサポートします。このオプションを明示的に指定しない場合、RSA 設定は現在の Platform Services Controller サイトの設定用になります。このオプションは、異なるサイトを追加する場合にのみ使用します。
<b>agentName</b>	RSA 認証マネージャ内で定義されます。
<b>sdConfFile</b>	sdconf.rec ファイルのコピーであり、RSA マネージャからダウンロードされたもので、IP アドレスなどの設定情報を含んでいます。

- 5 (オプション) テナント構成をデフォルト以外の値に変更するには、次のコマンドを実行します。

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

通常、デフォルト値が適切です。次に例を示します。

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

- 6 (オプション) アイデンティティ ソースでユーザー プリンシパル名がユーザー ID として使用されていない場合、アイデンティティ ソースの userID 属性を設定します。

この userID 属性により、RSA userID として使用される LDAP 属性が決定されます。

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

例：

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

- 7 現在の設定を表示するには、次のコマンドを実行します。

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

## 結果

ユーザー名とパスワードによる認証が無効で、SecurID トークンによる認証が有効な場合、ユーザーはユーザー名と SecurID トークンを使用してログインする必要があります。ユーザー名とパスワードでのログインはできません。

## ログイン バナーの管理

vSphere 6.0 Update 2 以降では、ユーザー環境にログイン バナーを表示できるようになりました。たとえば、ユーザーが使用条件に同意するように、テキストを表示したり、チェック ボックスのクリックを要求することができます。ログイン バナーの有効化と無効化を切り替えたり、明示的な承諾を得る際にユーザーがチェック ボックスをクリックするように求めたりできます。

## 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 Single Sign-On で、[構成] を選択して [ログイン バナー] タブをクリックします。
- 4 [編集] をクリックし、ログイン バナーを構成します。

オプション	説明
ステータス	ログイン バナーを有効にするには、[有効] チェック ボックスをクリックします。このチェック ボックスをクリックするまで、他のフィールドを変更することはできません。
明示的な承諾	ログイン前にユーザーがチェック ボックスをクリックするように求めるには、[明示的な承諾] チェック ボックスをクリックします。また、チェック ボックスを使用せずにメッセージを表示することもできます。
タイトル	バナーのタイトル。デフォルトでは、ログイン バナーのテキストは I agree to the です。このテキストに Terms and Conditionsなどを追加できます。
メッセージ	ユーザーがバナーをクリックすると表示されるメッセージ。たとえば、使用条件の文章などです。明示的な承諾を求める場合は、メッセージを表示する必要があります。

## 別のサービス プロバイダの ID プロバイダとして vCenter Single Sign-On を使用する

vSphere Web Client は、信頼される SAML 2.0 サービス プロバイダ (SP) として自動的に vCenter Single Sign-On に登録されます。他の信頼されるサービス プロバイダを、vCenter Single Sign-On が SAML ID プロバイダ (IDP) として動作する ID フェデレーションに追加することができます。サービス プロバイダは SAML 2.0

プロトコルに適合する必要があります。フェデレーションを設定した後、ユーザーが vCenter Single Sign-On の認証を受けることができれば、サービス プロバイダはそのユーザーにアクセス権を付与します。

---

**注：** vCenter Single Sign-On を別の SP に対する IDP にすることができます。vCenter Single Sign-On を別の IDP を使用する SP にすることはできません。

---

登録された SAML サービス プロバイダは、すでにライブ セッション中のユーザーに対してアクセス権を付与することができます。これは ID プロバイダにログインされているユーザーのことです。たとえば、vRealize Automation 7.0 以降では ID プロバイダとして vCenter Single Sign-On をサポートしています。vCenter Single Sign-On および vRealize Automation からフェデレーションを設定することができます。その後、vRealize Automation にログインするときに vCenter Single Sign-On は認証を実行することができます。

ID フェデレーションに SAML サービス プロバイダを参加させるには、SAML メタデータを SP と IDP の間で交換することで信頼関係を確立する必要があります。

vCenter Single Sign-On と、vCenter Single Sign-On を使用するサービスの両方に統合タスクを実行する必要があります。

- 1 IDP メタデータをファイルにエクスポートし、SP にインポートします。
- 2 SP メタデータをエクスポートし、IDP にインポートします。

IDP メタデータのエクスポート、および SP からのメタデータのインポートには、vCenter Single Sign-On との vSphere Web Client インターフェイスを使用することができます。vRealize Automation を SP として使用している場合は、SP メタデータのエクスポートおよび IDP メタデータのインポートの詳細について vRealize Automation のドキュメントを参照してください。

---

**注：** サービスが SAML 2.0 標準を完全にサポートしている必要があります。そうでない場合、連携に失敗します。

---

## SAML サービス プロバイダの追加

SAML サービス プロバイダを vCenter Single Sign-On に追加し、このサービスに ID プロバイダとして vCenter Single Sign-On を追加します。その後、ユーザーがこのサービス プロバイダにログインすると、サービス プロバイダが vCenter Single Sign-On を使用してこのユーザーを認証します。

VMware vRealize Automation 7.0 以降に含まれるシングル サインオン ソリューションと vCenter Single Sign-On ID プロバイダを統合する場合、または別の外部 SAML サービス プロバイダを使用する場合は、この手順を使用します。

このプロセスでは、SAML サービス プロバイダから vCenter Single Sign-On へ、また vCenter Single Sign-On から SAML サービス プロバイダへのメタデータのインポートが行われるため、2 つのプロバイダがすべてのデータを共有します。

### 前提条件

対象のサービスが SAML 2.0 標準を完全にサポートしている必要があります。

メタデータが SAML 2.0 メタデータ スキーマに正確に対応していない場合は、メタデータのインポート前にスキーマの編集が必要になることがあります。たとえば、Active Directory フェデレーション サービス (ADFS) の SAML サービス プロバイダを使用している場合、インポートする前にメタデータを編集する必要があります。次の非標準の要素を削除します：

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

この時点で、vSphere Web Client から SAML IDP メタデータをインポートすることはできません。

#### 手順

- 1 サービス プロバイダのメタデータをファイルにエクスポートします。
- 2 サービス プロバイダのメタデータを vCenter Single Sign-On にインポートします。
  - a administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。  
  
vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに含まれます。
  - b [シングル サインオン] - [構成] を参照します。
  - c [SAML サービス プロバイダ] タブを選択します。
  - d [SAML サービス プロバイダのメタデータ] フィールドで、[インポート] をクリックして XML 文字列をダイアログに貼り付けるか、[ファイルからインポート] をクリックしてファイルをインポートし、[インポート] をクリックします。
- 3 vCenter Single Sign-On メタデータをエクスポートします。
  - a [SAML サービス プロバイダのメタデータ] フィールドで [ダウンロード] をクリックします。
  - b ファイルの場所を指定します。
- 4 たとえば、VMware vRealize Automation 7.0 以降などの SAML サービス プロバイダに移動し、SAML サービス プロバイダの指示に従って、vCenter Single Sign-On メタデータをこのサービス プロバイダに追加します。  
  
メタデータのインポートに関する詳細については、vRealize Automation のドキュメントを参照してください。

## Security Token Service (STS)

vCenter Single Sign-On の Security Token Service (STS) は、セキュリティ トークンの発行、検証、更新を行う Web サービスです。

ユーザーはプライマリ認証情報を STS インターフェイスに提供して、SAML トークンを取得します。プライマリ認証情報は、ユーザーのタイプによって異なります。

#### ユーザー

vCenter Single Sign-On アイデンティティ ソースで利用できるユーザー名とパスワード

## アプリケーション ユーザー

### 有効な証明書

STS は、プライマリ認証情報に基づいてユーザーを認証し、ユーザー属性が含まれている SAML トークンを構築します。STS は、その STS 署名証明書を使用して SAML トークンに署名し、トークンをユーザーに割り当てます。デフォルトでは、STS 署名証明書は VMCA によって生成されます。デフォルトの STS 署名証明書は、vSphere Web Client から置き換えられます。会社のセキュリティ ポリシーですべての認証情報の置き換えが必要な場合を除いて、STS 署名証明書を置き換えしないでください。

ユーザーが SAML トークンを取得したら、SAML トークンはそのユーザーの HTTP 要求の一部として送信されます。このとき、さまざまなプロキシを通過する場合があります。対象受信者（サービス プロバイダ）のみが SAML トークンの情報を使用できます。

## アプライアンスでの新しい STS 署名証明書の生成

デフォルトの vCenter Single Sign-On の Security Token Service (STS) 署名証明書を置き換える場合は、新しい証明書を生成し、Java キーストアに追加する必要があります。ここでは、組み込まれたデプロイ アプライアンスまたは外部の Platform Services Controller アプライアンスに対する手順について説明します。

**注：** この証明書は 10 年間有効で、外部向けの証明書ではありません。会社のセキュリティ ポリシーで要求される場合を除き、この証明書を置き換えしないでください。

Platform Services Controller の Windows 環境を実行している場合は、[vCenter Server Windows 環境での新しい STS 署名証明書の生成](#)を参照してください。

### 手順

- 1 新しい証明書を保持するためのトップレベル ディレクトリを作成し、ディレクトリの場所を確認します。

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

- 2 新しいディレクトリに certtool.cfg ファイルをコピーします。

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

- 3 certtool.cfg ファイルのコピーを開き、ローカルの Platform Services Controller IP アドレスとホスト名を使用するように編集します。

国は必須で、次の例に示すように 2 文字で指定する必要があります。

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

# Country is needed and has to be 2 characters
Country = US
```

```
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

#### 4 キーを生成します。

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

#### 5 証明書を生成します

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

#### 6 証明書を PK12 形式に変換します。

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key
-certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout
pass:changeme -out newsts.pl2
```

#### 7 Java キーストア (JKS) に証明書を追加します。

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

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

#### 8 プロンプトが表示されたら、**Yes** と入力してキーストアへの証明書の追加を承諾します。

##### 次のステップ

これで、新しい証明書をインポートすることができます。[Security Token Service 証明書の更新](#)を参照してください。

## vCenter Server Windows 環境での新しい STS 署名証明書の生成

デフォルトの STS 署名証明書を置き換える場合は、最初に新しい証明書を生成し、Java キーストアに追加する必要があります。ここでは、Windows 環境での手順について説明します。

**注：** この証明書は 10 年間有効で、外部向けの証明書ではありません。会社のセキュリティ ポリシーで要求される場合を除き、この証明書を置き換えないでください。

仮想アプライアンスを使用している場合は、[アプライアンスでの新しい STS 署名証明書の生成](#)を参照してください。

## 手順

- 1 新しい証明書を保持するための新しいディレクトリを作成します。

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

- 2 certtool.cfg ファイルのコピーを作成し、新しいディレクトリに配置します。

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

- 3 certtool.cfg ファイルのコピーを開き、ローカルの Platform Services Controller IP アドレスとホスト名を使用するように編集します。

国は必須で、2 文字で指定する必要があります。以下に例を示します。

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

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

- 4 キーを生成します。

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

- 5 証明書を生成します

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

- 6 証明書を PK12 形式に変換します。

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

- 7 Java キーストア (JKS) に証明書を追加します。

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore
-srckeystore newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias
newstssigning -destkeystore root-trust.jks -deststoretype JKS -deststorepass testpassword
```

```
-destkeypass testpassword
"C:\Program Files\VMware\VMware Server\jre\bin\keytool.exe" -v -importcert -keystore root-trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword
-file ..\ssoserverRoot.crt -alias root-ca
```

### 次のステップ

これで、新しい証明書をインポートすることができます。[Security Token Service 証明書の更新](#)を参照してください。

## Security Token Service 証明書の更新

vCenter Single Sign-On サーバには、Security Token Service (STS) があります。Security Token Service は、セキュリティ トークンの発行、検証、更新を行う Web サービスです。既存の Security Token Service 証明書の有効期限が切れたり変更されると、vSphere Web Client から手動で更新することができます。

SAML トークンを取得するために、ユーザーはプライマリ認証情報を Secure Token Server (STS) に提供します。プライマリ認証情報は、ユーザーのタイプによって異なります。

### ソリューション ユーザー

有効な証明書

### その他のユーザー

vCenter Single Sign-On アイデンティティ ソースで利用できるユーザー名とパスワード

STS は、プライマリ認証情報を使用してユーザーを認証し、ユーザー属性が含まれている SAML トークンを構築します。STS サービスは、その STS 署名証明書を使用して SAML トークンを署名し、トークンをユーザーに割り当てます。デフォルトでは、STS 署名証明書は VMCA によって生成されます。

ユーザーが SAML トークンを取得したら、SAML トークンはそのユーザーの HTTP 要求の一部として送信されます。このとき、さまざまなプロキシを通過する場合があります。対象受信者（サービス プロバイダ）のみが SAML トークンの情報を使用できます。

会社のポリシーで求められている場合や、有効期限の切れた証明書を更新する場合、vSphere Web Client で既存の STS 署名証明書を置き換えることができます。

---

**注意：** ファイルシステムのファイルを置き換えないでください。置き換えた場合、予期せぬエラーが発生し、結果のデバッグは困難になります。

---

**注：** 証明書を置き換えた後に、vSphere Web Client サービスと STS サービスの両方を再起動するために、ノードを再起動する必要があります。

---

### 前提条件

Platform Services Controller から java キーストアに追加したばかりの証明書を、ローカル ワークステーションにコピーします。

### Platform Services Controller アプライアンス

`certificate_location/keys/root-trust.jks` 例: `/keys/root-trust.jks`



例：

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

## Windows インストール

```
certificate_location\root-trust.jks
```

例：

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

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。  
  
vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。
- 2 [証明書] タブを選択して、[STS 署名] サブタブを選択し、[STS 署名証明書の追加] アイコンをクリックします。
- 3 証明書を追加します。
  - a [参照] をクリックして、新しい証明書を含むキー ストア JKS ファイルを参照し、[開く] をクリックします。
  - b パスワードの入力が求められた場合は、入力します。
  - c STS エイリアス チェーンの最上部をクリックし、[OK] をクリックします。
  - d パスワードの入力が求められた場合は、再び入力します。
- 4 [OK] をクリックします。
- 5 Platform Services Controller ノードを再起動し、STS サービスと vSphere Web Client の両方を起動します。

再起動するまで認証は正しく機能しません。そのため、再起動は必須です。

## LDAPS SSL 証明書の有効期限日の判断

Active Directory LDAP Server および OpenLDAP Server アイデンティティ ソースを選択し、LDAPS の使用を決めた場合は、LDAP トラフィック用の SSL 証明書をアップロードできます。SSL 証明書は、事前定義された存続期間後に有効期限が切れます。証明書の有効期限を知ることで、有効期限の日付前に証明書を交換または更新することができます。

Active Directory LDAP Server および OpenLDAP Server を使用し、サーバに対して **ldaps://** URL を指定した場合に限り、証明書の有効期限情報を確認できます。他のタイプのアイデンティティ ソースまたは **ldap://** トラフィックの場合、[アイデンティティ ソースのトラストストア] タブには何も表示されません。

## 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [証明書] タブをクリックしてから、[アイデンティティ ソースのトラストストア] サブタブをクリックします。
- 4 証明書を検索し、[有効期間の終了] テキスト ボックスで有効期限の日付を確認してください。

タブの上部に、証明書の有効期限が間もなく切れることを示す警告が表示されることがあります。

## vCenter Single Sign-On ポリシーの管理

vCenter Single Sign-On ポリシーは、環境にセキュリティ ルールを適用します。デフォルトの vCenter Single Sign-On パスワード、ロックアウト ポリシー、およびトークン ポリシーを参照および編集できます。

### vCenter Single Sign-On のパスワード ポリシーの編集

vCenter Single Sign-On のパスワード ポリシーは、vCenter Single Sign-On ユーザー パスワードの形式と有効期限に関する一連のルールと制限です。パスワード ポリシーは vCenter Single Sign-On ドメイン (vsphere.local) 内のユーザーにのみ適用されます。

デフォルトでは、vCenter Single Sign-On パスワードは 90 日で有効期限が切れます。パスワードの有効期限が近づくと、vSphere Web Client が通知します。

## 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [ポリシー] タブをクリックし、[パスワード ポリシー] を選択します。
- 4 [[編集]] をクリックします。
- 5 パスワード ポリシーのパラメータを編集します。

オプション	説明
説明	パスワード ポリシーの説明。
最長有効期間	ユーザーによる変更が必要になるまでパスワードが存続できる最大日数。
再利用を制限	ユーザーが選択できない以前のパスワード数。たとえば、ユーザーが最後に使用した 6 つのパスワードをどれも再使用できない場合は、6 と入力します。
最大長	パスワードで使用できる最大文字数。

オプション	説明
最小長	パスワードに必要な最小文字数。最小長は、アルファベット、数字、および特殊文字の最小要件を組み合わせた文字数以上である必要があります。
文字要件	<p>パスワードに必要なさまざまな文字タイプの最小数。各タイプの文字の数は、次のように指定できます。</p> <ul style="list-style-type: none"> <li>■ 特殊： &amp; # %</li> <li>■ アルファベット： A b c D</li> <li>■ 大文字： A B C</li> <li>■ 小文字： a b c</li> <li>■ 数字： 1 2 3</li> </ul> <p>アルファベット文字の最小数は、大文字および小文字要件を組み合わせた数以上である必要があります。</p> <p>vSphere 6.0 以降では、ASCII 以外の文字はパスワードとしてはサポートされません。以前のバージョンの vCenter Single Sign-On には、サポートされる文字に制限があります。</p>
隣接した同一文字	パスワードで使用できる隣接した同一文字の最大数。ゼロより大きい値にする必要があります。たとえば 1 と入力すると、p@\$word というパスワードは許可されません。

6 [OK] をクリックします。

## vCenter Single Sign-On のロックアウト ポリシーの編集

vCenter Single Sign-On ロックアウト ポリシーは、ユーザーが不正な認証情報でログインを試みたときにユーザーの vCenter Single Sign-On アカウントがロックされる条件を指定します。ロックアウト ポリシーを編集できます。

ユーザーが vsphere.local に誤ったパスワードで何度もログインした場合、そのユーザーはロックアウトされます。ロックアウト ポリシーでは、失敗したログイン試行の最大回数と、最初の失敗からの経過時間を指定できます。このポリシーは、アカウントが自動的にロック解除されるまでの時間も指定できます。

**注：** ロックアウト ポリシーはユーザー アカウントにのみ適用され、administrator@vsphere.local などのシステム アカウントには適用されません。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [管理] - [Single Sign-On] - [構成] を参照します。
- 3 [ポリシー] タブをクリックし、[ロックアウト ポリシー] を選択します。
- 4 [Edit] をクリックします。

## 5 パラメータを編集します。

オプション	説明
説明	ロックアウト ポリシーの説明（オプション）。
ログイン試行失敗の最大回数	アカウントがロックアウトされるまでのログイン試行失敗が許可される最大回数。
失敗した試行の時間間隔	ロックアウトをトリガするための失敗したログイン試行間の時間。
ロック解除時間	アカウントがロックされ続けている時間。0 を入力すると、管理者は明示的にアカウントをロック解除しなければなりません。

## 6 [OK] をクリックします。

# vCenter Single Sign-On のトークン ポリシーの編集

vCenter Single Sign-On トークン ポリシーは、クロック許容値、更新回数、および他のトークン プロパティを指定します。vCenter Single Sign-On トークン ポリシーを編集して、トークンの仕様を企業のセキュリティ標準に確実に準拠させることができます。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [管理] - [Single Sign-On] を選択し、[構成] を選択します。
- 3 [ポリシー] タブをクリックして、[トークン ポリシー] を選択します。

vSphere Web Client に、現在の構成設定が表示されます。デフォルト設定を変更していない場合、vCenter Single Sign-On はその設定を使用します。

- 4 トークン ポリシー構成パラメータを編集します。

オプション	説明
クロック トレランス	vCenter Single Sign-On が許容するクライアント クロックとドメイン コントローラ クロック間のミリ秒単位の時差。時差が指定値を上回る場合、vCenter Single Sign-On により、トークンが無効であることが宣言されます。
トークンの最大更新数	トークンが更新できる最大回数です。更新の試行が最大回数を超えると、新しいセキュリティトークンが必要になります。
トークン最大委任数	キーホルダ トークンは、vSphere 環境のサービスに委任できます。委任されたトークンを使用するサービスは、トークンを提供したプリンシパルの代わりにサービスを実行します。トークン要求は、DelegateTo ID を指定します。DelegateTo 値は、ソリューション トークンまたはソリューション トークンへの参照にすることができます。この値では、1 つのキーホルダ トークンを委任できる回数を指定します。

オプション	説明
ベアラ トークンの最長有効期間	ベアラ トークンは、トークンの所有のみに基づいて認証を実行します。ベアラ トークンは、短期的な 1 回限りの操作の時に使用します。ベアラ トークンは、要求を送信しているユーザーまたはエンティティの ID 確認は行いません。この値では、ベアラ トークンを再発行するまでの有効期間の値を指定します。
キーホルダ トークンの最長有効期間	キーホルダ トークンは、トークンに組み込まれたセキュリティ製造物に基づいて認証を行います。キーホルダ トークンは委任用に使えます。クライアントはキーホルダ トークンを取得して、そのトークンを別のエンティティに委任できます。トークンには、委任元と委任先を識別するための請求権が含まれています。vSphere 環境で、vCenter Server システムはユーザーの代わりに委任済みトークンを取得し、これらのトークンを使用して処理を実行します。この値によって、キーホルダ トークンが無効とマークされるまでの有効期間が決まります。

5 [OK] をクリックします。

## vCenter Single Sign-On ユーザーおよびグループの管理

vCenter Single Sign-On 管理者ユーザーは、vSphere Web Client から vsphere.local ドメインのユーザーおよびグループを管理できます。

vCenter Single Sign-On 管理者ユーザーは、以下のタスクを実行できます。

- **vCenter Single Sign-On ユーザーの追加**

vSphere Web Client の [ユーザー] タブに表示されるユーザーは、vCenter Single Sign-On の内部ユーザーであり、vsphere.local ドメインに属します。

- **vCenter Single Sign-On ユーザーの無効化および有効化**

vCenter Single Sign-On ユーザー アカウントが無効になっている場合、管理者がそのアカウントを有効にするまでそのユーザーは vCenter Single Sign-On サーバにログインできません。ユーザーは、vSphere Web Client インターフェイスから無効または有効にすることができます。

- **vCenter Single Sign-On ユーザーの削除**

vsphere.local ドメインのユーザーは、vCenter Single Sign-On から削除できます。ローカル オペレーティング システム ユーザーや別のドメインのユーザーは、vSphere Web Client から削除することはできません。

- **vCenter Single Sign-On ユーザーの編集**

vSphere Web Client から vCenter Single Sign-On ユーザーのパスワードまたは他の詳細を変更できます。vsphere.local ドメインではユーザーの名前を変更できません。すなわち、administrator@vsphere.local の名前は変更できません。

- **vCenter Single Sign-On グループの追加**

vCenter Single Sign-On で、[グループ] タブにリストされたグループは vCenter Single Sign-On の内部のものです。グループでは、グループ メンバーの集合（プリンシパル）のためのコンテナを作成します。

- **vCenter Single Sign-On グループへのメンバーの追加**

vCenter Single Sign-On グループのメンバーは、1 つ以上のアイデンティティ ソースからのユーザーまたはその他のグループである場合があります。新しいメンバーは vSphere Web Client で追加できます。

#### ■ vCenter Single Sign-On グループからのメンバーの削除

vCenter Single Sign-On グループのメンバーは、vSphere Web Client から削除できます。ローカル グループからメンバー (ユーザーまたはグループ) を削除しても、システムからメンバーは削除されません。

#### ■ vCenter Single Sign-On ソリューション ユーザーの削除

vCenter Single Sign-On にソリューション ユーザーが表示されます。ソリューション ユーザーは、サービスのコレクションです。いくつかの vCenter Server ソリューション ユーザーは事前に定義されていて、インストールの一部として vCenter Single Sign-On の認証を受けることができます。トラブルシューティングが必要な場合 (クリーン アンインストールが完了しなかった場合など)、vSphere Web Client から個々のソリューション ユーザーを削除できます。

#### ■ vCenter Single Sign-On パスワードの変更

ローカル ドメイン (デフォルトで vsphere.local) のユーザーは、Web インターフェイスから vCenter Single Sign-On の自分のパスワードを変更することができます。他のドメインのユーザーはそのドメイン ルールに従ってパスワードを変更します。

## vCenter Single Sign-On ユーザーの追加

vSphere Web Client の [ユーザー] タブに表示されるユーザーは、vCenter Single Sign-On の内部ユーザーであり、vsphere.local ドメインに属します。

別のドメインを選択しそのドメインのユーザーに関する情報を表示できますが、vSphere Web Client の vCenter Single Sign-On 管理インターフェイスからユーザーを別のドメインに追加することはできません。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ]に移動します。

- 3 vsphere.local が現在選択されているドメインではない場合、ドロップダウン メニューから vsphere.local を選択します。

ユーザーを他のドメインに追加することはできません。

- 4 [ユーザー] タブで [新規ユーザー] アイコンをクリックします。

- 5 新規ユーザーのユーザー名とパスワードを入力します。

ユーザーの作成後、ユーザー名は変更できません。

このパスワードは、システムのパスワード ポリシー要件を満たしている必要があります。

- 6 (オプション) 新規ユーザーの姓名を入力します。

- 7 (オプション) ユーザーの E メール アドレスと説明を入力します。

- 8 [OK] をクリックします。

## 結果

ユーザーを追加する場合、そのユーザーには最初、管理操作を実行する権限がありません。

## 次のステップ

vsphere.local ドメインのグループ (VMCA を管理できるユーザーのグループ (CAAdmins) や、vCenter Single Sign-On を管理できるユーザーのグループ (Administrators) など) にユーザーを追加します。 [vCenter Single Sign-On グループへのメンバーの追加](#) を参照してください。

## vCenter Single Sign-On ユーザーの無効化および有効化

vCenter Single Sign-On ユーザー アカウントが無効になっている場合、管理者がそのアカウントを有効にするまでそのユーザーは vCenter Single Sign-On サーバにログインできません。ユーザーは、vSphere Web Client インターフェイスから無効または有効にすることができます。

無効化されたユーザー アカウントは引き続き vCenter Single Sign-On システムで使用可能ですが、そのユーザーはログインできず、サーバでの操作を実行できません。管理者権限を持つユーザーは、[vCenter ユーザーおよびグループ] ページからユーザーを無効および有効にすることができます。

## 前提条件

vCenter Single Sign-On ユーザーを無効化および有効化するには、vCenter Single Sign-On 管理者グループのメンバーである必要があります。

## 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。  
  
vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。
- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 ユーザーを選択し、[無効化] アイコンをクリックして、メッセージが表示されたら[はい]をクリックします。
- 4 ユーザーを再び有効にするには、ユーザーを右クリックし、[有効化]を選択して、メッセージが表示されたら[はい]をクリックします。

## vCenter Single Sign-On ユーザーの削除

vsphere.local ドメインのユーザーは、vCenter Single Sign-On から削除できます。ローカル オペレーティング システム ユーザーや別のドメインのユーザーは、vSphere Web Client から削除することはできません。

---

**注意：** vsphere.local ドメインの管理者ユーザーを削除すると、vCenter Single Sign-On にログインできなくなります。vCenter Server とそのコンポーネントを再インストールしてください。

---

**手順**

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [ユーザー] タブを選択して、vsphere.local ドメインを選択します。
- 4 削除するユーザーをユーザーのリストで選択して、[削除] アイコンをクリックします。

操作は慎重に行ってください。この操作を取り消すことはできません。

**vCenter Single Sign-On ユーザーの編集**

vSphere Web Client から vCenter Single Sign-On ユーザーのパスワードまたは他の詳細を変更できます。vsphere.local ドメインではユーザーの名前を変更できません。すなわち、administrator@vsphere.local の名前は変更できません。

administrator@vsphere.local と同じ権限を持つ別のユーザーを作成できます。

vCenter Single Sign-On ユーザーは vCenter Single Sign-On vsphere.local ドメイン内に保存されます。

vCenter Single Sign-On のパスワード ポリシーは、vSphere Web Client から確認できます。

administrator@vsphere.local としてログインし、[構成] - [ポリシー] - [パスワード ポリシー] を選択します。

**手順**

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [Users] タブをクリックします。
- 4 ユーザーを右クリックして [ユーザーの編集] を選択します。

- 5 ユーザーに変更を加えます。

ユーザー名は変更できません。

このパスワードは、システムのパスワード ポリシー要件を満たしている必要があります。

- 6 [OK] をクリックします。

**vCenter Single Sign-On グループの追加**

vCenter Single Sign-On で、[グループ] タブにリストされたグループは vCenter Single Sign-On の内部のもので、グループでは、グループ メンバーの集合（プリンシパル）のためのコンテナを作成します。



vSphere Web Client 管理インターフェイスから vCenter Single Sign-On グループを追加すると、グループは vsphere.local ドメインに追加されます。

#### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [グループ] タブを選択し、[新規グループ] アイコンをクリックします。
- 4 グループの名前と説明を入力します。

グループを作成した後で、グループ名を変更できません。

- 5 [OK] をクリックします。

#### 次のステップ

- メンバーをグループに追加します。

## vCenter Single Sign-On グループへのメンバーの追加

vCenter Single Sign-On グループのメンバーは、1 つ以上のアイデンティティ ソースからのユーザーまたはその他のグループである場合があります。新しいメンバーは vSphere Web Client で追加できます。

Microsoft Active Directory または OpenLDAP グループのメンバーを vCenter Single Sign-On グループに追加できます。外部アイデンティティ ソースのグループを vCenter Single Sign-On グループに追加することはできません。

vSphere Web Client の [グループ] タブに表示されるグループは、vsphere.local ドメインに属しています。[vsphere.local ドメイン内のグループ](#) を参照してください。

#### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [グループ] タブをクリックしてから、グループ (例: 管理者) をクリックします。
- 4 グループ メンバー領域で、[メンバーの追加] アイコンをクリックします。
- 5 グループに追加するメンバーを含むアイデンティティ ソースを選択します。
- 6 (オプション) 検索用語を入力し、[検索] をクリックします。

- 7 メンバーを選択し、[追加] をクリックします。

複数のメンバーを同時に追加できます。

- 8 [OK] をクリックします。

## vCenter Single Sign-On グループからのメンバーの削除

vCenter Single Sign-On グループのメンバーは、vSphere Web Client から削除できます。ローカル グループからメンバー (ユーザーまたはグループ) を削除しても、システムからメンバーは削除されません。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [グループ] タブを選択し、グループをクリックします。
- 4 グループ メンバーのリストで、削除するユーザーまたはグループを選択し、[メンバーを削除] アイコンをクリックします。
- 5 [OK] をクリックします。

### 結果

ユーザーはグループから削除されますが、その後もシステムで使用可能です。

## vCenter Single Sign-On ソリューション ユーザーの削除

vCenter Single Sign-On にソリューション ユーザーが表示されます。ソリューション ユーザーは、サービスのコレクションです。いくつかの vCenter Server ソリューション ユーザーは事前に定義されていて、インストールの一部として vCenter Single Sign-On の認証を受けることができます。トラブルシューティングが必要な場合 (クリーン アンインストールが完了しなかった場合など)、vSphere Web Client から個々のソリューション ユーザーを削除できます。

vCenter Server ソリューション ユーザーまたはサードパーティ製ソリューション ユーザーに関連付けられているサービスのセットを使用環境から削除すると、ソリューション ユーザーが vSphere Web Client の表示から削除されます。ソリューション ユーザーがまだシステム内にいるときにアプリケーションを強制的に削除した場合、またはシステムが回復不能になった場合は、ソリューション ユーザーを vSphere Web Client から明示的に削除できます。

---

**重要：** ソリューション ユーザーを削除すると、対応するサービスは vCenter Single Sign-On の認証を受けることができなくなります。

---

## 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On 管理者権限を持つ別のユーザーとして vSphere Web Client にログインします。

vCenter Single Sign-On 管理者権限を持つユーザーは vsphere.local ドメイン内の管理者グループに存在します。

- 2 [ホーム] をクリックして、[管理] - [Single Sign-On] - [ユーザーおよびグループ] に移動します。
- 3 [ソリューション ユーザー] タブをクリックして、ソリューション ユーザー名をクリックします。
- 4 [ソリューション ユーザーの削除] アイコンをクリックします。
- 5 [はい] をクリックします。

## 結果

ソリューション ユーザーに関連付けられているサービスは、vCenter Server にアクセスできず、vCenter Server サービスとして機能できなくなります。

## vCenter Single Sign-On パスワードの変更

ローカル ドメイン（デフォルトで vsphere.local）のユーザーは、Web インターフェイスから vCenter Single Sign-On の自分のパスワードを変更することができます。他のドメインのユーザーはそのドメイン ルールに従ってパスワードを変更します。

vCenter Single Sign-On ロックアウト ポリシーを使用して、パスワードの有効期限を指定します。デフォルトでは、vCenter Single Sign-On ユーザー パスワードは 90 日で有効期限が切れますが、administrator@vsphere.local などの管理者パスワードに有効期限はありません。パスワードの有効期限が近づくと、vCenter Single Sign-On 管理インターフェイスに警告が表示されます。

---

**注：** パスワードは有効期限内の場合にのみ変更できます。

---

パスワードの有効期限が切れた場合、ローカル ドメイン（デフォルトで administrator@vsphere.local）の管理者は `dir-cli password reset` コマンドを使用してパスワードをリセットすることができます。vCenter Single Sign-On ドメインの管理者グループのメンバーのみが、パスワードをリセットすることができます。

## 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 上部のナビゲーション ペインのヘルプ メニューの左側で、ユーザー名をクリックし、プルダウン メニューを表示します。

または、[Single Sign-On] - [ユーザーおよびグループ] の順に選択して、右ボタンのメニューから [ユーザーの編集] を選択できます。

- 4 [パスワードの変更] を選択し、現在のパスワードを入力します。

- 5 新しいパスワードを入力して確定します。

パスワードはパスワード ポリシーに従っている必要があります。

- 6 [OK] をクリックします。

## vCenter Single Sign-On のセキュリティのベスト プラクティス

vCenter Single Sign-On の次のセキュリティのベスト プラクティスに従って、vSphere 環境を保護します。

vSphere 6.0 の認証および証明書インフラストラクチャにより、vSphere 環境のセキュリティが強化されます。インフラストラクチャが危険にさらされないようにするには、vCenter Single Sign-On のベスト プラクティスに従います。

### パスワードの有効期限の確認

vCenter Single Sign-On のデフォルトのパスワード ポリシーの有効期限は 90 日です。90 日が経過すると、パスワードの有効期限が切れて、ログ機能が損なわれます。有効期限を確認して、適宜パスワードを更新してください。

### NTP の構成

すべてのシステムで同じ相対時間ソース（関連するローカライズ オフセットを含む）を使用し、決められた時間標準（協定世界時 (UTC) など）に相対時間ソースを関連付けられることを確認します。同期されたシステムは、vCenter Single Sign-On の証明書や vSphere のその他の証明書の有効性を確保するために不可欠です。

NTP により、ログ ファイルの攻撃者の追跡も容易になります。時間の設定が正しくないと、ログ ファイルの調査や関連付けを行って攻撃を検出することが難しくなり、監査が不正確になる可能性があります。

## vCenter Single Sign-On のトラブルシューティング

vCenter Single Sign-On の構成は複雑な処理になります。

次のトピックは、vCenter Single Sign-On をトラブルシューティングするための出発点となります。その他のアドバイスについては、このドキュメント センターおよび当社のナレッジ ベース システムを検索してください。

### Lookup Service エラーの原因の特定

vCenter Single Sign-On インストールには、vCenter Server または vSphere Web Client を参照するエラーが表示されます。

## 問題

vCenter Server および Web Client インストーラに次のエラーが表示されます。「Could not contact Lookup Service.Please check VM\_ssoreg.log...」

## 原因

この問題には、ホスト マシン上の非同期クロック、ファイアウォールのブロック、および起動していなければならないサービスなど、いくつかの原因があります。

## 解決方法

- 1 vCenter Single Sign-On、vCenter Server および Web Client を実行しているホスト マシンのクロックが同期していることを確認してください。
- 2 エラー メッセージに含まれる特定のログ ファイルを確認します。  
メッセージでは、システム一時フォルダが %TEMP% を参照します。
- 3 ログ ファイル内で、次のメッセージを検索します。

ログ ファイルには、すべてのインストールの試みからの出力が含まれます。「Initializing registration provider...」と表示されている最新のメッセージを探します。

メッセージ	原因と解決策
<b>java.net.ConnectException : 接続がタイムアウトしました : 接続</b>	<p>IP アドレスが正しくないか、ファイアウォールが vCenter Single Sign-On へのアクセスをブロックしているか、vCenter Single Sign-On に負荷がかかりすぎています。</p> <p>ファイアウォールが vCenter Single Sign-On ポート（デフォルトでは 7444）をブロックしていないこと、および vCenter Single Sign-On がインストールされているマシンに十分な空き CPU、I/O および RAM 容量があることを確認します。</p>
<b>java.net.ConnectException : 接続が拒否されました : 接続</b>	<p>IP アドレス または FQDN が不正であり、vCenter Single Sign-On サービスが起動していないか、経過分数以内に起動しませんでした。</p> <p>vCenter Single Sign-On サービスのステータス（Windows）および vmware-ssd デモン（Linux）をチェックして、vCenter Single Sign-On が動作していることを確認してください。</p> <p>サービスを再起動してください。これで問題が解決しない場合は、『vSphere トラブルシューティング ガイド』の復旧のセクションを参照してください。</p>

メッセージ	原因と解決策
予期しない状況コード：404。初期化中に SSO サーバに問題が発生しました	vCenter Single Sign-On を再起動してください。これで問題が解決しない場合は、『vSphere トラブルシューティング ガイド』の復旧のセクションを参照してください。
UI に表示されるエラーは、「Could not connect to vCenter Single Sign-on」から始まっています。	<p>戻りコード SslHandshakeFailed が表示される場合もあります。これは、まれなエラーです。これは、提供された IP アドレスまたは Center Single Sign-On ホストを解決する FQDN が、vCenter Single Sign-On のインストール時に使用されたものではないことを示しています。</p> <p>%TEMP%\VM_ssoreg.log で、次のメッセージを含む行を探します。</p> <pre>host name in certificate did not match: &lt;install-configured FQDN or IP&gt; != &lt;A&gt; or &lt;B&gt; or &lt;C&gt;</pre> <p>ここでは、A が vCenter Single Sign-On のインストール時に入力された FQDN であり、B および C がシステムによって生成された許容される代案となります。</p> <p>ログ ファイル中の != の記号の右側で、FQDN を使用するよう構成を修正します。ほとんどの場合、vCenter Single Sign-On のインストール時に指定した FQDN を使用してください。</p> <p>お使いのネットワーク構成でいずれの代案も使用できない場合は、vCenter Single Sign-On の SSL 構成を復旧してください。</p>

## Active Directory ドメイン認証を使用してログインできない

vSphere Web Client から vCenter Server コンポーネントにログインします。Active Directory のユーザー名とパスワードを使用します。認証に失敗します。

### 問題

Active Directory のアイデンティティ ソースを vCenter Single Sign-On に追加しましたが、ユーザーが vCenter Server にログインできません。

### 原因

ユーザーは、デフォルト ドメインにログインする場合、ユーザー名とパスワードを使用します。他のすべてのドメインについては、ユーザーはドメイン名（user@domain または DOMAIN\user）を追加する必要があります。

vCenter Server Appliance を使用している場合は、他の問題が存在する可能性があります。

### 解決方法

すべての vCenter Single Sign-On デプロイでは、デフォルトのアイデンティティ ソースを変更できます。変更後に、ユーザーは、ユーザー名とパスワードのみを使用してデフォルトのアイデンティティ ソースにログインできます。

Active Directory フォレスト内の子ドメインを使用して統合 Windows 認証アイデンティティ ソースを構成する方法については、当社のナレッジ ベースの記事 [2070433](#) を参照してください。統合 Windows 認証では、デフォルトで Active Directory フォレストのルート ドメインを使用します。

vCenter Server Appliance を使用しており、デフォルトのアイデンティティ ソースを変更しても問題が解決しない場合は、次のトラブルシューティング手順を追加で実行します。

- 1 vCenter Server Appliance と Active Directory ドメイン コントローラの時計を同期します。

- 2 それぞれのドメイン コントローラに Active Directory ドメイン DNS サービス内のポインタ レコード (PTR) があり、PTR レコード情報がコントローラの DNS 名と一致していることを確認します。vCenter Server Appliance を使用している場合は、次のコマンドを実行してタスクを実行できます。

- a ドメイン コントローラのリストを表示するには、次のコマンドを実行します。

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

次の例のように、関連するアドレスが ANSWER SECTION に表示されます。

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

- b ドメイン コントローラごとに、次のコマンドを実行して正引き/逆引き解決を確認します。

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

次の例のように、関連するアドレスが ANSWER SECTION に表示されます。

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

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

次の例のように、関連するアドレスが ANSWER SECTION に表示されます。

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

- 3 問題が解決しない場合は、vCenter Server Appliance を Active Directory ドメインから削除し、再度ドメインに参加させます。『vCenter Server Appliance の構成』ドキュメントを参照してください。
- 4 vCenter Server Appliance に接続されているすべてのブラウザ セッションを閉じ、すべてのサービスを再起動します。

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

## ユーザー アカウントがロックされているために vCenter Server ログインが失敗する

vSphere Web Client ログイン ページから vCenter Server にログインすると、アカウントがロックされていることを示すエラーが表示されます。

### 問題

何度か失敗すると、vCenter Single Sign-On を使用して vSphere Web Client にログインすることができなくなります。アカウントがロックされたことを示すメッセージが表示されます。

## 原因

ログイン失敗の最大数を超過しました。

## 解決方法

- ◆ システム ドメイン (vsphere.local) のユーザーとしてログインする場合、vCenter Single Sign-On 管理者に問い合わせアカウントのロックを解除してもらいます。パスワード ポリシーでロックが有効期限切れになるように設定されている場合は、アカウントのロックが解除されるまで待つこともできます。vCenter Single Sign-On 管理者は、CLI コマンドを使用してアカウントのロックを解除できます。
- ◆ Active Directory または LDAP ドメインのユーザーとしてログインする場合、Active Directory または LDAP 管理者に問い合わせアカウントのロックを解除してもらいます。

## VMware ディレクトリ サービスのレプリケーションに時間がかかることがある

環境内に複数の Platform Services Controller インスタンスが含まれていて、その Platform Services Controller インスタンスのいずれかが使用できなくなった場合、環境は引き続き機能し続けます。その Platform Services Controller が再び使用可能になると、ユーザー データおよびその他の情報は、通常、60 秒以内にレプリケートされます。しかし、特別な状況で、レプリケーションに時間がかかる場合があります。

## 問題

特定の状況、たとえば環境内の別々の場所に複数の Platform Services Controller インスタンスが含まれていて、1 つの Platform Services Controller が使用できないときに大幅な変更を加えると、VMware ディレクトリ サービス間のレプリケーションをすぐには確認できません。たとえば、使用可能な Platform Services Controller インスタンスに追加された新しいユーザーは、レプリケーションが完了するまでは、他のインスタンスでは確認できません。

## 原因

通常の動作では、ある Platform Services Controller インスタンス (ノード) 内の VMware ディレクトリ サービス (vmdir) への変更は、その直接のレプリケーション パートナーでは、約 60 秒以内に表示されます。レプリケーション トポロジによっては、あるノードでの変更は、各ノード内のそれぞれの vmdir インスタンスに到着する前に、中間ノードを経由した伝達が必要な場合があります。レプリケートされる情報には、VMware VMotion を使用して作成、クローン作成、または移行された仮想マシンのユーザー情報、証明書情報、ライセンス情報などがあります。

ネットワーク障害の発生やノードが利用できなくなったなどの理由で、レプリケーション リンクが壊れると、環境内の変更は収束しません。使用不可能なノードがリストアされた後、各ノードはすべての変更を取り込もうとします。その結果、すべての vmdir インスタンスが一定の状態に収束しますが、ノードの 1 つが使用できなかった間に多くの変更があった場合には、その一定の状態に到達するまでに時間がかかる可能性があります。

## 解決方法

レプリケーションの実行中、環境は通常通り機能します。この問題が 1 時間以上続くのでない限り、問題の解決を試みないでください。



# vSphere セキュリティ証明書

# 3

vSphere コンポーネントは、相互通信や ESXi との通信を安全に行うために、SSL を使用します。SSL 通信により、データの機密性と整合性が確保されます。データは保護されるため、通信時にデータが気づかれずに変更されることはありません。

証明書は、vCenter Single Sign-On への初期認証に vSphere Web Client などの vCenter Server サービスでも使用されます。vCenter Single Sign-On は、各コンポーネントが今後認証に使用する SAML トークンを使用してコンポーネントをプロビジョニングします。

vSphere 6.0 以降では、VMware 認証局 (VMCA) が、VMCA で署名された証明書をデフォルトで使用して、各 ESXi ホストと各 vCenter Server サービスをプロビジョニングします。

既存の証明書を新しい VMCA 署名付き証明書に置き換えたり、VMCA を従属 CA にしたり、すべての証明書をカスタム証明書に置き換えることもできます。オプションは次のとおりです。

表 3-1. 証明書を置き換えるための異なるアプローチ

オプション	詳細については、ドキュメントを参照してください。
Platform Services Controller Web インターフェイス (vSphere 6.0 Update 1 以降) を使用する。	<a href="#">Platform Services Controller Web インターフェイスを使用した証明書の管理</a>
コマンド ラインから vSphere Certificate Manager ユーティリティを使用する。	<a href="#">vSphere Certificate Manager ユーティリティによる証明書の管理</a>
CLI コマンドを使用して証明書を手動で置き換える。	<a href="#">CLI コマンドによる証明書とサービスの管理</a>



## vSphere 証明書管理

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

この章には、次のトピックが含まれています。

- 異なるソリューション パスの証明書の要件
- 証明書管理の概要
- Platform Services Controller Web インターフェイスを使用した証明書の管理
- vSphere Certificate Manager ユーティリティによる証明書の管理
- 証明書の手動での置き換え
- CLI コマンドによる証明書とサービスの管理

- [vSphere Web Client](#) での vCenter 証明書の表示
- [vCenter 証明書の有効期限の警告に対するしきい値の設定](#)

## 異なるソリューション パスの証明書の要件

証明書の要件は、VMware 認証局 (VMCA) を中間認証局 (CA) として使用するか、カスタム証明書を使用するかによって異なります。要件は、マシン証明書およびソリューション ユーザー証明書に対しても異なります。

開始する前に、環境内ですべてのノードの時刻が確実に同期されるようにします。

### すべてのインポートされた証明書の要件

- キー サイズ: 2,048 ビット以上 (PEM エンコード)
- PEM 形式。VMware では、PKCS8 および PKCS1 (RSA キー) がサポートされます。VECS に追加したキーは、PKCS8 に変換されます。
- x509 バージョン 3
- SubjectAltName には DNS Name=*machine\_FQDN* が含まれている必要があります。
- CRT 形式
- キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。
- クライアント認証とサーバ認証を拡張キー使用法に含めることはできません。

VMCA は、次の証明書をサポートしていません。

- ワイルドカードによる証明書
- 推奨されていないアルゴリズムは、md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4、および sha1WithRSAEncryption 1.2.840.113549.1.1.5 です。
- OID が 1.2.840.113549.1.1.10 のアルゴリズム RSASSA-PSS はサポートされていません。

## RFC 2253 に対する証明書のコンプライアンス

証明書は、RFC 2253 に準拠している必要があります。

CSR の生成に Certificate Manager を使用しない場合は、CSR に次のフィールドが確実に含まれるようにします。

文字列	X.500 属性のタイプ
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName

文字列	X.500 属性のタイプ
STREET	streetAddress
DC	domainComponent
UID	userid

CSR の生成に Certificate Manager を使用する場合は、次の情報を指定するように求められ、Certificate Manager によって CSR ファイルに対応するフィールドが追加されます。

- administrator@vsphere.local ユーザー、つまり接続している vCenter Single Sign-On ドメインの管理者のパスワード。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- Certificate Manager によって Certtool.cfg ファイルに保存される情報。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。
  - administrator@vsphere.local のパスワード。
  - 2 文字の国名コード
  - 会社名
  - 組織名
  - 組織単位
  - 状態
  - 地域
  - IP アドレス（オプション）
  - 電子メール
  - ホスト名、すなわち証明書を置き換えるマシンの完全修飾ドメイン名ホスト名が FQDN と一致しない場合、証明書の置き換えは正しく完了せず、環境が不安定な状態になる可能性があります。
  - Platform Services Controller の IP アドレス（コマンドを vCenter Server（管理）ノード上で実行している場合）

## VMCA を中間 CA として使用する場合の要件

VMCA を中間 CA として使用する場合、証明書は、次の要件を満たす必要があります。

証明書タイプ	証明書の要件
ルート証明書	<ul style="list-style-type: none"> <li>■ CSR は vSphere Certificate Manager を使用して作成できます。vSphere Certificate Manager で CSR を生成し、<a href="#">ルート証明書（中間認証局）を用意する</a>を参照してください。</li> <li>■ CSR を手動で作成する場合は、署名のために送付する証明書は以下の要件を満たしている必要があります。 <ul style="list-style-type: none"> <li>■ キー サイズ：2,048 ビット以上</li> <li>■ PEM 形式。VMware では、PKCS8 および PKCS1 (RSA キー) がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。</li> <li>■ x509 バージョン 3</li> <li>■ カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。</li> <li>■ CRL の署名は有効にしてください。</li> <li>■ 拡張キー用法には、クライアント認証またはサーバ認証を含めないでください。</li> <li>■ 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。</li> <li>■ ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。</li> <li>■ VMCA の従属認証局は作成できません。</li> </ul> </li> </ul> <p>Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事 2112009 の「vSphere 6.0 で SSL 証明書を作成するために Microsoft 認証局テンプレートを作成する」を参照してください。</p>
マシン SSL 証明書	<p>vSphere Certificate Manager を使用して CSR を作成するか、手動で CSR を作成することができます。</p> <p>CSR を手動で作成する場合、上記の「すべてのインポートされた証明書の要件」の下に記載されている要件を満たす必要があります。ホストの FQDN を指定する必要もあります。</p>
ソリューション ユーザー証明書	<p>vSphere Certificate Manager を使用して CSR を作成するか、手動で CSR を作成することができます。</p> <p><b>注：</b> 各ソリューション ユーザーの名前には異なる値を使用する必要があります。証明書を手動で生成する場合、使用するツールに応じて、[サブジェクト] の [CN] として表示される可能性があります。</p> <p>vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、certtool.cfg に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。</p>

## カスタム 証明書の要件

カスタム証明書を使用する場合、証明書は次の要件を満たす必要があります。

証明書タイプ	証明書の要件
マシン SSL 証明書	<p>各ノード上のマシン SSL 証明書には、サードパーティまたはエンタープライズ CA からの個別の証明書が必要です。</p> <ul style="list-style-type: none"> <li>■ vSphere Certificate Manager を使用して CSR を生成したり、手動で CSR を作成できます。CSR は、上記の「すべてのインポートされた証明書の要件」の下に記載されている要件を満たす必要があります。</li> <li>■ vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、<code>certtool.cfg</code> に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。</li> <li>■ ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。</li> </ul>
ソリューション ユーザー証明書	<p>各ノード上の各ソリューション ユーザーには、サードパーティまたはエンタープライズ CA からの個別の証明書が必要です。</p> <ul style="list-style-type: none"> <li>■ CSR は、vSphere Certificate Manager を使用して生成することも、CSR を自分で準備することもできます。CSR は、上記の「すべてのインポートされた証明書の要件」の下に記載されている要件を満たす必要があります。</li> <li>■ vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、<code>certtool.cfg</code> に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。</li> </ul> <p><b>注：</b> 各ソリューション ユーザーの名前には異なる値を使用する必要があります。証明書を手動で生成する場合、使用するツールに応じて、[サブジェクト] の [CN] として表示される可能性があります。</p> <p>後でソリューション ユーザー証明書をカスタム証明書と置き換える場合、サードパーティの CA の署名証明書チェーンすべてを指定します。</p>

**注：** カスタム証明書の CRL Distribution Point、Authority Information Access、または証明書テンプレートの情報を使用しないでください。

## 証明書管理の概要

新しい証明書インフラストラクチャの影響は、環境の要件、実行するのが新規インストールかアップグレードか、ESXi または vCenter Server を考慮しているかどうかによって異なります。

### 管理者が VMware 証明書を置き換えない場合

管理者が現時点で VMware 証明書を置き換えていない場合、VMCA ですべての証明書管理を扱うことができます。VMCA をルート認証局として使用する証明書を使って、vCenter Server コンポーネントおよび ESXi ホストを VMCA でプロビジョニングします。以前のバージョンの vSphere から vSphere 6 にアップグレードしている場合、自己署名証明書はすべて VMCA によって署名された証明書に置き換えられます。

## 管理者が VMware 証明書をカスタム証明書に置き換える場合

企業ポリシーで、サードパーティ認証局かエンタープライズ認証局によって署名された証明書、またはカスタム証明書の情報が求められる場合、新規インストールでは管理者に次の選択肢があります。

- VMCA ルート証明書を CA 署名付き証明書に置き換えます。このシナリオでは、VMCA 証明書がこのサードパーティ CA の中間証明書になります。完全な証明書チェーンを含む証明書を使用して、vCenter Server コンポーネントおよび ESXi ホストを VMCA でプロビジョニングします。
- 企業ポリシーで、チェーン内の中間証明書が許可されない場合は、証明書を明示的に置き換える必要があります。vSphere Certificate Manager ユーティリティを使用するか、証明書管理 CLI を使用して証明書を手動で置き換えることができます。

カスタム証明書を使用する環境をアップグレードする場合、一部の証明書を保持できます。

- ESXi ホストは、アップグレード中にカスタム証明書を保持します。vCenter Server アップグレード プロセスで、関連するすべてのルート証明書が、vCenter Server の VECS の TRUSTED\_ROOTS ストアに追加されたことを確認してください。

vCenter Server のアップグレード後に、管理者は、証明書モードを [カスタム] に設定できます（[証明書モードの変更](#)を参照）。証明書モードが VMCA（デフォルト）で、ユーザーが vSphere Web Client から証明書の更新を実行する場合、VMCA 署名付き証明書によってカスタム証明書が置き換えられます。

- vCenter Server コンポーネントでは、既存の環境によって処理が異なります。
  - シンプル インストールを組み込みデプロイにアップグレードする場合、vCenter Server のカスタム証明書は保持されます。アップグレード後の環境は、以前と同様に動作します。
  - vCenter Single Sign-On が他の vCenter Server コンポーネントとは別のマシン上にある複数サイトのデプロイをアップグレードする場合、アップグレード プロセスによって、1 つの Platform Services Controller ノードと 1 つ以上の管理ノードが含まれる、マルチノード デプロイが作成されます。

このシナリオで、既存の vCenter Server 証明書および vCenter Single Sign-On 証明書は保持され、マシン SSL 証明書として使用されます。VMCA 署名付き証明書が、VMCA によって各ソリューション ユーザー（vCenter サービスのコレクション）に割り当てられます。ソリューション ユーザーは、vCenter Single Sign-On への認証にのみ、この証明書を使用します。そのため、ソリューション ユーザー証明書の置き換えは不要な場合があります。

vSphere 5.5 のインストールで使用可能だった、vSphere 5.5 証明書置き換えツールは使用できなくなりました。これは、アーキテクチャが新しくなった結果、サービスの分布および配置が変わるためです。ほとんどの証明書管理タスクで、新しいコマンドライン ユーティリティ (vSphere Certificate Manager) を使用できます。

## vCenter 証明書インターフェイス

vCenter Server では、次のツールとインターフェイスを使用して、証明書の表示および置き換えを行えます。

### vSphere Certificate Manager ユーティリティ

証明書置き換えに関連するすべての一般的なタスクを、コマンドラインから実行します。

### 証明書管理 CLI

すべての証明書管理タスクを `dir-cli`、`certool`、および `vecs-cli` を使用して実行します。

## vSphere Web Client 証明書管理

証明書を表示します（有効期限情報を含む）。

ESXi では、vSphere Web Client から証明書管理を実行します。証明書は VMCA によってプロビジョニングされ、`vmdir` や `VECS` ではなく、ESXi ホストのローカルにのみ保存されます。[ESXi ホストの証明書管理](#) を参照してください。

## サポートされる vCenter 証明書

vCenter Server、Platform Services Controller、および関連するマシンとサービスでは、次の証明書がサポートされます。

- VMware 認証局 (VMCA) によって生成され、署名された証明書。
- カスタム証明書。
  - 独自の内部 PKI から生成されるエンタープライズ証明書。
  - Verisign や GoDaddy などの外部 PKI で生成された、サードパーティ CA 署名付き証明書。

ルート CA が存在しない OpenSSL を使用して作成された、自己署名証明書はサポートされません。

## 証明書の置き換えの概要

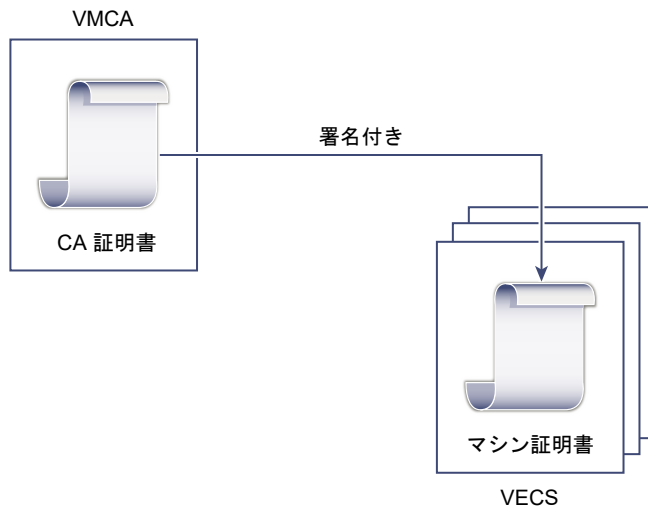
企業ポリシーおよび構成するシステムの要件に応じて、異なるタイプの証明書の置き換えを実行できます。置き換え作業はそれぞれ、vSphere Certificate Manager ユーティリティを使用して行うか、インストール製品に組み込まれている CLI を使用して手動で実行できます。

デフォルトの証明書は、置き換えることができます。vCenter Server のコンポーネントの場合は、インストール製品に組み込まれているコマンドライン ツールのセットを使用できます。いくつかのオプションが用意されています。

## VMCA によって署名された証明書との置き換え

VMCA 証明書の有効期限が切れたか、またはその他の理由でその証明書を置き換える場合は、証明書管理 CLI を使用してその処理を実行することができます。デフォルトでは、VMCA ルート証明書が 10 年後に期限切れになり、VMCA が署名するすべての証明書はルート証明書の有効期限が切れると期限切れになります。つまり、最大で 10 年です。

図 3-1. VMCA によって署名された証明書の VECS への保存

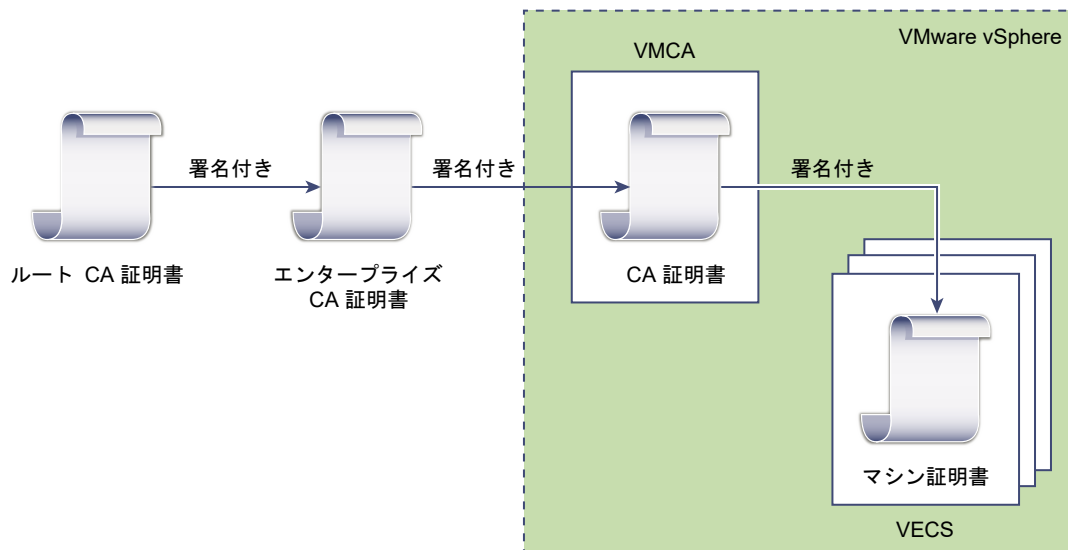


### VMCA を中間 CA にする

VMCA のルート証明書は、企業 CA やサードパーティ CA によって署名された証明書と置き換えることができます。VMCA は、証明書をプロビジョニングするごとにカスタム ルート証明書に署名し、VMCA を中間 CA にします。

**注：** 外部の Platform Services Controller を含めてフレッシュ インストールを実行する場合は、最初に Platform Services Controller をインストールして VMCA ルート証明書を置き換えます。次に、他のサービスをインストールし、使用環境に ESXi ホストを追加します。組み込み Platform Services Controller を含めてフレッシュ インストールを実行する場合は、VMCA ルート証明書を置き換えてから、ESXi ホストを追加します。そうすると、すべての証明書がチェーン全体によって署名され、新しい証明書を生成する必要がなくなります。

図 3-2. サードパーティまたは企業 CA によって署名された証明書で中間 CA として VMCA を使用する

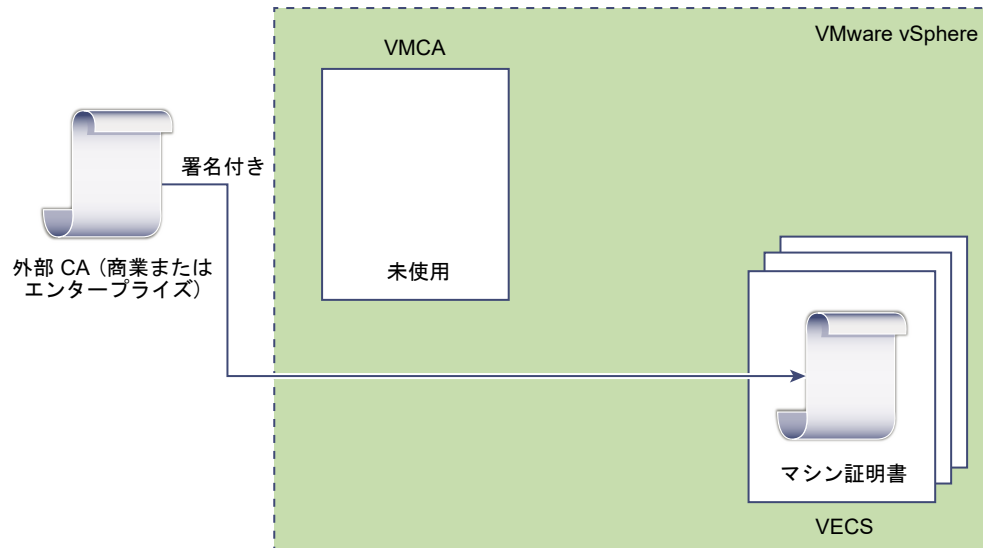




## VMCA を使用しない、カスタム証明書によるプロビジョニング

既存の VMCA 署名付き証明書は、カスタム証明書と置き換えることができます。この方法を使用する場合は、証明書のプロビジョニングと監視のすべてについて自分で責任を負ってください。

図 3-3. 外部証明書が VECS に直接保存される



## ハイブリッド デプロイ

VMCA によって証明書の一部を供給し、インフラストラクチャのその他の部分ではカスタム証明書を使用することができます。たとえば、ソリューション ユーザーの証明書は vCenter Single Sign-On への認証でのみ使用されるため、VMCA でそれらの証明書をプロビジョニングすることを検討してください。マシンの SSL 証明書をカスタム証明書と置き換え、すべての SSL トラフィックを保護します。

## ESXi 証明書の置き換え

ESXi ホストの場合は、vSphere Web Client から証明書のプロビジョニング処理を変更することができます。

### VMware 認証局モード (デフォルト)

vSphere Web Client からの証明書を更新する場合、VMCA はホストの証明書を発行します。VMCA ルート証明書を変更して証明書チェーンを含めるようにする場合、ホストの証明書には全チェーンが含まれます。

### カスタム認証局モード

VMCA による署名がないか、または発行されていない証明書を、手動で更新して証明書を使用することができます。

### サムプリント モード

更新中に 5.5 証明書を維持するために使用できます。このモードは、デバッグ状況のときに一時的にのみ使用してください。

## vSphere 6.0 で証明書が使用される場合

vSphere 6.0 以降では、VMware 認証局 (VMCA) が証明書を使用して環境のプロビジョニングを行います。これには、安全な接続用のマシン SSL 証明書、vCenter Single Sign-On への認証用のソリューション ユーザー証明書、vCenter Server に追加された ESXi ホスト用の証明書が含まれます。

次の証明書が使用されます。

表 3-2. vSphere 6.0 内の証明書

証明書	プロビジョニングの実施	保存場所
ESXi 証明書	VMCA (デフォルト)	ESXi ホストのローカル
マシン SSL 証明書	VMCA (デフォルト)	VECS
ソリューション ユーザー証明書	VMCA (デフォルト)	VECS
vCenter Single Sign-On SSL 署名証明書	インストール中にプロビジョニングされます。	この証明書は、vSphere Web Client から管理します。 <b>注意:</b> 予期しない動作が発生することを避けるため、ファイルシステム内でこの証明書を変更しないでください。
VMware ディレクトリ サービス (vmdir) SSL 証明書	インストール中にプロビジョニングされます。	特定のケースで、この証明書の置き換えが必要になる場合があります。 <a href="#">VMware ディレクトリ サービス証明書の置き換え</a> を参照してください。

## ESXi

ESXi 証明書は、各ホストの `/etc/vmware/ssl` ディレクトリでローカルに保存されます。ESXi 証明書は、デフォルトでは VMCA によってプロビジョニングされますが、代わりにカスタム証明書を使うこともできます。ESXi 証明書は、ホストが最初に vCenter Server に追加されたときと、ホストが再接続されたときにプロビジョニングされます。

## マシン SSL 証明書

各ノードのマシン SSL 証明書は、SSL クライアントの接続先となる、サーバ側の SSL ソケットの作成に使用されます。この証明書は、サーバの検証と、HTTPS や LDAPS などの安全な通信のために使われます。

すべてのサービスが、リバース プロキシを介して通信します。互換性を保つため、以前のバージョンの vSphere で使用されていたサービスでも、特定のポートが使用されます。たとえば、vpxd サービスは、エンドポイントを公開するために MACHINE\_SSL\_CERT を使います。

すべてのノード（組み込みデプロイ、管理ノード、または Platform Services Controller）に、独自のマシン SSL 証明書があります。そのノードで実行中のすべてのサービスが、このマシン SSL 証明書を使用して SSL エンドポイントを公開します。

マシン SSL 証明書がどのように使われるかを次に示します。

- 各 Platform Services Controller ノードのリバース プロキシ サービスによって使用されます。個々の vCenter サービスへの SSL 接続では、常にリバース プロキシに接続します。サービス自体にトラフィックが送られることはありません。
- 管理ノードと組み込みノード上の vCenter サービス (vpxd) によって使用されます。

- インフラストラクチャ ノードと組み込みノード上の VMware ディレクトリ サービス (vmdir) によって使用されます。

VMware 製品では、コンポーネント間で SSL を介して送られるセッション情報を、標準の X.509 バージョン 3 (X.509v3) 証明書を使用して暗号化します。

## ソリューション ユーザー証明書

ソリューション ユーザーは 1 つ以上の vCenter Server サービスをカプセル化し、証明書を使用して、SAML トークンの交換による vCenter Single Sign-On への認証を行います。各ソリューション ユーザーは、vCenter Single Sign-On への認証が必要です。

ソリューション ユーザー証明書は、vCenter Single Sign-On への認証に使用されます。ソリューション ユーザーは、最初に認証が必要になった時、再起動の後、およびタイムアウト時間の経過後に、vCenter Single Sign-On に証明書を提供します。タイムアウト（キーホルダ タイムアウト）は、vSphere Web Client から設定することができ、デフォルト値は 2,592,000 秒（30 日）です。

たとえば、vpxd ソリューション ユーザーは、vCenter Single Sign-On に接続するときに、vCenter Single Sign-On に証明書を提示します。vpxd ソリューション ユーザーは、vCenter Single Sign-On から SAML トークンを受け取り、そのトークンを使用して他のソリューション ユーザーやサービスへの認証を行います。

次のソリューション ユーザー証明書ストアが、各管理ノードと各組み込みデブロイの VECS に含まれています。

- `machine` : Component Manager、ライセンス サーバ、およびログ サービスにより使用されます。

---

**注：** マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は SAML トークン交換に使用される一方、マシン SSL 証明書はマシン向けのセキュリティで保護された SSL 接続に使用されます。

---

- `vpxd` : 管理ノードおよび組み込みデブロイ上の、vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに格納されているソリューション ユーザー証明書を使用して、vCenter Single Sign-On への認証を行います。
- `vpxd-extensions` : vCenter の拡張機能のストア。Auto Deploy サービス、Inventory Service、およびその他のソリューション ユーザーに含まれないその他のサービス。
- `vsphere-webclient` : vSphere Web Client ストア。パフォーマンス チャート サービスなどの一部の追加サービスも含まれます。

マシン ストアは、各 Platform Services Controller ノードにも含まれています。

## vCenter Single Sign-On 証明書

vCenter Single Sign-On 証明書は、VECS に保存されず、証明書管理ツールで管理しません。原則として変更は必要ありませんが、特別な状況ではこれらの証明書を置き換えることができます。

### vCenter Single Sign-On 署名証明書

vCenter Single Sign-On サービスには、vSphere 全体を通じて認証に使用される SAML トークンを発行する ID プロバイダ サービスが含まれます。SAML トークンは、ユーザーの ID を表すほか、グループ メンバーシップ情報を格納します。vCenter Single Sign-On が SAML トークンを発行すると、SAML トークンが信頼できるソースから取得されたことを vCenter Single Sign-On のクライアントが確認できるように、各トークンは署名証明書によって署名されます。

vCenter Single Sign-On は、ソリューション ユーザーにキーホルダ SAML トークンを発行し、ベアラ トークンをその他のユーザーに発行します。このユーザーは、ユーザー名とパスワードを使用してログインします。

この証明書は vSphere Web Client で置き換えることができます。[Security Token Service 証明書の更新](#)を参照してください。

## VMware ディレクトリ サービス SSL 証明書

カスタム証明書を使用している場合は、VMware ディレクトリ サービス SSL 証明書の明示的な置き換えが必要になることがあります。[VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

## VMCA および VMware コア ID サービス

コア ID サービスは、すべての組み込みデプロイおよびすべてのプラットフォーム サービス ノードに含まれています。VMCA は、すべての VMware コア ID サービス グループに含まれています。管理 CLI と vSphere Web Client を使用して、これらのサービスと連携します。

VMware コア ID サービスには、いくつかのコンポーネントがあります。

表 3-3. コア ID サービス

サービス	説明	サービスが含まれる場所
VMware ディレクトリ サービス (vmdir)	vCenter Single Sign-On と関連した認証の SAML 証明書管理を扱います。	Platform Services Controller 組み込みデプロイ
VMware 認証局 (VMCA)	VMware ソリューション ユーザーの証明書、サービスが実行されているマシンのマシン証明書、および ESXi ホスト証明書を発行します。VMCA は、そのまま使うことも、中間 CA として使うこともできます。  VMCA は、同じドメイン内の vCenter Single Sign-On への認証を行えるクライアントにのみ証明書を発行します。	Platform Services Controller 組み込みデプロイ
VMware 認証フレームワーク デモン (VMAFD)	VMware Endpoint 証明書ストア (VECS) やその他いくつかの認証サービスが含まれます。VECS は VMware 管理者が操作し、その他のサービスは内部的に使用されます。	Platform Services Controller vCenter Server 組み込みデプロイ

## VMware Endpoint 証明書ストアの概要

VMware Endpoint 証明書ストア (VECS) は、キーストアに保存できる証明書とプライベート キーなどの証明書情報のローカル (クライアント側) リポジトリとして機能します。VMCA を認証局および証明書署名者として使用しないようにすることもできますが、vCenter のすべての証明書、キーなどの保存には VECS を使用する必要があります。ESXi 証明書は、VECS 内ではなく各ホスト上にローカルに保存されます。

VECS は、VMware 認証フレームワーク デモン (VMAFD) の一部として実行されます。VECS は、組み込みデプロイ、Platform Services Controller ノード、および管理ノードのそれぞれで実行されます。VECS には、証明書とキーが含まれるキーストアが保持されます。

VECS は、更新のため定期的に VMware ディレクトリ サービス (vmdir) を TRUSTED\_ROOTS ストアにポーリングします。VECS 内の証明書とキーは、`vecs-cli` コマンドを使用して明示的に管理することもできます。[vecs-cli コマンド リファレンス](#) を参照してください。

VECS には、次のストアが含まれます。

表 3-4. VECS 内のストア

ストア	説明
マシン SSL ストア (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> <li>■ 各 vSphere ノード上のリバースプロキシ サービスにより使用されます。</li> <li>■ 組み込みデプロイおよび各 Platform Services Controller ノード上の VMware ディレクトリ サービス (vmdir) によって使用されます。</li> </ul> <p>vSphere 6.0 のすべてのサービスは、リバース プロキシを介して通信を行っており、ここで、マシン SSL 証明書が使用されます。下位互換性を保つため、5.x サービスでは特定のポートが引き続き使用されています。その結果、vpxd などの一部のサービスでは、自身のポートが開かれたままになっています。</p>
信頼されたルート ストア (TRUSTED_ROOTS)	すべての信頼済みルート証明書を含みます。
ソリューション ユーザー ストア <ul style="list-style-type: none"> <li>■ マシン</li> <li>■ vpxd</li> <li>■ vpxd-extensions</li> <li>■ vsphere-webclient</li> </ul>	<p>VECS には、ソリューション ユーザーごとに 1 つのストアが含まれます。各ソリューション ユーザー証明書の件名は一意でなければなりません。たとえば、マシン証明書には vpxd 証明書と同じ件名を指定できません。</p> <p>ソリューション ユーザー証明書は、vCenter Single Sign-On での認証に使用されます。vCenter Single Sign-On は、証明書が有効であることを確認しますが、その他の証明書の属性は確認しません。組み込みのデプロイでは、すべてのソリューション ユーザー証明書が同じシステム上に存在します。</p> <p>次のソリューション ユーザー証明書ストアが、各管理ノードと各組み込みデプロイの VECS に含まれています。</p> <ul style="list-style-type: none"> <li>■ <code>machine</code> : Component Manager、ライセンス サーバ、およびログ サービスにより使用されます。</li> </ul> <p><b>注：</b> マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は SAML トークン交換に使用される一方、マシン SSL 証明書はマシン向けのセキュリティで保護された SSL 接続に使用されます。</p> <ul style="list-style-type: none"> <li>■ <code>vpxd</code> : 管理ノードおよび組み込みデプロイ上の、vCenter サービス デモン (vpxd) ストア。vpxd は、このストアに格納されているソリューション ユーザー証明書を使用して、vCenter Single Sign-On への認証を行います。</li> <li>■ <code>vpxd-extensions</code> : vCenter の拡張機能のストア。Auto Deploy サービス、Inventory Service、およびその他のソリューション ユーザーに含まれないその他のサービス。</li> <li>■ <code>vsphere-webclient</code> : vSphere Web Client ストア。パフォーマンス チャート サービスなどの一部の追加サービスも含まれます。</li> </ul> <p>マシン ストアは、各 Platform Services Controller ノードにも含まれています。</p>

表 3-4. VECS 内のストア（続き）

ストア	説明
vSphere Certificate Manager ユーティリティのバックアップ ストア (BACKUP_STORE)	証明書の取り消しをサポートするために、VMCA (VMware Certificate Manager) によって使用されます。最新の状態のみがバックアップとして保存され、1 段階より多く戻ることはできません。
その他のストア	<p>その他のストアが、ソリューションによって追加される場合があります。たとえば、仮想ボリューム ソリューションにより SMS ストアが追加されます。VMware ドキュメントまたは当社のナレッジ ベースで指示されないかぎり、ストア内の証明書を変更しないでください。</p> <p><b>注：</b> vSphere 6.0 では CRLS はサポートされませんが、TRUSTED_ROOTS_CRLS ストアを削除すると、証明書インフラストラクチャが破損する可能性があります。TRUSTED_ROOTS_CRLS ストアの削除や修正は行わないでください。</p>

vCenter Single Sign-On サービスは、トークン署名証明書とその SSL 証明書をディスク上に保存します。トークン署名証明書は、vSphere Web Client から変更できます。

**注：** VMware のドキュメントやナレッジ ベース記事で指示されていない限り、ディスク上の証明書ファイルはいずれも変更しないでください。変更すると予期しない動作が生じる可能性があります。

証明書の中には、起動時に一時的にまたは永続的にファイル システム上に保存されるものがあります。ファイル システム上の証明書は変更しないでください。VECS に保存されている証明書に対する操作を行うには `vecs-cli` を使用します。

## 証明書の失効の管理

証明書のいずれかに侵害された疑いがある場合は、VMCA ルート証明書を含む、既存の証明書すべてを置き換えます。

vSphere 6.0 は、ESXi ホストまたは vCenter Server システムに対する証明書の置き換えをサポートしますが、証明書の失効は実施しません。

失効した証明書をすべてのノードから削除します。失効した証明書を削除しないと、中間者攻撃により、アカウントの認証情報を使用したなりすましが発生し、セキュリティが侵害される可能性があります。

## 大規模なデプロイでの証明書の置き換え

複数の管理ノードと 1 つ以上の Platform Services Controller ノードが含まれるデプロイでの証明書の置き換えは、組み込みデプロイでの置き換えに似ています。どちらの場合でも、vSphere 証明書管理ユーティリティを使用するか、証明書を手動で置き換えることができます。置き換えプロセスに役立つ、いくつかのベスト プラクティスを示します。

## ロード バランサーが含まれる高可用性環境での証明書の置き換え

vCenter Server システムが 7 つ以下の環境では、通常、単一の Platform Services Controller インスタンスと関連する vCenter Single Sign-On サービスを推奨しています。より大規模な環境では、ネットワーク ロード バランサーにより保護された、複数の Platform Services Controller インスタンスの使用を検討してください。この設定については、VMware Web サイトのホワイト ペーパー『vCenter Server 6.0 のデプロイ ガイド』で説明されています。

## 複数の管理ノードが含まれる環境でのマシン SSL 証明書の置き換え

複数の管理ノードと単一の Platform Services Controller が含まれる環境では、vSphere Certificate Manager ユーティリティを使用して証明書を置き換えるか、vSphere CLI コマンドを使用して証明書を手動で置き換えることができます。

### vSphere Certificate Manager

vSphere Certificate Manager を各マシンで実行します。管理ノードで Platform Services Controller の IP アドレスを指定するように求められます。実行するタスクによっては、証明書情報も求められます。

#### 証明書の手動での置き換え

証明書を手動で置き換える場合、各マシンで証明書置き換えコマンドを実行します。管理ノードで Platform Services Controller に `--server` パラメータを指定する必要があります。詳細については、次のトピックを参照してください。

- [VMCA 署名付き証明書によるマシン SSL 証明書の置き換え](#)
- [マシン SSL 証明書の置き換え（中間 CA）](#)
- [カスタム証明書によるマシン SSL 証明書の置き換え](#)

## 複数の管理ノードが含まれる環境でのソリューション ユーザー証明書の置き換え

複数の管理ノードと単一の Platform Services Controller が含まれる環境では、次の手順に従って証明書を置き換えます。

---

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、`dir-cli list` の出力にすべてのノードのソリューション ユーザーが含まれます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

---

### vSphere Certificate Manager

vSphere Certificate Manager を各マシンで実行します。管理ノードで Platform Services Controller の IP アドレスを指定するように求められます。実行するタスクによっては、証明書情報も求められます。

#### 証明書の手動での置き換え

- 1 証明書を生成するか、要求します。次の証明書が必要です。
  - Platform Services Controller のマシン ソリューション ユーザーの証明書。
  - 各管理ノードのマシン ソリューション ユーザーの証明書。



- 各管理ノードの、次のソリューション ユーザーそれぞれの証明書。
  - vpxd ソリューション ユーザー
  - vpxd-extension ソリューション ユーザー
  - vsphere-webclient ソリューション ユーザー
- 2 各ノードの証明書を置き換えます。正確なプロセスは、実行している証明書置き換えのタイプに応じて異なります。を参照してください。[vSphere Certificate Manager ユーティリティによる証明書の管理](#)

詳細については、次のトピックを参照してください。

- [新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え](#)
- [ソリューション ユーザー証明書の置き換え（中間 CA）](#)
- [カスタム証明書によるソリューション ユーザー証明書の置き換え](#)

企業ポリシーによって、すべての証明書の置き換えが求められる場合は、Platform Services Controller の VMware ディレクトリ サービス (vmdir) の証明書も置き換える必要があります。[VMware ディレクトリ サービス証明書の置き換え](#) を参照してください。

## 外部ソリューションが含まれる環境での証明書の置き換え

一部のソリューション（VMware vCenter Site Recovery Manager や VMware vSphere Replication など）は、常に vCenter Server システムでも Platform Services Controller でもない別のマシンにインストールされます。vCenter Server システムまたは Platform Services Controller 上のデフォルトのマシン SSL 証明書を置き換えると、そのソリューションによって vCenter Server システムへの接続が試みられると、接続エラーが発生します。

この問題は、ls\_update\_certs スクリプトを実行して解決できます。詳細については、[当社のナレッジ ベースの記事 2109074](#) を参照してください。

## Platform Services Controller Web インターフェイスを使用した証明書の管理

Platform Services Controller Web インターフェイスにログインすることで、証明書を表示および管理できます。vSphere Certificate Manager ユーティリティまたはこの Web インターフェイスを使用することで、多数の証明書管理タスクを実行できます。

Platform Services Controller Web インターフェイスを使用すると、次の管理タスクを実行できます。

- 現在の証明書ストアの表示、証明書ストア エントリの追加と削除。
- この Platform Services Controller に関連付けられた VMware Certificate Authority (VMCA) インスタンスの表示。
- VMware Certificate Authority によって生成された証明書の表示。
- 既存の証明書の更新または証明書の置き換え。

証明書の置き換えワークフローの大部分は、Platform Services Controller Web インターフェイスで完全にサポートされています。CSR を生成する場合は、vSphere Certificate Manager ユーティリティを使用できます。



## サポートされているワークフロー

Platform Services Controller のインストール後、このノード上の VMware Certificate Authority は、デフォルトの証明書を使用して環境内の他のすべてのノードをプロビジョニングします。次のワークフローのいずれかを使用して、証明書を更新または置き換えることができます。

### 証明書の更新

VMCA で新しいルート証明書を生成し、Platform Services Controller Web インターフェイスから環境内のすべての証明書を更新できます。

### VMCA を中間 CA にする

vSphere Certificate Manager ユーティリティを使用して CSR を生成し、CSR から受信する証明書を編集して VMCA をチェーンに追加したら、環境に証明書チェーンとプライベート キーを追加できます。すべての証明書を更新すると、VMCA は、完全なチェーンによって署名された証明書を使用して、すべてのマシンとソリューション ユーザーをプロビジョニングします。

### カスタム証明書による証明書の置き換え

VMCA を使用しない場合は、置き換える証明書の CSR を生成できます。認証局は、各 CSR にルート証明書および署名付き証明書を戻します。Platform Services Controller からルート証明書およびカスタム証明書をアップロードできます。

VMware Directory Service (vmdir) ルート証明書を置き換える必要がある場合、または混在モード環境で vCenter Single Sign-On 証明書を置き換えることが企業ポリシーで規定されている場合は、他の証明書を置き換えた後に、CLI コマンドを使用してそれらの証明書を置き換えることができます。[VMware ディレクトリ サービス証明書の置き換えおよび混合モード環境での VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

## Platform Services Controller Web インターフェイスからの証明書ストアの探索

VMware エンドポイント証明書ストア (VECS) のインスタンスは、各 Platform Services Controller ノードおよび各 vCenter Server ノードに含まれます。Platform Services Controller Web インターフェイスから VMware エンドポイント証明書ストア内のさまざまなストアを探索できます。

VECS 内のさまざまなストアの詳細については、[VMware Endpoint 証明書ストアの概要](#)を参照してください。

### 前提条件

管理タスクを実行するには、多くの場合、ローカル ドメイン アカウント administrator@vsphere.local、またはインストール中にドメインを変更した場合は異なるドメインの管理者のパスワードが必要です。

### 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 [証明書] の下の [証明書ストア] をクリックして、ストアを探索します。
- 4 ブルダウン メニューから探索対象の VMware エンドポイント証明書ストア (VECS) 内のストアを選択します。

個々のストアの内容については、[VMware Endpoint 証明書ストアの概要](#)を参照してください。

- 5 証明書の詳細を表示するには、証明書を選択し、[エントリの削除] アイコンをクリックします。
  - 6 選択したストアからエントリを削除するには、[エントリの削除] アイコンをクリックします。
- たとえば、既存の証明書を置き換える場合は、古いルート証明書を後で削除できます。その証明書がすでに使用されていないことが確認できた場合にのみ、証明書を削除してください。

## Platform Services Controller Web インターフェイスからの新しい VMCA 署名付き証明書への証明書の置き換え

すべての VMCA 署名付き証明書を新しい VMCA 署名付き証明書に置き換えることができます。この操作は証明書の更新と呼ばれます。Platform Services Controller Web インターフェイスから、選択した証明書または環境内のすべての証明書を更新できます。

### 前提条件

証明書を管理する場合、ローカル ドメイン（デフォルトでは administrator@vsphere.local）の管理者のパスワードを入力する必要があります。vCenter Server システムの証明書を更新する場合、vCenter Server システムの管理者権限のあるユーザーの vCenter Single Sign-On 認証情報も入力する必要があります。

### 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**https://psc\_hostname\_or\_IP/psc**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。
- インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。
- 3 [証明書] で、[証明書の管理] を選択し、Platform Services Controller の IP アドレスまたはホスト名と、ローカル ドメインの管理者（デフォルトでは administrator@vsphere.local）のユーザー名とパスワードを指定し、[送信] をクリックします。
  - 4 ローカル システムのマシン SSL 証明書を更新します。
    - a [マシン証明書] タブをクリックします。
    - b 証明書を選択し、[更新] をクリックして [はい] と応答します。

- 5 (オプション) ローカル システムのソリューション ユーザー証明書を更新します。
  - a [ソリューション ユーザー証明書] タブをクリックします。
  - b 証明書を選択し、[更新] をクリックして個別に選択した証明書を更新するか、[すべてを更新] をクリックしてすべてのソリューション ユーザー証明書を更新します。
  - c プロンプトで [はい] と応答します。
- 6 環境に外部 Platform Services Controller が含まれている場合は、その後に各 vCenter Server システムの証明書を更新できます。
  - a [証明書の管理] パネルで [ログアウト] ボタンをクリックします。
  - b プロンプトが表示されたら、vCenter Server システムの IP アドレスまたは FQDN と、vCenter Single Sign-On に対する認証が可能な vCenter Server 管理者のユーザー名とパスワードを指定します。
  - c vCenter Server でマシン SSL 証明書を更新し、オプションで各ソリューション ユーザー証明書を更新します。
  - d 環境内に複数の vCenter Server システムがある場合は、システムごとにこのプロセスを繰り返します。

#### 次のステップ

Platform Services Controller のサービスを再起動します。Platform Services Controller を再起動するか、または次のコマンドをコマンド ラインから実行することができます。

#### Windows

Windows では、service-control コマンドは `VCENTER_INSTALL_PATH\bin` にあります。

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

#### vCenter Server Appliance

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

## Platform Services Controller Web インターフェイスから VMware 認証局 (VMCA) を中間 CA にする

別の認証局で VMCA 証明書に署名することで、VMCA を中間 CA として使用できます。以降、VMCA が生成するすべての証明書に、完全なチェーンが含まれます。

この設定では、vSphere Certificate Manager ユーティリティまたは CLI を使用して実行することも、Platform Services Controller Web インターフェイスから実行することもできます。

## 前提条件

- 1 CSR を生成します。
- 2 受け取った証明書を編集して、現在の VMCA ルート証明書を一番下に配置します。

vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意するでは、両方の手順を説明しています。

## 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 既存の証明書をチェーン証明書に置き換えるには、次の手順を実行します。

- a [証明書] の下で、[認証局] をクリックし、[ルート証明書] タブを選択します。
- b [証明書の置き換え] をクリックします。プライベート キー ファイルおよび証明書ファイル（完全なチェーン）を追加し、[OK] をクリックします。
- c [ルート証明書の置き換え] ダイアログで、[参照] をクリックしてプライベート キーを選択し、[参照] を再度クリックして証明書を選択し、[OK] をクリックします。

以降、VMCA は、新しいチェーン ルート証明書と一緒に発行したすべての証明書に署名します。

- 4 ローカル システムのマシン SSL 証明書を更新します。

- a [証明書] の下で、[証明書の管理] をクリックし、[マシン証明書] タブをクリックします。
- b 証明書を選択し、[更新] をクリックして [はい] と応答します。

VMCA により、マシン SSL 証明書が新しい認証局で署名された証明書に置き換えられます。

- 5 (オプション) ローカル システムのソリューション ユーザー証明書を更新します。

- a [ソリューション ユーザー証明書] タブをクリックします。
- b 証明書を選択し、[更新] をクリックして選択した証明書を個別に更新するか、[すべてを更新] をクリックしてすべての証明書を置き換えて、プロンプトに対して [はい] と応答します。

VMCA により、選択したソリューション ユーザー証明書またはすべてのソリューション ユーザー証明書が、新しい認証局によって署名された証明書に置き換えられます。

- 6 環境に外部 Platform Services Controller が含まれている場合は、その後に各 vCenter Server システムの証明書を更新できます。
  - a [証明書の管理] パネルで [ログアウト] ボタンをクリックします。
  - b プロンプトが表示されたら、vCenter Server システムの IP アドレスまたは FQDN と、vCenter Single Sign-On に対して認証できる vCenter Server 管理者のユーザー名とパスワードを指定します。
  - c vCenter Server でマシン SSL 証明書を更新し、オプションで各ソリューション ユーザー証明書を更新します。
  - d 環境内に複数の vCenter Server システムがある場合は、システムごとにこのプロセスを繰り返します。

#### 次のステップ

Platform Services Controller のサービスを再起動します。Platform Services Controller を再起動するか、または次のコマンドをコマンド ラインから実行することができます。

#### Windows

Windows では、service-control コマンドは `VCENTER_INSTALL_PATH\bin` にあります。

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

#### vCenter Server Appliance

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

## Platform Services Controller からカスタム証明書を使用するためのシステムの設定

Platform Services Controller を使用して、カスタム証明書を使用するように環境を設定できます。

Certificate Manager ユーティリティを使用して、証明書署名要求 (CSR) を各マシンおよび各ソリューション ユーザー向けに生成できます。内部またはサードパーティの認証局に CSR を送信すると、認証局によって署名付き証明書およびルート証明書が返されます。Platform Services Controller ユーザー インターフェイスから、ルート証明書と署名付き証明書の両方をアップロードできます。

### vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）

vSphere Certificate Manager を使用すると、エンタープライズ CA で使用したり外部認証局に送信したりできる証明書署名要求 (CSR) を生成できます。サポートされているさまざまな証明書置き換えプロセスで、証明書を使用できます。

Certificate Manager ツールは、次に示すようにコマンド ラインから実行できます。

## Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

## Linux

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

### 前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

- CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者が求められます。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- マシン SSL 証明書の CSR を生成するには、certtool.cfg ファイルに保存されている証明書プロパティが求められます。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。

### 手順

- 1 環境内の各マシンで、vSphere Certificate Manager を起動してオプション 1 を選択します。
- 2 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
- 3 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。  
プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。
- 4 すべてのソリューション ユーザー証明書も置き換える場合は、Certificate Manager を再起動します。
- 5 オプション 5 を選択します。
- 6 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
- 7 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。  
プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。

Platform Services Controller ノードごとに、Certificate Manager により 1 つの証明書と鍵のペアが生成されます。vCenter Server ノードごとに、Certificate Manager により 4 つの証明書と鍵のペアが生成されます。

## 次のステップ

証明書の置き換えを実行します。

## 証明書ストアへの信頼できるルート証明書の追加

環境内でサードパーティ証明書を使用する場合は、信頼できるルート証明書を証明書ストアに追加する必要があります。

### 前提条件

サードパーティまたは社内の認証局 (CA) からカスタム ルート証明書を取得します。

### 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 [証明書] で、[証明書の管理] を選択し、Platform Services Controller の IP アドレスまたはホスト名と、ローカルドメインの管理者（デフォルトでは administrator@vsphere.local）のユーザー名とパスワードを指定し、[送信] をクリックします。

- 4 [信頼できるルート証明書] を選択し、[証明書の追加] をクリックします。

- 5 [参照] をクリックし、証明書チェーンの配置場所を選択します。

CER、PEM、または CRT の各ファイル タイプを使用できます。

## 次のステップ

マシンの SSL 証明書と、必要に応じてソリューション ユーザー証明書をこの認証局の署名付き証明書と置き換えます。

## Platform Services Controller からのカスタム証明書の追加

Platform Services Controller から、カスタム マシン SSL 証明書およびカスタム ソリューション ユーザー証明書を証明書ストアに追加できます。

通常は、各コンポーネントのマシン SSL 証明書を置き換えるだけで十分です。ソリューション ユーザー証明書はブロキシに置いたままにします。

### 前提条件

置き換える各証明書の証明書署名要求 (CSR) を生成します。CSR を生成するには、Certificate Manager ユーティリティを使用します。Platform Services Controller がアクセスできる場所に証明書およびプライベート キーを格納します。

## 手順

- 1 Web ブラウザで次の URL を指定して Platform Services Controller に接続します。

**`https://psc_hostname_or_IP/psc`**

組み込みデプロイでは、Platform Services Controller のホスト名または IP アドレスは vCenter Server のホスト名または IP アドレスと同じです。

- 2 administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

インストール時に異なるドメインを指定した場合は、administrator@mydomain としてログインします。

- 3 [証明書] で、[証明書の管理] を選択し、Platform Services Controller の IP アドレスまたはホスト名と、ローカル ドメインの管理者（デフォルトでは administrator@vsphere.local）のユーザー名とパスワードを指定し、[送信] をクリックします。

- 4 マシン証明書を置き換えるには次の手順を実行します。

- a [マシン証明書] タブを選択し、置き換える証明書をクリックします。
- b [置き換え] > [参照] の順にクリックして証明書チェーンを置き換え、[参照] をクリックしてプライベートキーを置き換えます。

- 5 ソリューション ユーザー証明書を置き換えるには、次の手順を実行します。

- a [ソリューション ユーザー証明書] タブを選択し、コンポーネント用の 4 つの証明書のうち、最初の証明書をクリックします（例 [マシン]）。
- b [置き換え] > [参照] の順にクリックして証明書チェーンを置き換え、[参照] をクリックしてプライベートキーを置き換えます。
- c 同じコンポーネントの残り 3 つの証明書に対して、この手順を繰り返します。

## 次のステップ

Platform Services Controller のサービスを再起動します。Platform Services Controller を再起動するか、または次のコマンドをコマンド ラインから実行することができます。

## Windows

Windows では、service-control コマンドは `VCENTER_INSTALL_PATH\bin` にあります。

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

## vCenter Server Appliance

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



## vSphere Certificate Manager ユーティリティによる証明書の管理

vSphere Certificate Manager ユーティリティを使用すると、ほとんどの証明書管理タスクをコマンドラインから対話形式で実行することができます。vSphere Certificate Manager では、実行するタスクや証明書の場所などの情報を入力する画面が必要に応じて表示され、その後サービスがいったん停止されてから起動され、証明書が置き換えられます。

vSphere Certificate Manager を使用する場合、ユーザーが VECS (VMware Endpoint 証明書ストア) に証明書を配置したり、サービスの起動と停止を行う必要はありません。

vSphere Certificate Manager を実行する前に、必ず置き換えプロセスについて理解すると共に、使用する証明書を入手してください。

---

**注意：** vSphere Certificate Manager では、1 レベルの取り消しがサポートされます。vSphere Certificate Manager を 2 回実行し、誤って環境を壊したことに気付いた場合、2 回の実行のうちの最初の実行は取り消すことができません。

---

このツールは、次に示すようにコマンドラインで実行できます。

### Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

### Linux

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

### 手順

#### 1 古い証明書の再発行による、最後に実行された操作の取り消し

vSphere Certificate Manager を使用して証明書の管理操作を実行する際に、証明書が置き換えられる前に、現在の証明書の状態が BACKUP\_STORE ストアに格納されます。最後に実行した処理を取り消して、以前の状態に戻すことができます。

#### 2 すべての証明書のリセット

既存の vCenter 証明書すべてを VMCA によって署名された証明書に置き換えるには、すべての証明書をリセット オプションを使用します。

#### 3 新しい VMCA ルート証明書の再生成およびすべての証明書の置き換え

VMCA ルート証明書を再生成し、ローカル マシンの SSL 証明書およびローカル ソリューションのユーザー証明書を VMCA 署名付き証明書に置き換えることができます。マルチノードのデプロイでは、このオプションで vSphere Certificate Manager を Platform Services Controller 上で実行してから、再度このユーティリティを他のすべてのノード上で実行し、[マシンの SSL 証明書を VMCA 証明書と置き換える] および [ソリューションのユーザー証明書を VMCA 証明書と置き換える] を選択します。

#### 4 VMCA を中間認証局にする (Certificate Manager)

Certificate Manager ユーティリティからプロンプトに従って、VMCA を中間 CA にすることができます。プロセスの完了後、VMCA はすべての新規証明書に完全なチェーンで署名します。必要場合は、Certificate Manager を使用して、既存のすべての証明書を VMCA 署名付き証明書に置き換えることができます。

#### 5 カスタム証明書によるすべての証明書の置き換え (Certificate Manager)

vSphere Certificate Manager ユーティリティを使用して、すべての証明書をカスタム証明書に置き換えることができます。プロセスを始める前に、CA に CSR を送信する必要があります。Certificate Manager を使用して CSR を生成できます。

### 古い証明書の再発行による、最後に実行された操作の取り消し

vSphere Certificate Manager を使用して証明書の管理操作を実行する際に、証明書が置き換えられる前に、現在の証明書の状態が BACKUP\_STORE ストアに格納されます。最後に実行した処理を取り消して、以前の状態に戻すことができます。

---

**注：** 取り消し操作により、現在 BACKUP\_STORE 内にあるものがリストアされます。2 つの異なるオプションを使用して vSphere Certificate Manager を実行していて、取り消しを行う場合は、最後の操作のみが取り消されます。

---

### すべての証明書のリセット

既存の vCenter 証明書すべてを VMCA によって署名された証明書に置き換えるには、すべての証明書をリセット オプションを使用します。

このオプションを使用すると、現在 VECS にあるカスタム証明書がすべて上書きされます。

- Platform Services Controller ノードでは、vSphere Certificate Manager を使用して、ルート証明書の再生成と、マシン SSL 証明書およびマシン ソリューション ユーザー証明書の置き換えを行えます。
- 管理ノードでは、vSphere Certificate Manager を使用して、マシン SSL 証明書とすべてのソリューション ユーザー証明書を置き換えることができます。
- 組み込みデプロイでは、vSphere Certificate Manager を使用してすべての証明書を置き換えることができます。

どの証明書が置き換えられるかは、選択するオプションによって異なります。

### 新しい VMCA ルート証明書の再生成およびすべての証明書の置き換え

VMCA ルート証明書を再生成し、ローカル マシンの SSL 証明書およびローカル ソリューションのユーザー証明書を VMCA 署名付き証明書に置き換えることができます。マルチノードのデプロイでは、このオプションで vSphere Certificate Manager を Platform Services Controller 上で実行してから、再度このユーティリティを他のすべてのノード上で実行し、[マシンの SSL 証明書を VMCA 証明書と置き換える] および [ソリューションのユーザー証明書を VMCA 証明書と置き換える] を選択します。

このコマンドを実行すると、vSphere Certificate Manager によりパスワードおよび証明書情報の入力を求めるプロンプトが表示され、パスワード以外のすべての情報が `certtool.cfg` ファイルに保存されます。その後、サービスの停止、すべての証明書の置き換え、およびプロセスの再起動が自動で行われます。次の情報の入力が必要です。

- administrator@vsphere.local のパスワード。
- 2 文字の国名コード
- 会社名
- 組織名
- 組織単位
- 状態
- 地域
- IP アドレス（オプション）
- 電子メール
- ホスト名（証明書を置き換えるマシンの完全修飾ドメイン名）
- Platform Services Controller の IP アドレス（コマンドを管理ノード上で実行している場合）

#### 前提条件

新しい VMCA 署名付き証明書を生成するマシンの FQDN を把握しておく必要があります。他のプロパティはすべて、デフォルトで事前定義された値になります。IP アドレスはオプションです。

#### 次のステップ

マルチノード デプロイでルート証明書を置き換えた後は、外部の Platform Services Controller ノードを使用するすべての vCenter Server 上でサービスを再起動する必要があります。

## VMCA を中間認証局にする (Certificate Manager)

Certificate Manager ユーティリティからプロンプトに従って、VMCA を中間 CA にすることができます。プロセスの完了後、VMCA はすべての新規証明書に完全なチェーンで署名します。必要な場合は、Certificate Manager を使用して、既存のすべての証明書を VMCA 署名付き証明書に置き換えることができます。

### vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する

vSphere Certificate Manager を使用して証明書署名要求 (CSR) を生成できます。この CSR をエンタープライズまたは外部の認証局 (CA) に送信して署名を要求します。署名付きの証明書は、サポートされているさまざまな証明書置き換えプロセスで使用できます。

- CSR は vSphere Certificate Manager を使用して作成できます。
- CSR を手動で作成する場合は、署名のために送付する証明書は以下の要件を満たしている必要があります。
  - キー サイズ：2,048 ビット以上

- PEM 形式。VMware では、PKCS8 および PKCS1 (RSA キー) がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。
- CRL の署名は有効にしてください。
- 拡張キー使用法には、クライアント認証またはサーバ認証を含めないでください。
- 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。
- ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。
- VMCA の従属認証局は作成できません。

Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事 2112009 の「vSphere 6.0 で SSL 証明書を作成するために Microsoft 認証局テンプレートを作成する」を参照してください。

#### 前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者が求められます。

#### 手順

- 1 vSphere Certificate Manager を起動して、オプション 2 を選択します。  
最初はこのオプションを使用して証明書の置き換えではなく CSR の生成を行います。
- 2 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
- 3 オプション 1 を選択して CSR を生成し、プロンプトに応答します。  
プロセスの一部として、ディレクトリを指定する必要があります。署名対象の証明書 (\*.csr ファイル) と対応するキー ファイル (\*.key ファイル) は、Certificate Manager によってディレクトリ内に配置されます。
- 4 署名のために証明書をエンタープライズまたは外部の認証局 (CA) に送信し、ファイルに root\_signing\_cert.cer という名前を付けます。
- 5 テキスト エディタで次のように証明書を結合します。

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
```

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

6 ファイルを `root_signing_chain.cer` という名前で保存します。

#### 次のステップ

既存のルート証明書をチェーン ルート証明書に置き換えます。[VMCA ルート証明書をカスタム署名証明書で置き換え、すべての証明書で置き換える](#)を参照してください。

### VMCA ルート証明書をカスタム署名証明書で置き換え、すべての証明書で置き換える

VMCA ルート証明書は、証明書チェーンに VMCA が中間証明書として含まれる、CA 署名付き証明書に置き換えることができます。将来的に、VMCA によって生成されるすべての証明書には、完全なチェーンが含まれます。

組み込みインストールや外部 Platform Services Controller で vSphere Certificate Manager を実行して、VMCA ルート証明書をカスタム署名証明書に置き換えます。

vSphere Certificate Manager により、次の情報を指定するように求められます。

#### 前提条件

- CSR を生成します。
  - CSR は vSphere Certificate Manager を使用して作成できます。を参照してください。[vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する](#)
  - CSR を手動で作成する場合は、署名のために送付する証明書は以下の要件を満たしている必要があります。
    - キー サイズ：2,048 ビット以上
    - PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
    - x509 バージョン 3
    - カスタム証明書を使用している場合、ルート証明書の認証局の拡張を `true` に設定し、証明書の署名を要件の一覧に含める必要があります。
    - CRL の署名は有効にしてください。
    - 拡張キー使用法には、クライアント認証またはサーバ認証を含めないでください。
    - 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。
    - ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。
    - VMCA の従属認証局は作成できません。

Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事 2112009 の「vSphere 6.0 で SSL 証明書を作成するために Microsoft 認証局テンプレートを作成する」を参照してください。

- サードパーティまたはエンタープライズ CA から証明書を受け取った後、その証明書を初期 VMCA ルート証明書と結合し、VMCA ルート証明書が最下部となる完全なチェーンを生成します。[vSphere Certificate Manager](#) で CSR を生成し、[ルート証明書（中間認証局）を用意する](#) を参照してください。
- 必要な情報を収集します。
  - administrator@vsphere.local のパスワード。
  - ルートの有効なカスタム証明書（.crt ファイル）。
  - ルートの有効なカスタム キー（.key ファイル）。

#### 手順

- 1 Platform Services Controller の組み込みインストールまたは外部 Platform Services Controller 上で vSphere Certificate Manager を起動し、オプション 2 を選択します。
- 2 オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。
  - a 指示に従い、ルート証明書のフルパスを指定します。
  - b 証明書を初めて置き換えるときには、マシン SSL 証明書に使用される情報の入力を求められます。  
この情報は、マシンの必須 FQDN を含み、certtool.cfg ファイルに保存されます。
- 3 マルチノード デプロイでルート証明書を置き換える場合は、すべての vCenter Server でサービスを再起動する必要があります。
- 4 マルチノード デプロイでは、オプション 3（マシンの SSL 証明書を VMCA 証明書で置き換える）とオプション 6（VMCA 証明書によるソリューション ユーザー証明書の置き換え）を使用して、各 vCenter Server インスタンスですべての証明書を置き換えます。  
  
証明書を置き換えると、VMCA が完全なチェーンで署名します。

#### 次のステップ

環境によっては、他の証明書も明示的な置き換えが必要になる場合があります。

- 証明書をすべて置き換えることが企業ポリシーで規定されている場合は、vmdir ルート証明書を置き換えます。[を参照してください。VMware ディレクトリ サービス証明書の置き換え](#)
- vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。[を参照してください。混合モード環境での VMware ディレクトリ サービス証明書の置き換え](#)

### VMCA 証明書によるマシン SSL 証明書の置き換え（中間 CA）

VMCA を中間 CA として使用するマルチノード デプロイでは、マシン SSL 証明書を明示的に置き換える必要があります。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったマシン SSL 証明書を置き換えるためにも使用できます。

既存のマシン SSL 証明書を新しい VMCA 署名付きの証明書に置き換えると、vSphere Certificate Manager により次の情報が求められ、Platform Services Controller のパスワードと IP アドレスを除くすべての値が `certtool.cfg` ファイルに入力されます。

- administrator@vsphere.local のパスワード。
- 2 文字の国名コード
- 会社名
- 組織名
- 組織単位
- 状態
- 地域
- IP アドレス（オプション）
- 電子メール
- ホスト名、すなわち証明書を置き換えるマシンの完全修飾ドメイン名ホスト名が FQDN と一致しない場合、証明書の置き換えは正しく完了せず、環境が不安定な状態になる可能性があります。
- Platform Services Controller の IP アドレス（コマンドを管理ノード上で実行している場合）

#### 前提条件

- マルチノード デプロイで VMCA ルート証明書を置き換えた場合は、すべての vCenter Server ノードを明示的に再起動します。
- このオプションを指定して Certificate Manager を実行するためには、次の情報を把握している必要があります。
  - administrator@vsphere.local のパスワード。
  - 新しい VMCA 署名付き証明書を生成するマシンの FQDN。他のすべてのプロパティは事前定義された値にデフォルト設定されますが、変更が可能です。
  - 外部 Platform Services Controller を使用した vCenter Server システムで実行する場合は、Platform Services Controller のホスト名または IP アドレス。

#### 手順

- 1 vSphere Certificate Manager を起動して、オプション 3 を選択します。
- 2 プロンプトに応答します。

情報は `certtool.cfg` ファイルに保存されます。

#### 結果

vSphere Certificate Manager はマシン SSL 証明書を置き換えます。

## VMCA 証明書によるソリューション ユーザー証明書の置き換え（中間 CA）

VMCA を中間 CA として使用するマルチノードでは、ソリューション ユーザー証明書を明示的に置き換える必要があります。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったソリューション ユーザー証明書を置き換えるためにも使用できます。

### 前提条件

- マルチノード デプロイで VMCA ルート証明書を置き換えた場合は、すべての vCenter Server ノードを明示的に再起動します。
- このオプションを指定して Certificate Manager を実行するためには、次の情報を把握している必要があります。
  - administrator@vsphere.local のパスワード。
  - 外部 Platform Services Controller を使用した vCenter Server システムで実行する場合は、Platform Services Controller のホスト名または IP アドレス。

### 手順

- 1 vSphere Certificate Manager を起動して、オプション 6 を選択します。
- 2 プロンプトに応答します。

### 結果

vSphere Certificate Manager によって、すべてのソリューション ユーザー証明書が置き換えられます。

## カスタム証明書によるすべての証明書の置き換え (Certificate Manager)

vSphere Certificate Manager ユーティリティを使用して、すべての証明書をカスタム証明書に置き換えることができます。プロセスを始める前に、CA に CSR を送信する必要があります。Certificate Manager を使用して CSR を生成できます。

マシン SSL 証明書のみを置き換えて、VMCA によってプロビジョニングされたソリューション ユーザー証明書を使用することもできます。ソリューション ユーザー証明書は、vSphere コンポーネント間の通信にのみ使用されません。

カスタム証明書を使用する場合、カスタム証明書で環境に追加する各ノードをプロビジョニングする必要があります。VMCA では引き続き VMCA 署名付き証明書がプロビジョニングされるため、ユーザーがこれらの証明書を置き換える必要があります。手動による証明書の置き換えには、vSphere Certificate Manager ユーティリティを使用するか CLI を使用できます。証明書は VECS に保存されます。

## vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）

vSphere Certificate Manager を使用すると、エンタープライズ CA で使用したり外部認証局に送信したりできる証明書署名要求 (CSR) を生成できます。サポートされているさまざまな証明書置き換えプロセスで、証明書を使用できます。



Certificate Manager ツールは、次に示すようにコマンド ラインから実行できます。

## Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

## Linux

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

### 前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

- CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者が求められます。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- マシン SSL 証明書の CSR を生成するには、certtool.cfg ファイルに保存されている証明書プロパティが求められます。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。

### 手順

- 1 環境内の各マシンで、vSphere Certificate Manager を起動してオプション 1 を選択します。
- 2 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
- 3 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。  
プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。
- 4 すべてのソリューション ユーザー証明書も置き換える場合は、Certificate Manager を再起動します。
- 5 オプション 5 を選択します。
- 6 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
- 7 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。  
プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。

Platform Services Controller ノードごとに、Certificate Manager により 1 つの証明書と鍵のペアが生成されます。vCenter Server ノードごとに、Certificate Manager により 4 つの証明書と鍵のペアが生成されます。

## 次のステップ

証明書の置き換えを実行します。

## カスタム証明書によるマシン SSL 証明書の置き換え

マシン SSL 証明書は、各管理ノード、Platform Services Controller、および組み込みデプロイのリバース プロキシ サービスによって使用されます。各マシンには、他のサービスとの安全な通信を実現するため、マシン SSL 証明書が必要です。各ノードの証明書をカスタム証明書に置き換えることができます。

### 前提条件

開始する前に、環境内のマシンごとに CSR が存在している必要があります。CSR は、vSphere Certificate Manager を使用して生成することも、明示的に生成することもできます。

- 1 vSphere Certificate Manager を使用して CSR を生成するには、[vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）](#)を参照してください。
- 2 CSR を明示的に生成するには、サードパーティまたはエンタープライズ CA に各マシンの証明書を要求します。証明書は次の要件を満たす必要があります。
  - キー サイズ：2,048 ビット以上（PEM エンコード）
  - CRT 形式
  - x509 バージョン 3
  - SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。
  - キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。

当社のナレッジ ベースの記事「[Obtaining vSphere certificates from a Microsoft Certificate Authority](#)」(2112014) も参照してください。

### 手順

- 1 vSphere Certificate Manager を起動して、オプション 1 を選択します。
- 2 オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。

vSphere Certificate Manager により、次の情報を指定するように求められます。

- administrator@vsphere.local のパスワード。
- 有効なマシン SSL カスタム証明書（.crt ファイル）。
- 有効なマシン SSL カスタム キー（.key ファイル）。
- カスタム マシン SSL 証明書の有効な署名証明書（.crt ファイル）。
- マルチノード デプロイの管理ノードでコマンドを実行している場合は、Platform Services Controller の IP アドレス。

## 次のステップ

環境によっては、他の証明書も明示的な置き換えが必要になる場合があります。

- 証明書をすべて置き換えることが企業ポリシーで規定されている場合は、vmdir ルート証明書を置き換えます。  
を参照してください。 [VMware ディレクトリ サービス証明書の置き換え](#)
- vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。を参照してください。 [混合モード環境での VMware ディレクトリ サービス証明書の置き換え](#)

## カスタム証明書によるソリューション ユーザー証明書の置き換え

多くの企業では、置き換えが必要となるのは外部からアクセス可能なサービスの証明書のみです。ただし、Certificate Manager では、ソリューション ユーザー証明書の置き換えもサポートしています。ソリューション ユーザーはサービスのコレクションです。たとえば、vSphere Web Client に関連付けられたすべてのサービスもソリューション ユーザーになります。複数ノードのデプロイでは、Platform Services Controller 上のマシン ソリューション ユーザー証明書および各管理ノード上のソリューション ユーザーのフル セットを置き換えます。

ソリューション ユーザー証明書を求められたら、サードパーティ CA の完全な署名証明書チェーンを提供します。

次のような形式になります。

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

## 前提条件

開始する前に、環境内のマシンごとに CSR が存在している必要があります。CSR は、vSphere Certificate Manager を使用して生成することも、明示的に生成することもできます。

- 1 vSphere Certificate Manager を使用して CSR を生成するには、[vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）](#)を参照してください。
- 2 各ノードのソリューション ユーザーごとに、サードパーティ CA またはエンタープライズ CA の証明書を要求します。CSR は、vSphere Certificate Manager を使用して生成することも、管理者自身が準備することもできます。CSR は次の要件を満たす必要があります。
  - キー サイズ：2,048 ビット以上（PEM エンコード）
  - CRT 形式
  - x509 バージョン 3
  - SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。

- 各ソリューション ユーザー証明書には異なる Subject が指定されている必要があります。たとえば、ソリューション ユーザー名（例：vpxd）などの一意の識別子を含めることができます。
- キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。

当社のナレッジ ベースの記事「[Obtaining vSphere certificates from a Microsoft Certificate Authority](#)」(2112014) も参照してください。

#### 手順

- 1 vSphere Certificate Manager を起動して、オプション 5 を選択します。
- 2 オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。

vSphere Certificate Manager により、次の情報を指定するように求められます。

- administrator@vsphere.local のパスワード。
- マシン ソリューション ユーザーの証明書およびキー。
- vSphere Certificate Manager を Platform Services Controller ノード上で実行している場合は、マシン ソリューション ユーザーの証明書とキー（vpxd.crt および vpxd.key）を求めるメッセージが表示されます。
- vSphere Certificate Manager を管理ノードまたは組み込みデプロイで実行している場合は、すべてのソリューション ユーザーの証明書およびキー（vpxd.crt および vpxd.key）のフル セットを求めるメッセージが表示されます。

#### 次のステップ

vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。[混合モード環境での VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

## 証明書の手動での置き換え

一部の特殊な場合、たとえば、1 種類のソリューション ユーザー証明書のみを置き換える場合などでは、vSphere Certificate Manager ユーティリティは使用できません。この場合、証明書の置き換えのインストールに含まれた CLI を使用できます。

## サービスの起動および停止について

手動による証明書置き換え手順の一部では、すべてのサービスを停止してから、証明書インフラストラクチャを管理するサービスのみを開始する必要があります。必要なときにだけサービスを停止すると、ダウンタイムを最小化できます。

次の原則に従います。

- パブリック キーとプライベート キーのペアや証明書を新しく生成するためにサービスを停止することはしません。

- 管理者が 1 人しかいない場合、新しいルート証明書を追加するときにサービスを停止する必要はありません。古いルート証明書は使用可能なままで、その証明書を使用して引き続きすべてのサービスを認証できます。ホストとの間で問題が発生することを回避するため、ルート証明書を追加し終えたらすべてのサービスを停止し、すぐに再開します。
- 環境内に複数の管理者がいる場合は、新しいルート証明書を追加する前にサービスを停止し、追加が終わったらサービスを再開します。
- 次のタスクを実行する直前にサービスを停止します。
  - VECS でマシン SSL 証明書または任意のソリューション ユーザー証明書を削除します。
  - vmdir (VMware ディレクトリ サービス) でソリューション ユーザー証明書を置き換えます。

## 新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え

VMCA ルート証明書の有効期限が近付いているか、またはその他の理由で証明書を置き換える場合には、新しいルート証明書を生成し、VMware ディレクトリ サービスに追加できます。新しいルート証明書を使用すれば、新しいマシン SSL 証明書およびソリューション ユーザー証明書を生成することもできます。

多くの場合、vSphere Certificate Manager ユーティリティを使用して証明書を置き換えます。

詳細な制御が必要な場合には、このシナリオを参照すると、CLI コマンドを使用して証明書のセットをすべて置き換える具体的な手順が詳細に分かります。あるいは、該当するタスクの手順を使用して、個別の証明書のみを置き換えることもできます。

### 前提条件

administrator@vsphere.local または CAAdmins グループ内の他のユーザーのみが証明書管理タスクを実行できます。 [vCenter Single Sign-On グループへのメンバーの追加](#) を参照してください。

### 手順

#### 1 新規の VMCA 署名付きルート証明書の生成

certool CLI を使用して新しい VMCA 署名付き証明書を生成し、それらを vmdir に発行します。

#### 2 VMCA 署名付き証明書によるマシン SSL 証明書の置き換え

VMCA 署名付きルート証明書を新しく生成したら、環境内のすべてのマシン SSL 証明書を置き換えることができます。

#### 3 新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、すべてのソリューション ユーザー証明書を置き換えることができます。ソリューション ユーザー証明書は有効である必要があります。ここでの「有効」とは、有効期限が切れておらず、証明書に含まれるその他の情報が証明書インフラストラクチャで使用されていないことを意味します。

#### 4 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

## 新規の VMCA 署名付きルート証明書の生成

certool CLI を使用して新しい VMCA 署名付き証明書を生成し、それらを vmdir に発行します。

マルチノード デプロイでは、Platform Services Controller でルート証明書の生成コマンドを実行します。

### 手順

- 1 新しい自己署名証明書およびプライベート キーを生成します。

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

- 2 既存のルート証明書を新しい証明書に置き換えます。

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

このコマンドは、証明書を生成し、その証明書を vmdir に追加して、VECS に追加します。

- 3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

### Windows

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

### vCenter Server Appliance

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

- 4 (オプション) 新しいルート証明書を vmdir に発行します。

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

このコマンドを実行すると、vmdir のすべてのインスタンスがただちに更新されます。このように実行しない場合、すべてのインスタンスへの伝達には時間がかかることがあります。

- 5 すべてのサービスを再開します。

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

**例：新規の VMCA 署名付きルート証明書の生成**

次の例は、現在のルート CA 情報を確認し、ルート証明書を再生成するための完全な手順を示します。

- 1 (オプション) VMCA ルート証明書を一覧表示し、証明書ストア内に含まれていることを確認します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- 管理ノードで、次のように実行します (外部インストール)。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-  
ip-or-fqdn>
```

出力は次のようになります。

```
output:  
Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
cf:2d:ff:49:88:50:e5:af  
...
```

- 2 (オプション) VECS TRUSTED\_ROOTS ストアの内容を一覧表示し、そこに表示される証明書のシリアル番号と、手順 1 の出力を比較します。

VECS が vmdir をポーリングするため、このコマンドは Platform Services Controller と管理ノードの両方で機能します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS  
--text
```

ルート証明書が 1 つだけの単純なケースでは、出力は次のようになります。

```
Number of entries in store :    1  
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd  
Entry type :    Trusted Cert  
Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
cf:2d:ff:49:88:50:e5:af
```

- 3 新しい VMCA ルート証明書を生成します。証明書が VECS と vmdir (VMware ディレクトリ サービス) の TRUSTED\_ROOTS ストアに追加されます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program  
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Windows では、コマンドがデフォルトの certool.cfg ファイルを使用するため、--config はオプションです。

## VMCA 署名付き証明書によるマシン SSL 証明書の置き換え

VMCA 署名付きルート証明書を新しく生成したら、環境内のすべてのマシン SSL 証明書を置き換えることができます。

各マシンには、他のサービスとの安全な通信を実現するため、マシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

### 前提条件

すべてのサービスを停止し、証明書の伝達およびストレージを処理するサービスを開始する準備ができています。

### 手順

- 1 新しい証明書を必要とするマシンごとに、`certtool.cfg` のコピーを 1 つ作成します。

`certtool.cfg` は次の場所で見つけることができます。

OS	パス
Windows	C:\Program Files\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 マシンの完全修飾ドメイン名 (FQDN) を含めるように、各マシンのカスタム構成ファイルを編集します。

マシンの IP アドレスに対して `NSLookup` を実行して、名前の DNS リストを表示し、ファイルのホスト名フィールドでその名前を使用します。

- 3 各ファイルに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```



- すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

## Windows

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

## vCenter Server Appliance

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

- 新しい証明書を VECS に追加します。

SSL を介して通信するには、すべてのマシンのローカル証明書ストアに、新しい証明書が必要です。最初に既存のエントリを削除し、次に新しいエントリを追加します。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- すべてのサービスを再開します。

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

### 例：VMCA 署名付き証明書によるマシン証明書の置き換え

- SSL 証明書用の構成ファイルを作成し、そのファイルを現在のディレクトリに ssl-config.cfg として保存します。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

- マシン SSL 証明書にキー ペアを生成します。このコマンドを各管理ノードと Platform Services Controller ノードで実行します。--server オプションは必要ありません。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

現在のディレクトリに ssl-key.priv および ssl-key.pub ファイルが作成されます。

- 3 新しいマシン SSL 証明書を生成します。この証明書は VMCA によって署名されます。VMCA ルート証明書をカスタム証明書で置き換える場合には、VMCA はすべての証明書に完全なチェーンで署名します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server（外部インストール）の場合：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

現在のディレクトリに new-vmca-ssl.crt ファイルが作成されます。

- 4 （オプション）VECS のコンテンツをリスト表示します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Platform Services Controller への出力は以下のようになります。

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server への出力は以下のようになります。

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

- 5 VECS 内のマシン SSL 証明書を新しいマシン SSL 証明書で置き換えます。--store と --alias の値はデフォルト名と正確に一致させる必要があります。

- Platform Services Controller で、次のコマンドを実行して MACHINE\_SSL\_CERT ストア内のマシン SSL 証明書を更新します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 各管理ノードまたは組み込みデプロイで、次のコマンドを実行して MACHINE\_SSL\_CERT ストア内のマシン SSL 証明書を更新します。FQDN はマシンごとに異なるため、各マシンの証明書は別々に更新する必要があります。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

#### 次のステップ

使用している ESXi ホストの証明書を置き換えることもできます。『vSphere セキュリティ』ドキュメントを参照してください。

マルチノード デプロイでルート証明書を置き換えた後は、外部の Platform Services Controller ノードを使用するすべての vCenter Server 上でサービスを再起動する必要があります。

### 新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、すべてのソリューション ユーザー証明書を置き換えることができます。ソリューション ユーザー証明書は有効である必要があります。ここでの「有効」とは、有効期限が切れておらず、証明書に含まれるその他の情報が証明書インフラストラクチャで使用されていないことを意味します。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 Platform Services Controller がある管理ノードでコマンドを実行する場合は、`--server` パラメータを使用して Platform Services Controller を指定します。

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、`dir-cli list` の出力にすべてのノードのソリューション ユーザーが含まれます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

#### 前提条件

すべてのサービスを停止し、証明書の伝達およびストレージを処理するサービスを開始する準備ができています。

#### 手順

- 1 `certool.cfg` のコピーを 1 つ作成し、名前、IP アドレス、DNS 名、および電子メールのフィールドを削除して、ファイルの名前を `sol_usr.cfg` のような名前に変更します。

生成プロセスの一部として、コマンド ラインから証明書に名前を付けることができます。その他の情報は、ソリューション ユーザーには必要ありません。デフォルトの情報を残すと、生成される証明書により混乱が生じる可能性があります。

- 2 各ソリューション ユーザーに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=vpzd.priv --pubkey=vpzd.pub
certool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次のようになります。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、dir-cli リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。vmafd-cli get-machine-id --server-name localhost を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

- 4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

## Windows

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

## vCenter Server Appliance

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

- 5 各ソリューション ユーザーの既存の証明書を、vmdir、VECS の順に置き換えます。

次の例は、vpzd サービスの証明書を置き換える方法を示します。

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

**注：** vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On への認証ができません。

- 6 すべてのサービスを再開します。

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

#### 例：VMCA 署名付きソリューション ユーザー証明書の使用

- 1 各ソリューション ユーザーにパブリック/プライベート キーのペアを生成します。これには、各 Platform Services Controller のマシン証明書ユーザーおよび各管理ノードのペアと、各管理ノードの各追加ソリューション ユーザー (vpzd、vpzd-extension、vsphere-webclient) のペアが含まれます。

- a 組み込みデプロイのマシン ソリューション ユーザーまたは Platform Services Controller のマシン ソリューション ユーザーのキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (オプション) 外部 Platform Services Controller を使用したデプロイの場合、各管理ノードのマシン ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- c 各管理ノードの vpzd ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-
key.priv --pubkey=vpzd-key.pub
```

- d 各管理ノードの vpzd-extension ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-
extension-key.priv --pubkey=vpzd-extension-key.pub
```

- e 各管理ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-
webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 各 Platform Services Controller および各管理ノードのマシン ソリューション ユーザーと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) に新しい VMCA ルート証明書によって署名されたソリューション ユーザー証明書を生成します。

**注：** --Name パラメータは一意である必要があります。vpxd または vpxd-extension などのソリューション ユーザー ストアの名前も含めると、ソリューション ユーザーごとにどの証明書を適用するのかが確認しやすくなります。

- a 以下のコマンドを Platform Services Controller ノードで実行し、そのノードのマシン ソリューション ユーザーにソリューション ユーザー証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 各管理ノードのマシン ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c 各管理ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d 各管理ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e 次のコマンドを実行して、各管理ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 VECS のソリューション ユーザー証明書を、新しいソリューション ユーザー証明書で置き換えます。

**注：** --store と --alias パラメータは、サービスのデフォルト名と正確に一致させる必要があります。

- a Platform Services Controller ノードで、以下のコマンドを実行してマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 以下のように、各管理ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 各管理ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 各管理ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

- e 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

- 4 新しいソリューション ユーザー証明書をを使用して VMware ディレクトリ サービス (vmdir) を更新します。  
vCenter Single Sign-On 管理者パスワードを求められます。

- a `dir-cli service list` を実行し、ソリューション ユーザーごとに一意のサービス ID サフィックス  
を取得します。このコマンドは、Platform Services Controller または vCenter Server システム上で  
実行できます。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、`dir-cli list` の出力  
にすべてのノードのソリューション ユーザーが含まれます。 `vmafd-cli get-machine-id --`  
`server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューシ  
ョン ユーザーの名前には、マシン ID が含まれています。

- b Platform Services Controller の vmdir にあるマシン証明書を置き換えます。たとえば、machine-29a45d00-60a7-11e4-96ff-00505689639a が Platform Services Controller のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c 各管理ノードの vmdir にあるマシン証明書を置き換えます。たとえば、machine-6fd7f140-60a9-11e4-9e28-005056895a69 が vCenter Server のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d 各管理ノードの vmdir にある vpxd ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 各管理ノードの vmdir にある vpxd-extension ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd-extension ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。たとえば、vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 が vsphere-webclient ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

## 次のステップ

各 Platform Services Controller ノードおよび各管理ノード上のすべてのサービスを再起動します。

## 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。



これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。
- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

---

**注：** サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

---

#### 手順

- 1 vCenter Single Sign-On 6.x サービスが実行されているノードで、vmdir SSL 証明書とキーを置き換えます。

[VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

- 2 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

- a C:\ProgramData\VMware\CIS\cfg\vmdir 内のすべてのファイルをバックアップします。
- b 6.x ノード上の vmldircert.pem ファイルのコピーを作成し、このコピーの名前を <sso\_node2.domain.com>.pem (<sso\_node2.domain.com> は 6.x ノードの FQDN) に変更します。
- c 名前を変更した証明書を C:\ProgramData\VMware\CIS\cfg\vmdir にコピーすることにより、既存の複製証明書を置き換えます。

- 3 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

サービスを vSphere Web Client から再起動することも、service-control コマンドを使用することもできます。

## 中間認証局としての VMCA の使用

VMCA ルート証明書は、証明書チェーンに VMCA が含まれるサードパーティの CA 署名付き証明書に置き換えることができます。将来的に、VMCA によって生成されるすべての証明書には、完全なチェーンが含まれます。既存の証明書は、新しく生成された証明書に置き換えることができます。この方法により、サードパーティの CA 署名付き証明書のセキュリティと、自動化された証明書管理の利便性が組み合わせられます。

#### 手順

- 1 [ルート証明書の置き換え \(中間 CA\)](#)

VMCA 証明書をカスタム証明書に置き換える際の最初の手順は、CSR を生成し、VMCA に返される証明書をルート証明書として追加することです。

## 2 マシン SSL 証明書の置き換え（中間 CA）

CA から署名付き証明書を受信し、それを VMCA ルート証明書にした後で、すべてのマシン SSL 証明書を置き換えることができます。

## 3 ソリューション ユーザー証明書の置き換え（中間 CA）

マシン SSL 証明書を置き換えたら、ソリューション ユーザー証明書を置き換えることができます。

## 4 VMware ディレクトリ サービス証明書の置き換え

新しい VMCA ルート証明書を使用することを決定し、環境のプロビジョニング時に使用していた VMCA ルート証明書の発行を解除する場合、マシン SSL 証明書、ソリューション ユーザー証明書、およびいくつかの内部サービス用証明書を置き換える必要があります。

## 5 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

## ルート証明書の置き換え（中間 CA）

VMCA 証明書をカスタム証明書に置き換える際の最初の手順は、CSR を生成し、VMCA に返される証明書をルート証明書として追加することです。

署名のために送信する証明書は、次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。
- CRL の署名は有効にしてください。
- 拡張キー使用法には、クライアント認証またはサーバ認証を含めないでください。
- 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。
- ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。
- VMCA の従属認証局は作成できません。

Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事 2112009 の「vSphere 6.0 で SSL 証明書を作成するために Microsoft 認証局テンプレートを作成する」を参照してください。

VMCA は、ルート証明書を置き換えるときに、証明書の次の属性を検証します。

- キーのサイズ：2,048 ビット以上

- キーの使用：証明書の署名
- 基本制約：サブジェクト タイプ CA

#### 手順

- 1 CSR を生成して、CA に送ります。

CA の指示に従います。

- 2 署名付き VMCA 証明書と一緒に、サード パーティ CA またはエンタープライズ CA の完全な CA チェーンが含まれる証明書ファイルを用意し、そのファイルを rootca1.crt などの名前で保存します。

これは、PEM 形式のすべての CA 証明書を単一ファイルにコピーすることで行えます。VMCA 証明書のルートから始めて、ルート CA PEM 証明書で終わる必要があります。例：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

#### Windows

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

#### vCenter Server Appliance

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

- 4 既存の VMCA ルート CA を置き換えます。

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

このコマンドを実行すると、次の処理が行われます。

- ファイル システム内の証明書がある場所に、新しいカスタム ルート証明書が追加されます。
- VECS の TRUSTED\_ROOTS ストアに、カスタム ルート証明書が追加されます（一定時間の経過後）。
- vmdir にカスタム ルート証明書が追加されます（一定時間の経過後）。

- 5 (オプション) vmdir (VMware ディレクトリ サービス) のすべてのインスタンスに変更を伝達するには、新しいルート証明書を vmdir に発行し、各ファイルのフル パスを指定します。

例：

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

vmdir ノード間のレプリケーションは 30 秒おきに実行されます。VECS は vmdir に対する新しいルート証明書ファイルのポーリングを 5 分おきに実行するため、VECS にルート証明書を明示的に追加する必要はありません。

- 6 (オプション) 必要な場合は、VECS の更新を強制できます。

```
vecs-cli force-refresh
```

- 7 すべてのサービスを再開します。

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

#### 例：ルート証明書の置き換え

certool コマンドに --rootca オプションを指定して、VMCA ルート証明書をカスタムの CA ルート証明書に置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-certs\root.pem --privkey=C:\custom-certs\root.key
```

このコマンドを実行すると、次の処理が行われます。

- ファイル システム内の証明書がある場所に、新しいカスタム ルート証明書が追加されます。
- VECS の TRUSTED\_ROOTS ストアに、カスタム ルート証明書が追加されます。
- vmdir にカスタム ルート証明書が追加されます。

#### 次のステップ

元の VMCA ルート証明書は証明書ストアから削除できます（会社のポリシーで求められている場合）。削除する場合は、次の内部証明書を更新する必要があります。

- vCenter Single Sign-On 署名証明書を置き換えます。[Security Token Service 証明書の更新](#) を参照してください。
- VMware ディレクトリ サービス証明書を置き換えます。[VMware ディレクトリ サービス証明書の置き換え](#) を参照してください。

### マシン SSL 証明書の置き換え（中間 CA）

CA から署名付き証明書を受信し、それを VMCA ルート証明書にした後で、すべてのマシン SSL 証明書を置き換えることができます。

これらの手順は、VMCA を認証局として使用する証明書を置き換える場合と基本的に同じです。ただし、この場合、VMCA はすべての証明書に完全なチェーンで署名します。

各マシンには、他のサービスとの安全な通信を実現するため、マシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

#### 前提条件

各マシン SSL 証明書の場合、SubjectAltName に `DNS Name=<Machine FQDN>` が含まれている必要があります。

#### 手順

- 1 新しい証明書を必要とするマシンごとに、`certtool.cfg` のコピーを 1 つ作成します。

`certtool.cfg` は次の場所で見つけることができます。

#### Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

#### Linux

`/usr/lib/vmware-vmca/share/config/`

- 2 マシンの完全修飾ドメイン名 (FQDN) を含めるように、各マシンのカスタム構成ファイルを編集します。

マシンの IP アドレスに対して `NSLookup` を実行して、名前の DNS リストを表示し、ファイルのホスト名フィールドでその名前を使用します。

- 3 各マシンにパブリック/プライベート キー ファイル ペアおよび証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

- すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

## Windows

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

## vCenter Server Appliance

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

- 新しい証明書を VECS に追加します。

SSL を介して通信するには、すべてのマシンのローカル証明書ストアに、新しい証明書が必要です。最初に既存のエントリを削除し、次に新しいエントリを追加します。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

- すべてのサービスを再開します。

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

### 例：マシン SSL 証明書の置き換え (VMCA が中間 CA)

- SSL 証明書用の構成ファイルを作成し、そのファイルを現在のディレクトリに ssl-config.cfg として保存します。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- マシン SSL 証明書にキー ペアを生成します。このコマンドを各管理ノードと Platform Services Controller ノードで実行します。--server オプションは必要ありません。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

現在のディレクトリに ssl-key.priv および ssl-key.pub ファイルが作成されます。

- 3 新しいマシン SSL 証明書を生成します。この証明書は VMCA によって署名されます。VMCA ルート証明書をカスタム証明書で置き換える場合には、VMCA はすべての証明書に完全なチェーンで署名します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server（外部インストール）の場合：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

現在のディレクトリに new-vmca-ssl.crt ファイルが作成されます。

- 4 （オプション）VECS のコンテンツをリスト表示します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli store list
```

- Platform Services Controller への出力は以下のようになります。

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server への出力は以下のようになります。

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

- 5 VECS 内のマシン SSL 証明書を新しいマシン SSL 証明書で置き換えます。--store と --alias の値はデフォルト名と正確に一致させる必要があります。

- Platform Services Controller で、次のコマンドを実行して MACHINE\_SSL\_CERT ストア内のマシン SSL 証明書を更新します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 各管理ノードまたは組み込みデプロイで、次のコマンドを実行して MACHINE\_SSL\_CERT ストア内のマシン SSL 証明書を更新します。FQDN はマシンごとに異なるため、各マシンの証明書は別々に更新する必要があります。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

#### 次のステップ

使用している ESXi ホストの証明書を置き換えることもできます。『vSphere セキュリティ』ドキュメントを参照してください。

マルチノード デプロイでルート証明書を置き換えた後は、外部の Platform Services Controller ノードを使用するすべての vCenter Server 上でサービスを再起動する必要があります。

### ソリューション ユーザー証明書の置き換え（中間 CA）

マシン SSL 証明書を置き換えたら、ソリューション ユーザー証明書を置き換えることができます。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 Platform Services Controller がある管理ノードでコマンドを実行する場合は、`--server` パラメータを使用して Platform Services Controller を指定します。

---

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、`dir-cli list` の出力にすべてのノードのソリューション ユーザーが含まれます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

---

#### 前提条件

各ソリューション ユーザー証明書には異なる Subject が指定されている必要があります。たとえば、ソリューション ユーザー名（例：vpxd）などの一意の識別子を含めることができます。

#### 手順

- 1 `certtool.cfg` のコピーを 1 つ作成し、名前、IP アドレス、DNS 名、および電子メールのフィールドを削除して、ファイルの名前を `sol_usr.cfg` のような名前に変更します。

生成プロセスの一部として、コマンド ラインから証明書に名前を付けることができます。その他の情報は、ソリューション ユーザーには必要ありません。デフォルトの情報を残すと、生成される証明書により混乱が生じる可能性があります。



- 2 各ソリューション ユーザーに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=vpzd.priv --pubkey=vpzd.pub
certool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次のようになります。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、dir-cli リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。vmafd-cli get-machine-id --server-name localhost を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

- 4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

## Windows

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

## vCenter Server Appliance

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

- 5 vmdir 内の既存の証明書を置き換え、次に VECS 内の証明書を置き換えます。

ソリューション ユーザーに対して、その順序で証明書を追加する必要があります。例：

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

**注：** vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On にログインできません。

- 6 すべてのサービスを再開します。

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

例：ソリューション ユーザー証明書の置き換え（中間 CA）

- 1 各ソリューション ユーザーにパブリック/プライベート キーのペアを生成します。これには、各 Platform Services Controller のマシン証明書ユーザーおよび各管理ノードのペアと、各管理ノードの各追加ソリューション ユーザー (vpzd、vpzd-extension、vsphere-webclient) のペアが含まれます。

- a 組み込みデプロイのマシン ソリューション ユーザーまたは Platform Services Controller のマシン ソリューション ユーザーのキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- b (オプション) 外部 Platform Services Controller を使用したデプロイの場合、各管理ノードのマシン ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-
key.priv --pubkey=machine-key.pub
```

- c 各管理ノードの vpzd ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-
key.priv --pubkey=vpzd-key.pub
```

- d 各管理ノードの vpzd-extension ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-
extension-key.priv --pubkey=vpzd-extension-key.pub
```

- e 各管理ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-
webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 各 Platform Services Controller および各管理ノードのマシン ソリューション ユーザーと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) に新しい VMCA ルート証明書によって署名されたソリューション ユーザー証明書を生成します。

**注：** --Name パラメータは一意である必要があります。vpxd または vpxd-extension などのソリューション ユーザー ストアの名前も含めると、ソリューション ユーザーごとにどの証明書を適用するのかが確認しやすくなります。

- a 以下のコマンドを Platform Services Controller ノードで実行し、そのノードのマシン ソリューション ユーザーにソリューション ユーザー証明書を生成します。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 各管理ノードのマシン ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c 各管理ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d 各管理ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e 次のコマンドを実行して、各管理ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 VECS のソリューション ユーザー証明書を、新しいソリューション ユーザー証明書で置き換えます。

**注：** --store と --alias パラメータは、サービスのデフォルト名と正確に一致させる必要があります。

- a Platform Services Controller ノードで、以下のコマンドを実行してマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\VCenter Server\vmaddd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCenter Server\vmaddd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 以下のように、各管理ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 各管理ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 各管理ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- 4 新しいソリューション ユーザー証明書をを使用して VMware ディレクトリ サービス (vmdir) を更新します。vCenter Single Sign-On 管理者パスワードを求められます。

- a dir-cli service list を実行し、ソリューション ユーザーごとに一意のサービス ID サフィックスを取得します。このコマンドは、Platform Services Controller または vCenter Server システム上で実行できます。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、dir-cli list の出力にすべてのノードのソリューション ユーザーが含まれます。vmafd-cli get-machine-id --server-name localhost を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

- b Platform Services Controller の vmdir にあるマシン証明書を置き換えます。たとえば、machine-29a45d00-60a7-11e4-96ff-00505689639a が Platform Services Controller のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c 各管理ノードの vmdir にあるマシン証明書を置き換えます。たとえば、machine-6fd7f140-60a9-11e4-9e28-005056895a69 が vCenter Server のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d 各管理ノードの vmdir にある vpxd ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 各管理ノードの vmdir にある vpxd-extension ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd-extension ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。たとえば、vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 が vsphere-webclient ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

## VMware ディレクトリ サービス証明書の置き換え

新しい VMCA ルート証明書を使用することを決定し、環境のプロビジョニング時に使用していた VMCA ルート証明書の発行を解除する場合、マシン SSL 証明書、ソリューション ユーザー証明書、およびいくつかの内部サービス用証明書を置き換える必要があります。

VMCA ルート証明書の発行を解除する場合は、vCenter Single Sign-On によって使われている SSL 署名証明書を置き換える必要があります。[Security Token Service 証明書の更新](#) を参照してください。また、VMware ディレクトリ サービス (vmdir) の証明書も置き換える必要があります。

### 前提条件

サードパーティ CA またはエンタープライズ CA に、vmdir の証明書を要求します。

## 手順

- 1 vmdir を停止します。

## Linux

```
service-control --stop vmdird
```

## Windows

```
service-control --stop VMWareDirectoryService
```

- 2 生成した証明書およびキーを、vmdir の場所にコピーします。

## Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

## Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 vSphere Web Client から、または service-control コマンドを使って、vmdir を再起動します。

## Linux

```
service-control --start vmdird
```

## Windows

```
service-control --start VMWareDirectoryService
```

## 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。

これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。

- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

---

**注：** サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

---

#### 手順

- 1 vCenter Single Sign-On 6.x サービスが実行されているノードで、vmdir SSL 証明書とキーを置き換えます。

VMware ディレクトリ サービス証明書の置き換えを参照してください。

- 2 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

- a C:\ProgramData\VMware\CIS\cfg\vmdir 内のすべてのファイルをバックアップします。
- b 6.x ノード上の vmDIRcert.pem ファイルのコピーを作成し、このコピーの名前を <sso\_node2.domain.com>.pem (<sso\_node2.domain.com> は 6.x ノードの FQDN) に変更します。
- c 名前を変更した証明書を C:\ProgramData\VMware\CIS\cfg\vmdir にコピーすることにより、既存の複製証明書を置き換えます。

- 3 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

サービスを vSphere Web Client から再起動することも、service-control コマンドを使用することもできます。

## vSphere でのサードパーティ証明書の使用

企業ポリシーで規定されている場合は、vSphere で使用されているすべての証明書を、サードパーティ CA 署名付き証明書に置き換えることができます。これを行った場合、VMCA は証明書チェーンには含まれなくなりますが、すべての vCenter 証明書が VECS に格納される必要があります。

すべての証明書を置き換えるか、ハイブリッド ソリューションを使用できます。たとえば、ネットワーク トラフィックに使用されるすべての証明書を置き換え、VMCA 署名付きソリューション ユーザー証明書はそのまま残すことを考えます。ソリューション ユーザー証明書は、vCenter Single Sign-On への認証にのみ使用されます。

---

**注：** VMCA を使用しない場合には、証明書を使用して新しいコンポーネントをプロビジョニングしたり、証明書の期限を常に把握するために、すべての証明書を自分自身で置き換える必要があります。

---

#### 手順

- 1 証明書の要求およびカスタム ルート証明書のインポート

会社のポリシーで中間 CA が許可されていない場合、VMCA で証明書を生成することはできません。エンタープライズまたはサードパーティ CA からのカスタム証明書を使用します。

## 2 カスタム証明書によるマシン SSL 証明書の置き換え

カスタム証明書を取得したら、各マシン証明書を置き換えることができます。

## 3 カスタム証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、VMCA 署名付きソリューション ユーザー証明書をサードパーティ証明書またはエンタープライズ証明書に置き換えることができます。

## 4 VMware ディレクトリ サービス証明書の置き換え

新しい VMCA ルート証明書を使用することを決定し、環境のプロビジョニング時に使用していた VMCA ルート証明書の発行を解除する場合、マシン SSL 証明書、ソリューション ユーザー証明書、およびいくつかの内部サービス用証明書を置き換える必要があります。

## 5 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

## 証明書の要求およびカスタム ルート証明書のインポート

会社のポリシーで中間 CA が許可されていない場合、VMCA で証明書を生成することはできません。エンタープライズまたはサードパーティ CA からのカスタム証明書を使用します。

### 前提条件

証明書は次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- ルート証明書の場合、認証局の拡張を true に設定する必要があり、証明書の署名を要件の一覧に含める必要があります。
- SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。
- CRT 形式
- キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。
- 現在時刻の 1 日前の開始時刻
- vCenter Server インベントリにある、ESXi ホストのホスト名（または IP アドレス）に設定された CN（および SubjectAltName）

### 手順

- 1 以下の証明書の CSR をエンタープライズまたはサードパーティ証明書プロバイダに送信します。

- 各マシンのマシン SSL 証明書。マシン SSL 証明書の場合、SubjectAltName フィールドには、完全修飾ドメイン名 (DNS NAME=*machine\_FQDN*) が含まれている必要があります。



- (オプション) 組み込みシステムまたは管理ノードごとに 4 つのソリューション ユーザー証明書。ソリューション ユーザー証明書には IP アドレス、ホスト名、電子メール アドレスを含めることはできません。証明書の Subject は、各証明書で異なっている必要があります。

通常、その結果は信頼されたチェーンの PEM ファイルで、Platform Services Controller または管理ノードごとの署名付き SSL 証明書も追加されます。

## 2 TRUSTED\_ROOTS およびマシン SSL ストアをリストします。

```
vecs-cli store list
```

- 現在のルート証明書とすべてのマシン SSL 証明書が VMCA によって署名されていることを確認します。
- シリアル番号、発行者、Subject の CN フィールドを書き留めておきます。
- (オプション) Web ブラウザを使用して、証明書を置き換えるノードへの HTTPS 接続を開き、証明書情報を参照して、マシン SSL 証明書と一致していることを確認します。

## 3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

### Windows

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

### vCenter Server Appliance

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

## 4 サードパーティ CA からの署名証明書であるカスタム ルート証明書を公開します。

```
dir-cli trustedcert publish --cert <my_custom_root>
```

コマンドラインでユーザー名とパスワードを指定しないと、指定するように求められます。

## 5 すべてのサービスを再開します。

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

### 次のステップ

元の VMCA ルート証明書は証明書ストアから削除できます (会社のポリシーで求められている場合)。削除する場合は、次の内部証明書を更新する必要があります。

- vCenter Single Sign-On 署名証明書を置き換えます。 [Security Token Service 証明書の更新](#) を参照してください。

- VMware ディレクトリ サービス証明書を置き換えます。[VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

## カスタム証明書によるマシン SSL 証明書の置き換え

カスタム証明書を取得したら、各マシン証明書を置き換えることができます。

各マシンには、他のサービスとの安全な通信を実現するため、マシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

証明書の置き換えを開始する前に、次の情報を確認しておく必要があります。

- `administrator@vsphere.local` のパスワード。
- 有効なマシン SSL カスタム証明書（.crt ファイル）。
- 有効なマシン SSL カスタム キー（.key ファイル）。
- ルートの有効なカスタム証明書（.crt ファイル）。
- マルチノード 環境内の外部の Platform Services Controller を使用する vCenter Server 上でこのコマンドを実行する場合は、Platform Services Controller の IP アドレス。

### 前提条件

サードパーティまたはエンタープライズ認証局から各マシンの証明書を取得している必要があります。

- キー サイズ : 2,048 ビット以上 (PEM エンコード)
- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。
- キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。

**手順**

- 1 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

**Windows**

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

**vCenter Server Appliance**

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

- 2 各ノードにログインし、取得した新しいマシン証明書を CA から VECS に追加します。

SSL を介して通信するには、すべてのマシンのローカル証明書ストアに、新しい証明書が必要です。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 すべてのサービスを再開します。

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

**例：カスタム証明書によるマシン SSL 証明書の置き換え**

各ノードのマシン SSL 証明書も同様に置き換えることができます。

- 1 最初に、VECS にある既存の証明書を削除します。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

- 2 次に置き換える証明書を追加します。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

**次のステップ**

使用している ESXi ホストの証明書を置き換えることもできます。『vSphere セキュリティ』ドキュメントを参照してください。

マルチノード デプロイでルート証明書を置き換えた後は、外部の Platform Services Controller ノードを使用するすべての vCenter Server 上でサービスを再起動する必要があります。

## カスタム証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、VMCA 署名付きソリューション ユーザー証明書をサードパーティ証明書またはエンタープライズ証明書に置き換えることができます。

ソリューション ユーザーは、vCenter Single Sign-On への認証を行うためだけに、証明書を使用します。証明書が有効な場合、vCenter Single Sign-On はソリューション ユーザーに SAML トークンを割り当てます。ソリューション ユーザーは、他の vCenter コンポーネントへの認証を行うために SAML トークンを使用します。

環境内で、ソリューション ユーザー証明書の置き換えが必要かどうかを考慮してください。ソリューション ユーザーはプロキシ サーバの内側に位置し、SSL トラフィックのセキュリティを確保するためにマシン SSL 証明書が使用されるため、ソリューション ユーザー証明書がセキュリティ上の懸念にならない場合もあります。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 Platform Services Controller がある管理ノードでコマンドを実行する場合は、`--server` パラメータを使用して Platform Services Controller を指定します。

---

**注：** 大規模なデプロイで、ソリューション ユーザー証明書をリストする場合は、`dir-cli list` の出力にすべてのノードのソリューション ユーザーが含まれます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

---

### 前提条件

- キー サイズ：2,048 ビット以上（PEM エンコード）
- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。
- 各ソリューション ユーザー証明書には異なる Subject が指定されている必要があります。たとえば、ソリューション ユーザー名（例：vpxd）などの一意の識別子を含めることができます。
- キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。

### 手順

- 1 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

## 2 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次のようになります。

```
C:\Program Files\VMware\VMware vCenter Server\vmaddd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、dir-cli リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。vmaddd-cli get-machine-id --server-name localhost を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

## 3 各ソリューション ユーザーの既存の証明書を、VECS、vmdir の順に置き換えます。

その順番で証明書を追加する必要があります。

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

**注：** vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On への認証ができません。

## 4 すべてのサービスを再開します。

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

## VMware ディレクトリ サービス証明書の置き換え

新しい VMCA ルート証明書を使用することを決定し、環境のプロビジョニング時に使用していた VMCA ルート証明書の発行を解除する場合、マシン SSL 証明書、ソリューション ユーザー証明書、およびいくつかの内部サービス用証明書を置き換える必要があります。

VMCA ルート証明書の発行を解除する場合は、vCenter Single Sign-On によって使われている SSL 署名証明書を置き換える必要があります。[Security Token Service 証明書の更新](#) を参照してください。また、VMware ディレクトリ サービス (vmdir) の証明書も置き換える必要があります。

### 前提条件

サードパーティ CA またはエンタープライズ CA に、vmdir の証明書を要求します。

## 手順

- 1 vmdir を停止します。

### Linux

```
service-control --stop vmdird
```

### Windows

```
service-control --stop VMWareDirectoryService
```

- 2 生成した証明書およびキーを、vmdir の場所にコピーします。

### Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

### Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 vSphere Web Client から、または service-control コマンドを使って、vmdir を再起動します。

### Linux

```
service-control --start vmdird
```

### Windows

```
service-control --start VMWareDirectoryService
```

## 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。

これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。

- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

**注：** サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

#### 手順

- 1 vCenter Single Sign-On 6.x サービスが実行されているノードで、vmdir SSL 証明書とキーを置き換えます。

[VMware ディレクトリ サービス証明書の置き換え](#)を参照してください。

- 2 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

- a C:\ProgramData\VMware\CIS\cfg\vmdir 内のすべてのファイルをバックアップします。
- b 6.x ノード上の vmDIRcert.pem ファイルのコピーを作成し、このコピーの名前を <sso\_node2.domain.com>.pem (<sso\_node2.domain.com> は 6.x ノードの FQDN) に変更します。
- c 名前を変更した証明書を C:\ProgramData\VMware\CIS\cfg\vmdir にコピーすることにより、既存の複製証明書を置き換えます。

- 3 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

サービスを vSphere Web Client から再起動することも、service-control コマンドを使用することもできます。

## CLI コマンドによる証明書とサービスの管理

CLI のセットを使用すると、VMCA (VMware Certificate Authority)、VECS (VMware Endpoint 証明書ストア)、および VMware Directory Service (vmdir) を管理できます。vSphere Certificate Manager ユーティリティは、数多くの関連タスクをサポートしていますが、手動の証明書管理には CLI が必要になります。

表 3-5. 証明書および関連サービスを管理する CLI ツール

CLI	説明	詳細については、ドキュメントを参照してください。
certool	証明書およびキーを生成および管理します。VMCA の一部です。	<a href="#">certool 初期化コマンド リファレンス</a>
vecs-cli	VMware 証明書ストア インスタンスのコンテナを管理します。VMAFD の一部です。	<a href="#">vecs-cli コマンド リファレンス</a>
dir-cli	VMware Directory Service に証明書を作成し更新します。VMAFD の一部です。	<a href="#">dir-cli コマンド リファレンス</a>
service-control	証明書の置換ワークフローの一部などで、サービスを開始または停止します。	

## 証明書管理ツールの場所

デフォルトでは、ツールは次の場所にあります。

### Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe  
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe  
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe  
VCENTER_INSTALL_PATH\bin\service-control
```

### Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli  
/usr/lib/vmware-vmafd/bin/dir-cli  
/usr/lib/vmware-vmca/bin/certool
```

Linux では、`service-control` コマンドでパスを指定する必要はありません。

外部 Platform Services Controller を使用する管理ノードからコマンドを実行する場合、`--server` パラメータを使用して Platform Services Controller を指定できます。

## 証明書管理の操作に必要な権限

ほとんどの vCenter 証明書の管理操作では、ユーザーが `vsphere.local` ドメインの `CAAdmins` グループに属している必要があります。`administrator@vsphere.local` ユーザーは `CAAdmins` グループに属しています。一部の操作はすべてのユーザーに許可されています。

vCenter Certificate Manager ユーティリティを実行する場合、`administrator@vsphere.local` のパスワードを求められます。証明書を手動で置き換える場合は、証明書管理 CLI のオプションに応じて特定の権限が必要になります。

### dir-cli

`vsphere.local` ドメインの `CAAdmins` グループのメンバーである必要があります。`dir-cli` コマンドは、実行するたびにユーザー名とパスワードを求められます。

### vecs-cli

初期設定では、ストア オーナーにのみ、ストアへのアクセス権があります。ストア オーナーは Windows システムでは管理者ユーザーで、Linux システムではルート ユーザーです。ストア オーナーは他のユーザーにアクセス権を提供することができます。

`MACHINE_SSL_CERT` および `TRUSTED_ROOTS` ストアは特別なストアです。インストールのタイプによっては、ルート ユーザーまたは管理者ユーザーにのみ完全なアクセス権があります。

### certool



ほとんどの `certool` コマンドでは、ユーザーが `CAAdmins` グループに属している必要があります。  
`administrator@vsphere.local` ユーザーは `CAAdmins` グループに属しています。以下のコマンドはすべてのユーザーが実行できます。

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

ESXi ホストの証明書の管理には、証明書.証明書を管理 権限が必要です。権限は vSphere Web Client から設定できます。

## certool 構成の変更

`certool --gencert` と他の特定の証明書の初期化または管理コマンドを実行する場合、CLI は構成ファイルからすべての値を読み取ります。既存のファイルを編集したり、`--config=<file name>` オプションを使用してデフォルトの構成ファイル (`certool.cfg`) にオーバーライドしたり、コマンドラインのさまざまな値にオーバーライドしたりできます。

この構成ファイルには、以下のデフォルト値を持つ複数のフィールドがあります。

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

構成ファイルの値は以下のように変更できます。

- 構成ファイルのバックアップを作成し、ファイルを編集します。デフォルトの構成ファイルを使用している場合、指定する必要はありません。それ以外の場合、たとえば構成ファイルの名前を変更した場合などには、`--config` コマンドライン オプションを使用します。
- コマンドラインで構成ファイルの値をオーバーライドします。たとえば、`Locality` をオーバーライドするには次のコマンドを実行します。

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```

--Name を指定して証明書の Subject 名の CN フィールドを置き換えます。

- ソリューション ユーザー証明書の場合、規則に従って名前が <sol\_user name>@<domain> になりますが、お使いの環境で別の規則を使用している場合には名前を変更できます。
- マシン SSL 証明書の場合、SSL クライアントは、マシンのホスト名の検証時に証明書の Subject 名の CN フィールドを確認するため、マシンの FQDN が使用されます。マシンは複数のエイリアスを持つことができるため、証明書には別の名前（DNS 名、IP アドレスなど）を指定できる Subject Alternative Name フィールドの拡張があります。ただし、VMCA には DNSName（Hostname フィールド内）があるのみで他のエイリアス オプションは許容されません。ユーザーによって IP アドレスが指定されていると、SubAltName に同様に格納されます。

--Hostname パラメータは証明書の SubAltName の DNSName を指定するのに使用されます。

## certool 初期化コマンド リファレンス

certool 初期化コマンドにより証明書の署名要求の生成、VMCA によって署名された証明書およびキーの表示および生成、ルート証明書のインポート、およびその他の証明書管理操作を実行することができます。

多くの場合、構成ファイルを certool コマンドに渡します。[certool 構成の変更](#) を参照してください。使用例については、[新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え](#) を参照してください。

### certool --initcsr

証明書署名要求 (CSR) を生成します。このコマンドは、PKCS10 ファイルとプライベート キーを生成します。

オプション	説明
--initcsr	CSR を生成する場合に必要です。
--privkey <key_file>	プライベート キー ファイルの名前。
--pubkey <key_file>	パブリック キー ファイルの名前。
--csrfile <csr_file>	CA プロバイダに送信される CSR ファイルのファイル名。
--config <config_file>	構成ファイルのオプション名。デフォルトの名前は certool.cfg です。

例：

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

### certool --selfca

自己署名証明書を作成し、自己署名ルート CA により VMCA サーバをプロビジョニングします。このオプションを使用する方法は、VMCA サーバをプロビジョニングするための最も簡単な方法の 1 つです。代わりに、VMCA が中間 CA となるように、サードパーティのルート証明書によって VMCA サーバをプロビジョニングすることができます。[中間認証局としての VMCA の使用](#) を参照してください。

このコマンドにより、タイム ゾーンの競合を避けるため、3 日前の日付の証明書が生成されます。

オプション	説明
--selfca	自己署名証明書を生成する場合に必要です。
--predate <number_of_minutes>	ルート証明書の [有効期間の開始日] フィールドを、現在時刻より前の指定の時間（分単位）に設定することができます。このオプションは、潜在的なタイムゾーンの問題に対処するのに役立ちます。最大値は 3 日です。
--config <config_file>	構成ファイルのオプション名。デフォルトの名前は certtool.cfg です。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280 --selfca --server=192.0.2.24 --srp-upn=administrator@vsphere.local
```

## certool --rootca

ルート証明書をインポートします。指定した証明書およびプライベート キーを VMCA に追加します。VMCA は常に、署名に最新のルート証明書を使用しますが、その他のルート証明書も引き続き使用できます。つまり、一度に 1 段階ずつインフラストラクチャを更新し、最後に使用しなくなった証明書を削除できます。

オプション	説明
--rootca	ルート CA をインポートするために必要です。
--cert <certfile>	構成ファイルのオプション名。デフォルトの名前は certtool.cfg です。
--privkey <key_file>	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

## certool --getdc

vmdir によって使用されるデフォルトのドメイン名を戻します。

オプション	説明
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
--port <port_num>	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --getdc
```

## certool --waitVMDIR

VMware ディレクトリ サービスが稼動し始めるか、--wait によって指定されたタイムアウト時間が経過するまで待機します。他のオプションと関連付けてこのオプションを使用し、デフォルトのドメイン名を返すなど特定のタスクをスケジュールします。

オプション	説明
--wait	オプションで指定する待機時間（分）。デフォルトは 3 です。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
--port <port_num>	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --waitVMDIR --wait 5
```

## certool --waitVMCA

VMCA サービスが稼動し始めるか、指定されたタイムアウト時間が経過するまで待機します。他のオプションと関連付けてこのオプションを使用し、証明書を生成するなど特定のタスクをスケジュールします。

オプション	説明
--wait	オプションで指定する待機時間（分）。デフォルトは 3 です。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
--port <port_num>	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --waitVMCA --selfca
```

## certool --publish-roots

ルート証明書の更新を強制的に実行します。このコマンドには管理権限が必要です。

オプション	説明
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --publish-roots
```

## certool 管理コマンド リファレンス

certool 管理コマンドを使用すると、証明書の表示、生成、および失効や、証明書情報の表示を行うことができます。

### certool --genkey

プライベート キーとパブリック キーのペアを生成します。これらのファイルを使用して、VMCA が署名する証明書を生成できます。その証明書を使用すると、マシンやソリューション ユーザーをプロビジョニングできます。

オプション	説明
--genkey	プライベート キーとパブリック キーの生成に必要です。
--privkey <keyfile>	プライベート キー ファイルの名前。
--pubkey <keyfile>	パブリック キー ファイルの名前。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

### certool --gencert

VMCA サーバからの証明書を生成します。このコマンドでは、certool.cfg または指定された構成ファイルの情報が使用されます。

オプション	説明
--gencert	証明書の生成に必要です。
--cert <certfile>	証明書ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
--privkey <keyfile>	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
--config <config_file>	構成ファイルのオプション名。デフォルトの名前は certool.cfg です。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

## certool --getrootca

人間が解読可能な形式で、現在のルート CA 証明書を出力します。管理ノードからこのコマンドを実行する場合は、Platform Services Controller ノードのマシン名を使用して、ルート CA を取得します。この出力は証明書として使用できず、人間が解読可能な形式に変換されます。

オプション	説明
<code>--getrootca</code>	ルート証明書の出力に必要です。
<code>--server &lt;server&gt;</code>	VMCA サーバのオプション名。このコマンドでは、デフォルトで <code>localhost</code> を使用します。

例：

```
certool --getrootca --server=remoteserver
```

## certool --viewcert

人間が解読可能な形式で、証明書内のすべてのフィールドを出力します。

オプション	説明
<code>--viewcert</code>	証明書の表示に必要です。
<code>--cert &lt;certfile&gt;</code>	構成ファイルのオプション名。デフォルトの名前は <code>certool.cfg</code> です。

例：

```
certool --viewcert --cert=<filename>
```

## certool --enumcert

VMCA サーバが認識しているすべての証明書を一覧表示します。必須の `filter` オプションを使用すると、すべての証明書、失効している証明書のみ、アクティブな証明書のみ、または期限切れの証明書のみのリストを表示できます。

オプション	説明
<code>--enumcert</code>	すべての証明書のリストの表示に必要です。
<code>--filter [all   active]</code>	<code>filter</code> は必須です。all または active を指定します。現在、revoked および expired のオプションはサポートされていません。

例：

```
certool --enumcert --filter=active
```

## certool --status

指定された証明書を VMCA サーバに送信して、証明書が失効しているかどうかを確認します。証明書が失効している場合は [証明書：失効] が出力され、それ以外の場合は [証明書：アクティブ] が出力されます。

オプション	説明
--status	証明書のステータスの確認に必要です。
--cert <certfile>	構成ファイルのオプション名。デフォルトの名前は certtool.cfg です。
--server <server>	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certtool --status --cert=<filename>
```

## certtool --genselfcert

構成ファイルの値に基づいて、自己署名証明書を生成します。このコマンドにより、タイム ゾーンの競合を避けるため、3 日前の日付の証明書が生成されます。

オプション	説明
--genselfcert	自己署名証明書を生成する場合に必要です。
--outcert <cert_file>	証明書ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
--outprivkey <key_file>	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
--config <config_file>	構成ファイルのオプション名。デフォルトの名前は certtool.cfg です。

例：

```
certtool --genselfcert --privkey=<filename> --cert=<filename>
```

## vecs-cli コマンド リファレンス

vecs-cli コマンド セットを使用すると、VMware 証明書ストア (VECS) インスタンスを管理できます。証明書 インフラストラクチャを管理する場合は、次のコマンドを dir-cli および certtool と併用します。

### vecs-cli store create

証明書ストアを作成します。

オプション	説明
--name <名前>	証明書ストアの名前。

例：

```
vecs-cli store create --name <store>
```

## vecs-cli store delete

証明書ストアを削除します。システムによって事前定義された証明書ストアは削除できません。

オプション	説明
--name <名前>	削除する証明書ストアの名前。

例：

```
vecs-cli store delete --name <store>
```

## vecs-cli store list

証明書ストアのリストを表示します。

VECS には、次のストアが含まれます。

表 3-6. VECS 内のストア

ストア	説明
マシン SSL ストア (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> <li>■ 各 vSphere ノード上のリバースプロキシ サービスにより使用されます。</li> <li>■ 組み込みデプロイおよび各 Platform Services Controller ノード上の VMware ディレクトリ サービス (vmdir) によって使用されます。</li> </ul> <p>vSphere 6.0 のすべてのサービスは、リバース プロキシを介して通信を行っており、ここで、マシン SSL 証明書が使用されます。下位互換性を保つため、5.x サービスでは特定のポートが引き続き使用されています。その結果、vpxd などの一部のサービスでは、自身のポートが開かれたままになっています。</p>
信頼されたルート ストア (TRUSTED_ROOTS)	すべての信頼済みルート証明書を含みます。



表 3-6. VECS 内のストア（続き）

ストア	説明
ソリューション ユーザー ストア <ul style="list-style-type: none"> <li>■ マシン</li> <li>■ vpxd</li> <li>■ vpxd-extensions</li> <li>■ vsphere-webclient</li> </ul>	<p>VECS には、ソリューション ユーザーごとに 1 つのストアが含まれます。各ソリューション ユーザー証明書の件名は一意でなければなりません。たとえば、マシン証明書には vpxd 証明書と同じ件名を指定できません。</p> <p>ソリューション ユーザー証明書は、vCenter Single Sign-On での認証に使用されます。vCenter Single Sign-On は、証明書が有効であることを確認しますが、その他の証明書の属性は確認しません。組み込みのデプロイでは、すべてのソリューション ユーザー証明書が同じシステム上に存在します。</p> <p>次のソリューション ユーザー証明書ストアが、各管理ノードと各組み込みデプロイの VECS に含まれています。</p> <ul style="list-style-type: none"> <li>■ <code>machine</code> : Component Manager、ライセンス サーバ、およびログ サービスにより使用されます。</li> </ul> <p><b>注：</b> マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は SAML トークン交換に使用される一方、マシン SSL 証明書はマシン向けのセキュリティで保護された SSL 接続に使用されます。</p> <ul style="list-style-type: none"> <li>■ <code>vpxd</code> : 管理ノードおよび組み込みデプロイ上の、vCenter サービスデーモン (vpxd) ストア。vpxd は、このストアに格納されているソリューション ユーザー証明書を使用して、vCenter Single Sign-On への認証を行います。</li> <li>■ <code>vpxd-extensions</code> : vCenter の拡張機能のストア。Auto Deploy サービス、Inventory Service、およびその他のソリューション ユーザーに含まれないその他のサービス。</li> <li>■ <code>vsphere-webclient</code> : vSphere Web Client ストア。パフォーマンス チャート サービスなどの一部の追加サービスも含まれます。</li> </ul> <p>マシン ストアは、各 Platform Services Controller ノードにも含まれています。</p>
vSphere Certificate Manager ユーティリティのバックアップ ストア (BACKUP_STORE)	<p>証明書の取り消しをサポートするために、VMCA (VMware Certificate Manager) によって使用されます。最新の状態のみがバックアップとして保存され、1 段階より多く戻ることはできません。</p>
その他のストア	<p>その他のストアが、ソリューションによって追加される場合があります。たとえば、仮想ポリューム ソリューションにより SMS ストアが追加されます。VMware ドキュメントまたは当社のナレッジ ベースで指示されないかぎり、ストア内の証明書を変更しないでください。</p> <p><b>注：</b> vSphere 6.0 では CRLS はサポートされませんが、TRUSTED_ROOTS_CRLS ストアを削除すると、証明書インフラストラクチャが破損する可能性があります。TRUSTED_ROOTS_CRLS ストアの削除や修正は行わないでください。</p>

例：

```
vecs-cli store list
```

## vecs-cli store permissions

ストアに対するアクセス許可を付与または破棄します。--grant オプションまたは --revoke オプションを使用します。

ストアの所有者は、アクセス許可の付与、破棄など、所有するストアのあらゆる制御を行うことができます。管理者は、アクセス許可の付与、破棄など、すべてのストアに対する権限を持っています。

vecs-cli get-permissions --name <ストア名> を使用して、ストアの現在の設定を取得できます。

オプション	説明
--name <名前>	証明書ストアの名前。
--user <ユーザー名>	アクセス許可が付与されるユーザーの一意の名前。
--grant [read write]	付与するアクセス許可（読み取りまたは書き込み）。
--revoke [read write]	破棄するアクセス許可（読み取りまたは書き込み）。現在サポートされていません。

## vecs-cli entry create

VECS にエントリを作成します。このコマンドを使用して、プライベート キーまたは証明書をストアに追加します。

オプション	説明
--store <NameOfStore>	証明書ストアの名前。
--alias <Alias>	証明書のオプションのエイリアス。このオプションは、信頼されたルート ストアには無視されます。
--cert <certificate_file_path>	証明書ファイルのフル パス。
--key <key-file-path>	証明書に対応するキーのフル パス。 任意。

## vecs-cli entry list

指定したストア内のすべてのエントリのリストを表示します。

オプション	説明
--store <NameOfStore>	証明書ストアの名前。
--text	人間が解読可能な証明書のバージョンを表示します。

## vecs-cli entry getcert

VECS から証明書を取得します。証明書を出力ファイルに送信するか、人間が解読可能なテキストとして表示できます。

オプション	説明
--store <NameOfStore>	証明書ストアの名前。
--alias <Alias>	証明書のエイリアス。
--output <出力ファイルのパス>	証明書を書き込むファイル。
--text	人間が解読可能な証明書のバージョンを表示します。

## vecs-cli entry getkey

VECS に格納されているキーを取得します。証明書出力ファイルに送信するか、人間が解読可能なテキストとして表示できます。

オプション	説明
--store <NameOfStore>	証明書ストアの名前。
--alias <Alias>	キーのエイリアス。
--output <出力ファイルのパス>	キーを書き込む出力ファイル。
--text	人間が解読可能なキーのバージョンを表示します。

## vecs-cli entry delete

証明書ストア内のエントリを削除します。VECS 内のエントリを削除すると、そのエントリは VECS から完全に削除されます。唯一の例外は、現在のルート証明書です。VECS は vmdir をポーリングして、ルート証明書を確認します。

オプション	説明
--store <NameOfStore>	証明書ストアの名前。
--alias <Alias>	削除するエントリのエイリアス。

## vecs-cli force-refresh

vecs-cli を強制的に更新します。このとき、vecs-cli は、vmdir 内の最新情報を使用するように更新されます。デフォルトでは、VECS は 5 分ごとに vmdir をポーリングして、新しいルート証明書を確認します。vmdir 内の VECS を直ちに更新する場合は、このコマンドを使用します。

## dir-cli コマンド リファレンス

dir-cli ユーティリティでは、ソリューション ユーザーの作成および更新、他のユーザー アカウントの作成、vmdir の証明書やパスワードの管理を行うことができます。vecs-cli および certool とともにこのユーティリティを使用して、証明書インフラストラクチャを管理します。

## dir-cli service create

ソリューション ユーザーを作成します。主にサードパーティ製ソリューションで使用されます。

オプション	説明
--name <名前>	作成するソリューション ユーザーの名前。
--cert <証明書ファイル>	証明書ファイルへのパス。これは、VMCA で署名された証明書またはサードパーティ証明書を指定できます。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli service list

dir-cli で認識されるソリューション ユーザーをリストします。

オプション	説明
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli service delete

vmdir のソリューション ユーザーを削除します。ソリューション ユーザーを削除すると、vmdir のこのインスタンスを使用するすべての管理ノードで、関連するサービスがすべて使用できなくなります。

オプション	説明
--name	削除するソリューション ユーザーの名前。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli service update

指定したソリューション ユーザー（つまり、サービスのコレクション）の証明書を更新します。このコマンドを実行すると、5 分後に VECS によって変更が取得されます。または、vecs-cli force-refresh を使用して強制的に更新することもできます。

オプション	説明
--name <名前>	更新するソリューション ユーザーの名前。
--cert <証明書ファイル>	サービスに割り当てる証明書の名前。

オプション	説明
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli user create

vmdir 内に一般ユーザーを作成します。このコマンドは、ユーザー名とパスワードを使用して vCenter Single Sign-On の認証を受けるユーザー（人）に使用できます。このコマンドは、プロトタイピング時にのみ使用します。

オプション	説明
--account <名前>	作成する vCenter Single Sign-On ユーザーの名前。
--user-password <パスワード>	ユーザーの初期パスワード。
--first-name <名前>	ユーザーの名。
--last-name <名前>	ユーザーの姓。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli user delete

vmdir 内の指定したユーザーを削除します。

オプション	説明
--account <名前>	削除する vCenter Single Sign-On ユーザーの名前。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli group modify

すでに存在するグループにユーザーまたはグループを追加します。

オプション	説明
--name <名前>	vmdir のグループの名前。
--add <ユーザーまたはグループの名前>	追加するユーザーまたはグループの名前。

オプション	説明
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli group list

指定した vmdir グループをリストします。

オプション	説明
--name <名前>	vmdir のグループのオプション名。このオプションでは、グループが存在するかどうかを確認できます。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli trustedcert publish

信頼済みルート証明書を vmdir に発行します。

オプション	説明
--cert <ファイル>	証明書ファイルへのパス。
--login <admin_user_id>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli trustedcert unpublish

現在 vmdir にある信頼済みルート証明書を発行解除します。たとえば、現在の使用環境の他のすべての証明書のルート証明書となっている別のルート証明書を vmdir に追加した場合、このコマンドを使用します。使用されなくなった証明書の発行解除は、使用環境の堅牢化に寄与します。

オプション	説明
--cert-file <ファイル>	発行解除する証明書ファイルへのパス。
--crl <ファイル>	この証明書に関連付けられている CRL ファイルへのパス。現在使用されていません。

オプション	説明
<code>--login &lt;admin_user_id&gt;</code>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
<code>--password &lt;admin_password&gt;</code>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli trustedcert list

すべての信頼済みルート証明書と対応する ID をリストします。dir-cli trustedcert get を使用して証明書を取得するには、証明書 ID が必要です。

オプション	説明
<code>--login &lt;admin_user_id&gt;</code>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
<code>--password &lt;admin_password&gt;</code>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli trustedcert get

vmdir から信頼済みルート証明書を取得し、指定したファイルに書き込みます。

オプション	説明
<code>--id &lt;証明書 ID&gt;</code>	取得する証明書の ID。ID は、dir-cli trustedcert list コマンドで表示されます。
<code>--outcert &lt;パス&gt;</code>	証明書ファイルの書き込み先のパス。
<code>--outcrl &lt;パス&gt;</code>	CRL ファイルの書き込み先のパス。現在使用されていません。
<code>--login &lt;admin_user_id&gt;</code>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
<code>--password &lt;admin_password&gt;</code>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli password create

パスワード要件を満たしているランダムなパスワードを作成します。このコマンドは、サードパーティ製ソリューション ユーザーが使用できます。

オプション	説明
<code>--login &lt;admin_user_id&gt;</code>	デフォルトでは、administrator@vsphere.local。この管理者が、他のユーザーを CAAdmins vCenter Single Sign-On グループに追加して、それらのユーザーに管理者権限を付与できます。
<code>--password &lt;admin_password&gt;</code>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli password reset

管理者がユーザーのパスワードをリセットできるようにします。管理者以外のユーザーがパスワードをリセットするには、代わりに `dir-cli password change` を使用します。

オプション	説明
<code>--account</code>	新しいパスワードを割り当てるアカウントの名前。
<code>--new</code>	指定されたユーザーの新しいパスワード。
<code>--login &lt;admin_user_id&gt;</code>	デフォルトでは、 <code>administrator@vsphere.local</code> 。この管理者が、他のユーザーを <code>CAAdmins vCenter Single Sign-On</code> グループに追加して、それらのユーザーに管理者権限を付与できます。
<code>--password &lt;admin_password&gt;</code>	管理者ユーザーのパスワード。パスワードを指定しないと、入力を求められます。

## dir-cli password change

ユーザーがパスワードを変更できるようにします。この変更を行うアカウントを所有するユーザーである必要があります。管理者は `dir-cli password reset` を使用して、パスワードをリセットできます。

オプション	説明
<code>--account</code>	アカウント名。
<code>--current</code>	アカウントを所有するユーザーの現在のパスワード。
<code>--new</code>	アカウントを所有するユーザーの新しいパスワード。

## vSphere Web Client での vCenter 証明書の表示

vCenter Certificate Authority (VMCA) に認識されている証明書を表示して、有効な証明書の有効期限が近付いているかどうかを確認したり、有効期限切れの証明書を参照したり、ルート証明書のステータスを確認したりできます。すべての証明書管理タスクは、証明書の CLI を使用して実行します。

組み込みデプロイまたは Platform Services Controller に含まれている VMCA インスタンスに関連付けられた証明書を表示します。証明書の情報は VMware Directory Service (vmdir) のインスタンス全体にレプリケートされます。

vSphere Web Client で証明書を表示しようとすると、ユーザー名とパスワードを求められます。VMware 認証局の権限を持つユーザー、すなわち `CAAdmins vCenter Single Sign-On` グループのユーザーのユーザー名とパスワードを指定します。

### 手順

- 1 vCenter Server に `administrator@vsphere.local` または `CAAdmins vCenter Single Sign-On` グループの他のユーザーとしてログインします。
- 2 [管理] を選択し、[デプロイ] をクリックして、[システム構成] をクリックします。
- 3 [ノード] をクリックし、証明書を表示または管理する対象ノードを選択します。



- 4 [管理] タブをクリックし、[認証局] をクリックします。
- 5 証明書情報を表示する証明書のタイプをクリックします。

オプション	説明
有効な証明書	有効な証明書を、検証情報とともに表示します。緑の [有効期間の終了] アイコンは、証明書の有効期限が近付くと変化します。
失効した証明書	失効した証明書のリストを表示します。今回のリリースではサポートされていません。
有効期限の切れた証明書	有効期限の切れた証明書を表示します。
ルート証明書	vCenter Certificate Authority の、このインスタンスで使用可能なルート証明書を表示します。

- 6 証明書を選択して [証明書の詳細の表示] ボタンをクリックして証明書の詳細を表示します。  
詳細には Subject Name、Issuer、Validity および Algorithm が含まれています。

## vCenter 証明書の有効期限の警告に対するしきい値の設定

vSphere 6.0 以降では、vCenter Server は VMware Endpoint Certificate Store (VECS) にあるすべての証明書を監視し、証明書が有効期限まで 30 日以内になるとアラームを発行します。警告を受けるタイミングは `vpzd.cert.threshold` 詳細オプションを使用して変更できます。

### 手順

- 1 vSphere Web Client にログインします。
- 2 vCenter Server オブジェクトを選択してから、[管理] タブと [設定] サブタブを選択します。
- 3 [詳細設定] をクリックし、[編集] を選択して、しきい値でフィルタリングします。
- 4 `vpzd.cert.threshold` の設定を任意の値に変更し、[OK] をクリックします。

# vSphere のアクセス許可とユーザー管理タスク

# 4

vCenter Single Sign-On は認証をサポートします。すなわち、ユーザーが vSphere コンポーネントにアクセスできるかどうかを全面的に決定します。さらに、各ユーザーは vSphere オブジェクトを表示または操作する際にも認証が必要です。

vSphere では、さまざまな認可メカニズムがサポートされています。詳細は、[vSphere での認可について](#)を参照してください。このセクションでは、vCenter Server のアクセス許可モデルとユーザー管理タスクの実行方法に焦点を絞って説明します。

vCenter Server では、権限とロールを使用したきめ細かい認可が可能です。vCenter Server オブジェクト階層内のオブジェクトにアクセス許可を設定する際には、ユーザーまたはグループがそのオブジェクトに対して所有する権限を指定します。権限を指定するには、ロール、すなわち権限のセットを使用します。

インストール直後は、ユーザー administrator@vsphere.local だけが、vCenter Server システムにログインする権限を付与されます。ログイン権限を与えられた administrator@vsphere.local は、以下の手順を実行します。

- 1 追加のユーザーおよびグループが定義されたアイデンティティ ソースを vCenter Single Sign-On に追加します。 [vCenter Single Sign-On アイデンティティ ソースの追加](#)を参照してください。
- 2 ユーザーまたはグループに権限を付与します。具体的には、仮想マシンまたは vCenter Server システムなどのオブジェクトを選択し、そのオブジェクトに対するロールをユーザーまたはグループに割り当てます。



ロール、権限、アクセス許可

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_8vla7txu/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/))

この章には、次のトピックが含まれています。

- [vSphere での認可について](#)
- [vCenter Server のアクセス許可モデルについて](#)
- [権限の階層的な継承](#)
- [複数の権限の設定](#)
- [vCenter コンポーネントの権限の管理](#)
- [グローバル権限](#)
- [ロールを使用した権限の割り当て](#)
- [ロールと権限のベスト プラクティス](#)
- [一般的なタスクに必要な権限](#)

## vSphere での認可について

vSphere のユーザーまたはグループを認可する主な方法は、vCenter Server アクセス許可を使用する方法です。実行するタスクによっては、他の認可が必要になることがあります。

vSphere 6.0 以降では、権限のあるユーザーが、次の方法で他のユーザーにアクセス許可を付与してタスクを実行します。これらの方法は、大部分が相互に排他的です。ただしグローバル権限を使用すると、すべてのソリューションに対して特定のユーザーを認可できます。またローカルな vCenter Server アクセス許可を使用すると、個々の vCenter Server システムに対して他のユーザーを認可できます。

### vCenter Server のアクセス許可

vCenter Server システムのアクセス許可モデルは、その vCenter Server のオブジェクト階層内のオブジェクトにアクセス許可を割り当てることによって成立しています。各アクセス許可によって、1 人のユーザーまたは 1 つのグループに権限のセット、すなわち、選択したオブジェクトのロールが付与されます。たとえば、ESXi ホストを選択してユーザーのグループにロールを割り当てて、そのホストに対応する権限をユーザーに付与することができます。

### グローバル権限

グローバル権限は、複数のソリューションに対応するグローバル ルート オブジェクトに適用されます。たとえば、vCenter Server と vCenter Orchestrator の両方がインストールされている場合は、グローバル権限を使用して、両方のオブジェクト階層内のすべてのオブジェクトにアクセス許可を付与できます。

グローバル権限は、vsphere.local ドメイン間で複製されます。グローバル権限では、vsphere.local グループで管理されているサービスを認証しません。[グローバル権限](#) を参照してください。

### vsphere.local グループにおけるグループ メンバーシップ

administrator@vsphere.local ユーザーは、Platform Services Controller に含まれるサービスに関連付けられているタスクを実行できます。さらに、vsphere.local グループのメンバーは該当するタスクを実行できます。たとえば、LicenseService.Administrators グループのメンバーであれば、ライセンス管理を実行できます。[vsphere.local ドメイン内のグループ](#) を参照してください。

### ESXi ローカル ホストのアクセス許可

vCenter Server システムに管理されないスタンドアロンの ESXi ホストを管理している場合は、事前定義されたロールの 1 つをユーザーに割り当てることができます。『vSphere Client による vSphere 管理』ドキュメントを参照してください。

## vCenter Server のアクセス許可モデルについて

vCenter Server システムのアクセス許可モデルは、vSphere オブジェクト階層内のオブジェクトにアクセス許可を割り当てることによって成立しています。各アクセス許可によって、1 人のユーザーまたは 1 つのグループに権限のセット、すなわち、選択したオブジェクトのロールが付与されます。

次の概念を理解する必要があります。

### 権限

vCenter Server オブジェクト階層内の各オブジェクトには、関連付けられた権限があります。各権限には、そのオブジェクトに対してグループまたはユーザーに設定される権限が、グループまたはユーザーごとに指定されます。

## ユーザーおよびグループ

vCenter Server システムでは、認証されたユーザーまたは認証されたユーザーのグループに対してのみ権限を割り当てることができます。ユーザーは vCenter Single Sign-On を介して認証されます。ユーザーとグループは、vCenter Single Sign-On が認証するのに使用するアイデンティティ ソースで定義されている必要があります。Active Directory などのアイデンティティ ソース内のツールを使用して、ユーザーとグループを定義します。

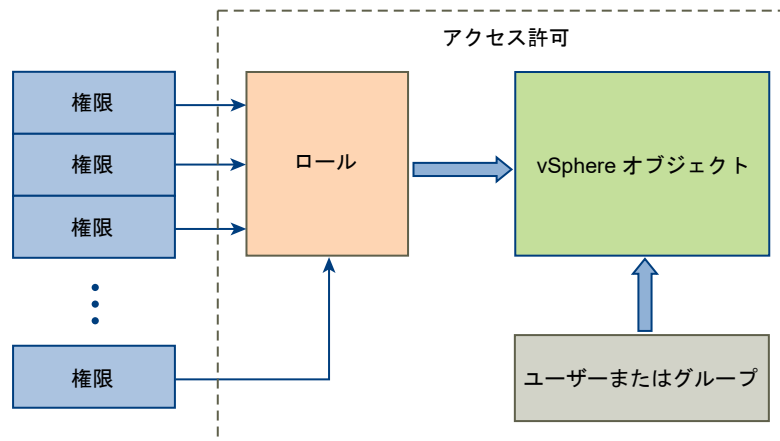
## ロール

ロールにより、ユーザーが実行する標準的なタスクのセットに基づいて、オブジェクトでのアクセス許可を割り当てることができます。管理者などのデフォルト ロールは vCenter Server で事前定義済みであり、変更できません。リソース プール管理者などのその他のロールは、事前定義されたサンプル ロールです。一から、またはサンプル ロールをクローン作成して変更することで、カスタム ロールを作成できます。

## 権限

権限は、きめ細かなアクセス制御です。このような権限をロールにグループ化することができ、これにより、ユーザーやグループにマップすることができます。

図 4-1. vSphere のアクセス許可



アクセス許可をオブジェクトに割り当てるには、次の手順に従います。

- 1 vCenter オブジェクト階層内でアクセス許可を適用するオブジェクトを選択します。
- 2 そのオブジェクトに対するアクセス許可を必要とするグループまたはユーザーを選択します。
- 3 グループまたはユーザーがオブジェクトに対して持つ必要があるロール、つまり権限のセットを選択します。デフォルトでは、アクセス許可は伝播されます。つまり、グループまたはユーザーには、選択したオブジェクトおよびその子オブジェクトに対して、選択したロールが割り当てられます。

アクセス許可モデルでは、事前定義のロールが提供されており、作業を迅速に行うことができます。権限を組み合わせ、カスタムのロールを作成することもできます。すべての権限、および権限を適用できるオブジェクトのリファレンスについては、[11 章 事前定義された権限](#)を参照してください。これらのタスクを実行するために必要な権限のセットの例については、[一般的なタスクに必要な権限](#)を参照してください。

多くの場合、アクセス許可はソース オブジェクトとターゲット オブジェクトの両方で定義する必要があります。たとえば、仮想マシンを移動する場合、その仮想マシンに対する権限が必要ですが、ターゲットのデータセンターに対する権限も必要になります。

スタンドアロンの ESXi ホストのアクセス許可モデルは、これより簡単です。を参照してください。 [ESXi への権限の割り当て](#)

## vCenter Server のユーザー検証

ディレクトリ サービスを使用している vCenter Server システムは、ユーザー ディレクトリのドメインに対するユーザーとグループの検証を定期的に行います。vCenter Server の設定で指定された定期的な間隔で検証が実行されます。たとえば、Smith というユーザーがいくつかのオブジェクトに対するロールを割り当てられており、ドメインでそのユーザー名が Smith2 に変更された場合、ホストは Smith が存在しなくなったと見なし、次の検証時に、Smith に関連付けられたアクセス許可を vSphere オブジェクトから削除します。

同様に、Smith というユーザーがドメインから削除された場合、次の検証時に、Smith に関連付けられたすべてのアクセス許可が削除されます。次の検証前に Smith という新しいユーザーがドメインに追加された場合、すべてのオブジェクトに対するアクセス許可において、古いユーザーの Smith が新しいユーザーの Smith で置換されません。

## 権限の階層的な継承

オブジェクトに権限を割り当てるときに、オブジェクト階層の下に向かって権限を伝達するかどうかを選択できます。伝達は、権限ごとに設定します。伝達は、全体的には適用されません。子オブジェクトに定義された権限は、親オブジェクトから伝達された権限を常にオーバーライドします。

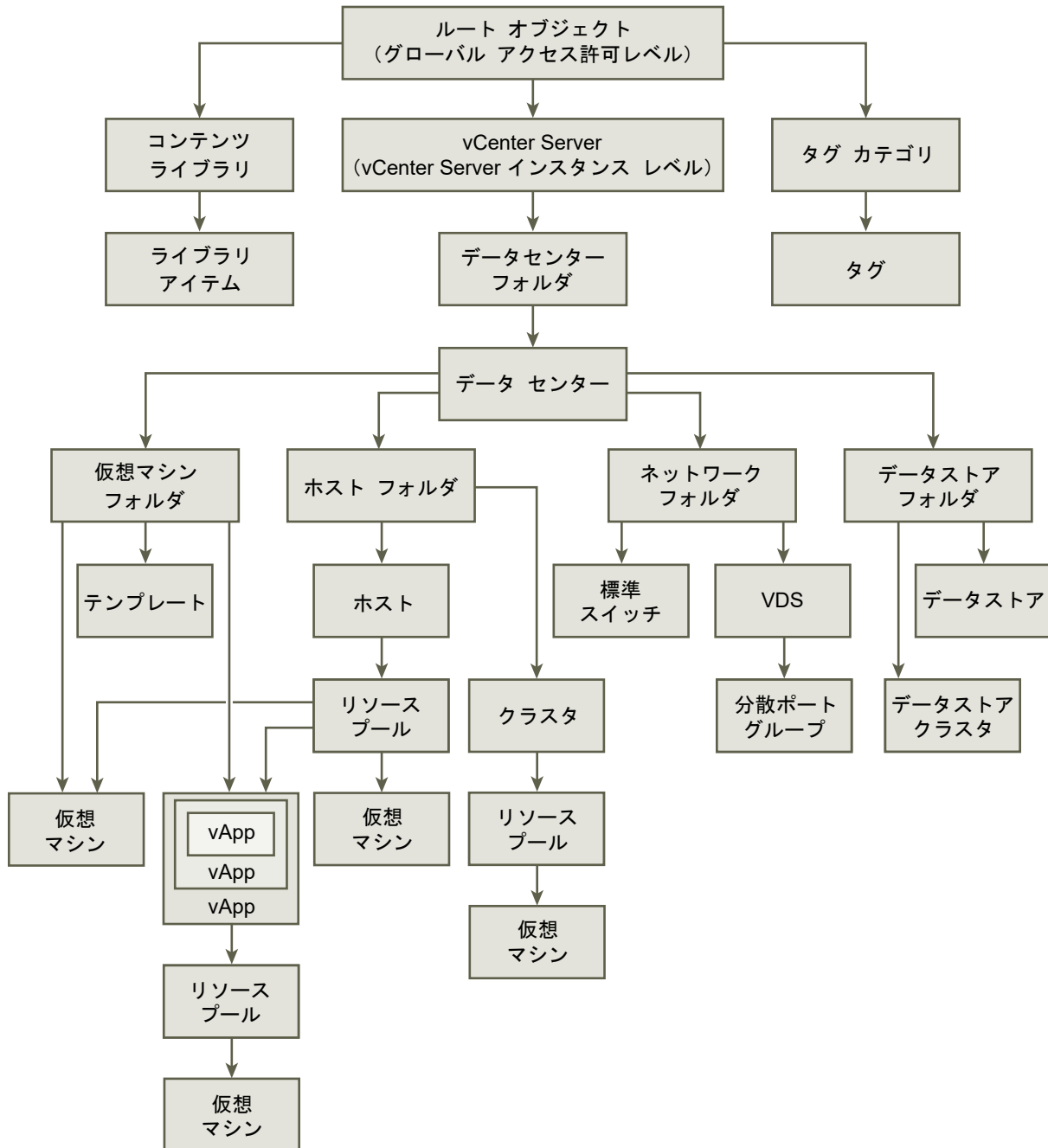
次の図に、vSphere のインベントリ階層と、権限を伝達できるパスを示します。

---

**注：** グローバル権限では、グローバル ルート オブジェクトから複数のソリューションに渡り権限を割り当てることができます。 [グローバル権限](#) を参照してください。

---

図 4-2. vSphere のインベントリ階層



ほとんどのインベントリ オブジェクトは、階層での単一の親から権限を継承します。たとえば、データストアは親データストア フォルダまたは親データセンターから権限を継承します。仮想マシンは、親仮想マシン フォルダと親のホスト、クラスター、またはリソース プールの両方から同時に権限を継承します。

たとえば、Distributed Switch、およびそれに関連付けられている分散ポート グループに権限を設定するには、フォルダやデータセンターなど、親オブジェクトに権限を設定します。また、それらの権限を子オブジェクトに伝達するオプションも選択する必要があります。

階層内の権限には、いくつかの形式があります。

### 管理対象エンティティ

権限のあるユーザーは、管理対象エンティティに対して権限を定義できます。

- クラスタ
- データセンター
- データストア
- データストア クラスタ
- フォルダ
- ホスト
- ネットワーク (vSphere Distributed Switch を除く)
- 分散ポート グループ
- リソース プール
- テンプレート
- 仮想マシン
- vSphere の vApps

### グローバル エンティティ

ルート vCenter Server システムから権限を派生するエンティティの権限は変更できません。

- カスタム フィールド
- ライセンス
- ロール
- 統計間隔
- セッション

## 複数の権限の設定

オブジェクトは複数の権限を保持できますが、ユーザーまたはグループごとに 1 つしか保持できません。たとえば、1 つの権限で、グループ A にオブジェクトの管理者権限を付与します。別の権限では、グループ B に、同じオブジェクトの仮想マシン管理者権限を付与するように指定できます。

1 つのオブジェクトが 2 つの親オブジェクトからアクセス許可を継承する場合は、1 つのオブジェクトのアクセス許可がもう 1 つのオブジェクトのアクセス許可に追加されます。たとえば、ある仮想マシンが仮想マシン フォルダに格納されており、同時に、リソース プールにも属している場合、その仮想マシンは、仮想マシン フォルダとリソースプールの両方からすべてのアクセス許可を継承します。

子オブジェクトで適用される権限は、常に、親オブジェクトで適用されている権限をオーバーライドします。[例 2：子の権限による親の権限のオーバーライド](#)を参照してください。

複数のグループのアクセス許可が同じオブジェクトに定義されており、1人のユーザーがそれらのグループのうち2つ以上に属している場合は、次の2つのケースが考えられます。

- そのオブジェクトに関するユーザーの権限が定義されていない場合、ユーザーにはそのオブジェクトに関してグループに割り当てられた権限のセットが割り当てられます。
- そのオブジェクトに関するユーザーの権限が定義されている場合、ユーザーの権限がすべてのグループ権限より優先されます。

## 例 1：複数の権限の継承

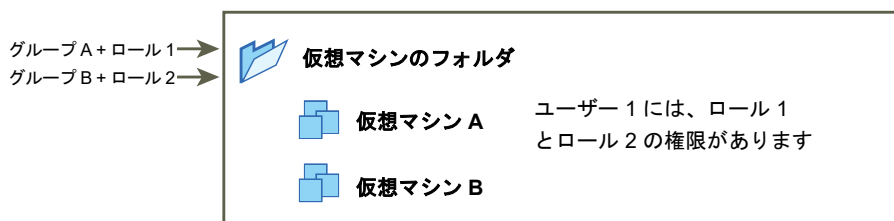
この例では、親オブジェクトで権限が付与されているグループから、オブジェクトが複数の権限を継承する方法を示します。

この例では、2つの異なるグループの同じオブジェクトに、2つの権限が割り当てられています。

- ロール 1 は、仮想マシンをパワーオンできる。
- ロール 2 は、仮想マシンのスナップショットを作成できる。
- グループ A は、仮想マシン フォルダでロール 1 を付与されており、子オブジェクトに伝達するように権限が設定されている。
- グループ B は、仮想マシン フォルダでロール 2 を付与されており、子オブジェクトに伝達するように権限が設定されている。
- ユーザー 1 には、特定の権限は割り当てられていない。

グループ A、B の両方に属するユーザー 1 がログオンします。ユーザー 1 は、仮想マシン A と仮想マシン B のパワーオンとスナップショットの作成の両方を実行できます。

図 4-3. 例 1：複数の権限の継承



## 例 2：子の権限による親の権限のオーバーライド

この例では、子オブジェクトに割り当てられた権限が、親オブジェクトに割り当てられている権限をオーバーライドする方法を示します。このオーバーライド機能によって、ユーザーのアクセスをインベントリの特定の領域に制限できます。

この例では、2つの異なるグループに、2つの異なるオブジェクトに関する権限が定義されています。

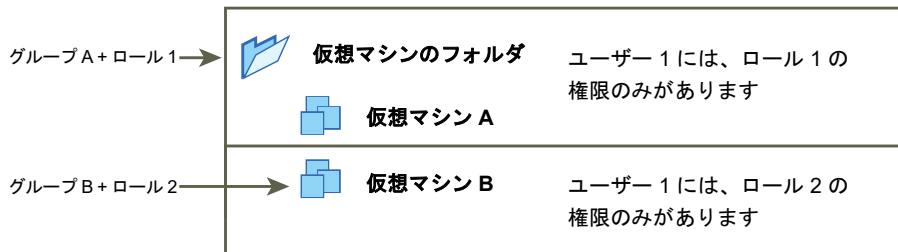
- ロール 1 は、仮想マシンをパワーオンできる。
- ロール 2 は、仮想マシンのスナップショットを作成できる。



- グループ A は、仮想マシン フォルダでロール 1 を付与されており、子オブジェクトに伝達するように権限が設定されている。
- グループ B は、仮想マシン B でロール 2 を付与されている。

グループ A、B の両方に属するユーザー 1 がログオンします。ロール 2 は、ロール 1 よりも低い階層で割り当てられているため、仮想マシン B のロール 1 をオーバーライドします。ユーザー 1 は仮想マシン A をパワーオンできますが、スナップショットは作成できません。ユーザー 1 は、仮想マシン B のスナップショットを作成できますが、パワーオンはできません。

図 4-4. 例 2：子の権限による親の権限のオーバーライド



### 例 3：ユーザー ロールによるグループ ロールのオーバーライド

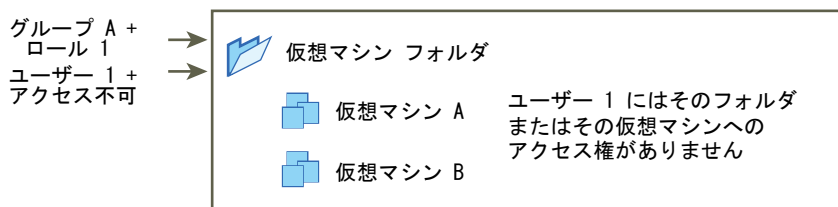
この例では、個々のユーザーに直接ロールを割り当てることによって、グループに割り当てられたロールに関連付けられた権限をオーバーライドする方法を示します。

この例では、異なるアクセス許可を同じオブジェクトに定義します。1 つは、グループをロールに関連付けるアクセス許可、もう 1 つはユーザーをロールに関連付けるアクセス許可です。後者のユーザーは前者のグループのメンバーです。

- ロール 1 は、仮想マシンをパワーオンできる。
- グループ A は、仮想マシン フォルダでロール 1 を割り当てられている。
- ユーザー 1 は、仮想マシン フォルダでアクセスなしロールを割り当てられている。

グループ A に属するユーザー 1 がログオンします。仮想マシン フォルダでユーザー 1 に付与されているアクセスなしロールによって、グループに割り当てられたロールがオーバーライドされます。ユーザー 1 は、仮想マシン フォルダ、仮想マシン A、仮想マシン B のいずれにもアクセスできません。

図 4-5. 例 3：ユーザー権限によるグループ権限のオーバーライド



## vCenter コンポーネントの権限の管理

アクセス許可は、vCenter オブジェクト階層内のオブジェクトに設定されます。各アクセス許可によって、グループまたはユーザー、およびグループまたはユーザーのアクセス ロールがオブジェクトに関連付けられます。たとえば、仮想マシン オブジェクトを選択し、グループ 1 に読み取り専用ロールを与えるアクセス許可を追加し、ユーザー 2 に管理者ロールを与える別のアクセス許可を追加できます。

異なるオブジェクトのユーザーのグループに異なるロールを割り当てることにより、それらのユーザーが vSphere 環境で実行できるタスクを制御します。たとえば、グループがホストのメモリを構成できるようにするには、ホストを選択し、ホスト.構成.メモリ構成 権限を含むロールをグループに付与するアクセス許可を追加します。

vSphere Web Client から権限を管理するには、次の概念を理解する必要があります。

### 権限

vCenter Server オブジェクト階層内の各オブジェクトには、関連付けられた権限があります。各権限には、そのオブジェクトに対してグループまたはユーザーに設定される権限が、グループまたはユーザーごとに指定されます。

### ユーザーおよびグループ

vCenter Server システムでは、認証されたユーザーまたは認証されたユーザーのグループに対してのみ権限を割り当てることができます。ユーザーは vCenter Single Sign-On を介して認証されます。ユーザーとグループは、vCenter Single Sign-On が認証するのに使用するアイデンティティ ソースで定義されている必要があります。Active Directory などのアイデンティティ ソース内のツールを使用して、ユーザーとグループを定義します。

### ロール

ロールにより、ユーザーが実行する標準的なタスクのセットに基づいて、オブジェクトでのアクセス許可を割り当てることができます。管理者などのデフォルト ロールは vCenter Server で事前定義済みであり、変更できません。リソース プール管理者などのその他のロールは、事前定義されたサンプル ロールです。一から、またはサンプル ロールをクローン作成して変更することで、カスタム ロールを作成できます。

### 権限

権限は、きめ細かなアクセス制御です。このような権限をロールにグループ化することができ、これにより、ユーザーやグループにマップすることができます。

アクセス許可は、階層内のさまざまなレベルのオブジェクトに設定できます。たとえば、ホスト オブジェクト、またはすべてのホスト オブジェクトが格納されたフォルダ オブジェクトにアクセス許可を設定できます。[権限の階層的な継承](#) を参照してください。また、グローバル ルート オブジェクトにアクセス許可を設定することで、すべてのソリューションのすべてのオブジェクトにそのアクセス許可を適用できます。[グローバル権限](#) を参照してください。

## インベントリ オブジェクトへのアクセス許可の追加

ユーザーおよびグループを作成し、ロールを定義したあと、関連するインベントリ オブジェクトに対してユーザーおよびグループと、そのロールを割り当てる必要があります。オブジェクトをフォルダに移動し、そのフォルダにアクセス許可を設定することで、同じアクセス許可を複数のオブジェクトに同時に割り当てることができます。

vSphere Web Client からアクセス許可を割り当てるには、ユーザー名とグループ名が、大文字小文字の区別も含め、Active Directory の設定と厳密に一致している必要があります。古いバージョンの vSphere からアップグレードする際にグループに問題が発生する場合は、大文字と小文字の整合性をチェックしてください。

#### 前提条件

オブジェクトのアクセス許可を変更するには、権限.権限の変更 権限を含むロールが必要です。

#### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、アクセス許可の割り当て先オブジェクトを探します。
- 2 [管理] タブをクリックして、[権限] を選択します。
- 3 追加アイコンをクリックして、[追加] をクリックします。
- 4 選択したロールによって定義される権限を付与するユーザーまたはグループを特定します。
  - a [ドメイン] ドロップダウン メニューから、ユーザーまたはグループが配置されているドメインを選択します。
  - b [検索] ボックスに名前を入力するか、リストから名前を選択します。  
システムはユーザー名、グループ名、および説明を検索します。
  - c ユーザーまたはグループを選択し、[追加] をクリックします。  
[ユーザー] または [グループ] リストのいずれかに名前が追加されます。
  - d (オプション) [名前の確認] をクリックして、アイデンティティ ソースに存在するユーザーまたはグループを確認します。
  - e [OK] をクリックします。
- 5 [割り当てられたロール] ドロップダウン メニューからロールを選択します。  
オブジェクトに割り当てられているロールがメニューに示されます。そのロールに含まれている権限は、ロールタイトルの下のセクションに一覧表示されます。
- 6 (オプション) 伝達を制限するには、[子オブジェクトへ伝達] チェック ボックスを選択解除します。  
ロールは選択したオブジェクトにのみ適用され、子オブジェクトには伝達されません。
- 7 [OK] をクリックしてアクセス許可を追加します。

## 権限の変更

インベントリ オブジェクトにユーザーまたはグループとロールとのペアを設定したあとで、ユーザーまたはグループに組み合わせたロールの変更、または [伝達] チェック ボックスの設定変更ができます。権限の設定を削除することもできます。

#### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、オブジェクトを参照して移動します。
- 2 [管理] タブをクリックし、[権限] を選択します。

- 3 行項目をクリックして、ユーザーまたはグループとロールとのペアを選択します。
- 4 [権限に基づいてロールを変更] をクリックします。
- 5 ユーザーまたはグループのロールを [割り当てられたロール] ドロップダウン メニューから選択します。
- 6 割り当てたインベントリ オブジェクトの子に権限を伝達するには、[伝達] チェック ボックスをクリックして [OK] をクリックします。

## 権限の削除

個々のユーザーまたはグループのオブジェクト階層内のオブジェクトのアクセス許可を削除できます。これを行うと、オブジェクトのロールに関連付けられている権限がなくなります。

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、オブジェクトを参照して移動します。
- 2 [管理] タブをクリックして、[権限] を選択します。
- 3 適切な行項目をクリックして、ユーザーまたはグループとロールとのペアを選択します。
- 4 [権限の削除] をクリックします。

### 結果

vCenter Server が、アクセス許可の設定を削除します。

## 権限の検証設定の変更

vCenter Server は、ユーザー ディレクトリでユーザーおよびグループと比較して、ユーザーおよびグループのリストを定期的に検証します。そのあとで、ドメインに存在しなくなったユーザーまたはグループを削除します。検証を無効にしたり、検証の間隔を変更したりできます。ドメインに数千のユーザーまたはグループが含まれている場合、または検索に長時間かかる場合は、検索設定を調整することを検討してください。

vCenter Server 5.0 よりも前の vCenter Server バージョンの場合、これらの設定は、vCenter Server に関連付けられている Active Directory に適用されます。vCenter Server 5.0 以降の場合、これらの設定は vCenter Single Sign-On アイデンティティ ソースに適用されます。

---

**注：** この手順は、vCenter Server のユーザー リストのみに該当します。ESXi のユーザー リストを同じ方法で検索することはできません。

---

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、vCenter Server システムを参照して移動します。
- 2 [管理] タブを選択して、[設定] をクリックします。
- 3 [全般] をクリックして、[編集] をクリックします。
- 4 [ユーザー ディレクトリ] を選択します。

## 5 必要に応じて値を変更します。

オプション	説明
ユーザー ディレクトリのタイムアウト	Active Directory サーバへの接続タイムアウト間隔 (秒)。この値により、選択されたドメインでの検索のために vCenter Server で許容される最大時間を指定します。大規模なドメインの検索は、時間がかかる可能性があります。
クエリ制限	チェック ボックスを選択して、vCenter Server が表示するユーザーおよびグループの最大数を設定します。
クエリ制限サイズ	vCenter Server が表示する、[ユーザーまたはグループの選択] ダイアログ ボックスで選択したドメインのユーザーおよびグループの最大数を指定します。「0」を入力すると、ユーザーおよびグループがすべて表示されます。
検証	検証を無効にするには、このチェック ボックスを選択解除します。
検証期間	vCenter Server で権限を検証する頻度を分単位で指定します。

## 6 [OK] をクリックします。

# グローバル権限

グローバル権限は、vCenter Server と vCenter Orchestrator の両方など、複数のソリューションが関係するグローバル ルート オブジェクトに適用されます。グローバル権限を使用して、すべてのオブジェクト階層のすべてのオブジェクトについての権限をユーザーまたはグループに付与します。

各ソリューションには、それ自体のオブジェクト階層内にルート オブジェクトが存在します。グローバル ルート オブジェクトは、各ソリューション オブジェクトに対する親オブジェクトとして動作します。ユーザーまたはグループにグローバル権限を割り当て、ユーザーまたはグループごとにロールを決定することができます。ロールによって権限のセットが決まります。事前定義されたロールを割り当てるか、カスタム ロールを作成することができます。[ロールを使用した権限の割り当て](#) を参照してください。vCenter Server のアクセス許可とグローバル権限を区別することは重要です。

## vCenter Server のアクセス許可

ほとんどの場合、ESXi ホストや仮想マシンなどの vCenter Server インベントリ オブジェクトにアクセス許可を適用します。適用する場合は、ユーザーまたはグループが、そのオブジェクトについてロールと呼ばれる権限のセットを持つことを指定します。

## グローバル権限

グローバル権限では、ユーザーまたはグループに、デプロイの各インベントリ階層にあるすべてのオブジェクトを表示または管理する権限が与えられます。

グローバル権限を割り当てて [伝達] を選択しない場合、この権限に関連付けられたユーザーまたはグループは、階層内のオブジェクトにアクセスできません。これらのユーザーまたはグループは、ロールの作成などの一部のグローバル機能へのアクセス権のみを持ちます。

**重要：** グローバル権限は慎重に使用してください。すべてのインベントリ階層にあるすべてのオブジェクトに対して権限を割り当てる必要が本当にあるかどうか確認してください。

## グローバル権限の追加

グローバル権限を使用すると、ユーザーまたはグループに、デプロイ環境のすべてのインベントリ階層のすべてのオブジェクトに対する権限を付与できます。

グローバル権限は慎重に使用してください。すべてのインベントリ階層にあるすべてのオブジェクトに対して権限を割り当てる必要が本当にあるかどうか確認してください。

### 前提条件

このタスクを実行するには、すべてのインベントリ階層の root オブジェクトに対する `.権限.権限の変更` 権限が必要です。

### 手順

- 1 [管理] をクリックし、[アクセス コントロール] 領域で [グローバル権限] を選択します。
- 2 [管理] をクリックし、[権限の追加] アイコンをクリックします。
- 3 選択したロールによって定義される権限を付与するユーザーまたはグループを特定します。
  - a [ドメイン] ドロップダウン メニューから、ユーザーまたはグループが配置されているドメインを選択します。
  - b [検索] ボックスに名前を入力するか、リストから名前を選択します。  
システムはユーザー名、グループ名、および説明を検索します。
  - c ユーザーまたはグループを選択し、[追加] をクリックします。  
[ユーザー] または [グループ] リストのいずれかに名前が追加されます。
  - d (オプション) [名前の確認] をクリックして、アイデンティティ ソースに存在するユーザーまたはグループを確認します。
  - e [OK] をクリックします。
- 4 [割り当てられたロール] ドロップダウン メニューからロールを選択します。  
オブジェクトに割り当てられているロールがメニューに示されます。そのロールに含まれている権限は、ロールタイトルの下のセクションに一覧表示されます。
- 5 ほとんどの場合、[子へ伝達] チェック ボックスを選択したままにします。  
グローバル権限を割り当てて [伝達] を選択しない場合、この権限に関連付けられたユーザーまたはグループは、階層内のオブジェクトにアクセスできません。これらのユーザーまたはグループは、ロールの作成などの一部のグローバル機能へのアクセス権のみを持ちます。
- 6 [OK] をクリックします。

## タグ オブジェクトに対する権限

vCenter Server オブジェクト階層では、タグ オブジェクトは vCenter Server の子でなく、vCenter Server のルート レベルに作成されます。複数の vCenter Server インスタンスがある環境では、タグ オブジェクトは vCenter Server インスタンス全体で共有されます。タグ オブジェクトに対する権限は、vCenter Server オブジェクト階層のその他のオブジェクトに対する権限とは機能が異なります。

## グローバル権限またはタグ オブジェクトに割り当てられた権限のみ適用される

ESXi ホストや仮想マシンなどの vCenter Server インベントリ オブジェクトに対する権限をユーザーに付与しても、そのユーザーはそのオブジェクトに対してタグ操作を実行できません。

たとえば、ホスト TPA に vSphere タグを割り当て権限をユーザー Dana に付与しても、その権限によって Dana がホスト TPA にタグを割り当てることはできません。Dana は vSphere タグを割り当て権限を root レベルで取得する（つまりグローバル権限を取得する）か、そのタグ オブジェクトに対する権限を持つ必要があります。

表 4-1. グローバル権限およびタグ オブジェクト権限が、ユーザーの操作に与える影響

グローバル権限	タグレベル権限	vCenter Server オブジェクト レベル権限	有効な権限
タグ付け権限が割り当てられていない。	Dana には、そのタグに関して、vSphere タグを割り当てまたは割り当て解除権限がある。	Dana には、ESXi ホスト TPA における vSphere タグを削除権限がある。	Dana には、そのタグに関して、vSphere タグを割り当てまたは割り当て解除権限がある。
Dana には、vSphere タグを割り当てまたは割り当て解除権限がある。	そのタグに関する権限が割り当てられていない。	Dana には、ESXi ホスト TPA における vSphere タグを削除権限がある。	Dana には、vSphere タグを割り当てまたは割り当て解除グローバル権限がある。タグレベルの権限を含む。
タグ付け権限が割り当てられていない。	そのタグに関する権限が割り当てられていない。	Dana には、ESXi ホスト TPA における vSphere タグを割り当てまたは割り当て解除権限がある。	Dana には、ホスト TPA をはじめ、どのオブジェクトに対してもタグ付け権限がない。

## タグ オブジェクト権限を補足するグローバル権限

グローバル権限とは、ルート オブジェクトに関して割り当てられる権限であり、タグ オブジェクトに対する権限が制限されている場合に、タグ オブジェクトに対する権限を補足します。vCenter Server 権限は、タグ オブジェクトに影響しません。

たとえば、グローバル権限を使用して、root レベルで vSphere タグを削除権限をユーザー Robin に割り当てると仮定します。タグ Production に対しては、vSphere タグを削除権限を Robin に割り当てません。この場合、Robin はグローバル権限を持っているため、タグ Production に対しても権限を持ちます。グローバル権限を変更しない限り、権限を制限することはできません。

表 4-2. タグレベル権限を補足するグローバル権限

グローバル権限	タグレベル権限	有効な権限
Robin には、vSphere タグを削除権限がある。	Robin には、そのタグに関して、vSphere タグを削除権限がない。	Robin には、vSphere タグを削除権限がある。
タグ付け権限が割り当てられていない。	Robin には、そのタグに関して、vSphere タグを削除権限が割り当てられていない。	Robin には、vSphere タグを削除権限がない。

## グローバル権限を拡張できるタグレベル権限

タグレベル権限を使用して、グローバル権限を拡張できます。つまり、ユーザーは 1 つのタグに関して、グローバル権限とタグレベル権限の両方を持つことができます。



表 4-3. タグレベル権限を拡張するグローバル権限

グローバル権限	タグレベル権限	有効な権限
Lee には、vSphere タグを割り当てまたは割り当て解除権限がある。	Lee には、vSphere タグを削除権限がある。	Lee には、そのタグに関して、vSphere タグを割り当て権限と vSphere タグを削除権限がある。
タグ付け権限が割り当てられていない。	Lee には、そのタグに関して、vSphere タグを削除権限が割り当てられている。	Lee には、そのタグに関して、vSphere タグを削除権限がある。

## ロールを使用した権限の割り当て

ロールとは、事前に定義された権限セットです。権限は、操作の実行やプロパティの読み取りを行う権利を定義します。たとえば、仮想マシン管理者ロールは、プロパティの読み取りと操作の実行を行う一連の権限で構成されます。ロールを使用して、仮想マシン属性の読み取りや変更をユーザーに許可します。

権限を割り当てるときは、ユーザーまたはグループをロールとペアにして、このペアをインベントリ オブジェクトに関連付けます。各ユーザーまたはグループには、インベントリのオブジェクトごとに異なるロールを設定できます。

たとえば、インベントリにプール A とプール B という 2 つのリソース プールがある場合、あるユーザーに、プール A では仮想マシン ユーザー ロールを割り当て、プール B では読み取り専用ロールを割り当てることができます。この場合、このユーザーはプール A の仮想マシンをパワーオンできますが、プール B の仮想マシンは表示のみが可能です。

vCenter Server では、デフォルトで次のシステム ロールとサンプル ロールが利用できます。

### システム ロール

システム ロールは永続的です。このロールに関連付けられている権限は編集できません。

### サンプル ロール

VMware は、頻繁に実行される特定のタスクの組み合わせのサンプル ロールを提供しています。これらのロールは、クローン作成、変更または削除できます。

**注：** サンプル ロールの事前定義済みの設定が失われないようにするには、まずロールのクローンを作成し、そのクローンを変更します。サンプルをデフォルト設定にリセットすることはできません。

ユーザーがタスクをスケジュールできるのは、タスクの作成時にそのタスクを実行する権限が含まれるロールを持っている場合だけです。

**注：** 対象ユーザーがログインしていても、ロールや権限を変更するとすぐに反映されます。ただし、検索では、ユーザーが一度ログアウトして再度ログインしてから権限が有効になるため、すぐには反映されません。

## vCenter Server および ESXi のカスタム ロール

vCenter Server とそれが管理するすべてのオブジェクト、または個々のホストのカスタム ロールを作成できます。

### vCenter Server カスタム ロール（推奨）



カスタム ロールを作成するには、vSphere Web Client のロール編集機能を使用して、ニーズに合った権限セットを作成します。

## ESXi カスタム ロール

CLI または vSphere Client を使用して、個々のホストのカスタム ロールを作成できます。『vSphere Client による vSphere 管理』ドキュメントを参照してください。vCenter Server からカスタム ホスト ロールにアクセスすることはできません。

ESXi ホストを vCenter Server を介して管理する場合、ホストと vCenter Server の両方でカスタム ロールを保持していると、混乱や誤用が起きる可能性があります。ほとんどの場合で、vCenter Server ロールを定義することをお勧めします。

vCenter Server を使用してホストを管理する場合、そのホストに関連付けられている権限は vCenter Server で作成され、vCenter Server に格納されます。ホストに直接接続する場合は、ホストで直接作成されたロールのみを使用できます。

---

**注：** カスタム ロールを追加し、それに権限を付与しない場合、そのロールは読み取り専用ロールとして作成され、System.Anonymous、System.View、および System.Read という 3 つのシステム定義権限が付与されます。

---



vSphere Web Client でのロールの作成

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_egsyxkp4/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/))

## vCenter Server システム ロール

ロールとは、事前に定義された権限セットです。オブジェクトにアクセス許可を追加すると、ユーザー（またはグループ）とロールのペアが形成されます。vCenter Server には、いくつかのシステム ロールが定義されています。ユーザーがシステム ロールを変更することはできません。

### vCenter Server システム ロール

vCenter Server には、少数のデフォルト ロールが用意されています。デフォルト ロールに関連付けられた権限を変更することはできません。デフォルト ロールは階層のように編成され、各ロールは上位のロールの権限を継承します。たとえば、システム管理者ロールは読み取り専用ロールの権限を引き継ぎます。ユーザーが作成したロールは、どのシステム ロールの権限も継承しません。

### 管理者ロール

オブジェクトの管理者ロールが割り当てられているユーザーは、オブジェクトのすべてのアクションを表示および実行できます。このロールには、読み取り専用ロールに与えられているすべての権限も含まれます。オブジェクトに対する管理者ロールを付与されたユーザーは、個々のユーザーおよびグループに権限を割り当てることができます。vCenter Server で管理者ロールを持つユーザーは、デフォルトの vCenter Single Sign-On アイデンティティ ソース内のユーザーおよびグループに権限を割り当てることができます。サポートされている ID サービスには、Windows Active Directory や OpenLDAP 2.4 などがあります。

デフォルトでは、インストール後、administrator@vsphere.local ユーザーに、vCenter Single Sign-On と vCenter Server の両方の管理者ロールが割り当てられます。この administrator@vsphere.local ユーザーによって、他のユーザーに vCenter Server の管理者ロールが割り当てられます。

### アクセスなしロール

オブジェクトに対して、アクセスなしロールが割り当てられているユーザーは、オブジェクトを表示または変更できません。新しいユーザーとグループには、デフォルトでこのロールが割り当てられます。ロールは、オブジェクトごとに変更できます。

デフォルトでアクセスなしロールが与えられていないユーザーは、administrator@vsphere.local ユーザー、root ユーザー、および vpxuser だけです。代わりに、これらのユーザーには、システム管理者ロールが割り当てられています。最初にシステム管理者ロールを持つ root レベルで代替アクセス許可を作成し、このアクセス許可を別のユーザーに割り当てている場合は、すべてのアクセス許可から root ユーザーを削除したり、そのロールをアクセスなしロールに変更したりできます。

### 読み取り専用ロール

オブジェクトに対して、読み取り専用ロールが割り当てられているユーザーは、オブジェクトの状態および詳細を表示できます。このロールが割り当てられているユーザーは、仮想マシン、ホスト、およびリソース プール属性を表示できます。ただし、ホストのリモート コンソールは表示できません。メニューおよびツールバーのすべてのアクションは無効になります。

## カスタム ロールの作成

環境に必要なアクセス コントロールに適合する vCenter Server のカスタム ロールを作成できます。

vCenter Server システムと同じ vCenter Single Sign-On ドメインに参加する vCenter Server システム上のロールを作成または編集すると、VMware Directory Service (vmdir) により、同じグループに含まれるその他すべての vCenter Server システムに、行った変更が伝播されます。vCenter Server システム間で、特定ユーザーおよびオブジェクトへのロールの割り当ては共有されません。

### 前提条件

システム管理者権限を持つユーザーとしてログインしていることを確認します。

### 手順

- 1 vSphere Web Client を使用して vCenter Server にログインします。
- 2 [ホーム] を選択し、[管理] をクリックして、[ロール] をクリックします。
- 3 [ロールの作成アクション] (+) ボタンをクリックします。
- 4 新しいロールの名前を入力します。
- 5 ロールの権限を選択し、[OK] をクリックします。

## ロールのクローン作成

既存のロールのコピーを作成して、その名前を変更したり、編集したりできます。コピーを作成しても、その新しいロールはユーザーまたはグループ、およびオブジェクトには適用されません。ユーザーまたはグループ、およびオブジェクトに、そのロールを割り当てる必要があります。

vCenter Server システムと同じ vCenter Single Sign-On ドメインに参加する vCenter Server システム上のロールを作成または編集すると、VMware Directory Service (vmdir) により、同じグループに含まれるその他すべての vCenter Server システムに、行った変更が伝播されます。vCenter Server システム間で、特定ユーザーおよびオブジェクトへのロールの割り当ては共有されません。

### 前提条件

システム管理者権限を持つユーザーとしてログインしていることを確認します。

### 手順

- 1 vSphere Web Client を使用して vCenter Server にログインします。
- 2 [ホーム] を選択し、[管理] をクリックして、[ロール] をクリックします。
- 3 ロールを選択して、[ロールのクローン作成アクション] をクリックします。
- 4 クローン作成されたロールの名前を入力します。
- 5 ロールの権限を選択または選択解除し、[OK] をクリックします。

## ロールの編集

ロールを編集するときに、そのロールに対して選択した権限を変更できます。処理が完了すると、編集されたロールに割り当てられているユーザーまたはグループに権限が適用されます。

vCenter Server システムと同じ vCenter Single Sign-On ドメインに参加する vCenter Server システム上のロールを作成または編集すると、VMware Directory Service (vmdir) により、同じグループに含まれるその他すべての vCenter Server システムに、行った変更が伝播されます。vCenter Server システム間で、特定ユーザーおよびオブジェクトへのロールの割り当ては共有されません。

### 前提条件

システム管理者権限を持つユーザーとしてログインしていることを確認します。

### 手順

- 1 vSphere Web Client を使用して vCenter Server にログインします。
- 2 [ホーム] を選択し、[管理] をクリックして、[ロール] をクリックします。
- 3 ロールを選択して、[ロールの編集アクション] をクリックします。
- 4 ロールの権限を選択または選択解除し、[OK] をクリックします。

## ロールと権限のベスト プラクティス

vCenter Server 環境のセキュリティと管理性を最大にするため、ロールと権限のベスト プラクティスを使用します。

vCenter Server 環境のロールと権限を構成するときは、次のベスト プラクティスが推奨されます。

- 可能な場合は、個々のユーザーではなくグループにロールを割り当てて、そのグループに権限を付与します。
- アクセス許可が必要なオブジェクトにのみアクセス許可を付与し、権限を持つ必要があるユーザーまたはグループに対してのみ権限を割り当てます。使用する権限の数を最小限にすることで、権限構造が分かりやすくなり、管理が簡単になります。

- 制限付きロールをグループに割り当てる場合は、そのグループにシステム管理者ユーザーまたはその他の管理権限を持つユーザーが含まれていないことを確認してください。含まれている場合、グループに制限付きロールを割り当てたインベントリ階層の一部で、管理者の権限が誤って制限されます。
- フォルダを使用してオブジェクトをグループ化します。たとえば、1つのホスト セットに変更アクセス許可を付与し、別のホスト セットに表示アクセス許可を付与する場合は、各ホスト セットを1つのフォルダに格納します。
- ルートの vCenter Server オブジェクトにアクセス許可を追加する場合は、注意してください。ルート レベルの権限を持つユーザーは、ロール、カスタム属性、vCenter Server の設定など、vCenter Server 上のグローバル データにアクセスできます。
- ほとんどの場合、アクセス許可をオブジェクトに割り当てるときに伝達を有効にします。これによって、新しいオブジェクトをインベントリ階層に挿入したときに、権限が継承され、ユーザーがアクセスできるようになります。
- 特定のユーザーまたはグループが、オブジェクト階層内の特定の領域にあるオブジェクトにアクセスできないようにするには、アクセスなしロールを使用して階層内のその領域をマスクします。
- ライセンスに対する変更は、ユーザーが vCenter Server システムのすべてに対する権限がない場合でも、同じ Platform Services Controller にリンクされているすべての vCenter Server システムに、または同じ vCenter Single Sign-On ドメインの Platform Services Controller に伝達されます。

## 一般的なタスクに必要な権限

多くのタスクが、インベントリの複数のオブジェクトでの権限を必要とします。タスクの実行に必要な権限、および、必要に応じて適切なサンプル ロールを確認できます。

以下の表に、複数の権限を必要とする一般的なタスクを示します。インベントリ オブジェクトにアクセス許可を追加するには、ユーザーに事前定義のロールの1つを割り当てます。繰り返し使用することが予想される権限のセットを使用してカスタムのロールを作成することもできます。

以下の表に、実行する必要があるタスクがない場合は、次のルールに基づいて、特定の操作を許可するためのアクセス許可の設定先を決定してください。

- 仮想ディスクの作成やスナップショットの作成など、ストレージ容量を使用する操作にはターゲット データストアへの データストア領域の割り当て 権限が必要です。また、操作を実行する権限も必要です。
- インベントリ階層でオブジェクトを移動するには、オブジェクト、移動元の親オブジェクト（フォルダ、クラスタなど）、および移動先の親オブジェクトに適切な権限が必要です。
- 各ホストおよびクラスタには、そのホストまたはクラスタのすべてのリソースが含まれる、独自のリソース プールが必ず存在します。仮想マシンをホストまたはクラスタに直接展開するには、リソース、仮想マシンのリソース プールへの割り当て 権限が必要です。

表 4-4. 一般的なタスクに必要な権限

タスク	必要な権限	適用可能なロール
仮想マシンの作成	作成先のフォルダまたはデータセンター： <ul style="list-style-type: none"> <li>■ 仮想マシン.インベントリ.新規作成</li> <li>■ 仮想マシン.構成.新規ディスクの追加（新規仮想ディスクを作成する場合）</li> <li>■ 仮想マシン.構成.既存ディスクの追加（既存の仮想ディスクを使用している場合）</li> <li>■ 仮想マシン.構成.Raw デバイス（RDM または SCSI パススルー デバイスを使用している場合）</li> </ul>	システム管理者
	ターゲットのホスト、クラスタ、またはリソース プール：           リソース.仮想マシンのリソース プールへの割り当て	リソース プール管理者または管理者
	作成先のデータストア、またはデータストアを含むフォルダ           データストア.領域の割り当て	データストアの利用者または管理者
	仮想マシンを割り当てるネットワーク           ネットワーク.ネットワークの割り当て	ネットワークの利用者または管理者
テンプレートからの仮想マシンのデプロイ	作成先のフォルダまたはデータセンター： <ul style="list-style-type: none"> <li>■ 仮想マシン.インベントリ.既存のものから作成</li> <li>■ 仮想マシン.構成.新規ディスクの追加</li> </ul>	システム管理者
	テンプレートまたはテンプレートのフォルダ           仮想マシン.プロビジョニング.テンプレートのデプロイ	システム管理者
	デプロイ先のホスト、クラスタ、またはリソース プール：           リソース.仮想マシンのリソース プールへの割り当て	システム管理者
	デプロイ先のデータストア、またはデータストアのフォルダ           データストア.領域の割り当て	データストアの利用者または管理者
	仮想マシンを割り当てるネットワーク           ネットワーク.ネットワークの割り当て	ネットワークの利用者または管理者
仮想マシンのスナップショットの作成	仮想マシンまたは仮想マシンのフォルダ           仮想マシン.スナップショット管理.スナップショットの作成	仮想マシンのパワー ユーザーまたは管理者
リソース プールへの仮想マシンの移動	仮想マシンまたは仮想マシンのフォルダ <ul style="list-style-type: none"> <li>■ リソース.仮想マシンのリソース プールへの割り当て</li> <li>■ 仮想マシン.インベントリ.移動</li> </ul>	システム管理者
	移動先のリソース プール           リソース.仮想マシンのリソース プールへの割り当て	システム管理者

表 4-4. 一般的なタスクに必要な権限（続き）

タスク	必要な権限	適用可能なロール
仮想マシンへのゲスト OS のインストール	仮想マシンまたは仮想マシンのフォルダ <ul style="list-style-type: none"> <li>■ 仮想マシン.相互作用.質問への回答</li> <li>■ 仮想マシン.相互作用.コンソールでの相互作用</li> <li>■ 仮想マシン.相互作用.デバイス接続</li> <li>■ 仮想マシン.相互作用.パワーオフ</li> <li>■ 仮想マシン.相互作用.パワーオン</li> <li>■ 仮想マシン.相互作用.リセット</li> <li>■ 仮想マシン.相互作用.CD メディアの構成（CD からインストールする場合）</li> <li>■ 仮想マシン.相互作用.フロッピー メディアの構成（フロッピー ディスクからインストールする場合）</li> <li>■ 仮想マシン.相互作用.VMware Tools のインストール</li> </ul>	仮想マシンのパワー ユーザーまたは管理者
	インストール メディアの ISO イメージを含むデータストア データストア.データストアの参照（データストアの ISO イメージからインストールする場合） インストール メディア ISO イメージをアップロードするデータストア： <ul style="list-style-type: none"> <li>■ データストア.データストアの参照</li> <li>■ データストア.低レベルのファイル操作</li> </ul>	仮想マシンのパワー ユーザーまたは管理者
vMotion による仮想マシンの移行	仮想マシンまたは仮想マシンのフォルダ <ul style="list-style-type: none"> <li>■ リソース.パワーオン状態の仮想マシンの移行</li> <li>■ リソース.仮想マシンのリソース プールへの割り当て（移行先が移行元と異なるリソース プールの場合）</li> </ul>	リソース プール管理者または管理者
	移行先のホスト、クラスタ、またはリソース プール（移行元と異なる場合）： リソース.仮想マシンのリソース プールへの割り当て	リソース プール管理者または管理者
仮想マシンのコールド移行（再配置）	仮想マシンまたは仮想マシンのフォルダ <ul style="list-style-type: none"> <li>■ リソース.パワーオフ状態の仮想マシンの移行</li> <li>■ リソース.仮想マシンのリソース プールへの割り当て（移行先が移行元と異なるリソース プールの場合）</li> </ul>	リソース プール管理者または管理者
	移行先のホスト、クラスタ、またはリソース プール（移行元と異なる場合）： リソース.仮想マシンのリソース プールへの割り当て	リソース プール管理者または管理者
	移行先のデータストア（移行元と異なる場合） データストア.領域の割り当て	データストアの利用者または管理者
Storage vMotion での仮想マシンの移行	仮想マシンまたは仮想マシンのフォルダ リソース.パワーオン状態の仮想マシンの移行	リソース プール管理者または管理者
	移行先のデータストア データストア.領域の割り当て	データストアの利用者または管理者
ホストのクラスタへの移動	ホスト ホスト.インベントリ.クラスタへのホストの追加	システム管理者
	移動先クラスタ ホスト.インベントリ.クラスタへのホストの追加	システム管理者

# ESXi ホストのセキュリティ強化

# 5

ESXi ハイパーバイザー アーキテクチャには、CPU 隔離、メモリ隔離、およびデバイス隔離などの多くのセキュリティ機能が組み込まれています。ロックダウン モード、証明書の置き換え、およびスマート カード認証などの追加機能を構成し、セキュリティを強化することができます。

ESXi ホストは、ファイアウォールによっても保護されています。必要に応じて着信および発信トラフィック用にポートを開くことができますが、サービスとポートへのアクセスは制限する必要があります。さらに、ESXi ロックダウン モードを使用し、ESXi Shell へのアクセスを制限すれば、より安全な環境を実現できるようになります。vSphere 6.0 以降、ESXi ホストは証明書インフラストラクチャに参加するようになっています。ホストは、デフォルトで VMware 認証局 (VMCA) によって署名された証明書を使用してプロビジョニングされます。

ESXi のセキュリティの詳細については、VMware のホワイト ペーパー『Security of the VMware vSphere Hypervisor』を参照してください。

この章には、次のトピックが含まれています。

- ホストの構成設定を管理するスクリプトの使用
- ホスト プロファイルを使用した ESXi ホストの構成
- ESXi のセキュリティに関する一般的推奨事項
- ESXi ホストの証明書管理
- セキュリティ プロファイルによるホストのカスタマイズ
- ESXi への権限の割り当て
- Active Directory を使用した ESXi ユーザーの管理
- vSphere Authentication Proxy の使用
- ESXi のセキュリティのベスト プラクティス
- ESXi のスマート カード認証の構成
- ESXi SSH キー
- ESXi Shell の使用
- ESXi Web プロキシの設定の変更
- vSphere Auto Deploy のセキュリティの考慮事項
- ESXi ログ ファイルの管理

## ホストの構成設定を管理するスクリプトの使用

多くのホストが存在する環境では、スクリプトを使用してホストを管理した方が、vSphere Web Client からホストを管理するよりも迅速に作業することができ、エラーが発生する確率も低くなります。

vSphere には、ホスト管理用のスクリプト言語がいくつか組み込まれています。参照情報およびプログラミングのヒントについては、『vSphere コマンドラインのドキュメント』および『vSphere API/SDK のドキュメント』を参照してください。また、スクリプトによる管理のその他のヒントについては VMware コミュニティを参照してください。vSphere 管理者のドキュメントでは、管理のために vSphere Web Client を使用する方法について主に説明されています。

### vSphere PowerCLI

VMware vSphere PowerCLI は、vSphere API への Windows PowerShell インターフェイスです。vSphere PowerCLI には、vSphere コンポーネントを管理するための PowerShell コマンドレットが含まれています。

vSphere PowerCLI には、200 以上の cmdlet、サンプル スクリプトのセット、管理および自動化のための関数ライブラリがあります。『vSphere PowerCLI のドキュメント』を参照してください。

### vSphere Command-Line Interface (vCLI)

vCLI には、ESXi ホストおよび仮想マシンを管理するためのコマンドのセットが組み込まれています。インストーラは、vSphere SDK for Perl もインストールし、Windows または Linux システムを実行して、ESXCLI コマンド、vicfg- コマンド、およびその他の vCLI コマンドのセットをインストールします。『vSphere Command-Line Interface のドキュメント』を参照してください。

vSphere 6.0 以降、vCloud Suite SDK for Python などの vCloud Suite SDK に対するスクリプト インターフェイスの 1 つを使用することもできます。

#### 手順

- 1 権限に制限のあるカスタム ロールを作成します。

たとえば、ホストを管理するための権限セットを持ち、仮想マシン、ストレージ、またはネットワークを管理するための権限は持たないロールを作成することを検討します。使用するスクリプトで情報を抽出するだけの場合は、ホストに対して読み取り専用権限を持つロールを作成できます。

- 2 vSphere Web Client で、サービス アカウントを作成してカスタム ロールに割り当てます。

特定のホストに対するアクセス権限を適度に制限する場合は、さまざまなレベルのアクセス権限を指定して複数のカスタム ロールを作成できます。



### 3 パラメータのチェックまたは変更を実行するスクリプトを記述して実行します。

たとえば、次のようにして、ホストでのシェルの対話式タイムアウトをチェックまたは設定できます。

言語	コマンド
<b>vCLI (ESXCLI)</b>	<pre>esxcli &lt;conn_options&gt; system settings advanced get / UserVars/ESXiShellTimeOut  esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list   grep /UserVars/ ESXiShellTimeOut</pre>
<b>PowerCLI</b>	<pre>#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 }</pre>

### 4 大規模な環境で、異なるアクセス特権を持つロールを作成し、実行するタスクに従ってホストをフォルダにグループ化します。これで、異なるサービス アカウントから異なるフォルダに対してスクリプトを実行できます。

### 5 コマンドを実行した結果を確認します。

## ホスト プロファイルを使用した ESXi ホストの構成

ホスト プロファイルにより、ESXi ホストの標準構成を設定し、それらの構成設定へのコンプライアンスを自動化することができます。またホスト プロファイルにより、メモリ、ストレージ、ネットワークなどのホスト構成の多くの側面を管理できます。

vSphere Web Client から参照ホストのホスト プロファイルを構成し、参照ホストの特性を共有するすべてのホストにそのホスト プロファイルを適用することができます。また、ホスト プロファイルを使用して、ホスト構成に変更がないかどうかホストを監視することもできます。『vSphere ホスト プロファイル』ドキュメントを参照してください。

ホスト プロファイルをクラスタに添付し、クラスタ内のすべてのホストに適用することができます。

#### 手順

- 1 仕様に合わせて参照ホストを設定し、ホスト プロファイルを作成します。
- 2 ホストまたはクラスタにプロファイルを添付します。
- 3 参照ホストのホスト プロファイルを、別のホストまたはクラスタに適用します。

## ESXi のセキュリティに関する一般的推奨事項

VMware は、不正侵入や不正使用から ESXi ホストを保護するために、パラメータ、設定、およびアクティビティに制約を設けています。構成上の必要に応じて、制約を緩和できます。緩和する場合は、信頼できる環境で作業していることを確認し、他の適切なセキュリティ対策を十分にとることでネットワーク全体とホストの接続デバイスを保護してください。

### 組み込みのセキュリティ機能

初期設定では、次のようにホストのリスクが低減されています。

- ESXi Shell および SSH はデフォルトで無効になっています。
- デフォルトでは、限られた数のファイアウォール ポートのみが開いています。特定のサービスに関連付けられている追加のファイアウォール ポートを明示的に開くことができます。
- ESXi は、その機能の管理に不可欠なサービスのみを実行します。ESXi の実行に必要な機能しか配布できません。
- デフォルトでは、ホストを管理するために必要でないポートは、すべて閉じられています。追加サービスが必要な場合、そのためにポートを開く必要があります。
- デフォルトでは、強度の低い暗号は無効になっており、クライアントからの通信は SSL で保護されます。チャネルの保護に使用するアルゴリズムは、SSL ハンドシェイクによって異なります。ESXi で作成されたデフォルトの証明書は、署名アルゴリズムとして、RSA 暗号化の PKCS#1 SHA-256 を使用します。
- Tomcat Web サービスは、Web クライアントからのアクセスをサポートするため、ESXi によって内部で使用されます。このサービスは、Web クライアントによる管理および監視に必要な機能のみを実行するように修正されています。そのため、ESXi は、さまざまな使用環境で報告されている Tomcat のセキュリティ問題による脆弱性に対応できます。
- VMware は、ESXi のセキュリティに影響する恐れのあるすべてのセキュリティ警告を監視し、必要に応じてセキュリティ パッチを発行します。
- FTP や Telnet などのセキュリティ保護されていないサービスはインストールされません。これらのサービス用のポートはデフォルトで閉じられています。SSH や SFTP など、よりセキュアなサービスを簡単に使用するため、これらの安全性の高いサービスを選択し、セキュリティ保護されていないサービスの使用は避けるようにしてください。たとえば、SSH を使用できず Telnet を使用する必要がある場合、SSL を使用した Telnet を使用して仮想シリアル ポートにアクセスします。

セキュリティ保護されていないサービスを使用する必要があり、ホストに十分な保護を実装している場合は、明示的にポートを開くことで対応できます。

### 追加のセキュリティ対策

ホストのセキュリティと管理を評価する際には、次の推奨事項を考慮してください。

#### アクセスを制限する

ダイレクト コンソール ユーザー インターフェイス (DCUI)、ESXi Shell、または SSH へのアクセスを有効にする場合、厳格なアクセス セキュリティ ポリシーを適用します。

ESXi Shell には、ホストの特定の分野に対するアクセス権があります。ESXi Shell へのログインおよびアクセス権限は信頼できるユーザーのみに付与してください。

### 管理対象ホストに直接アクセスしない

vSphere Web Client を使用して、vCenter Server の管理下にある ESXi ホストを管理します。vSphere Client で管理対象ホストに直接アクセスしないでください。また、ホストの DCUI から管理対象ホストに変更を加えないでください。

スクリプト インターフェイスまたは API を使用してホストを管理する場合、ホストを直接ターゲットとして指定しないでください。代わりに、ホストを管理する vCenter Server システムをターゲットにして、ホスト名を指定します。

### vSphere Client や、VMware CLI または API を使用して、スタンドアロン ESXi ホストを管理する

vSphere Client や、VMware CLI または API のいずれかを使用して、ESXi ホストを管理します。トラブルシューティングを行う場合にのみ、DCUI または ESXi Shell から root ユーザーとしてホストにアクセスします。ESXi Shell を使用する場合、アクセス権でアカウントを制限し、タイムアウトを設定します。

### ESXi コンポーネントのアップグレードには VMware ソースのみを使用する

ホストは、さまざまなサードパーティ製のパッケージを実行して、管理インターフェイスや実行する必要があるタスクをサポートします。VMware は、VMware が提供するもの以外、パッケージのアップグレードをサポートしていません。VMware が提供したものでないパッケージやパッチを使用すると、管理インターフェイスのセキュリティや機能が低下する場合があります。セキュリティに関する注意事項については、サードパーティ ベンダーのサイトや VMware のナレッジベースを定期的に確認してください。

---

**注：** <http://www.vmware.com/security/>から入手可能な VMware のセキュリティ情報の指示に従ってください。

---

## ESXi のパスワードとアカウントのロックアウト

ESXi ホストに対して、事前に定義された要件を満たすパスワードを使用する必要があります。

Security.PasswordQualityControl の詳細オプションを使用して、パスワードの文字数や文字の種類の要件の変更や、パスフレーズの許可ができます。

ESXi では、パスワードの管理および制御に Linux PAM モジュール pam\_passwdqc を使用します。詳細については、pam\_passwdqc のマニュアルページを参照してください。

---

**注：** ESXi パスワードのデフォルト要件は、リリースごとに変更される場合があります。

Security.PasswordQualityControl の詳細オプションを使用して、デフォルトのパスワード制限を確認および変更できます。

---

## ESXi のパスワード

ESXi では、ダイレクト コンソール ユーザー インターフェイス、ESXi Shell、SSH、または vSphere Client からのアクセスに使用するパスワードの要件があります。パスワードを作成する際、デフォルトでは、小文字、大文字、数字、および特殊文字（アンダースコアやダッシュなど）の 4 種類の文字を混在させる必要があります。

**注：** パスワードの先頭で大文字を使用する場合、これは文字の種類に含まれません。パスワードの末尾を数字にする場合、これは文字の種類に含まれません。

パスワードには、辞書ファイル内の単語または単語の一部を含めることはできません。

## ESXi のパスワードの例

次のようにオプション設定の場合のパスワードの候補です

```
retry=3 min=disabled,disabled,disabled,7,7
```

この設定では、1 種類または 2 種類の文字が含まれるパスワードと、パスフレーズは許可されません。これは、最初の 3 つのアイテムが無効に設定されているためです。パスワードには 3 種類および 4 種類の文字を使用し、7 文字の長さが必要です。詳細については、`pam_passwdqc` のマニュアルページを参照してください。

この設定では、次のパスワードが許可されます。

- xQaTEhb! : 3 種類の文字を使用した 8 文字のパスワード。
- xQaT3#A : 4 種類の文字を使用した 7 文字のパスワード。

次のパスワード候補は、要件を満たしていません。

- Xqat3hi : 先頭が大文字であるため、有効な文字クラスの数に 2 が減っています。パスワードには、3 種類以上の文字を使用する必要があります。
- xQaTEh2 : 数字で終わるため、有効な文字クラスの数に 2 が減っています。パスワードには、3 種類以上の文字を使用する必要があります。

## ESXi のパスフレーズ

パスワードの代わりに、パスフレーズを使用することもできますが、パスフレーズはデフォルトで無効になっています。このデフォルト設定やその他の設定を変更するには、vSphere Web Client から `Security.PasswordQualityControl` の詳細オプションを使用します。

たとえば、このオプションは次のように変更できます。

```
retry=3 min=disabled,disabled,16,7,7
```

この例では、最小で 16 文字を使用し、スペースで区切られた最小で 3 つの単語を含むパスフレーズを可能にしています。

レガシー ホストで `/etc/pamd/passwd` ファイルを変更することは引き続きサポートされますが、今後のリリースでは、ファイル変更のサポートは廃止されます。代わりに、`Security.PasswordQualityControl` の詳細オプションを使用します。

## デフォルトのパスワード制限の変更

パスワードまたはパスフレーズのデフォルトの制限を変更するには、ESXi ホストの `Security.PasswordQualityControl` 詳細オプションを使用します。ESXi 詳細オプションの設定の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

たとえば、最小 15 文字、最小で 4 つの単語数を要求するように変更するには、次のように指定します。

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

詳細については、`pam_passwdqc` のマニュアルページを参照してください。

---

**注：** `pam_passwdqc` のオプションは、可能なすべての組み合わせがテストされているわけではありません。デフォルトのパスワード設定を変更した後は、追加でテストを実行します。

---

## ESXi のアカウント ロックアウトの動作

vSphere 6.0 以降では、SSH 経由および vSphere Web Services SDK 経由のアクセスで、アカウントのロックがサポートされるようになりました。ダイレクト コンソール インターフェイス (DCUI) と ESXi Shell では、アカウント ロックアウトはサポートされていません。デフォルトでは、アカウントがロックされるまでに、ログイン試行の失敗が最大で 10 回許可されています。デフォルトでは 2 分後に、アカウントのロックが解除されます。

### ログイン動作の構成

ESXi ホストのログイン動作を構成するには、次の詳細オプションを使用します。

- `Security.AccountLockFailures`。ログインが失敗し、ユーザー アカウントがロックされるまでの最大試行回数です。ゼロにすると、アカウントのロックは無効になります。
- `Security.AccountUnlockTime`。ユーザーがロックアウトされる秒数です。

ESXi 詳細オプションの設定の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

## ESXi ネットワーク セキュリティに関する推奨事項

ESXi 環境の保護には、ネットワーク トラフィックの隔離が不可欠です。それぞれのネットワークで、さまざまなアクセスおよび隔離レベルが必要です。

ESXi ホストは、複数のネットワークを使用します。各ネットワークに適切なセキュリティ対策を使用し、特定のアプリケーションと機能のトラフィックを隔離します。たとえば、仮想マシンが配置されたネットワーク上を vSphere vMotion トラフィックが通過しないようにします。隔離するとスヌーピングされません。パフォーマンス上の理由からも、別個のネットワークを使用することを推奨します。

- VMware vSphere vMotion®、VMware vSphere Fault Tolerance、およびストレージなどの機能には、vSphere インフラストラクチャ ネットワークを使用します。このネットワークは、これらの特定の機能用に隔離されていると見なされ、単一の物理的なサーバ ラック セットの外にトラフィックが送信されることはほとんどありません。
- 管理ネットワークは、クライアントのトラフィック、コマンドライン インターフェイス (CLI) または API トラフィック、およびサードパーティ製のソフトウェア トラフィックを通常のトラフィックから隔離します。このネ

ットワークは、システム管理者、ネットワーク管理者、およびセキュリティ管理者のみがアクセスできるようにする必要があります。ジャンプ ボックスまたは仮想プライベート ネットワーク (VPN) を使用して管理ネットワークへのアクセスを保護します。このネットワーク内でマルウェアの発生源へのアクセスを厳しく制御します。

- 仮想マシンのトラフィックは、1 つ以上または多数のネットワークを通過できます。仮想ネットワーク コントローラーでファイアウォール ルールを設定した仮想ファイアウォール ソリューションを使用すると、仮想マシンの隔離を強化できます。vSphere 環境内のホスト間で仮想マシンを移行すると、これらの設定も仮想マシンとともに移行されます。

## 管理対象オブジェクト ブラウザ (MOB) の無効化

管理対象オブジェクト ブラウザには、VMkernel オブジェクト モデルを確認する方法が用意されています。ただし、この管理対象オブジェクト ブラウザを使用することでホストの構成を変更できるため、攻撃者がこのインターフェイスを使用して、悪意のある構成変更やアクションを実行する可能性があります。管理対象オブジェクト ブラウザはデバッグ用にのみ使用するようにし、本番システムでは無効にしてください。

vSphere 6.0 以降では、デフォルトで MOB が無効になっています。ただし、一部のタスク（システムから古い証明書を抽出する場合など）では MOB を使用する必要があります。

### 手順

- 1 vSphere Web Client でホストを選択し、[システムの詳細設定] に移動します。
- 2 [Config.HostAgent.plugins.solo.enableMob] の値を確認し、必要に応じて変更します。

ESXi Shell から `vim-cmd` を使用する方法は推奨されなくなりました。

## 許可されている (SSH) キーの無効化

許可されているキーを使用すると、ユーザー認証を経る必要なしに、SSH を介して ESXi ホストにアクセスできます。ホストのセキュリティを向上するには、ユーザーが許可されているキーを使用してホストにアクセスできないようにします。

ホスト上の `/etc/ssh/keys-root/authorized_keys` ファイルにパブリック キーを持つユーザーは、信頼済みユーザーとみなされます。信頼済みのリモート ユーザーは、パスワードを必要とせずにホストにアクセスできます。

### 手順

- ◆ 日常の運用では、ESXi ホストの SSH を無効します。
- ◆ SSH を有効にするときは、それがたとえ一時的であっても、`/etc/ssh/keys-root/authorized_keys` ファイルの内容を監視し、正しい認証を経ずにホストへアクセスするユーザーがいないことを確認します。
- ◆ `/etc/ssh/keys-root/authorized_keys` ファイルを監視し、ファイルに SSH 鍵が加えられていない空の状態であることを確認します。
- ◆ `/etc/ssh/keys-root/authorized_keys` ファイルが空でない場合は、鍵をすべて削除します。

## 結果

許可されているキーを使ったリモート アクセスを無効にすると、有効なログインなしではホスト上でコマンドをリモート実行する場合に制限を受ける可能性があります。たとえば、リモートで自動スクリプトを実行できなくなる場合があります。

## ESXi ホストの証明書管理

vSphere 6.0 以降では、VMware 認証局 (VMCA) が、VMCA をデフォルトでルート認証局とする署名付き証明書を使用して、新規の各 ESXi ホストをプロビジョニングします。プロビジョニングは、ホストが vCenter Server に明示的に追加される場合に、または ESXi 6.0 以降のインストールまたは 6.0 以降へのアップグレードの一環として実行されます。

これらの証明書は、vSphere Web Client から、または vSphere Web Services SDK の `vim.CertificateManager` API を使用して、表示および管理することができます。vCenter Server の証明書の管理に使用可能な証明書管理 CLI を使用して ESXi の証明書を表示または管理することはできません。

## vSphere 5.5 および vSphere 6.0 での証明書

ESXi および vCenter Server の通信では、ほとんどすべての管理トラフィックで SSL を使用します。

vSphere 5.5 以前の場合、SSL エンドポイントは、ユーザー名、パスワード、およびサムプリントの組み合わせによってのみ保護されています。ユーザーは、ユーザー独自の証明書を対応する自己署名証明書に置き換えることができます。vSphere 5.5 ドキュメント センターを参照してください。

vSphere 6.0 以降の場合、vCenter Server は、ESXi ホストで次の証明書モードをサポートします。

表 5-1. ESXi ホストの証明書モード

証明書モード	説明
VMware 認証局（デフォルト）	<p>このモードは、VMCA が、トップレベル CA または中間 CA のいずれかとしてすべての ESXi ホストをプロビジョニングする場合に使用します。</p> <p>デフォルトで VMCA は、証明書を使用して ESXi ホストをプロビジョニングします。</p> <p>このモードでは、vSphere Web Client から証明書を更新することができます。</p>
カスタム認証局	<p>このモードは、サードパーティ CA によって署名されたカスタム証明書のみを使用する場合に使用します。</p> <p>このモードでは、ユーザーが証明書を管理する必要があります。vSphere Web Client から証明書を更新することはできません。</p> <p><b>注：</b> 証明書モードをカスタム認証局に変更しない限り、VMCA により、たとえば vSphere Web Client で [更新] を選択するときに、カスタム証明書が置き換えられる可能性があります。</p>
サムプリント モード	<p>vSphere 5.5 ではサムプリント モードが使用されており、このモードは、vSphere 6.0 のフォールバック オプションとして引き続き使用することができます。このモードの場合、vCenter Server は、証明書の形式が正しいかどうかチェックしますが、証明書の有効性はチェックしません。期限切れの証明書であっても受諾されます。</p> <p>このモードは、他の 2 つのモードのいずれかによって解決できない問題が発生した場合以外は使用しないでください。vCenter 6.0 以降の一部のサービスは、サムプリント モードで正常に動作しない可能性があります。</p>

## 証明書有効期限

vSphere 6.0 以降、VMCA またはサードパーティ CA によって署名された証明書の証明書有効期限に関する情報を vSphere Web Client で表示することができます。vCenter Server によって管理されるすべてのホスト、または個別のホストに関する情報を表示できます。証明書が [間もなく期限切れ] 状態（8 か月未満）になっている場合は、黄色のアラームが表示されます。証明書が [期限切れ間近] 状態（2 か月未満）になっている場合は、赤のアラームが表示されます。

## ESXi のプロビジョニングと VMCA

インストール メディアから ESXi ホストを起動する場合、そのホストには初めに生成された証明書があります。ホストを vCenter Server システムに追加すると、そのホストは、ルート CA としての VMCA によって署名された証明書を使用してプロビジョニングされます。

このプロセスは、Auto Deploy でプロビジョニングされるホストの場合と同様です。ただし、それらのホストは状態を何も保存しないため、署名付き証明書は Auto Deploy サーバによってそのローカル証明書ストアに保存されません。その証明書は、ESXi ホストのその後の起動時に再使用されます。Auto Deploy サーバは、任意の組み込みデプロイ ノードまたは管理ノードの一部です。

Auto Deploy ホストは、初めて起動するときに VMCA が使用可能になっていない場合、最初に接続を試みてから、VMCA が使用可能になって、署名付き証明書を使用してホストをプロビジョニングできるようになるまで、シャットダウンと再起動の動作を繰り返します。



## ホスト名と IP アドレスの変更

vSphere 6.0 以降では、ホスト名または IP アドレスを変更すると、vCenter Server でホストの証明書が有効とみなされるかどうかに影響する場合があります。ホストを vCenter Server に追加したときの方法により、手動での介入が必要かどうかが決まります。手動での介入とは、ホストを再接続すること、つまり vCenter Server からホストを削除して再び追加することを意味します。

表 5-2. ホスト名または IP アドレスの変更により手動での介入が必要になる場合

ホストを vCenter Server に追加する方法	ホスト名の変更	IP アドレスの変更
ホスト名	vCenter Server の接続問題。手動での介入が必要。	介入不要。
IP アドレス	介入不要。	vCenter Server の接続問題。手動での介入が必要。



ESXi 証明書管理

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_vkuyp3rf/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/))

## ホストのアップグレードと証明書

ESXi ホストを ESXi 6.0 以降にアップグレードすると、アップグレード プロセスで自己署名証明書が VMCA 署名付き証明書に置き換えられます。このプロセスでは、証明書が有効期限切れまたは無効な場合でもカスタム証明書は保持されます。

推奨されるアップグレード ワークフローは、現在の証明書によって異なります。

### サムプリント証明書でプロビジョニングされたホスト

現在、ホストでサムプリント証明書が使用されている場合、アップグレード プロセスの一部として VMCA 証明書が自動的に割り当てられます。

**注：** VMCA 証明書を使用してレガシー ホストをプロビジョニングすることはできません。ESXi 6.0 以降にアップグレードする必要があります。

### カスタム証明書でプロビジョニングされたホスト

カスタム証明書（通常はサードパーティ CA 署名付き証明書）を使用してホストがプロビジョニングされている場合、これらの証明書は有効なままです。証明書モードをカスタムに変更すると、証明書が誤って置き換えられることを回避できます。

**注：** VMCA モードの環境の場合、vSphere Web Client から証明書を更新すると、既存の証明書が VMCA で署名された証明書に置き換えられます。

その後、vCenter Server によって証明書が監視され、証明書の有効期限などの情報が vSphere Web Client に表示されます。

ホストを vSphere 6.0 以降にアップグレードしない場合、VMCA 証明書を使用する vCenter Server システムによってホストが管理されていても、現在使用している証明書がホストで保持されます。

Auto Deploy でプロビジョニングされるホストには、ESXi 6.0 ソフトウェアを使用して最初に起動したときに常に新しい証明書が割り当てられます。Auto Deploy でプロビジョニングされたホストをアップグレードする場合、Auto Deploy サーバによってホストの証明書署名要求 (CSR) が生成され、VMCA に送信されます。VMCA には、ホストの署名証明書が保存されています。Auto Deploy サーバがホストをプロビジョニングすると、VMCA から証明書を取得し、プロビジョニング プロセスの一部としてその証明書を含めます。

Auto Deploy は、カスタム証明書とともに使用できます。

## ESXi 証明書のデフォルト設定

vCenter Server は、証明書署名要求 (CSR) を ESXi ホストに要求するとき、デフォルトの設定を使用します。デフォルト値の大部分は多くの状況に適していますが、会社固有の情報を変更できます。

組織および場所の情報を変更することを検討します。デフォルト設定の多くは、vSphere Web Client を使用して変更できます。[証明書のデフォルト設定の変更](#) を参照してください。

表 5-3. CSR 設定

パラメータ	デフォルト値	詳細オプション
キーのサイズ	2048	N.A.
キーのアルゴリズム	RSA	N.A.
証明書署名アルゴリズム	sha256WithRSAEncryption	N.A.
共通名	ホストがホスト名に基づいて vCenter Server に追加された場合は、ホスト名。 ホストが IP アドレスに基づいて vCenter Server に追加された場合は、IP アドレス。	N.A.
国	USA	vpxd.certmgmt.certs.cn.country
電子メール アドレス	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
地域 (市)	Palo Alto	vpxd.certmgmt.certs.cn.localityName
組織単位名	VMware エンジニアリング	vpxd.certmgmt.certs.cn.organizationalUnitName
組織名	VMware	vpxd.certmgmt.certs.cn.organizationName
州または県	California	vpxd.certmgmt.certs.cn.state
証明書が有効な日数。	1825	vpxd.certmgmt.certs.cn.daysValid
証明書有効期限切れのハードしきい値 このしきい値に到達すると、vCenter Server は赤いアラームを表示します。	30 日	vpxd.certmgmt.certs.cn.hardThreshold
vCenter Server 証明書の有効性検査 間隔をポーリングします。	5 日	vpxd.certmgmt.certs.cn.pollIntervalDays

表 5-3. CSR 設定（続き）

パラメータ	デフォルト値	詳細オプション
証明書有効期限切れのソフトしきい値 このしきい値に到達すると、vCenter Server はイベントを表示します。	240 日	vpxd.certmgmt.certs.cn.softThreshold
既存の証明書が置換されているかどうかを判断するために vCenter Server が使用するモード。アップグレード中にカスタム証明書を保持するには、このモードを変更します。 <a href="#">ホストのアップグレードと証明書</a> を参照してください。	デフォルトは vmca です。 サンプリントまたはカスタムを指定することもできます。 <a href="#">証明書モードの変更</a> を参照してください。	vpxd.certmgmt.mode

## 複数の ESXi ホストの証明書有効期限情報の表示

ESXi 6.0 以降を使用している場合は、vCenter Server システムで管理しているすべてのホストの証明書ステータスを表示できます。表示される情報により、間もなく期限切れになる証明書があるかどうかを判断できます。

vSphere Web Client では、VMCA モードを使用しているホストとカスタム モードを使用しているホストの証明書ステータス情報を表示できます。サンプリント モードのホストの証明書ステータス情報は表示できません。

### 手順

- 1 vSphere Web Client インベントリ階層で、ホストに移動して参照します。  
デフォルトでは、[ホスト] の表示に証明書ステータスは含まれていません。
- 2 [名前] フィールドを右クリックし、[列の表示/非表示] を選択します。
- 3 [証明書の有効期限終了日] を選択し、[OK] をクリックして、必要に応じて右方向にスクロールします。  
証明書情報に、証明書の有効期限が表示されます。  
ホストを vCenter Server に追加するか、または一度切断してから再接続すると、vCenter Server は、ステータスが [期限切れ]、[有効期限間近]、[間もなく期限切れ]、または [期限切れ間近] になっている場合、証明書を更新します。ステータスは、残りの有効期間が 8 か月を切ると [有効期限間近]、2 か月を切ると [間もなく期限切れ]、1 か月を切ると [期限切れ間近] になります。
- 4 （オプション） その他の列は選択解除し、作業中の対象が見やすくなるようにしてください。

### 次のステップ

間もなく期限が切れる証明書を更新します。[ESXi 証明書の更新](#) を参照してください。

## 単一 ESXi ホストの証明書の詳細の表示

VMCA モードまたはカスタム モードの ESXi 6.0 以降のホストの場合は、vSphere Web Client から証明書の詳細を表示できます。証明書に関する情報は、デバッグで役立つことができます。

### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。

- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] を選択し、[証明書] をクリックします。

次の情報を調査することができます。この情報は、単一ホスト表示でのみ表示可能です。

フィールド	説明
件名	証明書の生成中に使用される件名。
発行者	証明書の発行者。
有効期間の開始	証明書が生成された日付。
有効期間の終了	証明書の有効期限。
ステータス	次のいずれかの証明書のステータス。
	<b>良好</b>
	通常動作。
	<b>期限切れ</b>
	証明書はもうすぐ有効期限が切れます。
	<b>間もなく期限切れ</b>
	証明書は 8 か月以内に期限切れになります（デフォルト）。
	<b>期限切れ間近</b>
	証明書は 2 か月以内に期限切れになります（デフォルト）。
	<b>期限切れ</b>
	証明書は期限切れのため有効ではありません。

## ESXi 証明書の更新

使用する ESXi ホスト（6.0 以降）に VMCA によって証明書が割り当てられた場合は、vSphere Web Client からそれらの証明書を更新することができます。また、vCenter Server に関連付けられている TRUSTED\_ROOTS ストアからすべての証明書を更新することもできます。

証明書は、もう少しで期限切れになる場合、またはそれ以外の理由により新規証明書を使用してホストをプロビジョニングする必要がある場合に、更新することができます。証明書がすでに期限切れになっている場合は、ホストをいったん切断して再接続する必要があります。

デフォルトで vCenter Server は、ホストがインベントリに追加されるか再接続されるたびに、ステータスが [期限切れ]、[期限切れ間近]、または [有効期限間近] になっている証明書を更新します。

### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] を選択し、[証明書] をクリックします。

選択したホストの証明書に関する詳細を表示できます。

- 4 [更新] または [CA 証明書の更新] をクリックします。

オプション	説明
更新	VMCA から、ホストの更新された署名証明書を取得します。
CA 証明書の更新	vCenter Server VECS ストアの TRUSTED_ROOTS ストアにあるすべての証明書をホストにプッシュします。

- 5 [はい] をクリックして確認します。

## 証明書のデフォルト設定の変更

ホストが vCenter Server システムに追加されると、vCenter Server はホストの証明書署名要求 (CSR) を VMCA に送信します。vSphere Web Client の vCenter Server 詳細設定を使用して、CSR のデフォルト設定の一部を変更できます。

組織に特有のデフォルト証明書設定を変更します。デフォルト設定の完全なリストについては、[ESXi 証明書のデフォルト設定](#)を参照してください。一部のデフォルトは変更できません。

### 手順

- 1 vSphere Web Client で、ホストを管理している vCenter Server システムを選択します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [詳細設定] をクリックし、[編集] をクリックします。
- 4 [フィルタ] ボックスに「**certmgmt**」と入力し、証明書管理パラメータのみを表示します。
- 5 会社のポリシーに合わせて既存のパラメータの値を変更し、[OK] をクリックします。

次に vCenter Server にホストを追加するときに、vCenter Server から VMCA に送信される CSR と、ホストに割り当てられる証明書で新しい設定が使用されます。

### 次のステップ

証明書のメタデータへの変更は、新しい証明書にのみ影響します。すでに vCenter Server システムで管理されているホストの証明書を変更する場合、ホストを切断してから再接続します。

## 証明書モードの切り替えについて

vSphere 6.0 以降では、ESXi ホストはデフォルトで VMCA によって証明書を使用してプロビジョニングされます。代わりに、カスタム証明書モードまたはサムプリント モード (デバッグ用) を使用することもできます。ほとんどの場合、モードの切り替えは無停止で行うことはできず、切り替える必要ありません。モードの切り替えが必要な場合、開始する前に潜在的な影響を確認してください。

vSphere 6.0 以降の場合、vCenter Server は、ESXi ホストで次の証明書モードをサポートします。

表 5-4. ESXi ホストの証明書モード

証明書モード	説明
VMware 認証局（デフォルト）	デフォルトでは、VMware 認証局が ESXi ホスト証明書の CA として使用されます。デフォルトでは VMCA がルート CA ですが、別の CA への中間 CA として設定できます。このモードでは、ユーザーは vSphere Web Client から証明書を管理できます。これは、VMCA が従属証明書の場合も使用されます。
カスタム認証局	各自の外部認証局を管理する方が都合が良い場合もあります。このモードでは顧客が証明書を管理するため、vSphere Web Client から管理することはできません。
サムプリント モード	vSphere 5.5 ではサムプリント モードが使用されており、このモードは、vSphere 6.0 のフォールバック オプションとして引き続き使用することができます。このモードは、他の 2 つのモードで解決できない問題が発生した場合にのみ使用してください。vCenter 6.0 以降の一部のサービスは、サムプリント モードで正常に動作しない可能性があります。

## カスタム ESXi 証明書の使用

会社のポリシーで、VMCA とは異なるルート CA が求められる場合、綿密に計画した上で使用環境の証明書モードを切り替えることができます。推奨ワークフローは次のとおりです。

- 1 使用する証明書を取得します。
- 2 ホストをメンテナンス モードにして、vCenter Server から切断します。
- 3 カスタム CA のルート証明書を VECS に追加します。
- 4 カスタム CA 証明書を各ホストにデプロイし、そのホストでサービスを再起動します。
- 5 カスタム CA モードに切り替えます。[証明書モードの変更](#)を参照してください。
- 6 ホストを vCenter Server システムに接続します。

## カスタム CA モードから VMCA モードへの切り替え

カスタム CA モードを使用していて、使用環境では VMCA を使用の方が適切だと判断した場合、綿密に計画してからモードの切り替えを実行できます。推奨ワークフローは次のとおりです。

- 1 vCenter Server システムからすべてのホストを削除します。
- 2 vCenter Server システムで、VECS からサードパーティ CA のルート証明書を削除します。
- 3 VMCA モードに切り替えます。[証明書モードの変更](#)を参照してください。
- 4 ホストを vCenter Server システムに追加します。

**注：** このモードの切り替えを他のワークフローで行うと、予期しない動作が発生する可能性があります。

## アップグレード時のサムプリント モードの証明書の取得

VMCA 証明書に問題が発生した場合、VMCA モードからサムプリント モードへの切り替えが必要になることがあります。サムプリント モードでは、vCenter Server システムにより、証明書が存在していて、正しい形式であるかどうかのみがチェックされ、証明書が有効であるかどうかはチェックされません。構成方法については、[証明書モードの変更](#) を参照してください。

## サムプリント モードから VMCA モードへの切り替え

サムプリント モードを使用していて、VMCA 署名付き証明書の使用を開始する場合、計画を立てた上で切り替えを行う必要があります。推奨ワークフローは次のとおりです。

- 1 vCenter Server システムからすべてのホストを削除します。
- 2 VMCA 証明書モードに切り替えます。[証明書モードの変更](#)を参照してください。
- 3 ホストを vCenter Server システムに追加します。

---

**注：** このモードの切り替えを他のワークフローで行うと、予期しない動作が発生する可能性があります。

---

## カスタム CA モードからサムプリント モードへの切り替え

カスタム CA に問題が発生した場合、一時的にサムプリント モードに切り替えることを検討してください。[証明書モードの変更](#)の指示に従えば、切り替えをシームレスに行うことができます。モードを切り替えると、vCenter Server システムにより証明書の形式のみがチェックされ、証明書自体の有効性はチェックされなくなります。

## サムプリント モードからカスタム CA モードへの切り替え

トラブルシューティング時に使用環境をサムプリント モードに設定していて、カスタム CA モードの使用を開始する場合、まず必要な証明書を生成する必要があります。推奨ワークフローは次のとおりです。

- 1 vCenter Server システムからすべてのホストを削除します。
- 2 カスタム CA ルート証明書を vCenter Server システムの VECS の TRUSTED\_ROOTS ストアに追加します。[vCenter Server TRUSTED\\_ROOTS ストア（カスタム証明書）の更新](#)を参照してください。
- 3 各 ESXi ホストで、次の操作を実行します。
  - a カスタム CA 証明書およびキーをデプロイします。
  - b ホストのサービスを再起動します。
- 4 カスタム モードに切り替えます。[証明書モードの変更](#)を参照してください。
- 5 ホストを vCenter Server システムに追加します。

## 証明書モードの変更

ほとんどの場合、VMCA を使用して ESXi ホストを使用環境にプロビジョニングすることが最適な解決方法になります。企業のポリシーで、異なるルート CA のカスタム証明書を使用することが求められている場合は、証明書の更新時に VMCA 証明書を使用してホストが自動的にプロビジョニングされないように vCenter Server 詳細オプションを編集できます。その後、ユーザーが使用環境で証明書を管理します。

vCenter Server 詳細設定を使用して、サムプリント モードまたはカスタム CA モードに変更できます。サムプリント モードは、フォールバック オプションとしてのみ使用します。

#### 手順

- 1 ホストを管理する vCenter Server を選択し、[設定] をクリックします。
- 2 [詳細設定] をクリックし、[編集] をクリックします。
- 3 [フィルタ] ボックスに、**certmgmt** と入力し、証明書管理キーのみを表示します。
- 4 独自の証明書を管理する場合は `vpxd.certmgmt.mode` の値を [custom] に変更し、一時的にサムプリント モードを使用する場合は [thumbprint] に変更して、[OK] をクリックします。
- 5 vCenter Server サービスを再起動します。

## ESXi SSL 証明書とキーの置き換え

会社のセキュリティ ポリシーにより、各ホストでデフォルトの ESXi SSL 証明書をサードパーティ CA 署名付き証明書と置き換えるように要求される場合があります。

vSphere コンポーネントは、デフォルトで、インストール時に作成される VMCA 署名付き証明書とキーを使用します。誤って VMCA 署名付き証明書を削除してしまった場合、その vCenter Server システムからホストを削除し、再度追加します。ホストを追加すると、vCenter Server は、VMCA の新しい証明書を要求し、その証明書を使用してホストをプロビジョニングします。

会社のポリシー上必要な場合は、VMCA 署名付き証明書を、商業認証局または組織認証局のいずれかの信頼できる CA からの証明書で置き換えます。

デフォルトの証明書は、vSphere 5.5 証明書と同じ場所にあります。デフォルトの証明書は、いくつかの方法で信頼できる証明書と置き換えることができます。

---

**注：** vSphere Web Services SDK の `vim.CertificateManager` および `vim.host.CertificateManager` 管理対象オブジェクトを使用することもできます。vSphere Web Services SDK のドキュメントを参照してください。

---

証明書を置き換えたら、vCenter Server および ESXi ホストの信頼関係を確保するために、ホストを管理する vCenter Server システムの VECS の TRUSTED\_ROOTS ストアを更新する必要があります。

#### ■ ESXi 証明書署名要求の要件

サードパーティ CA 署名付き証明書を使用する場合（VMCA またはカスタム認証局のいずれかが従属局）、証明書署名要求 (CSR) を CA に送信する必要があります。

#### ■ ESXi Shell からのデフォルトの証明書とキーの置き換え

ESXi Shell からのデフォルトの VMCA 署名付き ESXi 証明書は、置き換えることができます。

#### ■ vifs コマンドを使用したデフォルトの証明書と鍵の置き換え

`vifs` コマンドにより、デフォルトの VMCA 署名付き ESXi 証明書を置き換えることができます。



## ■ HTTPS PUT を使用したデフォルトの証明書の置き換え

サードパーティ製のアプリケーションを使用して、証明書とキーをアップロードできます。HTTPS の PUT 操作をサポートするアプリケーションは、ESXi に含まれている HTTPS インターフェイスと連動します。

## ■ vCenter Server TRUSTED\_ROOTS ストア（カスタム証明書）の更新

カスタム証明書を使用するように ESXi ホストを設定した場合は、ホストを管理する vCenter Server システムの TRUSTED\_ROOTS ストアを更新する必要があります。

## ESXi 証明書署名要求の要件

サードパーティ CA 署名付き証明書を使用する場合（VMCA またはカスタム認証局のいずれかが従属局）、証明書署名要求 (CSR) を CA に送信する必要があります。

次の特性を持つ CSR を使用します。

- 2048 ビット
- PKCS1
- ワイルドカードなし
- 現在時刻の 1 日前の開始時刻
- vCenter Server インベントリにある、ESXi ホストのホスト名（または IP アドレス）に設定された CN（および SubjectAltName）

## ESXi Shell からのデフォルトの証明書とキーの置き換え

ESXi Shell からのデフォルトの VMCA 署名付き ESXi 証明書は、置き換えることができます。

### 前提条件

- サードパーティ CA 署名付き証明書を使用する場合は、証明書要求を生成し、それを認証局に送信して、各 ESXi ホストに証明書を保存します。
- 必要に応じて、ESXi Shell を有効にするか、または vSphere Web Client からの SSH トラフィックを有効にします。ESXi Shell へのアクセスを有効にする方法については、vSphere セキュリティ のドキュメントを参照してください。
- ファイルのすべての転送および通信は、安全な HTTPS セッションを介して行われます。セッションの認証に使用するユーザーには、ホストに対する ホスト.構成.詳細構成権限が必要です。ロールを介した権限の割り当てについては、vSphere セキュリティドキュメントを参照してください。

### 手順

- 1 ESXi Shell に、管理者権限を持つユーザーとして、DCUI から直接、または SSH クライアントからログインします。
- 2 ディレクトリ /etc/vmware/ssl で、次のコマンドを使用して、既存の証明書の名前を変更します。

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

- 3 使用する証明書を `/etc/vmware/ssl` にコピーします。
- 4 新しい証明書と鍵を、`rui.crt` および `rui.key` にそれぞれ名前変更します。
- 5 新しい証明書をインストールしたら、ホストを再起動します。

または、ホストをメンテナンス モードにして、新しい証明書をインストールした後、ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用して管理エージェントを再起動し、メンテナンス モードを終了するようにホストを設定することができます。

#### 次のステップ

vCenter Server TRUSTED\_ROOTS ストアを更新します。 [vCenter Server TRUSTED\\_ROOTS ストア \(カスタム証明書\) の更新](#) を参照してください。

### vifs コマンドを使用したデフォルトの証明書と鍵の置き換え

`vifs` コマンドにより、デフォルトの VMCA 署名付き ESXi 証明書を置き換えることができます。

#### 前提条件

- サードパーティ CA 署名付き証明書を使用する場合は、証明書要求を生成し、それを認証局に送信して、各 ESXi ホストに証明書を保存します。
- 必要に応じて、ESXi Shell を有効にするか、または vSphere Web Client からの SSH トラフィックを有効にします。ESXi Shell へのアクセスを有効にする方法については、vSphere セキュリティ のドキュメントを参照してください。
- ファイルのすべての転送および通信は、安全な HTTPS セッションを介して行われます。セッションの認証に使用するユーザーには、ホストに対する `ホスト.構成.詳細構成権限` が必要です。ロールを介した権限の割り当てについては、vSphere セキュリティドキュメントを参照してください。

#### 手順

- 1 既存の証明書をバックアップします。
- 2 認証局からの指示に従って証明書要求を生成します。
- 3 証明書がある場合は、`vifs` コマンドを使用して、SSH 接続からホストの適切な場所に証明書をアップロードします。

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

- 4 ホストを再起動します。

#### 次のステップ

vCenter Server TRUSTED\_ROOTS ストアを更新します。 [vCenter Server TRUSTED\\_ROOTS ストア \(カスタム証明書\) の更新](#) を参照してください。

## HTTPS PUT を使用したデフォルトの証明書の置き換え

サードパーティ製のアプリケーションを使用して、証明書とキーをアップロードできます。HTTPS の PUT 操作をサポートするアプリケーションは、ESXi に含まれている HTTPS インターフェイスと連動します。

### 前提条件

- サードパーティ CA 署名付き証明書を使用する場合は、証明書要求を生成し、それを認証局に送信して、各 ESXi ホストに証明書を保存します。
- 必要に応じて、ESXi Shell を有効にするか、または vSphere Web Client からの SSH トラフィックを有効にします。ESXi Shell へのアクセスを有効にする方法については、vSphere セキュリティ のドキュメントを参照してください。
- ファイルのすべての転送および通信は、安全な HTTPS セッションを介して行われます。セッションの認証に使用するユーザーには、ホストに対する ホスト構成.詳細構成権限が必要です。ロールを介した権限の割り当てについては、vSphere セキュリティドキュメントを参照してください。

### 手順

- 1 既存の証明書をバックアップします。
- 2 アップロード アプリケーションで、各ファイルを次のように処理します。
  - a ファイルを開きます。
  - b 次のいずれかの場所にファイルをパブリッシュします。

オプション	説明
証明書	<code>https://hostname/host/ssl_cert</code>
鍵	<code>https://hostname/host/ssl_key</code>

場所 `/host/ssl_cert` および `host/ssl_key` は、`/etc/vmware/ssl` 内の証明書ファイルにリンクします。

- 3 ホストを再起動します。

### 次のステップ

vCenter Server TRUSTED\_ROOTS ストアを更新します。 [vCenter Server TRUSTED\\_ROOTS ストア（カスタム証明書）の更新](#) を参照してください。

## vCenter Server TRUSTED\_ROOTS ストア（カスタム証明書）の更新

カスタム証明書を使用するように ESXi ホストを設定した場合は、ホストを管理する vCenter Server システムの TRUSTED\_ROOTS ストアを更新する必要があります。

### 前提条件

各ホストの証明書をカスタム証明書で置き換えます。

## 手順

- 1 ESXi ホストを管理する vCenter Server システムにログインします。

ソフトウェアをインストールした Windows システムにログインするか、vCenter Server Appliance シェルにログインします。

- 2 たとえば次のように、vecs-cli を実行して、新しい証明書を TRUSTED\_ROOTS ストアに追加します。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

オプション	説明
Linux	<pre>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/ custom1.crt</pre>
Windows	<pre>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt -- cert c:\ssl\custom1.crt</pre>

## 次のステップ

証明書モードをカスタムに設定します。証明書モードがデフォルトの VMCA の場合、証明書の更新を実行すると、カスタム証明書は VMCA 署名付き証明書に置き換えられます。[証明書モードの変更](#)を参照してください。

## Auto Deploy でのカスタム証明書の使用

デフォルトでは、Auto Deploy サーバは VMCA が署名した証明書を使用して各ホストをプロビジョニングします。VMCA が署名していないカスタム証明書を使用してすべてのホストをプロビジョニングするように、Auto Deploy サーバを設定できます。このシナリオでは、Auto Deploy サーバはサードパーティ認証局の従属認証局になります。

## 前提条件

- 要件を満たす証明書を認証局に要求します。
  - キー サイズ : 2,048 ビット以上 (PEM エンコード)
  - PEM 形式。VMware では、PKCS8 および PKCS1 (RSA キー) がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
  - x509 バージョン 3
  - ルート証明書の場合、認証局の拡張を true に設定する必要があり、証明書の署名を要件の一覧に含める必要があります。
  - SubjectAltName には DNS Name=<machine\_FQDN> が含まれている必要があります。
  - CRT 形式
  - キー使用法として、デジタル署名、非否認、キー暗号化が含まれている必要があります。
  - 現在時刻の 1 日前の開始時刻

- vCenter Server インベントリにある、ESXi ホストのホスト名（または IP アドレス）に設定された CN（および SubjectAltName）
- 証明書とキーのファイル（`rbd-ca.crt` と `rbd-ca.key`）に名前を付けます。

#### 手順

- 1 デフォルトの ESXi 証明書をバックアップします。  
証明書は、`/etc/vmware-rbd/ssl/` にあります。
- 2 vSphere Web Client から Auto Deploy サービスを停止します。
  - a [管理] を選択し、[デプロイ] で [システム構成] をクリックします。
  - b [サービス] をクリックします。
  - c 停止するサービスを右クリックして、[停止] を選択します。
- 3 Auto Deploy サービスが動作しているシステムで、`/etc/vmware-rbd/ssl/` 内の `rbd-ca.crt` と `rbd-ca.key` を、カスタム証明書とキーのファイルに置換します。
- 4 Auto Deploy サービスが動作しているシステムで、新しい証明書を使用するように、VECS 内の TRUSTED\_ROOTS ストアを更新します。

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
                        rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
                        rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

#### Windows

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

#### Linux

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

- 5 TRUSTED\_ROOTS の内容を含む `castore.pem` ファイルを作成して、そのファイルを `/etc/vmware-rbd/ssl/` ディレクトリに格納します。  
カスタム モードでは、このファイルの保守が必要になります。
- 6 vCenter Server システムの証明書モードを **custom** に変更します。  
[証明書モードの変更](#) を参照してください。
- 7 vCenter Server サービスを再開し、Auto Deploy サービスを開始します。

#### 結果

次に Auto Deploy を使用するように設定されているホストをプロビジョニングするとき、Auto Deploy サーバは、TRUSTED\_ROOTS ストアに追加したルート証明書を使用して、証明書を生成します。

## ESXi 証明書とキー ファイルのリストア

vSphere Web Services SDK を使用して ESXi ホストの証明書を置き換えると、以前の証明書とキーが .bak ファイルに追加されます。 .bak ファイルの情報を現在の証明書とキー ファイルに移動すれば、以前の証明書をリストアできます。

ホストの証明書とキーは /etc/vmware/ssl/rui.crt と /etc/vmware/ssl/rui.key にあります。 vSphere Web Services SDK の vim.CertificateManager 管理対象オブジェクトを使用してホストの証明書とキーを置き換えると、以前のキーと証明書が /etc/vmware/ssl/rui.bak ファイルに追加されます。

**注：** HTTP PUT、vifs、または ESXi Shell を使用して証明書を置き換えると、既存の証明書は .bak ファイルに追加されません。

### 手順

- 1 ESXi ホストで、 /etc/vmware/ssl/rui.bak ファイルを探します。

ファイルの形式は次のようになります。

```
## 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 -----BEGIN PRIVATE KEY----- から -----END PRIVATE KEY----- までのテキストを /etc/vmware/ssl/rui.key ファイルにコピーします。

-----BEGIN PRIVATE KEY----- および -----END PRIVATE KEY----- も含めます。

- 3 -----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- までのテキストを /etc/vmware/ssl/rui.crt ファイルにコピーします。

-----BEGIN CERTIFICATE----- および -----END CERTIFICATE----- も含めます。

- 4 ホストを再起動するか、キーを使用するすべてのサービスに ssl\_reset イベントを送信します。

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

## セキュリティ プロファイルによるホストのカスタマイズ

ホストの基本的なセキュリティ設定の大半は、vSphere Web Client の [セキュリティ プロファイル] パネルでカスタマイズできます。[セキュリティ プロファイル] は、特に単一のホストの管理に有用です。複数のホストを管理する場合は、CLI または SDK のどちらかを使用してカスタマイズ作業を自動化することを検討してください。

## ESXi ファイアウォールの構成

ESXi には、デフォルトで有効になっているファイアウォールが含まれています。

インストール時、ESXi ファイアウォールは、受信トラフィックと送信トラフィックをブロックするように構成されています。ただし、ホストのセキュリティ プロファイルで有効なサービスのトラフィックは除外されます。

ファイアウォールのポートを開くときには、ESXi ホストで実行されているサービスへのアクセスを制限しなければ、そのホストが外部攻撃と不正アクセスの危険にさらされることを考慮します。認証済みのネットワークからのアクセスのみを許可するように ESXi ファイアウォールを構成してリスクを軽減します。

---

**注：** ファイアウォールは、ICMP (Internet Control Message Protocol) の ping と、DHCP および DNS (UDP のみ) クライアントとの通信も許可します。

---

次のように ESXi ファイアウォール ポートを管理できます。

- vSphere Web Client の各ホストのセキュリティ プロファイルを使用します。 [ESXi ファイアウォール設定の管理](#)を参照してください。
- コマンド ラインまたはスクリプトで ESXCLI コマンドを使用します。 [ESXi ESXCLI ファイアウォールのコマンド](#)を参照してください。
- 開く必要があるポートがセキュリティ プロファイルに含まれていない場合にカスタム VIB を使用します。

VMware Lab で入手できる vibauthor ツールを使用してカスタム VIB を作成します。カスタム VIB をインストールするには、ESXi ホストの許容レベルを CommunitySupported に変更する必要があります。弊社のナレッジ ベースの記事 [2007381](#) を参照してください。

---

**注：** CommunitySupported VIB がインストールされた ESXi ホストで VMware テクニカル サポートを使用して問題を調査する場合、VMware サポートは、トラブルシューティング手順として、VIB が調査している問題に関係があるかどうかを判断するためにこの CommunitySupported VIB のアンインストールを要求する場合があります。

---



ESXi ファイアウォールの概念

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_8qp59yqe/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/))

NFS クライアントのルール セット (nfsClient) の動作は、ほかのルール セットとは異なります。NFS クライアントのルール セットが有効な場合、すべての送信 TCP ポートは、許可された IP アドレス一覧のターゲット ホストに対して開かれます。詳細については [NFS クライアント ファイアウォールの動作](#)を参照してください。

## ESXi ファイアウォール設定の管理

vSphere Web Client またはコマンドラインでサービスや管理エージェント用の着信および発信ファイアウォール接続を構成できます。

---

**注：** 異なるサービスに重複するポート ルールが適用されている場合は、1 つのサービスを有効にすると、他のサービスも暗黙的に有効化されます。どの IP アドレスにホストの各サービスへのアクセスを許可するかを指定するとこの問題を回避できます。

---

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [セキュリティ プロファイル] をクリックします。

vSphere Web Client により、アクティブな着信および発信接続や、それを対応するファイアウォール ポートのリストが表示されます。

- 4 [ファイアウォール] セクションで [編集] をクリックします。  
ルール名と関連情報を含むファイアウォール ルール セットが画面に表示されます。
- 5 ルール セットを選択して有効にするか、ルール セットを選択解除して無効にします。

列	説明
着信ポートおよび発信ポート	vSphere Web Client がサービス用に開くポート
プロトコル	サービスが使用するプロトコル。
デーモン	サービスに関連付けられたデーモンのステータス。

- 6 一部のサービスでは、サービスの詳細を管理できます。
  - [開始] ボタン、[停止] ボタン、または [再起動] ボタンを使用して、一時的にサービスのステータスを変更します。
  - ホストまたはポートに連動してサービスを開始するように、開始ポリシーを変更します。
- 7 一部のサービスでは、接続を許可する IP アドレスを明示的に指定できます。  
[ESXi ホストで許可される IP アドレスの追加](#) を参照してください。
- 8 [OK] をクリックします。

## ESXi ホストで許可される IP アドレスの追加

デフォルトでは、各サービスのファイアウォールはすべての IP アドレスのアクセスを許可します。トラフィックを制限するには、管理サブネットからのトラフィックのみを許可するように各サービスを変更します。環境で使用されないサービスがある場合には、それらの選択を解除することもできます。

vSphere Web Client、vCLI、または PowerCLI を使用して、サービスへの接続を許可された IP アドレスのリストを更新できます。デフォルトでは、1 つのサービスに対してすべての IP アドレスが許可されています。



ESXi ファイアウォールへの許可された IP アドレスの追加

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_Ougsspa2/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/))

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックします。



- 4 [ファイアウォール] セクションで [編集] をクリックし、リストからサービスを選択します。
- 5 [許可された IP アドレス] セクションで [任意の IP アドレスからの接続を許可します] の選択を解除し、ホストへの接続を許可するネットワークの IP アドレスを入力します。

IP アドレスをコンマで区切ります。次のアドレス形式を使用できます。

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

- 6 [OK] をクリックします。

## ESXi ホストの送受信ファイアウォール ポート

vSphere Web Client では、各サービスのファイアウォール ポートの開閉や、選択した IP アドレスからのトラフィックの許可が可能になります。

次の表に、通常インストールされるサービスのファイアウォールを一覧表示します。他の VIB をホストにインストールすることで、その他のサービスおよびファイアウォール ポートを追加で利用できるようになる場合があります。

表 5-5. 受信ファイアウォール接続

サービス	ポート	コメント
CIM サーバ	5988 (TCP)	CIM (Common Information Model) のサーバ。
CIM セキュア サーバ	5989 (TCP)	CIM のセキュア サーバ。
CIM SLP	427 (TCP、UDP)	CIM クライアントは、サービス ロケーション プロトコル バージョン 2 (SLPv2) を使用して、CIM サーバを検索します。
DHCPv6	546 (TCP、UDP)	IPv6 の DHCP クライアント。
DVSSync	8301、8302 (UDP)	DVSSync ポートは、VMware FT の記録/再生が有効なホスト間で分散仮想ポートの状態を同期するために使用されます。これらのポートは、プライマリまたはバックアップ仮想マシンを実行しているホストでのみ開いている必要があります。VMware FT を使用していないホストでは、これらのポートが開いている必要はありません。
NFC	902 (TCP)	NFC (ネットワーク ファイル コピー) によって、vSphere コンポーネントでファイル タイプに対応した FTP サービスを使用できます。ESXi は、データストア間のデータのコピーや移動などの操作にデフォルトで NFC を使用します。
Virtual SAN クラスタリング サービス	12345、23451 (UDP)	Virtual SAN クラスタ監視およびメンバーシップ ディレクトリ サービス。UDP ベースの IP マルチキャストを使用してクラスタ メンバーを確立し、Virtual SAN メタデータをすべてのクラスタ メンバーに配布します。無効になっている場合、Virtual SAN は機能しません。
DHCP クライアント	68 (UDP)	IPv4 の DHCP クライアント。
DNS クライアント	53 (UDP)	DNS クライアント。

表 5-5. 受信ファイアウォール接続 (続き)

サービス	ポート	コメント
Fault Tolerance	8200、8100、8300 (TCP、UDP)	vSphere Fault Tolerance (FT) 用のホスト間のトラフィック。
NSX 分散論理ルータ サービス	6999 (UDP)	NSX 仮想分散ルーター サービス。NSX VIB がインストールされていて、VDR モジュールが作成されている場合、このサービスに関連付けられているファイアウォール ポートが開きます。VDR インスタンスがホストに関連付けられていない場合、ポートが開いている必要はありません。 このサービスは、この製品の以前のバージョンでは NSX 分散論理ルータと呼ばれていました。
Virtual SAN 転送	2233 (TCP)	Virtual SAN の信頼性の高いデータグラム転送。TCP を使用し、Virtual SAN ストレージ IO で使用されます。無効になっている場合、Virtual SAN は機能しません。
SNMP サーバ	161 (UDP)	ホストから SNMP サーバに接続できます。
SSH サーバ	22 (TCP)	SSH アクセスに必要です。
vMotion	8000 (TCP)	vMotion を使用した仮想マシンの移行に必要です。
vSphere Web Client	902、443 (TCP)	クライアント接続
vsanvp	8080 (TCP)	VSAN VASA ベンダー プロバイダ。Virtual SAN ストレージのプロファイル、機能、およびコンプライアンスに関する情報にアクセスするために、vCenter の一部であるストレージ管理サービス (SMS) で使用されます。無効になっている場合、Virtual SAN ストレージ プロファイル ベース管理 (SPBM) は機能しません。
vSphere Web Access	80 (TCP)	別のインターフェイスのダウンロード リンクがある [ようこそ] ページ。
RFB プロトコル	5900 ~ 5964 (TCP)	VNC などの管理ツールによって使用されます。

表 5-6. 送信ファイアウォール接続

サービス	ポート	コメント
CIM SLP	427 (TCP、UDP)	CIM クライアントは、サービス ロケーション プロトコル バージョン 2 (SLPv2) を使用して、CIM サーバを検索します。
DHCPv6	547 (TCP、UDP)	IPv6 の DHCP クライアント。
DVSSync	8301、8302 (UDP)	DVSSync ポートは、VMware FT の記録/再生が有効なホスト間で分散仮想ポートの状態を同期するために使用されます。これらのポートは、プライマリまたはバックアップ仮想マシンを実行しているホストでのみ開いている必要があります。VMware FT を使用していないホストでは、これらのポートが開いている必要はありません。
HBR	44046、31031 (TCP)	vSphere Replication および VMware Site Recovery Manager によって、実行中のレプリケーション トラフィックで使用されます。

表 5-6. 送信ファイアウォール接続（続き）

サービス	ポート	コメント
NFC	902 (TCP)	NFC（ネットワーク ファイル コピー）によって、vSphere コンポーネントでファイル タイプに対応した FTP サービスを使用できます。ESXi は、データストア間のデータのコピーや移動などの操作にデフォルトで NFC を使用します。
WOL	9 (UDP)	Wake-on-LAN によって使用されます。
Virtual SAN クラスティング サービス	12345、23451 (UDP)	Virtual SAN で使用されるクラスタ監視、メンバーシップ、およびディレクトリ サービス。
DHCP クライアント	68 (UDP)	DHCP クライアント。
DNS クライアント	53 (TCP、UDP)	DNS クライアント。
Fault Tolerance	80、8200、8100、8300 (TCP、UDP)	VMware Fault Tolerance に対応します。
ソフトウェア iSCSI クライアント	3260 (TCP)	ソフトウェア iSCSI に対応します。
NSX 分散論理ルータ サービス	6999 (UDP)	NSX VIB がインストールされていて、VDR モジュールが作成されている場合、このサービスに関連付けられているファイアウォール ポートが開きます。VDR インスタンスがホストに関連付けられていない場合、ポートが開いている必要はありません。
rabbitmqproxy	5671 (TCP)	仮想マシン内で実行されるアプリケーションと、vCenter ネットワーク ドメインで実行される AMQP ブローカが通信できるようにする、ESXi ホストで実行されるプロキシ。仮想マシンはネットワーク上に存在している必要はありません。つまり、NIC は必要ありません。プロキシは、vCenter ネットワーク ドメインのブローカに接続します。そのため、送信接続 IP アドレスには、少なくとも現在使用中のブローカまたは後で使用するブローカが含まれている必要があります。拡張が必要な場合にブローカを追加できます。
Virtual SAN 転送	2233 (TCP)	Virtual SAN ノード間の RDT トラフィック（ピア ツー ピアのユニキャスト通信）で使用されます。
vMotion	8000 (TCP)	vMotion を使用した仮想マシンの移行に必要です。
VMware vCenter Server Agent	902 (UDP)	vCenter Server エージェント。
vsanvp	8080 (TCP)	Virtual SAN ベンダー プロバイダ トラフィックで使用されます。

## NFS クライアント ファイアウォールの動作

NFS クライアントのファイアウォール ルール セットの動作は、他の ESXi ファイアウォール ルール セットとは異なります。ESXi では、NFS データストアをマウントまたはアンマウントするときに NFS クライアント設定が構成されます。動作は、NFS のバージョンによって異なります。

NFS データストアの追加、マウント、アンマウントを行ったときの動作は、NFS のバージョンによって異なります。

## NFS v3 ファイアウォールの動作

NFS v3 データストアを追加またはマウントする際、ESXi は、NFS クライアント (nfsClient) のファイアウォール ルール セットの状態を確認します。

- nfsClient のルール セットが無効な場合、ESXi はこのルール セットを有効にし、allowedAll フラグを FALSE に設定することで、すべての IP アドレスを許可するポリシーを無効にします。NFS サーバの IP アドレスが発信 IP アドレスの許可リストに追加されます。
- nfsClient のルール セットが有効な場合、ルール セットの状態と、許可される IP アドレスのポリシーは変更されません。NFS サーバの IP アドレスが発信 IP アドレスの許可リストに追加されます。

**注：** nfsClient のルール セットを手動で有効にするか、すべての IP アドレスを許可するポリシーを手動で設定すると、NFS v3 データストアをシステムに追加する前または後で、以前の NFS v3 データストアがアンマウントされる際に設定がオーバーライドされます。すべての v3 NFS データストアがアンマウントされると、nfsClient のルール セットは無効になります。

NFS v3 データストアを削除またはアンマウントすると、ESXi によって次のいずれかの操作が実行されます。

- 残りの NFS v3 データストアのいずれもアンマウントされるデータストアのサーバからマウントされない場合、ESXi はサーバの IP アドレスを発信 IP アドレスのリストから削除します。
- アンマウント操作後にマウントされている NFS v3 データストアが残っていない場合、ESXi は、nfsClient ファイアウォール ルール セットを無効にします。

## NFS v4.1 ファイアウォールの動作

最初の NFS v4.1 データストアをマウントすると、ESXi は nfs41client のルール セットを有効にし、allowedAll フラグを TRUE に設定します。この操作により、すべての IP アドレスに対してポート 2049 が開きます。NFS v4.1 データストアをアンマウントしても、ファイアウォールの状態には影響しません。つまり、最初の NFS v4.1 のマウントでポート 2049 が開き、そのポートは、明示的に閉じられない限り、有効な状態を維持します。

## ESXi ESXCLI ファイアウォールのコマンド

環境内に複数の ESXi ホストが含まれている場合は、ESXCLI コマンドまたは vSphere Web Services SDK を使用してファイアウォール構成を自動化することをお勧めします。

コマンドラインで ESXi Shell または vSphere CLI コマンドを使用して、ファイアウォール構成を自動化するように ESXi を構成できます。概要については、『vSphere Command-Line Interface スタート ガイド』を参照してください。ESXCLI を使用してファイアウォールおよびファイアウォール ルールを操作する例については、『vSphere コマンドライン インターフェイスの概念と範例』を参照してください。

表 5-7. ファイアウォールのコマンド

コマンド	説明
esxcli network firewall get	ファイアウォールのステータス（有効または無効）を返し、デフォルトのアクションのリストを表示します。
esxcli network firewall set --default-action	パスさせるようにデフォルトの操作を設定するには true に設定し、ドロップさせるようにデフォルトの操作を設定するには false に設定します。

表 5-7. ファイアウォールのコマンド（続き）

コマンド	説明
<code>esxcli network firewall set --enabled</code>	ESXi のファイアウォールを有効または無効にします。
<code>esxcli network firewall load</code>	ファイアウォール モジュールとルール セットの構成ファイルをロードします。
<code>esxcli network firewall refresh</code>	ファイアウォール モジュールがロードされている場合に、ルール セット ファイルを読み取ることでファイアウォールの構成を更新します。
<code>esxcli network firewall unload</code>	フィルタを破棄し、ファイアウォール モジュールをアンロードします。
<code>esxcli network firewall ruleset list</code>	ルール セット情報を一覧表示します。
<code>esxcli network firewall ruleset set --allowed-all</code>	すべての IP へのすべてのアクセスを許可するには true に設定し、許可された IP アドレスのリストを使用するには false に設定します。
<code>esxcli network firewall ruleset set --enabled --ruleset-id=&lt;string&gt;</code>	enabled を true または false に設定して、指定されたルールセットを有効または無効にします。
<code>esxcli network firewall ruleset allowedip list</code>	指定したルール セットの許可された IP アドレスを一覧表示します。
<code>esxcli network firewall ruleset allowedip add</code>	指定した IP アドレスまたは一定範囲内の IP アドレスからルール セットへのアクセスを許可します。
<code>esxcli network firewall ruleset allowedip remove</code>	指定した IP アドレスまたは一定範囲内の IP アドレスからルール セットへのアクセスを解除します。
<code>esxcli network firewall ruleset rule list</code>	ファイアウォール内の各ルールセットのルールをリストします。

## セキュリティ プロファイルによる ESXi サービスのカスタマイズ

ESXi ホストには、デフォルトで実行されるサービスがいくつかあります。たとえば SSH などのその他のサービスは、ホストのセキュリティ プロファイルに含まれています。企業ポリシーで許可されている場合、それらのサービスは必要に応じて有効および無効にすることができます。

[vSphere Web Client を使用した ESXi Shell へのアクセスの有効化](#) は、サービスを有効にする方法の一例です。

**注：** サービスを有効にすると、ホストのセキュリティに影響します。サービスは確実に必要な場合のみ有効にするようにしてください。

使用可能なサービスは、ESXi ホストにインストールされる VIB によって決まります。VIB をインストールせずにサービスを追加することはできません。vSphere HA などの一部の VMware 製品は、ホストに VIB をインストールし、サービスおよび対応するファイアウォールのポートを使用可能にします。

デフォルトのインストールでは、vSphere Web Client から次のサービスのステータスを変更できます。

表 5-8. セキュリティ プロファイルでの ESXi サービス

サービス	デフォルト	説明
ダイレクト コンソール UI	実行中	ダイレクト コンソール ユーザー インターフェイス (DCUI) サービスにより、テキストベースのメニューを使用して、ローカル コンソール ホストから ESXi ホストを対話形式で操作することができます。
ESXi Shell	停止	ESXi Shell は、ダイレクト コンソール ユーザー インターフェイスから使用することができ、完全にサポートされているコマンドのセットと、トラブルシューティングおよび修正のためのコマンドのセットが組み込まれています。ESXi Shell へのアクセスは、各システムのダイレクト コンソールから有効にする必要があります。ローカル ESXi Shell へのアクセス、または SSH による ESXi Shell へのアクセスを有効にすることができます。
SSH	停止	セキュア シェルによるリモート接続を許可するホストの SSH クライアント サービス。
負荷に基づくチーミング デモン	実行中	負荷に基づくチーミング。
ローカル セキュリティ 認証サーバ (Active Directory サービス)	停止	Active Directory サービスの一部。Active Directory を使用するように ESXi を構成すると、このサービスが開始されます。
I/O リダイレクタ (Active Directory サービス)	停止	Active Directory サービスの一部。Active Directory を使用するように ESXi を構成すると、このサービスが開始されます。
ネットワーク ログオン サーバ (Active Directory サービス)	停止	Active Directory サービスの一部。Active Directory を使用するように ESXi を構成すると、このサービスが開始されます。
NTP デモン	停止	ネットワーク時間プロトコル デモン。
CIM サーバ	実行中	Common Information Model (CIM) アプリケーションで使用可能なサービス。
SNMP サーバ	停止	SNMP デモン。SNMP v1、v2、および v3 の構成の詳細については、「vSphere の監視とパフォーマンス」を参照してください。
Syslog サーバ	停止	Syslog デモン。Syslog は、vSphere Web Client の [システムの詳細設定] から有効にすることができます。vSphere のインストールとセットアップを参照してください。
vSphere High Availability Agent	停止	vSphere High Availability 機能をサポートします。
vProbe デモン	停止	vProbe デモン。
VMware vCenter Agent	実行中	vCenter Server エージェント。vCenter Server が ESXi ホストに接続できるようにします。特に、vpxa はホスト デモンへの通信ルートであり、これにより ESXi カーネルと通信します。
X.Org サーバ	停止	X.Org サーバ。このオプション機能は、仮想マシンの 3D グラフィックスの内部で使用されます。

## セキュリティ プロファイルでのサービスの有効化または無効化

vSphere Web Client から、セキュリティ プロファイルに一覧表示されているいずれかのサービスを有効または無効にできます。

インストール後に特定のサービスがデフォルトで実行され、その他のサービスは停止します。vSphere Web Client UI でサービスを使用できるようにするには、事前に追加の設定が必要になる場合もあります。たとえば、NTP サービスは正確な時間情報を取得するための方法の 1 つですが、このサービスはファイアウォール内に必要なポートが開いている場合にのみ動作します。

#### 前提条件

vSphere Web Client を使用して vCenter Server に接続します。

#### 手順

- 1 vSphere Web Client インベントリでホストに移動して参照し、ホストを選択します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] を選択し、[編集] をクリックします。
- 4 変更するサービスまでスクロールします。
- 5 [サービスの詳細] ペインで、ホストのステータスを 1 回だけ変更する場合は [開始]、[停止]、または [再起動] を選択し、ホストのステータスを変更して再起動後もその変更を維持する場合は [起動ポリシー] メニューから選択します。
  - [いずれかのポートが開くと自動的に開始し、すべてのポートが閉じると停止]：これらのサービスのデフォルトの設定です。いずれかのポートが開いている場合、クライアントはサービスのネットワーク リソースへの接続を試みます。いくつかのポートが開いていて、特定のサービス用のポートが閉じている場合、この試行は失敗します。該当する発信ポートが開いている場合、サービスはその起動の実行を開始します。
  - [ホストに連動して開始および停止]：サービスは、ホストが起動した直後に開始され、ホストがシャットダウンする直前に終了します。[いずれかのポートが開くと自動的に開始し、すべてのポートが閉じると停止]と同様に、このオプションで、サービスはそのタスクの完了を定期的に試行します（指定された NTP サーバとの接続など）。ポートが閉じていたが、その後開いた場合、クライアントはその直後にタスクの実行を開始します。
  - [手動で開始および停止]：ホストは、ポートが開いているかどうかにかかわらず、ユーザーが決定したサービス設定を保持します。ユーザーが NTP サービスを起動する場合、そのサービスはホストがパワーオン状態にあるかぎり、実行を続けます。サービスが起動されてホストがパワーオフ状態にある場合、そのサービスはシャットダウン プロセスの一環として停止されます。しかし、ホストがパワーオン状態になった直後に、そのサービスはユーザーにより決定された状態を保持して、再び起動されます。

---

**注：** これらの設定は、vSphere Web Client または vSphere Web Services SDK で作成したアプリケーションを通じて構成されたサービス設定のみに適用されます。ESXi Shell または構成ファイルなど、その他の方法で行なった構成は、これらの設定の影響を受けません。

---

## ロックダウン モード

ESXi ホストのセキュリティを向上させるために、ロックダウン モードにすることができます。ロックダウン モードでは、デフォルトで vCenter Server から操作を実行する必要があります。

vSphere 6.0 以降では、通常ロックダウン モードまたは厳密なロックダウン モードを選択し、程度の異なるロックダウン機能を提供することができます。vSphere 6.0 には、例外ユーザー リストも導入されています。ホストがロックダウン モードになっても、例外ユーザーは自分に付与された権限を失いません。例外ユーザー リストを使用して、ホストがロックダウン モードのときに、ホストに直接アクセスする必要があるサードパーティのソリューションおよび外部アプリケーションのアカウントを追加します。[ロックダウン モード例外ユーザーの指定](#)を参照してください。



vSphere 6 のロックダウン モード

([https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1\\_zg4ylgu0/uiConfId/49694343/](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/))

## 通常ロックダウン モードと厳密なロックダウン モード

vSphere 6.0 以降では、通常ロックダウン モードまたは厳密なロックダウン モードを選択し、程度の異なるロックダウン機能を提供することができます。

### 通常ロックダウン モード

通常ロックダウン モードでは、DCUI サービスが停止しません。vCenter Server システムへの接続が失われ、vSphere Web Client 経由でアクセスできなくなった場合は、権限のあるアカウントで ESXi ホストのダイレクト コンソール インターフェイスにログインし、ロックダウン モードを終了することができます。ダイレクト コンソール ユーザー インターフェイスには、次のアカウントのみがアクセスできます。

- ホストでの管理権限を持っている、ロックダウン モードの例外ユーザー リストにあるアカウント。例外ユーザー リストは、非常に特殊なタスクを実行するサービス アカウントのリストです。このリストに ESXi 管理者を追加することは、ロックダウン モードの趣旨に反します。
- ホストの DCUI.Access 詳細オプションに定義されているユーザー。このオプションは、vCenter Server への接続が失われた場合に、ダイレクト コンソール インターフェイスに緊急アクセスするためのものです。これらのユーザーは、ホストの管理権限が不要になります。

### 厳密なロックダウン モード

厳密なロックダウン モードは vSphere 6.0 の新機能であり、このモードでは DCUI サービスが停止します。vCenter Server への接続が失われ、vSphere Web Client が使用できなくなると、ESXi Shell サービスと SSH サービスが有効で、かつ例外ユーザーが定義されていない限り、ESXi ホストが使用できなくなります。vCenter Server システムへの接続を回復できない場合は、ホストを再インストールする必要があります。

## ロックダウン モードと ESXi Shell および SSH サービス

厳密なロックダウン モードでは DCUI サービスが停止します。ただし、ESXi Shell サービスと SSH サービスは、ロックダウン モードに依存しません。ロックダウン モードを有効なセキュリティ対策とするため、ESXi Shell サービスと SSH サービスも必ず無効にしてください。それらのサービスは、デフォルトで無効になっています。



ホストがロックダウン モードになっている場合、例外ユーザー リストのユーザーは、ホストでの管理者ロールを持っていれば、ESXi Shell から、および SSH を介して、そのホストにアクセスすることができます。このアクセスは、厳密なロックダウン モードになっている場合でも可能です。ESXi Shell サービスと SSH サービスを無効のままにするのが最も安全なオプションです。

---

**注：** 例外ユーザー リストは、ホストのバックアップなどの特殊なタスクを実行するサービス アカウントを登録するために用意されたものであり、管理者を対象とするものではありません。管理者を例外ユーザー リストに追加するのは、ロックダウン モードの目的を無視した使い方です。

---

## ロックダウン モードを有効および無効にする

権限を持つユーザーは、いくつかの方法でロックダウン モードを有効にすることができます。

- [ホストの追加] ウィザードを使用して vCenter Server システムにホストを追加する場合。
- vSphere Web Client を使用する場合。[vSphere Web Client を使用したロックダウン モードの有効化](#)を参照してください。通常ロックダウン モードと厳密なロックダウン モードは、どちらも vSphere Web Client から有効にすることができます。
- ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用する場合。[ダイレクト コンソール ユーザー インターフェイスからの通常ロックダウン モードの有効化または無効化](#)を参照してください。

権限を持つユーザーは、vSphere Web Client からロックダウン モードを無効にすることができます。通常ロックダウン モードはダイレクト コンソール インターフェイスから無効にすることができますが、厳密なロックダウン モードはダイレクト コンソール インターフェイスから無効にすることはできません。

---

**注：** ダイレクト コンソール ユーザー インターフェイスを使用してロックダウン モードを有効または無効にする場合、ホスト上のユーザーおよびグループの権限は破棄されます。これらのアクセス許可を保存するため、vSphere Web Client を使用してロックダウン モードを有効および無効にすることができます。

---

## ロックダウン モードの動作

ロックダウン モードでは、いくつかのサービスが無効になり、いくつかのサービスは特定のユーザーのみがアクセスできます。

### 異なるユーザーのロックダウン モード サービス

ホストが稼動している場合、使用可能なサービスは、ロックダウン モードが有効かどうかと、ロックダウン モードのタイプに応じて決まります。

- 厳密なロックダウン モードおよび通常ロックダウン モードの場合、権限のあるユーザーは、vSphere Web Client から、または vSphere Web Services SDK を使用することにより、vCenter Server を介してホストにアクセスすることができます。
- ダイレクト コンソール インターフェイスの動作は、厳密なロックダウン モードと通常ロックダウン モードで異なります。
  - 厳密なロックダウン モードの場合、ダイレクト コンソール ユーザー インターフェイス (DCUI) サービスは無効になっています。
  - 通常ロックダウン モードでは、管理者権限を持つ例外ユーザー リストのアカウント、および DCUI.Access 詳細システム設定で指定されたユーザーが、ダイレクト コンソール インターフェイスにアクセスできます。

- ESXi Shell または SSH が有効で、ホストが厳密または通常ロックダウン モードになっている場合、管理者権限を持つ例外ユーザー リストのアカウントがこれらのサービスを使用できます。その他のユーザーの場合、ESXi Shell または SSH アクセスは無効です。vSphere 6.0 以降では、管理者権限を持たないユーザーの ESXi または SSH セッションは終了します。

厳密および通常両方のロックダウン モードで、すべてのアクセスがログに記録されます。

表 5-9. ロックダウン モードの動作

サービス	通常モード	通常ロックダウン モード	厳密なロックダウン モード
vSphere Web Services API	アクセス許可に基づくすべてのユーザー	vCenter (vpxuser) アクセス許可に基づく例外ユーザー vCloud Director (vsiauser、使用可能な場合)	vCenter (vpxuser) アクセス許可に基づく例外ユーザー vCloud Director (vsiauser、使用可能な場合)
CIM プロバイダ	ホストで管理者権限を持つユーザー	vCenter (vpxuser) アクセス許可に基づく例外ユーザー。 vCloud Director (vsiauser、使用可能な場合)	vCenter (vpxuser) アクセス許可に基づく例外。 vCloud Director (vsiauser、使用可能な場合)
ダイレクト コンソール UI (DCUI)	ホストで管理者権限を持つユーザー、および DCUI.Access 詳細オプションでのユーザー	DCUI.Access 詳細オプションで定義されているユーザー ホストで管理者権限を持つ例外ユーザー	DCUI サービス停止
ESXi Shell (有効な場合)	ホストで管理者権限を持つユーザー	DCUI.Access 詳細オプションで定義されているユーザー ホストで管理者権限を持つ例外ユーザー	DCUI.Access 詳細オプションで定義されているユーザー ホストで管理者権限を持つ例外ユーザー
SSH (有効な場合)	ホストで管理者権限を持つユーザー	DCUI.Access 詳細オプションで定義されているユーザー ホストで管理者権限を持つ例外ユーザー	DCUI.Access 詳細オプションで定義されているユーザー ホストで管理者権限を持つ例外ユーザー

#### ロックダウン モードが有効な場合に ESXi Shell にログインしたユーザー

ユーザーが ESXi Shell にログインしている場合、またはロックダウン モードが有効になる前に SSH を介してホストにアクセスする場合は、例外ユーザーのリストに含まれ、ホストで管理者権限を持つユーザーはログインしたままの状態になります。vSphere 6.0 以降では、他のすべてのユーザーのセッションは終了します。これは、通常と厳密の両方のロックダウン モードに適用されます。

#### vSphere Web Client を使用したロックダウン モードの有効化

すべての構成変更が vCenter Server 経由で実行されるようにするには、ロックダウン モードを有効にします。vSphere 6.0 以降では、通常ロックダウン モードと厳密なロックダウン モードがサポートされています。

ホストに対するすべての直接アクセスを完全に拒否するには、厳密なロックダウン モードを選択します。厳密なロックダウン モードを使用すると、vCenter Server が使用不可で、SSH および ESXi Shell が無効になっている場合に、ホストにアクセスできなくなります。[ロックダウン モードの動作](#) を参照してください。

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックします。
- 4 [ロックダウン モード] パネルで [編集] をクリックします。
- 5 [ロックダウン モード] をクリックして、いずれかのロックダウン モードを選択します。

オプション	説明
通常	vCenter Server 経由でホストにアクセスできます。例外ユーザー リストに登録されていて管理者権限を持っているユーザーのみが、ダイレクト コンソール ユーザー インターフェイスにログインできます。SSH または ESXi Shell が有効化されている場合はアクセスできる可能性があります。
厳密	vCenter Server 経由でのみホストにアクセスできます。SSH または ESXi Shell が有効化されていれば、DCUI.Access 詳細オプションのアカウントおよび管理者権限を持つ例外ユーザー アカウントの実行中セッションは有効な状態に保たれます。その他のセッションは終了します。

- 6 [OK] をクリックします。

## vSphere Web Client を使用したロックダウン モードの無効化

ESXi ホストに直接接続して構成を変更できるようにするには、ロックダウン モードを無効にします。ロックダウン モードを有効にしておいた方が、セキュアな環境になります。

vSphere 6.0 では、次の方法でロックダウン モードを無効化できます。

### vSphere Web Client から操作する場合

vSphere Web Client から、通常ロックダウン モードと厳密なロックダウン モードの両方を無効化できます。

### ダイレクト コンソール ユーザー インターフェイスから操作する場合

ESXi のダイレクト コンソール ユーザー インターフェイスにアクセスできるユーザーは通常ロックダウン モードを無効化できます。厳密なロックダウン モードでは、ダイレクト コンソール インターフェイス サービスが停止します。

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックします。
- 4 [ロックダウン モード] パネルで [編集] をクリックします。
- 5 k[ロックダウン モード] をクリックし、[なし] を選択してロックダウン モードを無効化します。

## 結果

システムがロックダウン モードを終了し、vCenter Server にアラームが表示され、監査ログにエントリが追加されます。

## ダイレクト コンソール ユーザー インターフェイスからの通常ロックダウン モードの有効化または無効化

ダイレクト コンソール ユーザー インターフェイスから通常ロックダウン モードを有効化または無効化できます。厳密なロックダウン モードは、vSphere Web Client からのみ有効化および無効化できます。

ホストが通常ロックダウン モードになっている場合は、次のアカウントからダイレクト コンソール ユーザー インターフェイスにアクセスできます。

- ホスト上で管理者権限を持つ例外ユーザー リストのアカウント。例外ユーザー リストは、バックアップ エージェントなどのサービス アカウントに使用します。
- ホストの DCUI.Access 詳細オプションに定義されているユーザー。このオプションは、致命的な障害の発生時にアクセスを有効化するために使用します。

ESXi 6.0 以降では、ユーザーのアクセス許可は、ロックダウン モードを有効にしたときに保存され、ダイレクト コンソール インターフェイスからロックダウン モードを無効化したときにリストアされます。

---

**注：** ロックダウン モードのホストをロックダウン モードを終了せずに ESXi 6.0 にアップグレードし、アップグレード後にロックダウン モードを終了した場合は、ホストがロックダウン モードに入る前に定義されていたアクセス許可がすべて失われます。システムは、DCUI.Access 詳細オプションに定義されているすべてのユーザーに管理者ロールを割り当て、ホストに引き続きアクセスできるようにします。

アクセス許可が失われないようにするには、vSphere Web Client からホストのロックダウン モードを無効にしてからアップグレードを実行してください。

---

## 手順

- 1 ホストのダイレクト コンソール ユーザー インターフェイスで、F2 を押してログインします。
- 2 [ロックダウン モードの構成] 設定にスクロールし、Enter を押して現在の設定を切り替えます。
- 3 ダイレクト コンソール ユーザー インターフェイスのメイン メニューに戻るまで、Esc を押します。

## ロックダウン モードでのアクセス権を持つアカウントの指定

サービス アカウントを例外ユーザー リストに追加することによって、ESXi ホストに直接アクセスできるサービス アカウントを指定できます。vCenter Server の致命的な障害に備えて、ESXi ホストにアクセスできる個別のユーザーを指定できます。

ロックダウン モードが有効になっている場合に、各アカウントがデフォルトで実行できる操作およびデフォルトの動作を変更する方法は、vSphere 環境のバージョンによって異なります。

- vSphere 5.1 より前のバージョンでは、ロックダウン モードの ESXi ホストのダイレクト コンソール ユーザー インターフェイスにログインできるのは root ユーザーだけです。

- vSphere 5.1 以降では、各ホストの DCUI.Access 詳細システム設定にユーザーを追加できます。このオプションは、vCenter Server の致命的な障害に備えるもので、このアクセス権を持つユーザーのパスワードは通常、金庫で保管します。DCUI.Access リストのユーザーは、ホストに対する完全な管理者権限を保有している必要はありません。
- vSphere 6.0 以降でも、DCUI.Access 詳細システム設定はサポートされています。それに加えて、vSphere 6.0 以降では、例外ユーザー リストがサポートされています。これはホストに直接ログインする必要があるサービス アカウントを登録するためのリストです。例外ユーザー リストに登録されている管理者権限を持つアカウントは、ESXi Shell にログインできます。また、それらのユーザーは、通常ロックダウン モードになっているホストの DCUI にログインして、ロックダウン モードを終了できます。

例外ユーザーは、vSphere Web Client から指定します。

---

**注：** 例外ユーザーは、ESXi ホストにローカルに定義された権限を持つホスト ローカル ユーザーまたは Active Directory ユーザーです。Active Directory グループのメンバーであるユーザーは、ホストがロックダウン モードのときにその権限を失います。

---

### DCUI.Access 詳細オプションへのユーザーの追加

DCUI.Access 詳細オプションの主な目的は、致命的な障害が発生して、vCenter Server からホストにアクセスできないときにロックダウン モードを終了できるようにすることです。ユーザーは、vSphere Web Client からホストの [詳細設定] を編集することによってリストに追加します。

---

**注：** DCUI.Access リストに登録されているユーザーは、自分に与えられている権限に関係なくロックダウン モード設定を変更できます。これは、ホストのセキュリティに影響する可能性があります。ホストに直接アクセスする必要があるサービス アカウントの場合は、代わりに例外ユーザー リストにユーザーを追加することを検討してください。例外ユーザーであれば、自分に権限が与えられているタスクしか実行できません。[ロックダウン モード例外ユーザーの指定](#) を参照してください。

---

#### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] を選択します。
- 3 [システムの詳細設定] をクリックし、[DCUI.Access] を選択します。
- 4 [編集] をクリックしてユーザー名をコンマ区切りで入力します。

デフォルトでは、root ユーザーも含まれます。システムの可監査性を高めるため、DCUI.Access リストから root を削除して名前付きアカウントを指定することを検討してください。

- 5 [OK] をクリックします。

### ロックダウン モード例外ユーザーの指定

vSphere 6.0 以降では、vSphere Web Client から例外ユーザー リストにユーザーを追加できます。例外ユーザー リストに追加されたユーザーは、ホストがロックダウン モードになってもアクセス許可を失いません。バックアップ エージェントなどのサービス アカウントを例外ユーザー リストに追加しておくことを推奨します。

ホストがロックダウン モードになっても、例外ユーザーは自分に付与された権限を失いません。通常、こうしたアカウントは、ロックダウン モードでも機能し続ける必要があるサードパーティ製ソリューションや外部アプリケーションによって使用されます。

---

**注：** 例外ユーザー リストは、非常に特殊なタスクを実行するサービス アカウントを登録するために用意されたものです。管理者を登録するものではありません。管理者を例外ユーザー リストに追加するのは、ロックダウン モードの目的を無視した使い方です。

---

例外ユーザーは、ESXi ホストにローカルに定義された権限を持つホスト ローカル ユーザーまたは Active Directory ユーザーです。例外ユーザーは Active Directory グループのメンバーではなく、vCenter Server ユーザーでもありません。例外ユーザーがホスト上で実行できる操作は、そのユーザーに付与されている権限によって決まります。たとえば、読み取り専用ユーザーがホスト上のロックダウン モードを無効にすることはできません。

#### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックします。
- 4 [ロックダウン モード] パネルで [編集] をクリックします。
- 5 [例外ユーザー] をクリックし、プラス記号アイコンをクリックして例外ユーザーを追加します。

## ホストと VIB の許容レベルの確認

ESXi ホストの整合性を保護するため、署名なし（コミュニティがサポートする）VIB のユーザーによるインストールを禁止します。署名なしの VIB には、VMware やそのパートナーによって認証、承諾、またはサポートされていないコードが含まれます。コミュニティがサポートする VIB にはデジタル署名がありません。

ESXCLI コマンドを使用して、ホストの許容レベルを設定できます。ホストの許容レベルに対する制限は、ホストに追加する VIB の許容レベルと同程度か少なくなければなりません。ESXi ホストのセキュリティと整合性を保護するには、署名なし（コミュニティがサポートする）VIB を稼働システムのホストにインストールすることを禁止します。

次の許容レベルがサポートされています。

### VMwareCertified

VMwareCertified 許容レベルは、最も厳しい要件です。このレベルの VIB では、同じテクノロジーに対して VMware 内部で行われる品質保証テストと完全に同等な、詳細なテストが行われます。現在このレベルで公開されているのは IOVP ドライバのみです。この許容レベルの場合は、VMware が VIB に対するサポート コールを受けます。

### VMwareAccepted

この許容レベルの VIB では検証テストが行われますが、このテストはソフトウェアのすべての機能を完全にテストするものではありません。テストはパートナーが実行し、VMware がテスト結果を確認します。現在このレベルで公開されている VIB には、CIM プロバイダや PSA プラグインがあります。VMware は、この許容レベルの VIB に対するサポート コールを、パートナーのサポート組織に送ります。

## PartnerSupported

PartnerSupported 許容レベルの VIB は、VMware が信頼するパートナーによって公開されます。そのパートナーがすべてのテストを実行します。VMware はテスト結果を確認しません。このレベルは、パートナーが VMware システム用に採用する、新しいテクノロジー、または主要ではないテクノロジーに使用されます。現在は、標準以外のハードウェア ドライバを使用する、Infiniband、ATAoE、SSD などのドライバ VIB テクノロジーがこのレベルにあります。VMware は、この許容レベルの VIB に対するサポート コールを、パートナーのサポート組織に送ります。

## CommunitySupported

CommunitySupported 許容レベルは、VMware パートナー プログラムに参加していない個人または企業が作成した VIB に使用されます。このレベルの VIB に対しては VMware が承認したテスト プログラムが実行されておらず、VMware のテクニカル サポートや VMware パートナーによるサポートを受けられません。

### 手順

- 1 各 ESXi ホストに接続し、次のコマンドを実行して、許容レベルが VMwareCertified または VMwareAccepted に設定されていることを確認します。

```
esxcli software acceptance get
```

- 2 ホストの許容レベルが VMwareCertified または VMwareAccepted でない場合は、次のコマンドを実行して、VMwareCertified または VMwareAccepted レベルでない VIB があるかどうかを判断します。

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

- 3 次のコマンドを使用して、PartnerSupported または CommunitySupported レベルの VIB を削除します。

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

- 4 次のコマンドを実行して、ホストの許容レベルを変更します。

```
esxcli software acceptance set --level acceptance_level
```

## ESXi への権限の割り当て

多くの場合、vCenter Server システムに管理される ESXi ホスト オブジェクトに権限を割り当てて、ユーザーに権限を付与します。スタンドアロンの ESXi ホストを使用している場合は、権限を直接付与することができます。

### vCenter Server に管理される ESXi ホストへの権限の割り当て

ESXi ホストが vCenter Server で管理される場合は、vSphere Web Client を使用して管理タスクを実行します。

vCenter Server オブジェクト階層で ESXi ホスト オブジェクトを選択してから、ESXi ホストで直接管理を実行する可能性のある、限定された数のユーザーに管理者ロールを割り当てることができます。[ロールを使用した権限の割り当て](#)を参照してください。



ベスト プラクティスは、名前付きのユーザー アカウントを 1 つ以上作成し、ホスト上でそのアカウントに完全な管理者権限を割り当て、root アカウントの代わりにこのアカウントを使用することです。root アカウントに極めて複雑なパスワードを設定し、root アカウントの使用を制限します（root アカウントは削除しないでください）。

## スタンドアロン ESXi ホストへの権限の割り当て

使用中の環境に vCenter Server システムが含まれていない場合は、次のユーザーが事前定義されています。

- root ユーザー。 [ルート ユーザーの権限](#) を参照してください。
- vpxuser。 [vpxuser の権限](#) を参照してください。
- DCUI ユーザー。 [DCUI ユーザーの権限](#) を参照してください。

vSphere Client の [管理] タブで、ローカル ユーザーを追加してカスタム ロールを定義できます。

ESXi のすべてのバージョンでは、`/etc/passwd` ファイル内の事前定義されたユーザーのリストを表示できます。

次のロールが事前定義されています。

### 読み取り専用

ユーザーは、ESXi ホストに関連付けられたオブジェクトを表示できますが、オブジェクトを変更することはできません。

### 管理者

管理者ロール。

### アクセスなし

アクセスなし。これはデフォルトです。必要に応じてデフォルトをオーバーライドできます。

ESXi ホストに直接接続された vSphere Client を使用して、ローカル ユーザーおよびグループを管理し、ローカルなカスタム ロールを ESXi ホストに追加できます。

vSphere 6.0 から、ESXCLI のアカウント管理コマンドを使用して、ESXi ローカル ユーザー アカウントを管理できます。ESXCLI の権限管理コマンドを使用すると、Active Directory アカウント（ユーザーおよびグループ）と ESXi ローカル アカウント（ユーザーのみ）の両方で権限の設定や削除を行うことができます。

---

**注：** ESXi ホストに直接接続して ESXi ホストのユーザーを定義し、同じ名前のユーザーが vCenter Server にも存在する場合、それらは異なるユーザーです。これらのユーザーの一方にロールを割り当てても、もう一方のユーザーに同じロールが割り当てられるわけではありません。

---

## ルート ユーザーの権限

デフォルトでは、各 ESXi ホストに、管理者ロールのある単一のルート ユーザー アカウントがあります。このルート ユーザー アカウントは、ローカル管理や vCenter Server にホストを接続するために使用できます。

この共通のルート アカウントでは、ESXi ホストへの割り込みが容易になりますが、特定の管理者に合った操作を行うことは難しくなります。



ルート アカウントに極めて複雑なパスワードを設定し、ルート アカウントの使用（vCenter Server にホストを追加する場合など）を制限します。ルート アカウントは削除しないでください。vSphere 5.1 以降では、vCenter Server へのホストの追加はルート ユーザーのみが許可されており、管理者ロールを持つ他の名前のユーザーは許可されていません。

ベスト プラクティスは、ESXi ホストの管理者ロールを持つアカウントを名前付きアカウントを持つ特定のユーザーに割り当てることです。可能であれば、Active Directory 認証情報を管理できるようにする ESXi Active Directory 機能を使用します。

---

**重要：** ルート ユーザーのアクセス権限を削除する場合は、最初に、別のユーザーを管理者ロールに割り当てたアクセス許可をルート レベルに作成する必要があります。

---

## vpxuser の権限

vCenter Server は、ホストに対するアクティビティを管理するときに vpxuser の権限を使用します。

vCenter Server には、管理対象ホストに対する管理者権限があります。たとえば、vCenter Server は、ホスト間で仮想マシンを移動して、仮想マシンのサポートに必要な構成変更を実行できます。

vCenter Server の管理者は、root ユーザーとほとんど同じタスクをホストで実行できます。また、タスクのスケジュール設定やテンプレートの使用なども実行できます。ただし、vCenter Server の管理者は、ホストのユーザーおよびグループを直接作成、削除、または編集することはできません。これらの作業は、各ホストに対して直接に管理者権限を持っているユーザーのみが実行できます。

---

**注：** Active Directory を使用して vpxuser を管理することはできません。

---

**注意：** vpxuser はどのような方法であっても変更しないでください。パスワードも変更しないでください。権限を変更することはできません。これらの変更を行うと、vCenter Server を介してホストで作業する場合に、問題が発生することがあります。

---

## DCUI ユーザーの権限

dcui ユーザーはホスト上で実行され、システム管理者権限で動作します。このユーザーの主要目的は、ダイレクト コンソール ユーザー インターフェイス (DCUI) からロックダウン モードのホストを構成することです。

このユーザーは、ダイレクト コンソールのエージェントとして機能します。対話形式のユーザーが変更または使用することはできません。

## Active Directory を使用した ESXi ユーザーの管理

Active Directory などのディレクトリ サービスを使用してユーザーを管理するように ESXi を構成できます。

各ホストにローカル ユーザー アカウントを作成すると、複数のホストのアカウント名およびパスワードを同期しなければならないという問題が生じます。ESXi ホストを Active Directory ドメインに参加させて、ローカル ユーザー アカウントを作成および管理しなくても済むようにします。ユーザー認証に Active Directory を使用すると、簡単に ESXi ホストを構成し、未承認のアクセスにつながる構成問題のリスクを減らすことができます。

Active Directory を使用している場合は、ホストをドメインに追加する際に Active Directory 認証情報と Active Directory サーバのドメイン名を指定します。

## vSphere Authentication Proxy のインストールまたはアップグレード

vSphere Authentication Proxy をインストールすると、Active Directory の認証情報を使用せずに ESXi ホストをドメインに参加させることができます。vSphere Authentication Proxy は、ホスト構成に Active Directory の認証情報を保存する必要をなくすことにより、PXE 起動のホストや、Auto Deploy を使用してプロビジョニングされるホストのセキュリティを強化します。

お使いのシステムに vSphere Authentication Proxy の以前のバージョンがインストールされている場合、この手順を実行することで vSphere Authentication Proxy が最新のバージョンにアップグレードされます。

vSphere Authentication Proxy は、関連付けられた vCenter Server と同じマシンか、vCenter Server にネットワーク接続できる別のマシンにインストールできます。vSphere Authentication Proxy は、バージョン 5.0 以降の vCenter Server でサポートされています。

vSphere Authentication Proxy サービスは、vCenter Server との通信のために IPv4 アドレスに拘束され、IPv6 はサポートされません。vCenter Server インスタンスは、IPv4 のみ、IPv4/IPv6 混在モード、または IPv6 のみのネットワーク環境内のホスト マシンにインストールできますが、vSphere Web Client 経由で vCenter Server に接続するマシンで vSphere Authentication Proxy サービスを機能させるには、IPv4 アドレスを使用する必要があります。

### 前提条件

- vSphere Authentication Proxy をインストールするマシンに、Microsoft .NET Framework 3.5 をインストールします。
- 管理者権限があることを確認します。
- ホスト マシンに、サポートされているプロセッサおよびオペレーティング システムがあることを確認します。
- ホスト マシンに有効な IPv4 アドレスがあることを確認します。vSphere Authentication Proxy は、ネットワーク環境が IPv4 のみのマシンまたは IPv4/IPv6 混合モードのマシンにインストールできますが、IPv6 のみの環境内のマシンにはインストールできません。
- vSphere Authentication Proxy を Windows Server 2008 R2 ホスト マシンにインストールする場合は、support.microsoft.com Web サイトにある Windows のナレッジ ベースの記事 981506 で説明されている、Windows のホットフィックスをダウンロードしてインストールします。このホットフィックスがインストールされていないと、vSphere Authentication Proxy Adapter の初期化に失敗します。この問題が発生すると、「Failed to bind CAM website with CTL」および「Failed to initialize CAMAdapter」に類似したエラー メッセージが camadapter.log に表示されます。
- vCenter Server のインストーラをダウンロードします。

次の情報を収集してインストールまたはアップグレードを完了します。

- vSphere Authentication Proxy をインストールする場所（デフォルトの場所を使用しない場合）。
- vSphere Authentication Proxy が接続する vCenter Server のアドレスおよび認証情報：IP アドレスまたは名前、HTTP ポート、ユーザー名、およびパスワード。
- vSphere Authentication Proxy をネットワーク上で識別するためのホスト名または IP アドレス。

## 手順

- 1 認証プロキシ サービスをインストールするホスト マシンをドメインに追加します。
- 2 ドメイン管理者のアカウントを使用して、ホスト マシンにログインします。
- 3 ソフトウェアのインストール ディレクトリで `autorun.exe` ファイルをダブルクリックし、インストーラーを起動します。
- 4 [VMware vSphere Authentication Proxy] を選択し、[インストール] をクリックします。
- 5 ウィザードの指示に従って、インストールまたはアップグレードを完了します。

インストール中、認証サービスは、Auto Deploy が登録されている vCenter Server インスタンスに登録されます。

## 結果

vSphere Authentication Proxy サービスのインストール時、インストーラにより、認証プロキシ サービスを実行するために適切な権限のあるドメイン アカウントが作成されます。アカウント名は接頭辞 `CAM-` で始まり、32 文字で構成されます。また、ランダムに生成されたパスワードが関連付けられます。パスワードは、期限なしで設定されます。アカウントの設定は変更しないでください。

## Active Directory を使用するためのホストの構成

Active Directory などのディレクトリ サービスを使用してユーザーやグループを管理するようにホストを構成できます。

あるホストに完全な管理者権限が割り当てするには、ESXi ホストを Active Directory のドメイン グループ `ESX Admins` に追加します。完全な管理者権限を割り当てないようにするには、VMware のナレッジベースの記事 1025569 で回避策を参照してください。

ホストが Auto Deploy でプロビジョニングされている場合、Active Directory 認証情報をホストに格納することはできません。vSphere Authentication Proxy を使用して、ホストを Active Directory ドメインに参加させることができます。vSphere Authentication Proxy とホストの間には信頼チェーンが存在するため、Authentication Proxy はホストを Active Directory ドメインに参加させることができます。[vSphere Authentication Proxy の使用](#)を参照してください。

---

**注：** Active Directory でユーザー アカウント設定を定義するときに、コンピュータ名を指定することで、ユーザーがログインできるコンピュータを限定できます。デフォルトでは、ユーザー アカウントにこのような制限は設定されていません。この制限を設定すると、アクセス制御リスト内のコンピュータであっても、ユーザー アカウントの LDAP バインドの要求に失敗し、LDAP バインドは成功しませんでした というメッセージが表示されます。この問題を避けるには、ユーザー アクセスを管理するコンピュータのリストに Active Directory サーバの NetBIOS 名を追加します。

---

## 前提条件

- Active Directory ドメインがあることを確認します。ディレクトリ サーバのドキュメントを参照してください。
- ESXi のホスト名が、Active Directory フォレストの完全修飾ドメイン名であることを確認します。

*fully qualified domain name = host\_name.domain\_name*

#### 手順

- 1 NTP を使用して ESXi とディレクトリ サービス システムの間で時刻の同期をとります。  
ESXi の時間を Microsoft ドメイン コントローラと同期させる方法については、[ネットワーク タイム サーバによる ESXi の時計の同期](#)または VMware のナレッジベースを参照してください。
- 2 ホストに構成した DNS サーバで、Active Directory コントローラのホスト名を解決できることを確認します。
  - a vSphere Web Client オブジェクト ナビゲータで、ホストに移動して参照します。
  - b [管理] タブをクリックして、[ネットワーク] をクリックします。
  - c [DNS] をクリックし、ホスト名と、ホストの DNS サーバ情報が正しいことを確認します。

#### 次のステップ

vSphere Web Client を使用してディレクトリ サービスのドメインに参加します。Auto Deploy でプロビジョニングされたホストの場合、vSphere Authentication Proxy を設定します。[vSphere Authentication Proxy の使用](#)を参照してください。

## ディレクトリ サービス ドメインへのホストの追加

ホストがディレクトリ サービスを使用するようにするには、ディレクトリ サービス ドメインにホストを追加する必要があります。

ドメイン名は次のいずれかの方法で入力できます。

- **name.tld** (たとえば **domain.com**) : アカウントはデフォルトのコンテナ下に作成されます。
- **name.tld/container/path** (たとえば **domain.com/OU1/OU2**) : アカウントは特定の組織単位 (OU) 下に作成されます。

vSphere Authentication Proxy サービスの使用については、「[vSphere Authentication Proxy の使用](#)」を参照してください。

#### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[認証サービス] を選択します。
- 4 [ドメインへの参加] をクリックします。
- 5 ドメインを入力します。  
**name.tld** または **name.tld/container/path** の形式を使用します。
- 6 ドメインにホストを追加する権限を持つディレクトリ サービス ユーザーのユーザー名とパスワードを入力し、[OK] をクリックします。
- 7 (オプション) 認証プロキシを使用する場合は、プロキシ サーバの IP アドレスを入力します。

- 8 [OK] をクリックして、ディレクトリ サービスの構成ダイアログ ボックスを閉じます。

## ディレクトリ サービス設定の表示

ホストがユーザー認証に使用しているディレクトリ サーバのタイプ（ある場合）、およびディレクトリ サーバの設定を表示できます。

### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[認証サービス] を選択します。  
[認証サービス] ページに、ディレクトリ サービスおよびドメイン設定が表示されます。

## vSphere Authentication Proxy の使用

vSphere Authentication Proxy を使用する場合、Active Directory の認証情報をホストに送信する必要はありません。ユーザーがホストをドメインに追加する際には、Active Directory サーバのドメイン名と認証プロキシ サーバの IP アドレスを指定します。

vSphere Authentication Proxy と Auto Deploy と組み合わせると、より便利に使用できます。Authentication Proxy をポイントするリファレンス ホストを構成し、ルールを設定して、リファレンス ホストのプロファイルに適用します。このプロファイルは、Auto Deploy でプロビジョニングされたすべての ESXi ホストに含まれます。VMware 認証局 (VMCA) でプロビジョニングされた証明書またはサードパーティ証明書を使用する環境で、vSphere Authentication Proxy を使用する場合は、Auto Deploy でカスタム証明書を使用する方法を実行することで、プロセスはシームレスに機能します。[Auto Deploy でのカスタム証明書の使用](#)を参照してください。

---

**注：** IPv6 のみをサポートする環境では、vSphere Authentication Proxy を使用できません。

---

## vSphere Authentication Proxy のインストールまたはアップグレード

vSphere Authentication Proxy をインストールすると、Active Directory の認証情報を使用せずに ESXi ホストをドメインに参加させることができます。vSphere Authentication Proxy は、ホスト構成に Active Directory の認証情報を保存する必要をなくすことにより、PXE 起動のホストや、Auto Deploy を使用してプロビジョニングされるホストのセキュリティを強化します。

お使いのシステムに vSphere Authentication Proxy の以前のバージョンがインストールされている場合、この手順を実行することで vSphere Authentication Proxy が最新のバージョンにアップグレードされます。

vSphere Authentication Proxy は、関連付けられた vCenter Server と同じマシンか、vCenter Server にネットワーク接続できる別のマシンにインストールできます。vSphere Authentication Proxy は、バージョン 5.0 以降の vCenter Server でサポートされています。

vSphere Authentication Proxy サービスは、vCenter Server との通信のために IPv4 アドレスに拘束され、IPv6 はサポートされません。vCenter Server インスタンスは、IPv4 のみ、IPv4/IPv6 混在モード、または IPv6 のみのネットワーク環境内のホスト マシンにインストールできますが、vSphere Web Client 経由で vCenter Server に接続するマシンで vSphere Authentication Proxy サービスを機能させるには、IPv4 アドレスを使用する必要があります。

#### 前提条件

- vSphere Authentication Proxy をインストールするマシンに、Microsoft .NET Framework 3.5 をインストールします。
- 管理者権限があることを確認します。
- ホスト マシンに、サポートされているプロセッサおよびオペレーティング システムがあることを確認します。
- ホスト マシンに有効な IPv4 アドレスがあることを確認します。vSphere Authentication Proxy は、ネットワーク環境が IPv4 のみのマシンまたは IPv4/IPv6 混合モードのマシンにインストールできますが、IPv6 のみの環境内のマシンにはインストールできません。
- vSphere Authentication Proxy を Windows Server 2008 R2 ホスト マシンにインストールする場合は、support.microsoft.com Web サイトにある Windows のナレッジ ベースの記事 981506 で説明されている、Windows のホットフィックスをダウンロードしてインストールします。このホットフィックスがインストールされていないと、vSphere Authentication Proxy Adapter の初期化に失敗します。この問題が発生すると、「Failed to bind CAM website with CTL」および「Failed to initialize CAMAdapter」に類似したエラー メッセージが camadapter.log に表示されます。
- vCenter Server のインストーラをダウンロードします。

次の情報を収集してインストールまたはアップグレードを完了します。

- vSphere Authentication Proxy をインストールする場所（デフォルトの場所を使用しない場合）。
- vSphere Authentication Proxy が接続する vCenter Server のアドレスおよび認証情報：IP アドレスまたは名前、HTTP ポート、ユーザー名、およびパスワード。
- vSphere Authentication Proxy をネットワーク上で識別するためのホスト名または IP アドレス。

#### 手順

- 1 認証プロキシ サービスをインストールするホスト マシンをドメインに追加します。
- 2 ドメイン管理者のアカウントを使用して、ホスト マシンにログインします。
- 3 ソフトウェアのインストール ディレクトリで autorun.exe ファイルをダブルクリックし、インストーラーを起動します。
- 4 [VMware vSphere Authentication Proxy] を選択し、[インストール] をクリックします。
- 5 ウィザードの指示に従って、インストールまたはアップグレードを完了します。

インストール中、認証サービスは、Auto Deploy が登録されている vCenter Server インスタンスに登録されます。

## 結果

vSphere Authentication Proxy サービスのインストール時、インストーラにより、認証プロキシ サービスを実行するために適切な権限のあるドメイン アカウントが作成されます。アカウント名は接頭辞 CAM- で始まり、32 文字で構成されます。また、ランダムに生成されたパスワードが関連付けられます。パスワードは、期限なしで設定されます。アカウントの設定は変更しないでください。

## vSphere Authentication Proxy を認証に使用するようホストを構成

vSphere Authentication Proxy サービス (CAM サービス) のインストール後、ホストを構成して認証用プロキシ サーバーがユーザー認証を行うよう構成する必要があります。

### 前提条件

ホストに vSphere Authentication Proxy サービス (CAM サービス) をインストールします。[vSphere Authentication Proxy のインストールまたはアップグレード](#) を参照してください。

### 手順

- 1 ホストの IIS マネージャーを使用して DHCP の範囲を設定します。

範囲を設定することで、管理ネットワークの DHCP を使用しているホストが認証プロキシ サービスを使用できるようになります。

オプション	操作
IIS 6 の場合	<ol style="list-style-type: none"> <li>[コンピュータ アカウント管理 Web サイト] を参照します。</li> <li>仮想ディレクトリの [CAM ISAPI] を右クリックします。</li> <li>[プロパティ] - [ディレクトリ セキュリティ] - [IP アドレスおよびドメイン名の制限の編集] - [コンピュータ グループを追加] を選択します。</li> </ol>
IIS 7 の場合	<ol style="list-style-type: none"> <li>[コンピュータ アカウント管理 Web サイト] を参照します。</li> <li>左のペインにある仮想ディレクトリの [CAM ISAPI] をクリックして、[IPv4 アドレスおよびドメイン制限] を開きます。</li> <li>[エントリの許可を追加] - [IPv4 アドレス範囲] を選択します。</li> </ol>

- 2 ホストが Auto Deploy でプロビジョニングされていない場合、デフォルトの SSL 証明書を、自己署名の証明書か商業認証局 (CA) 署名のある証明書に変更します。

オプション	説明
<b>VMCA 証明書</b>	<p>デフォルトの VMCA 署名付き証明書を使用する場合は、Authentication Proxy ホストが VMCA 証明書を信頼するようにしておく必要があります。</p> <ol style="list-style-type: none"> <li>信頼されたルート証明機関の証明書ストアに、VMCA 証明書を手動で追加します。</li> <li>VMCA 署名付き証明書 (<code>root.cer</code>) を、vSphere Authentication Proxy サービスがインストールされたシステムの、ローカルの信頼されている証明書ストアに追加します。ファイルは、<code>C:\ProgramData\VMware\CIS\data\vmca</code> に格納されています。</li> <li>vSphere Authentication Proxy サービスを再起動します。</li> </ol>
<b>サードパーティ CA 署名付き証明書</b>	<p>CA 署名付き証明書 (DER で暗号化) を、vSphere Authentication Proxy サービスがインストールされたシステムの、ローカルで信頼されている証明書ストアに追加し、vSphere Authentication Proxy サービスを再起動します。</p> <ul style="list-style-type: none"> <li>Windows 2003 では、証明書ファイルを <code>C:\Documents および Settings\All Users\Application Data\VMware\vsphere Authentication Proxy\trust</code> にコピーします。</li> <li>Windows 2008 では、証明書ファイルを <code>C:\Program Data\VMware\vsphere Authentication Proxy\trust</code> にコピーします。</li> </ul>

## vSphere Authentication Proxy の設定

Authentication Proxy の証明書情報がある場合、ESXi ホストで vSphere Authentication Proxy を使用できます。

サーバを認証する必要があるのは 1 回だけです。

**注：** ESXi および Authentication Proxy サーバで認証できるようになっている必要があります。この認証機能は常に有効になっています。認証を無効にする必要がある場合は、[詳細設定] ダイアログ ボックスを使用して、`UserVars.ActiveDirectoryVerifyCAMCertificate` 属性を 0 に設定します。

## vSphere Authentication Proxy 証明書のエクスポート

ESXi に対し、vSphere Authentication Proxy を認証するには、ESXi にプロキシ サーバ証明書を用意する必要があります。

### 前提条件

ホストに vSphere Authentication Proxy (CAM サービス) をインストールします。[vSphere Authentication Proxy のインストールまたはアップグレード](#) を参照してください。



## 手順

- 1 認証プロキシ サーバ システムで、IIS マネージャを使用して証明書をエクスポートします。

オプション	操作
IIS 6 の場合	<ol style="list-style-type: none"> <li>a [コンピュータのアカウント管理 Web サイト] を右クリックします。</li> <li>b [プロパティ] - [ディレクトリ セキュリティ] - [証明書の表示] を選択します。</li> </ol>
IIS 7 の場合	<ol style="list-style-type: none"> <li>a 左側のペインで [Computer Account Management Web Site] を選択します。</li> <li>b [バインド] を選択して、[サイト バインド] ダイアログ ボックスを開きます。</li> <li>c [https] バインドを選択します。</li> <li>d [編集] - [SSL 証明書の表示] を選択します。</li> </ol>

- 2 [詳細] - [ファイルにコピー] を選択します。
- 3 [秘密キーをエクスポートしません] オプションと [Base-64 encoded X.509 (CER)] オプションを選択します。

## 次のステップ

証明書を ESXi にインポートします。

## ESXi へのプロキシ サーバ証明書のインポート

ESXi を、vSphere Authentication Proxy サーバで認証するには、プロキシ サーバ証明書を ESXi にアップロードします。

vSphere Web Client ユーザー インターフェイスを使用して、vSphere Authentication Proxy サーバ証明書を ESXi ホストにアップロードします。

## 前提条件

ホストに vSphere Authentication Proxy サービス（CAM サービス）をインストールします。[vSphere Authentication Proxy のインストールまたはアップグレード](#) を参照してください。

vSphere Authentication Proxy サーバ証明書を [vSphere Authentication Proxy 証明書のエクスポート](#) の説明に従ってエクスポートします。

## 手順

- 1 ホストを参照し、[管理] > [設定] > [認証サービス] の順にクリックします。
- 2 [証明書のインポート] をクリックします。
- 3 ホスト上の認証プロキシ サーバ証明書ファイルへのフル パスと、認証プロキシ サーバの IP アドレスを入力します。  
[datastore name] file path の形式を使用して、プロキシ サーバへのパスを入力します。
- 4 [OK] をクリックします。

## vSphere Authentication Proxy を使用した、ドメインへのホストの追加

ホストをディレクトリ サービス ドメインに追加する際には、ユーザーが指定した Active Directory 認証情報を送信する代わりに、vSphere Authentication Proxy サーバを使用して認証することができます。

ドメイン名は次のいずれかの方法で入力できます。

- **name.tld** (たとえば **domain.com**) : アカウントはデフォルトのコンテナ下に作成されます。
- **name.tld/container/path** (たとえば **domain.com/OU1/OU2**) : アカウントは特定の組織単位 (OU) 下に作成されます。

### 前提条件

- vSphere Web Client を使用して vCenter Server システムに接続します。
- ESXi が DHCP アドレスを使用して構成されている場合は、DHCP の範囲を設定します。
- ESXi が静的 IP アドレスを使用して構成されている場合は、関連付けられているプロファイルが、ドメインに参加するために vSphere Authentication Proxy サービスを使用するように構成されていることを確認してください。これにより、認証プロキシ サーバは、ESXi の IP アドレスを信頼できます。
- ESXi で VMCA 署名の証明書が使用されている場合は、vCenter Server にホストが追加されていることを確認してください。これにより、認証プロキシ サーバは、ESXi を信頼できます。
- ESXi で CA 署名の証明書が使用されており、Auto Deploy によってプロビジョニングされていない場合は、[vSphere Authentication Proxy を認証に使用するようホストを構成](#)の説明に従って、CA 証明書が、認証プロキシ サーバのローカルで信頼されている証明書ストアに追加されていることを確認してください。
- ホストに対して vSphere 認証プロキシ サーバを認証します。

### 手順

- 1 vSphere Web Client のホストを参照して移動し、[管理] タブをクリックします。
- 2 [設定] をクリックして、[認証サービス] を選択します。
- 3 [ドメインへの参加] をクリックします。
- 4 ドメインを入力します。  
**name.tld** または **name.tld/container/path** の形式を使用します。
- 5 [プロキシ サーバの使用] を選択します。
- 6 認証プロキシ サーバの IP アドレスを入力します。
- 7 [OK] をクリックします。

## ESXi ホスト用認証プロキシ証明書の置き換え

信頼できる証明機関が発行した証明書を vSphere Web Client からインポートできます。

### 前提条件

- ESXi ホストに認証プロキシ証明書ファイルをアップロードします。

## 手順

- 1 vSphere Web Client で、ESXi ホストを選択します。
- 2 [設定] タブで、[システム] 領域の [認証サービス] を選択します。
- 3 [証明書のインポート] をクリックします。
- 4 SSL 証明書のパスと vSphere Authentication Proxy サーバを入力します。

## ESXi のセキュリティのベスト プラクティス

ESXi のセキュリティのベスト プラクティスに従うことで、vSphere デプロイの整合性を確保できます。詳細については、『セキュリティ強化ガイド』を参照してください。

### インストール メディアの確認

ダウンロードしたファイルの整合性と信頼性を確認するために、ISO、オフライン バンドル、またはパッチをダウンロードしたら、必ずファイルのハッシュを確認します。VMware から入手した物理メディアのセキュリティ シールが破損している場合は、そのソフトウェアを VMware に返却して交換してください。

メディアをダウンロードしたら、MD5 サムの値を使用して、ダウンロードの整合性を確認します。MD5 サムの出力を VMware Web サイトで公開されている値と比較します。オペレーティング システムにより、MD5 サムの値を確認するための方法とツールが異なります。Linux の場合は、「md5sum」コマンドを使用します。Microsoft Windows の場合は、アドオン製品をダウンロードできます。

### CRL の手動チェック

デフォルトでは、ESXi ホストは、CRL チェックをサポートしません。失効した証明書は、手動で検索して削除する必要があります。通常、これらの証明書は、企業またはサードパーティの認証局 (CA) によってカスタム生成された証明書です。多くの企業では、ESXi ホスト上の失効した SSL 証明書を検索して置換するためにスクリプトを使用します。

### ESX Admins による Active Directory グループの監視

vSphere によって使用される Active Directory グループは、システムの詳細設定 `plugins.hostsvc.esxAdminsGroup` によって定義されます。このオプションは、デフォルトで [ESX Admins] に設定されています。ESX Admins グループのすべてのメンバーには、ドメイン内のすべての ESXi ホストに対する完全な管理アクセス権が付与されます。グループの作成では Active Directory を監視し、メンバーシップを信頼性の高いユーザーおよびグループに制限してください。

### 構成ファイルの監視

ほとんどの ESXi 構成は API によって制御されますが、いくつかの構成ファイルはホストに直接影を及ぼします。これらのファイルは、HTTPS を使用する vSphere ファイル転送 API によって公開されます。これらのファイルに変更を加える場合は、構成変更などの対応する管理アクションを実行する必要があります。

---

**注：** このファイル転送 API によって公開されていないファイルは監視しないでください。

---

### vmkfstools を使用した機密データの消去

機密データが含まれる VMDK ファイルを削除する場合は、仮想マシンをシャットダウンまたは停止してから、そのファイルに対して vCLI コマンド `vmkfstools --writezeros` を発行します。その後で、ファイルをデータストアから削除することができます。

## PCI および PCIe デバイスおよび ESXi

VMware DirectPath I/O 機能を使用して PCI または PCIe デバイスを仮想マシンへパススルーさせると、潜在的なセキュリティの脆弱性が発生します。脆弱性は、ゲスト OS で特権モードで動作するデバイス ドライバなど、バグの多いコードまたは悪意のあるコードによって引き起こされます。業界標準のハードウェアおよびファームウェアには現在、ESXi で脆弱性を完全に遮断できるだけの十分なエラー抑制サポートがありません。

VMware では、仮想マシンが信頼できるエンティティによって所有され管理されている場合のみ、仮想マシンへの PCI または PCIe パススルーを使用することをお勧めしています。そのエンティティが、仮想マシンからホストをクラッシュしたり悪用しようとしなかったことを確認する必要があります。

ホストは、次のいずれかの方法で侵害される可能性があります。

- ゲスト OS で、リカバリ不能な PCI または PCIe エラーが生成される可能性があります。このようなエラーによってデータが破損することはありませんが、ESXi ホストがクラッシュする可能性があります。このようなエラーは、パススルーされるハードウェア デバイスのバグまたは非互換性、またはゲスト OS のドライバの問題によって発生します。
- ゲスト OS で Direct Memory Access (DMA) 操作が生成され、それが ESXi ホストで IOMMU ページ障害の原因となる可能性があります。DMA 操作が仮想マシンのメモリ外部のアドレスを宛先とする場合などです。一部のマシンでは、IOMMU 障害が発生するとマスク不可能割り込み (NMI) を使用して致命的なエラーを報告するようにホストのファームウェアが構成されており、これが ESXi ホストがクラッシュする原因になります。この問題は、ゲスト OS のドライバの問題によって発生します。
- ESXi ホスト上のオペレーティング システムが割り込み再マッピングを使用していない場合、ゲスト OS は任意のベクトルで ESXi ホストに擬似割り込みを挿入する可能性があります。ESXi では現在、使用可能なときは Intel プラットフォームで割り込み再マッピングを使用します。割り込みマッピングは、Intel VT-d 機能セットの一部です。ESXi は、AMD プラットフォームでは割り込みマッピングを使用しません。擬似割り込みを行うと、ESXi ホストがクラッシュする確率が高くなります。ただし、これらの割り込みを利用する他の方法も理論的には存在します。

## ESXi のスマート カード認証の構成

スマート カード認証を使用して、ESXi ダイレクト コンソール ユーザー インターフェイス (DCUI) にログインできます。これを行うには、ユーザー名とパスワードを要求するデフォルトのプロンプトの代わりに、Personal Identity Verification (PIV)、Common Access Card (CAC) または SC650 スマート カードを使用します。

スマート カードは、集積回路チップが埋め込まれた小さなプラスチック製カードです。多くの政府機関および大企業では、スマート カード ベースの 2 要素認証を使用して、システムのセキュリティ向上やセキュリティ規制への準拠を実現しています。

スマート カード認証が ESXi ホストで有効になっている場合、DCUI では、ユーザー名とパスワードを要求するデフォルトのプロンプトの代わりに、有効なスマート カードと PIN の組み合わせが求められます。

- 1 スマート カードをスマート カード リーダーに挿入すると、ESXi ホストでその認証情報が読み取られます。

- 2 ESXi DCUI にログイン ID が表示され、PIN の入力が求められます。
- 3 PIN を入力すると、ESXi ホストによって、その PIN とスマート カードに保存されている PIN が照合され、Active Directory を使用してスマート カードの証明書が検証されます。
- 4 スマート カードの証明書の検証に成功すると、ESXi DCUI にログインできます。

DCUI から F3 を押すと、ユーザー名とパスワードの認証に切り替えることができます。

正しくない PIN を何回か連続して入力すると（通常は 3 回）、スマート カードのチップがロックされます。スマート カードがロックされた場合、特定の担当者のみがロックを解除できます。

## スマート カード認証を有効化

ESXi DCUI へのログインにスマート カードと PIN の組み合わせが求められるスマート カード認証を有効にします。

### 前提条件

- Active Directory ドメインのアカウント、スマート カード リーダー、スマート カードなど、スマート カード認証を処理するためのインフラストラクチャを設定します。
- ESXi を構成して、スマート カード認証をサポートする Active Directory に参加します。詳細については、[Active Directory を使用した ESXi ユーザーの管理](#) を参照してください。
- vSphere Web Client を使用してルート証明書を追加します。[ESXi ホストの証明書管理](#) を参照してください。

### 手順

- 1 vSphere Web Client で、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[認証サービス] を選択します。  
現在のスマート カード認証ステータスと、インポートされた証明書のリストが表示されます。
- 4 [スマート カード認証] パネルで、[編集] をクリックします。
- 5 [スマート カード認証の編集] ダイアログ ボックスで、[証明書] ページを選択します。
- 6 ルート CA 証明書や中間 CA 証明書など、信頼性のある認証局 (CA) の証明書を追加します。
- 7 [スマート カード認証] ページを開き、[スマート カード認証を有効化] チェック ボックスを選択して、[OK] をクリックします。

## スマート カード認証の無効化

ESXi DCUI ログイン用のデフォルトのユーザー名およびパスワード認証に戻るには、スマート カード認証を無効にします。

### 手順

- 1 vSphere Web Client で、ホストに移動して参照します。

2 [管理] タブをクリックして、[設定] をクリックします。

3 [システム] で、[認証サービス] を選択します。

現在のスマート カード認証ステータスと、インポートされた証明書の一覧が表示されます。

4 [スマート カード認証] パネルで、[編集] をクリックします。

5 [スマート カード認証] ページで [スマート カード認証を有効化] チェック ボックスの選択を解除して、[OK] をクリックします。

## 接続問題発生時のユーザー認証情報の認証

Active Directory (AD) ドメイン サーバにアクセスできない場合は、ホストでユーザー名とパスワードの認証を実行して緊急アクションを実行することによって、ESXi DCUI にログインすることができます。

例外的な状況では、接続問題、ネットワーク障害、または災害などの理由で、AD ドメイン サーバにアクセスしてスマート カード上のユーザー認証情報を認証できないことがあります。AD サーバへの接続が失われた場合は、ローカル ESXi ユーザーの認証情報を使用して ESXi DCUI にログインすることができます。これにより、診断その他の緊急アクションを実行できます。ユーザー名とパスワードのログインへのフォールバックは、ログに記録されます。

AD への接続が回復すると、スマート カード認証が再び有効化されます。

---

**注：** vCenter Server へのネットワーク接続が失われても、Active Directory (AD) ドメイン サーバが稼働していれば、スマート カード認証への影響はありません。

---

## ロックダウン モードでのスマート カード認証の使用

ESXi ホストのロックダウン モードが有効になっていると、ホストのセキュリティが向上し、DCUI へのアクセスが制限されます。ロックダウン モードでは、スマート カード認証機能が無効になる可能性があります。

通常のロックダウン モードでは、管理者権限のある例外ユーザー リストのユーザーのみが DCUI にアクセスできます。例外ユーザーは、ESXi ホストにローカルに定義されたアクセス許可を持つホスト ローカル ユーザーまたは Active Directory ユーザーです。通常のロックダウン モードでスマート カード認証を使用する場合、vSphere Web Client からユーザーを例外ユーザー リストに追加する必要があります。例外ユーザー リストに追加されたユーザーは、ホストが通常のロックダウン モードになってもアクセス許可は失われず、DCUI にログインできます。詳細については、[ロックダウン モード例外ユーザーの指定](#) を参照してください。

厳密なロックダウン モードでは、DCUI サービスが停止します。そのため、スマート カード認証を使用してホストにアクセスできません。

## ESXi SSH キー

SSH キーを使用して、ESXi ホストへのアクセスを制限、制御、および保護できます。SSH キーを使用して、信頼できるユーザーまたはスクリプトがパスワードを指定せずにホストにログインできるように設定できます。

`vifs` vSphere CLI コマンドを使用して、SSH キーをホストにコピーできます。vSphere CLI コマンド セットのインストールおよび使用について詳しくは、『vSphere コマンドライン インターフェイスのスタート ガイド（英語版）』を参照してください。HTTPS PUT を使用して、SSH キーをホストにコピーすることもできます。

キーを外部で生成してアップロードする代わりに、ESXi ホストでキーを作成してダウンロードできます。当社のナレッジ ベースの記事 [1002866](#) を参照してください。

SSH を有効にして SSH キーをホストに追加する操作には特有のリスクがあるため、堅牢な環境では推奨されません。許可されている (SSH) キーの無効化 を参照してください。

---

**注：** ESXi 5.0 以前の場合、SSH キーを所有するユーザーはホストがロックダウン モードでもホストにアクセスできます。これは、ESXi 5.1 で修正されています。

---

## SSH セキュリティ

SSH を使用して ESXi Shell にリモートからログインし、ホストのトラブルシューティング タスクを実行できます。

ESXi の SSH 構成は、より高度なセキュリティ レベルを提供できるよう拡張されています。

### Version 1 SSH プロトコルの無効化

VMware では、Version 1 SSH プロトコルはサポートされておらず、Version 2 プロトコルだけが使用されます。Version 2 では、Version 1 での特定のセキュリティ問題が解消されており、管理インターフェイスとの安全な通信が提供されます。

### 暗号強度の向上

SSH は、接続に 256 ビットと 128 ビットの AES 暗号のみをサポートしています。

これらの設定は、SSH 経由で管理インターフェイスに転送されるデータの保護を目的としています。これらの設定は変更できません。

## vifs コマンドを使用した SSH 鍵のアップロード

認証キーを使用して SSH でホストにログインする場合は、vifs コマンドで認証キーをアップロードできます。

---

**注：** 認証キーを使用するとユーザー認証なしで SSH アクセスが可能になるため、現在の環境で SSH キーを使用するかどうかは慎重に検討してください。

---

認証済み鍵を使用して、ホストへのリモート アクセスを認証できます。ユーザーまたはスクリプトが SSH でホストにアクセスを試みる場合、認証済み鍵を使用すればパスワードなしで認証できます。認証済み鍵を使用すれば認証を自動化でき、定型タスクを自動化するスクリプトを作成するのに役立ちます。

次のタイプの SSH 鍵をホストにアップロードできます。

- root ユーザー用認証済み鍵
- RSA 鍵
- RSA 公開鍵

vSphere 6.0 Update 2 リリース以降では、DSS/DSA キーはサポートされません。

---

**重要：** /etc/ssh/sshd\_config ファイルを変更しないでください。

---

## 手順

- ◆ コマンド ラインまたは管理サーバで `vifs` コマンドを使用して、SSH 鍵を ESXi ホスト上の適切な場所にアップロードします。

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

鍵の種類	場所
root ユーザー用認証済み鍵ファイル	/host/ssh_root_authorized_keys このファイルをアップロードするには、完全な管理者権限が必要です。
RSA 鍵	/host/ssh_host_rsa_key
RSA 公開鍵	/host/ssh_host_rsa_key_pub

## HTTPS の PUT を使用した SSH 鍵のアップロード

認証済み鍵を使用して、SSH でホストにログインできます。HTTPS の PUT を使用して認証済み鍵をアップロードできます。

認証済み鍵を使用して、ホストへのリモート アクセスを認証できます。ユーザーまたはスクリプトが SSH でホストにアクセスを試みる場合、認証済み鍵を使用すればパスワードなしで認証できます。認証済み鍵を使用すれば認証を自動化でき、定型タスクを自動化するスクリプトを作成するのに役立ちます。

HTTPS の PUT を使用して、次のタイプの SSH 鍵をホストにアップロードできます。

- root ユーザー用認証済み鍵
- DSA 鍵
- DSA 公開鍵
- RSA 鍵
- RSA 公開鍵

**重要：** `/etc/ssh/sshd_config` ファイルを変更しないでください。

## 手順

- 1 アプリケーションをアップロードする場合は、鍵ファイルを開きます。
- 2 次の場所にファイルを公開します。

鍵の種類	場所
root ユーザー用認証済み鍵ファイル	https://hostname_or_IP_address/host/ssh_root_authorized_keys このファイルをアップロードするには、ホストでの完全な管理者権限が必要です。
DSA 鍵	https://hostname_or_IP_address/host/ssh_host_dsa_key
DSA 公開鍵	https://hostname_or_IP_address/host/ssh_host_dsa_key_pub



鍵の種類	場所
RSA 鍵	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
RSA 公開鍵	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

## ESXi Shell の使用

ESXi Shell は、ESXi ホストでデフォルトで無効になっています。このシェルへのローカル アクセスおよびリモート アクセスは、必要に応じて有効にすることができます。

不正アクセスのリスクを低減するためには、トラブルシューティングにのみ ESXi Shell を有効にします。

ESXi Shell は、ロックダウン モードに依存しません。ホストがロックダウン モードで実行されている場合でも、有効な場合は ESXi Shell にログインできます。

### ESXi Shell

ローカルで ESXi Shell にアクセスする場合は、このサービスを有効にします。

### SSH

SSH を使用して ESXi Shell にリモート アクセスするには、このサービスを有効にします。

vSphere セキュリティ を参照してください。

root ユーザーおよび管理者ロールを持つユーザーは、ESXi Shell にアクセスできます。Active Directory グループ ESX Admins 内のユーザーには、管理者ロールが自動的に割り当てられます。デフォルトでは、root ユーザーのみが、ESXi Shell を使用してシステム コマンド（`vmware -v` など）を実行できます。

---

**注：** ESXi Shell は、実際に必要にならない限り有効にしないでください。

---

#### ■ vSphere Web Client を使用した ESXi Shell へのアクセスの有効化

vSphere Web Client を使用して、ESXi Shell へのローカルおよびリモート（SSH）のアクセスを有効にし、アイドル タイムアウトと可用性タイムアウトを設定できます。

#### ■ ダイレクト コンソール ユーザー インターフェイス（DCUI）を使用した ESXi Shell へのアクセスの有効化

ダイレクト コンソール ユーザー インターフェイス（DCUI）を使用すると、テキストベースのメニューを使用して、ローカルでホストとの対話を行うことができます。お使いの環境のセキュリティ要件の下で、ダイレクト コンソール ユーザー インターフェイスの有効化がサポートされるかどうか、慎重に評価します。

#### ■ トラブルシューティングのために ESXi Shell にログイン

vSphere Web Client、vSphere CLI、または vSphere PowerCLI を使用して、ESXi 構成タスクを実行します。ESXi Shell（以前の Tech Support モード（TSM））には、トラブルシューティングの目的でのみログインしてください。

## vSphere Web Client を使用した ESXi Shell へのアクセスの有効化

vSphere Web Client を使用して、ESXi Shell へのローカルおよびリモート（SSH）のアクセスを有効にし、アイドル タイムアウトと可用性タイムアウトを設定できます。

**注：** vSphere Web Client、リモートのコマンド ライン ツール（vCLI および PowerCLI）、および発行済みの API を使用してホストにアクセスします。特別な状況によって SSH アクセスを有効にする必要がある場合を除き、SSH を使用してホストへのリモート アクセスを有効にしないでください。

### 前提条件

認証済みの SSH キーを使用する必要がある場合は、それをアップロードできます。 [ESXi SSH キー](#) を参照してください。

### 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックします。
- 4 [サービス] パネルで [編集] をクリックします。
- 5 リストからサービスを選択します。
  - ESXi Shell
  - SSH
  - ダイレクト コンソール UI
- 6 [サービスの詳細] をクリックし、起動ポリシー [手動で開始および停止] を選択します。

[手動で開始および停止] を選択すると、ホストを再起動しても、サービスは開始されません。ホストの再起動時にサービスが開始されるようにするには、[ホストに連動して開始および停止] を選択します。
- 7 [開始] を選択してサービスを有効にします。
- 8 [OK] をクリックします。

### 次のステップ

ESXi Shell の可用性とアイドル タイムアウトを設定します。 [vSphere Web Client での ESXi Shell 可用性のタイムアウトの作成](#) および [vSphere Web Client でのアイドル ESXi Shell セッションのタイムアウトの作成](#) を参照してください。

## vSphere Web Client での ESXi Shell 可用性のタイムアウトの作成

ESXi Shell はデフォルトでは無効になっています。ESXi Shell の可用性タイムアウトを設定し、シェルを有効にした場合のセキュリティを強化できます。

可用性タイムアウト設定は、ESXi Shell を有効にしてからログインするまでの許容経過時間を示します。タイムアウト期間が過ぎると、サービスが無効となり、ユーザーはログインできなくなります。

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] の下で [システムの詳細設定] を選択します。
- 4 [UserVars.ESXiShellTimeOut] を選択し、[編集] アイコンをクリックします。
- 5 アイドル タイムアウト設定を入力します。

タイムアウトを有効にするには、SSH サービスと ESXi Shell サービスの再開が必要です。

- 6 [OK] をクリックします。

## 結果

タイムアウト期間が経過したときにログイン済みの場合は、セッションが維持されます。ただし、ログアウト後、またはセッション終了後は、ユーザーはログインできません。

## vSphere Web Client でのアイドル ESXi Shell セッションのタイムアウトの作成

ユーザーがホストで ESXi Shell を有効にしているセッションからログアウトし忘れた場合、アイドル セッションは無期限に接続されたままになります。接続を開いたままにすると、誰かがホストに対するアクセス権を取得する潜在性が高くなります。アイドル セッションのタイムアウトを設定することによって、これを防止できます。

アイドル タイムアウト設定は、ユーザーが対話形式のアイドル セッションからログアウトされるまでの許容経過時間を示します。ダイレクト コンソール インターフェイス (DCUI) から、または vSphere Web Client からのローカル セッションとリモート (SSH) セッションの両方について、時間の長さを制御できます。

## 手順

- 1 vSphere Web Client インベントリで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] の下で [システムの詳細設定] を選択します。
- 4 [UserVars.ESXiShellInteractiveTimeOut] を選択し、[編集] アイコンをクリックして、タイムアウト設定を入力します。
- 5 SSH サービスと ESXi Shell サービスを再起動して、タイムアウトを反映させます。

## 結果

セッションがアイドル状態の場合、タイムアウト期間が経過した後、ユーザーがログアウトされます。

## ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用した ESXi Shell へのアクセスの有効化

ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用すると、テキストベースのメニューを使用して、ローカルでホストとの対話を行うことができます。お使いの環境のセキュリティ要件の下で、ダイレクト コンソール ユーザー インターフェイスの有効化がサポートされるかどうか、慎重に評価します。

ダイレクト コンソール ユーザー インターフェイスを使用して、ESXi Shell へのローカル アクセスおよびリモート アクセスを有効にできます。

**注：** ダイレクト コンソール ユーザー インターフェイス、vSphere Web Client、ESXCLI、またはその他の管理 ツールを使用してホストに加えられた変更は、1 時間ごと、または適切にシャットダウンされたときに、永続的なストレージにコミットされます。コミットされる前にホストに障害が発生すると、変更内容は失われる場合があります。

#### 手順

- 1 ダイレクト コンソール ユーザー インターフェイスで、F2 を押してシステムのカスタマイズ メニューにアクセスします。
- 2 [トラブルシューティング オプション] を選択し、Enter を押します。
- 3 [トラブルシューティング モード オプション] メニューから、有効にするサービスを選択します。
  - ESXi Shell の有効化
  - SSH の有効化
- 4 Enter を押してサービスを有効にします。
- 5 ダイレクト コンソール ユーザー インターフェイスのメイン メニューに戻るまで、Esc を押します。

#### 次のステップ

ESXi Shell の可用性とアイドル タイムアウトを設定します。[ダイレクト コンソール ユーザー インターフェイスでの ESXi Shell 可用性のタイムアウトの作成](#) および [アイドル ESXi Shell セッションのタイムアウトの作成](#) を参照してください。

### ダイレクト コンソール ユーザー インターフェイスでの ESXi Shell 可用性のタイムアウトの作成

ESXi Shell はデフォルトでは無効になっています。ESXi Shell の可用性タイムアウトを設定し、シェルを有効にした場合のセキュリティを強化できます。

可用性タイムアウト設定は、ESXi Shell を有効にしてからログインするまでの許容経過時間を示します。タイムアウト期間が過ぎると、サービスが無効となり、ユーザーはログインできなくなります。

#### 手順

- 1 トラブルシューティング モード オプション メニューから、[ESXi Shell および SSH のタイムアウトの変更] を選択し、Enter を押します。
- 2 可用性タイムアウトを入力します。

タイムアウトを有効にするには、SSH サービスと ESXi Shell サービスの再開が必要です。
- 3 ダイレクト コンソール ユーザー インターフェイスのメイン メニューに戻るまで、Enter を押し、Esc を押します。
- 4 [OK] をクリックします。

## 結果

タイムアウト期間が経過したときにログイン済みの場合は、セッションが維持されます。ただし、ログアウト後、またはセッション終了後は、ユーザーはログインできません。

## アイドル ESXi Shell セッションのタイムアウトの作成

ユーザーがホストで ESXi Shell を有効にしているセッションからログアウトし忘れた場合、アイドル セッションは無期限に接続されたままになります。接続を開いたままにすると、誰かがホストに対するアクセス権を取得する潜在性が高くなります。アイドル セッションのタイムアウトを設定することによって、これを防止できます。

アイドル タイムアウト設定は、ユーザーが対話形式のアイドル セッションからログアウトされるまでの許容経過時間を示します。アイドル タイムアウトの変更は、ユーザーが次に ESXi Shell にログインする際に適用されるため、既存のセッションは影響を受けません。

タイムアウトをダイレクト コンソール ユーザー インターフェイスで指定するか（秒単位）、または vSphere Web Client で指定します（分単位）。

## 手順

- 1 トラブルシューティング モード オプション メニューから、[ESXi Shell および SSH のタイムアウトの変更] を選択し、Enter を押します。

- 2 アイドル タイムアウトを秒単位で入力します。

タイムアウトを有効にするには、SSH サービスと ESXi Shell サービスの再開が必要です。

- 3 ダイレクト コンソール ユーザー インターフェイスのメイン メニューに戻るまで、Enter を押し、Esc を押します。

## 結果

セッションがアイドル状態の場合、タイムアウト期間が経過した後、ユーザーがログアウトされます。

## トラブルシューティングのために ESXi Shell にログイン

vSphere Web Client、vSphere CLI、または vSphere PowerCLI を使用して、ESXi 構成タスクを実行します。ESXi Shell（以前の Tech Support モード（TSM））には、トラブルシューティングの目的でのみログインしてください。

## 手順

- 1 次のいずれかの方法で ESXi Shell にログインします。

- ホストに直接アクセス可能な場合は、マシンの物理コンソールで Alt + F2 を押してログイン ページを開きます。
- ホストにリモート接続する場合は、SSH などのリモート コンソール接続を使用して、ホスト上でセッションを開始します。

- 2 ホストで認識されるユーザー名とパスワードを入力します。

## ESXi Web プロキシの設定の変更

Web プロキシ設定を変更する場合、暗号化とユーザー セキュリティについて考慮すべきガイドラインがいくつかあります。

**注：** ホストのディレクトリまたは認証メカニズムに変更を加えた後で、ホスト プロセスを再開します。

- パスワードまたはパス フレーズを使用する証明書を設定しないでください。ESXi は、パスワードやパス フレーズ（暗号鍵とも呼ばれる）を使用する Web プロキシをサポートしていません。パスワードまたはパス フレーズを必要とする Web プロキシを設定すると、ESXi プロセスが正しく起動できません。
- ユーザー名、パスワード、およびパケットの暗号化をサポートするために、vSphere Web Services SDK 接続では、デフォルトで SSL が有効になっています。これらの接続が送信内容を暗号化しないように構成する場合は、接続を HTTPS から HTTP に切り替えて、vSphere Web Services SDK 接続の SSL を無効にします。

ファイアウォールが適切に設定されてホスト間の転送が完全に隔離された、完全に信頼できる環境をそれらのクライアントに作成した場合のみ、SSL を無効にすると考えてください。SSL を無効にすると、暗号化の実行に必要なオーバーヘッドが回避されるので、パフォーマンスが向上します。

- ESXi サービスの悪用を防ぐために、ほとんどの内部 ESXi サービスは、HTTPS 転送に使用されるポート 443 からのみアクセスできます。ポート 443 は、ESXi のリバース プロキシとして機能します。ESXi のサービスのリストは HTTP の「ようこそ」ページから参照できますが、適切な権限がないと、ストレージ アダプタ サービスに直接アクセスすることはできません。

HTTP 接続を介して個々のサービスに直接アクセスできるように、この構成を変更できます。ただし、完全に信頼できる環境で ESXi を使用していないかぎり、このような変更は行わないでください。

- 環境をアップグレードしても、証明書はそのまま残ります。

## vSphere Auto Deploy のセキュリティの考慮事項

環境を最適に保護するには、ホスト プロファイルを使って Auto Deploy を使用する際に発生する可能性のあるセキュリティ リスクに留意する必要があります。

### ネットワーク セキュリティ

他の PXE ベースのデプロイ方法の場合と同様に、ネットワークを保護します。vSphere Auto Deploy は SSL 経由でデータを転送することで、不正な干渉やアクセスを防ぎます。しかし、PXE 起動の間は、クライアントや Auto Deploy サーバの整合性は確認されません。

Auto Deploy が使用されているネットワークを完全に隔離すると、Auto Deploy のセキュリティ リスクを大幅に低減することができます。

## 起動イメージおよびホスト プロファイルのセキュリティ

vSphere Auto Deploy サーバがマシンにダウンロードする起動イメージには、次のコンポーネントが含まれる場合があります。

- イメージ プロファイルから構成される VIB パッケージは、起動イメージに必ず含まれます。
- ホスト プロファイルまたはホストのカスタマイズ設定を使用してホストをプロビジョニングするように Auto Deploy ルールが設定されている場合は、ホスト プロファイルとホストのカスタマイズが起動イメージに含まれます。
  - ホスト プロファイルおよびホストのカスタマイズに含まれる、管理者（root）パスワードおよびユーザーパスワードは、MD5 で暗号化されています。
  - プロファイルに関連するその他すべてのパスワードは、暗号化されていません。ホスト プロファイルを使用して Active Directory を設定する場合は、パスワードは保護されません。

Active Directory パスワードの漏洩を防ぐように Active Directory を設定するため、vSphere 認証サービスを使用します。ホスト プロファイルを使用して Active Directory を設定すると、パスワードは保護されません。

- ホストの SSL のパブリック キーおよびプライベート キーと証明書が、起動イメージに含まれます。

## ESXi ログ ファイルの管理

ログ ファイルは、攻撃のトラブルシューティング、およびホスト セキュリティの侵害に関する情報の取得を行うための、重要なコンポーネントです。セキュリティで保護された集中管理されたログ サーバにログ記録することにより、ログの改ざんを防ぐことができます。リモート ログは、長期間の監査記録にも使用できます。

ホストのセキュリティを強化するために次の対策を講じます。

- データストアへの永続的なログ記録を構成します。デフォルトでは、ESXi ホスト上のログはメモリ内のファイル システムに保存されます。そのため、ホストの再起動時にログが失われ、ログ データは 24 時間のみ保存されます。永続的なログ記録を有効にすると、ホストで実行可能なサーバ アクティビティ専用のログが記録されます。
- 中央ホストにリモートでログを記録することで、中央ホストでログ ファイルを収集し、1 つのツールですべてのホストを監視できます。ログ データの集計分析および検索を実行し、複数のホストへの組織的攻撃などの情報を特定することもできます。
- vCLI や PowerCLI などのリモート コマンド ラインまたは API クライアントを使用して、ESXi ホストのセキュリティで保護されたリモート syslog を構成します。
- syslog 構成をクエリして、有効な syslog サーバ（正しいポートを含む）が構成されていることを確認します。

## ESXi ホストでの syslog の構成

すべての ESXi ホストは、VMkernel およびその他のシステム コンポーネントからのメッセージをログ ファイルに記録する syslog サービス（vmsyslogd）を実行しています。

vSphere Web Client または `esxcli system syslog vCLI` コマンドを使用して syslog サービスを構成できます。

vCLI コマンドの使い方の詳細については、vSphere Command-Line Interface スタート ガイドを参照してください。

#### 手順

- 1 vSphere Web Client のインベントリでホストを選択します。
- 2 [管理] タブをクリックします。
- 3 システム パネルで、[システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] リストで、[Syslog] セクションに移動します。
- 5 ロギングをグローバルに設定するには、変更する設定を選択し、[編集] アイコンをクリックします。

オプション	説明
<b>Syslog.global.defaultRotate</b>	保持するアーカイブの最大数を設定します。この数字はグローバルに、また個別のサブロガーについて設定できます。
<b>Syslog.global.defaultSize</b>	システムのログ ローテーションを行う際のログのデフォルト サイズを KB で設定します。この数字はグローバルに、また個別のサブロガーについて設定できます。
<b>Syslog.global.LogDir</b>	ログが保管されるディレクトリです。ディレクトリは、マウントされた NFS または VMFS ボリュームに置くことができます。リポートしても継続するのは、ローカル ファイル システムの <code>/scratch</code> ディレクトリのみです。ディレクトリは、 <code>[datastorename] path_to_file</code> と指定します。ここでパスはデータストアをバックアップするボリュームのルートからの相対パスです。例えば、パスの <code>[storage1] /systemlogs</code> はパスの <code>/vmfs/volumes/storage1/systemlogs</code> にマップします。
<b>Syslog.global.logDirUnique</b>	このオプションを選択すると、ESXi ホストの名前を持つサブディレクトリを <code>[Syslog.global.LogDir]</code> で指定されるディレクトリの下に作成します。同一の NFS ディレクトリが複数の ESXi ホストで使用される場合、独自のディレクトリは役に立ちます。
<b>Syslog.global.LogHost</b>	syslog メッセージの転送先のリモート ホストと、そのリモート ホストが syslog メッセージを受信するポート。 <code>ssl://hostname:1514</code> のようにしてプロトコルとポートを含められます。UDP (デフォルト)、TCP、および SSL がサポートされています。リモート ホストには syslog がインストールされ、転送された syslog メッセージを受信するように正しく構成されている必要があります。構成の情報については、リモート ホストにインストールされた syslog サービスのドキュメントを参照してください。

- 6 (オプション) 任意のログに対して、デフォルトのログ サイズとログ ローテーションを上書きします。
  - a カスタマイズするログの名前をクリックします。
  - b [編集] アイコンをクリックし、ローテーション数とログ サイズを入力します。
- 7 [OK] をクリックします。

#### 結果

syslog オプションの変更がすぐに有効になります。



## ESXi ログ ファイルの場所

ESXi は、syslog 機能を使用してログ ファイルにホスト アクティビティを記録します。

コンポーネント	場所	目的
VMkernel	/var/log/vmkernel.log	仮想マシンおよび ESXi に関するアクティビティを記録します。
VMkernel 警告	/var/log/vmkwarning.log	仮想マシンに関するアクティビティを記録します。
VMkernel サマリ	/var/log/vmksummary.log	ESXi のアップタイムおよび可用性の統計を確認するために使用します（コンマ区切り）。
ESXi ホスト エージェント ログ	/var/log/hostd.log	ESXi ホストとその仮想マシンを管理および構成するエージェントの情報が含まれます。
vCenter エージェント ログ	/var/log/vpxa.log	vCenter Server と通信するエージェントに関する情報が含まれます（ホストが vCenter Server によって管理されている場合）。
シェル ログ	/var/log/shell.log	ESXi Shell に入力されたすべてのコマンドおよびシェル イベント（シェルが有効になった日時など）の記録が含まれます。
認証	/var/log/auth.log	ローカル システムの認証に関するすべてのイベントが含まれます。
システム メッセージ	/var/log/syslog.log	すべての一般的なログ メッセージが含まれ、トラブルシューティングに使用できます。この情報は、以前はメッセージ ログ ファイルに記録されていました。
仮想マシン	影響を受ける仮想マシンの構成ファイルと同じディレクトリにある vmware.log および vmware*.log。例： /vmfs/volumes/データストア/仮想マシン/vmware.log	仮想マシンの電源イベント、システム障害情報、ツールのステータスとアクティビティ、時間の同期、仮想ハードウェアの変更、vMotion の移行、マシンのクローンなどが含まれます。

## フォールト トレランス ログ記録トラフィックのセキュリティ強化

フォールト トレランス（FT）を有効にすると、VMware vLockstep は、プライマリ仮想マシンで発生する入力とイベントを取得し、それを別のホストで稼動しているセカンダリ仮想マシンに送信します。

プライマリ仮想マシンとセカンダリ仮想マシン間のこのログ記録トラフィックは暗号化されず、このトラフィックにはゲスト ネットワーク、ストレージ I/O データ、およびゲスト OS のメモリの内容が含まれます。このトラフィックには、パスワードなどの機密情報がプレーンテキストで含まれる可能性があります。このようなデータの漏洩を回避するため、このネットワークは確実にセキュリティ保護し、特に中間者攻撃が防止されるように注意してください。たとえば、FT ログ記録トラフィック用のプライベート ネットワークを使用します。

# vCenter Server システムのセキュリティ

# 6

vCenter Server のセキュリティ保護には、vCenter Server が実行されているホストのセキュリティの確保、権限およびロールの割り当てのベスト プラクティス、および vCenter Server に接続するクライアントの整合性の確認が含まれます。

この章には、次のトピックが含まれています。

- vCenter Server のセキュリティのベスト プラクティス
- レガシー ESXi ホストのサンプリの検証
- ネットワーク ファイル コピーによる SSL 証明書検証が有効かどうかの確認
- vCenter Server の TCP および UDP ポート
- CIM ベースのハードウェア監視ツールのアクセス制御

## vCenter Server のセキュリティのベスト プラクティス

vCenter Server のセキュリティのベスト プラクティスに従うことで、vSphere 環境の整合性を確保できます。

### vCenter Server アクセス コントロールのベスト プラクティス

システムのセキュリティを強化するには、さまざまな vCenter Server コンポーネントへのアクセスを厳密に管理します。

次のガイドラインは、ご使用の環境のセキュリティを確保するのに役立ちます。

#### 名前付きアカウントの使用

- ローカルの Windows 管理者アカウントが、現在、vCenter Server に対する完全な管理者権限を持っている場合は、それらのアクセス権を削除してから、同じアクセス権を 1 つ以上の名前付き vCenter Server 管理者アカウントに付与します。完全な管理者権限は、その権限を必要とする管理者にのみ付与します。メンバーシップが厳格に管理されていないグループには、管理者権限を付与しないようにします。

---

**注：** vSphere 6.0 から、デフォルトでは、ローカル管理者は vCenter Server に対する完全な管理者権限を持たなくなりました。ローカル オペレーティング システム ユーザーの使用はお勧めしません。

---

- vCenter Server のインストールには、Windows アカウントではなくサービス アカウントを使用します。サービス アカウントは、ローカル マシンの管理者である必要があります。

- vCenter Server システムへの接続時に、アプリケーションが一意的サービス アカウントを使用するようにしてください。

## アクセスの抑制

ユーザーが直接 vCenter Server ホスト マシンにログインできないようにします。vCenter Server にログインしたユーザーが設定やプロセスの変更を行うことで、意図的または無意識に悪影響を及ぼす可能性があります。SSL 証明書などの vCenter の認証情報にアクセスする可能性もあります。正当なタスクを実行するユーザーにのみシステムへのログインを許可し、ログイン イベントを確実に監査します。

## vCenter Server 管理者ユーザーの権限の監視

すべての管理者ユーザーが管理者ロールを持つ必要はありません。代わりに、適切な一連の権限を持つカスタム ロールを作成して、そのロールを他の管理者に割り当てます。

vCenter Server 管理者ロールを持つユーザーには、階層内のすべてのオブジェクトに対する権限があります。たとえば、管理者ロールのユーザーは、デフォルトで、仮想マシンのゲスト OS 内のファイルおよびプログラムを操作できます。このロールを割り当てたユーザーが多すぎると、仮想マシン データの機密性、可用性、または正当性が低減する可能性があります。必要な権限を管理者に付与するロールを作成しますが、仮想マシンの管理権限の一部は除外します。

## vCenter Server データベース ユーザーへの最小限の権限の付与

データベース ユーザーに必要なのは、データベースへのアクセスに関連する特定の一部権限のみです。これらのほかに、インストールとアップグレードにのみ必要な権限があります。このような権限は、製品のインストールやアップグレード後に削除できます。

## データストア ブラウザ アクセスの制限

データストア ブラウザ機能を使用すると、適切な権限があるユーザーは、vSphere デプロイに関連付けられているデータストア上のファイルを Web ブラウザまたは vSphere Web Client を使用して表示、アップロード、またはダウンロードできます。データストア.データストアの参照権限は、それらの権限が本当に必要なユーザーまたはグループにのみ割り当てるようにしてください。

## ユーザーによる仮想マシンでのコマンドの実行を制限

vCenter Server 管理者ロールのユーザーは、デフォルトで、仮想マシンのゲスト OS 内のファイルおよびプログラムを操作できます。ゲストの機密性、可用性、または整合性が損なわれるリスクを軽減するため、ゲスト操作権限を持たない非ゲスト アクセス ロールを作成します。[ユーザーによる仮想マシン内のコマンドの実行を制限](#) を参照してください。

## vpxuser のパスワード ポリシーの確認

vCenter Server は、vpxuser のパスワードをデフォルトで 30 日ごとに自動的に変更します。この設定がポリシーを満たしていることを確認するか、企業のパスワード有効期限ポリシーを満たすようにポリシーを構成します。

[vCenter Server パスワード ポリシーの設定](#) を参照してください。

---

**注：** パスワード有効期限ポリシーが短すぎないかを確認します。

---

## vCenter Server の再起動後に権限を確認

vCenter Server を再起動するときは、権限の再割り当てを確認します。ルート フォルダで管理者ロールが割り当てられているユーザーまたはユーザー グループが、再起動時に有効なユーザーまたはグループとして確認できない場合は、そのユーザーまたはグループから管理者ロールが削除されます。vCenter Server は、ルート フォルダで、vCenter Single Sign-On アカウントの administrator@vsphere.local に管理者ロールを付与します。このアカウントは管理者として機能できるようになります。

名前付き管理者アカウントを再設定し、管理者ロールをそのアカウントに割り当てて、匿名の administrator@vsphere.local アカウントの使用を回避します。

## 高い RDP 暗号化レベルの使用

インフラストラクチャ内の各 Windows コンピュータで、リモート デスクトップ ホスト構成の各設定値を確実に設定し、環境に適した最高レベルの暗号化が確保されていることを確認します。

## vSphere Web Client 証明書の確認

vSphere Web Client または他のクライアント アプリケーションのいずれかを使用しているユーザーに、証明書検証の警告は決して無視しないように指導してください。証明書を検証しないでいると、ユーザーは MiTM 攻撃の対象となる可能性があります。

## vCenter Server パスワード ポリシーの設定

vCenter Server は、vpxuser のパスワードをデフォルトで 30 日ごとに自動的に変更します。値は vSphere Web Client から変更できます。

### 手順

- 1 vSphere Web Client オブジェクト階層で vCenter Server を選択します。
- 2 [管理] タブをクリックし、[設定] サブタブをクリックします。
- 3 [詳細設定] をクリックし、フィルタ ボックスに「**VimPasswordExpirationInDays**」と入力します。
- 4 要件を満たすように VirtualCenter.VimPasswordExpirationInDays を設定します。

## vCenter Server Windows ホストの保護

ホスト環境をできる限りセキュアにすることによって、vCenter Server が実行されている Windows ホストを脆弱性の低い状態に保ち、攻撃から保護します。

- vCenter Server システムでサポートされているオペレーティング システム、データベース、およびハードウェアを常に使用します。vCenter Server がサポートされているオペレーティング システムで実行されていない場合、正常に稼動しない可能性があり、vCenter Server が攻撃を受けやすくなります。
- vCenter Server システムに常に適切なパッチを適用します。オペレーティング システムのパッチを最新の状態に保つことで、サーバが攻撃を受けにくくなります。
- vCenter Server ホストでオペレーティング システムを保護します。この保護には、アンチウィルスおよびアンチマルウェア ソフトウェアが含まれます。

- インフラストラクチャ内の各 Windows コンピュータで、業界標準のガイドラインまたは社内ガイドラインに沿ってリモート デスクトップ (RDP) ホスト構成が設定され、最高レベルの暗号化が確保されていることを確認します。

オペレーティング システムおよびデータベースの互換性情報については、『vSphere 互換性マトリックス』を参照してください。

## 期限が切れたかまたは失効した証明書とログを失敗したインストールから削除

vCenter Server システムで、有効期限の切れた証明書、失効した証明書、失敗したインストールの vCenter Server インストール ログを放置すると、環境が損なわれる恐れがあります。

有効期限の切れた証明書、または失効した証明書は、次の理由により、削除する必要があります。

- 有効期限の切れた証明書、または失効した証明書を vCenter Server システムから削除しない場合、その環境が MiTM 攻撃の対象になる恐れがあります。
- 場合によっては、vCenter Server のインストールに失敗すると、システムにおいて、プレーン テキストでデータベース パスワードが記載されたログ ファイルが作成される場合があります。vCenter Server システムに侵入しようとする攻撃者が、このパスワードへのアクセスを取得すると同時に vCenter Server データベースにアクセスする恐れがあります。

## vCenter Server ネットワーク接続の制限

セキュリティの強化のため、vCenter Server システムを管理ネットワーク以外のネットワークに置くことを避け、vSphere 管理トラフィックが制限されたネットワークにあることを確認してください。ネットワーク接続を制限することで、特定のタイプの攻撃を制限できます。

vCenter Server は、管理ネットワークにのみアクセスする必要があります。他のネットワーク（本番環境のネットワークやストレージ ネットワーク、またはインターネットにアクセスできるネットワークなど）に vCenter Server システムを配置することを避けてください。vCenter Server は vMotion が動作しているネットワークにアクセスする必要はありません。

vCenter Server は次のシステムへのネットワーク接続が必要です。

- すべての ESXi ホスト。
- vCenter Server データベース。
- 他の vCenter Server システム（タグや権限などを複製するために vCenter Server システムが共通の vCenter Single Sign-On ドメインの一部である場合）。
- 管理クライアントの実行が許可されたシステム。たとえば、vSphere Web Client、PowerCLI を使用する Windows システム、またはその他の SDK ベースのクライアント。
- VMware vSphere Update Manager などのアドオン コンポーネントを実行するシステム。
- DNS、Active Directory、NTP などのインフラストラクチャ サービス。
- vCenter Server システムの機能に不可欠なコンポーネントを実行するその他のシステム。

vCenter Server システムが実行されている Windows システムのローカル ファイアウォールまたはネットワーク ファイアウォールを使用します。必要なコンポーネントのみが vCenter Server システムと通信できるように、IP ベースのアクセス制限を含めます。

## Linux クライアントの使用制限の検討

クライアント コンポーネントと vCenter Server システムまたは ESXi ホスト間の通信は、デフォルトでは SSL ベースの暗号化で保護されます。これらのコンポーネントの Linux バージョンでは、証明書の検証は実行されません。これらのクライアントの使用制限を検討してください。

vCenter Server システムおよび ESXi ホスト上の VMCA 署名付き証明書を、サードパーティの CA によって署名された証明書に置き換えても、Linux クライアントとの特定の通信は中間者攻撃に対して脆弱なままです。次のコンポーネントは、Linux オペレーティング システムで実行される場合は攻撃を受けやすくなります。

- vCLI コマンド
- vSphere SDK for Perl スクリプト
- vSphere Web Services SDK を使用して記述されたプログラム

適切な制御を行っている場合、Linux クライアントの使用に対する制限を緩和できます。

- 認証済みシステムのみ管理ネットワークのアクセスを制限します。
- ファイアウォールを使用して、認証済みホストのみが vCenter Server にアクセスできるようにします。
- JumpBox システムを使用して、Linux クライアントが Jump の制限を受けていることを確認します。

## インストール済みプラグインの確認

vSphere Web Client の拡張機能は、ログインしているユーザーと同じ権限レベルで実行されます。悪意のある拡張機能は便利なプラグインを装いながら、認証情報の不正入手、システム構成の変更などの有害な操作を実行できます。セキュリティを強化するには、信頼できるソースからの認証済み拡張機能のみが含まれた vSphere Web Client インストールを使用します。

vCenter のインストールには vSphere Web Client 拡張フレームワークが含まれ、vCenter アドオン コンポーネントや外部の Web ベース機能にアクセスできるメニュー選択項目またはツールバー アイコンで vSphere Web Client を拡張できます。この柔軟性は、予期しない機能が導入されるリスクを伴います。たとえば、管理者が vSphere Web Client のインスタンスにプラグインをインストールすると、そのプラグインは管理者の権限レベルで任意のコマンドを実行できます。

vSphere Web Client を潜在的な危険性から保護するために、インストールされたすべてのプラグインを定期的に調べ、プラグインがすべて信頼できるソースからのものであることを確認します。

### 前提条件

vCenter Single Sign-On サービスにアクセスする権限が必要です。これらの権限は、vCenter Server の権限とは異なります。

### 手順

- 1 administrator@vsphere.local または vCenter Single Sign-On の権限を持つユーザーとして vSphere Web Client にログインします。

- 2 ホーム ページから、[管理] を選択し、[ソリューション] で [クライアント プラグイン] を選択します。
- 3 クライアント プラグインのリストを調べます。

## vCenter Server Appliance のセキュリティのベスト プラクティス

vCenter Server システムを保護するすべてのベスト プラクティスに従って、vCenter Server Appliance を保護します。追加の手順を実行すると、使用環境のセキュリティを高めることができます。

### NTP の構成

すべてのシステムで同じ相対時間ソース（関連するローカライズ オフセットを含む）を使用し、決められた時間標準（協定世界時 (UTC) など）に相対時間ソースを関連付けられることを確認します。同期されたシステムは、証明書の有効性を確保するために不可欠です。NTP により、ログ ファイルの攻撃者の追跡も容易になります。時間の設定が正しくないと、ログ ファイルの調査や関連付けを行って攻撃を検出することが難しくなり、監査が不正確になる可能性があります。 [vCenter Server Appliance と NTP サーバとの時刻同期](#) を参照してください。

### vCenter Server Appliance のネットワーク アクセスの制限

vCenter Server Appliance と通信するために必要な基本コンポーネントにのみアクセスを制限します。不要なシステムからのアクセスをブロックすると、オペレーティング システムに対する一般的な攻撃の可能性を軽減できます。これらの基本コンポーネントにのみアクセスを制限することで、リスクを最小限に抑えることができます。

## レガシー ESXi ホストのサムプリントの検証

vSphere 6 以降では、デフォルトで VMCA 証明書がホストに割り当てられています。証明書モードをサムプリント モードに変更している場合、レガシー ホストでもサムプリント モードを引き続き使用できます。vSphere Web Client で、サムプリントを検証することができます。

---

**注：** デフォルトでは、証明書は複数のアップグレードにわたって保持されます。

---

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、vCenter Server システムを参照して移動します。
- 2 [管理] タブを選択し、[設定] をクリックして、[全般] をクリックします。
- 3 [Edit] をクリックします。
- 4 [SSL 設定] をクリックします。

- ESXi 5.5 以前のホストのいずれかを手動で検証する必要がある場合、ホスト用に一覧表示されたサムプリントとホスト コンソール内のサムプリントを比較します。

ホストのサムプリントを取得するには、ダイレクト コンソール ユーザー インターフェイス (DCUI) を使用します。

- ダイレクト コンソールにログインし、[F2] を押してシステムのカスタマイズ メニューにアクセスします。
- [サポート情報の表示] を選択します。

右側の列にホストのサムプリントが表示されます。

- サムプリントが一致している場合、ホストの横にある [検証] を選択します。

選択しなかったホストは、[OK] をクリックすると切断されます。

- [OK] をクリックします。

## ネットワーク ファイル コピーによる SSL 証明書検証が有効かどうかの確認

NFC（ネットワーク ファイル コピー）によって、vSphere コンポーネントでファイル タイプに対応した FTP サービスを使用できます。vSphere 5.5 以降では、ESXi は、データストア間のデータのコピーや移動などの操作にデフォルトで NFC を使用しますが、無効になっている場合は有効にする必要があります。

NFC 経由の SSL が有効な場合、NFC を介した vSphere コンポーネント間の接続はセキュリティで保護されます。この接続は、データセンター内の中間者攻撃からの防御に役立ちます。

SSL 経由で NFC を使用するとパフォーマンスが低下するため、一部の開発環境ではこの詳細設定を無効にすることを検討してください。

---

**注：** スクリプトを使用して値を確認する場合は、この値を明示的に true に設定します。

---

### 手順

- vSphere Web Client を使用して vCenter Server に接続します。
- [設定] タブを選択し、[詳細設定] をクリックします。
- [編集] をクリックします。
- ダイアログの下で、次のキーと値を入力します。

フィールド	値
キー	config.nfc.useSSL
値	true

- [OK] をクリックします。



## vCenter Server の TCP および UDP ポート

vCenter Server には、事前に設定された TCP および UDP ポートを経由してアクセスします。ファイアウォールの外からネットワーク コンポーネントを管理する場合、ファイアウォールを再設定して、該当するポートへのアクセスを許可する必要があります。

次の表に、TCP および UDP ポートと、それぞれの目的およびタイプを示します。インストール時にデフォルトで開かれたポートは、「(デフォルト)」で示されます。vSphere の各バージョンで提供されているすべての vSphere コンポーネントのポートについては、[VMware ナレッジベースの記事 1012382](#) で最新のリストを参照してください。

表 6-1. vCenter Server の TCP および UDP ポート

ポート	目的
80 (デフォルト)	HTTP アクセス vCenter Server では、直接 HTTP 接続用にポート 80 が必要です。ポート 80 は、要求を HTTPS ポート 443 にリダイレクトします。これは、https://server ではなく、誤って http://server にアクセスした場合のリダイレクトに利用できます。 WS-Management (ポート 443 の開放が必要)
88, 2013	vCenter Single Sign-On で使用される Kerberos の制御インターフェイス RPC。
123	NTP クライアント
135 (デフォルト)	vCenter Server Appliance の場合、このポートは Active Directory の認証用に指定されます。 vCenter Server Windows インストールの場合、このポートはリンク モードに使用され、ポート 88 は Active Directory の認証に使用されます。
161 (デフォルト)	SNMP サーバ。これは、ESXi ホストと vCenter Server Appliance の両方でデフォルトのポートです。
389	vCenter Single Sign-On LDAP (6.0 以降)
636	vCenter Single Sign-On LDAPS (6.0 以降)
443 (デフォルト)	vCenter Server システムは、ポート 443 を使用して SDK クライアントからのデータ転送を監視します。 このポートは、次のサービスでも使用されます。 <ul style="list-style-type: none"> <li>■ WS-Management (ポート 80 の開放が必要)</li> <li>■ サードパーティ製ネットワーク管理クライアントから vCenter Server への接続</li> <li>■ サードパーティ製ネットワーク管理クライアントからホストへのアクセス</li> </ul>
2012	VMware Directory Service (vmdir) 用の RPC ポート。
2014	VMware Certificate Authority (VMCA) サービス用の RPC ポート。
2020	VMware Authentication Framework サービス (vmafd) 用の RPC ポート。
31031, 44046 (デフォルト)	vSphere Replication
7444	vCenter Single Sign-On の HTTPS。
8093	クライアント統合プラグインはローカル ループバック ホスト名を使用し、ポート 8093 と 50100 から 60099 の範囲のランダム ポートを使用します。ローカル通信の場合は、ポート 8093 のみを使用します。このポートは、ファイアウォールでブロックしたままにできます。

表 6-1. vCenter Server の TCP および UDP ポート（続き）

ポート	目的
8109	VMware Syslog Collector。
9443	vSphere Web Client の ESXi ホストに対する HTTP アクセス。
10080	Inventory Service。
11711	vCenter Single Sign-On の LDAP（vSphere 5.5 からアップグレードされた環境）
11712	vCenter Single Sign-On の LDAPS（vSphere 5.5 からアップグレードされた環境）
12721	VMware Identity Management Service。
15005	ESX Agent Manager (EAM)。ESX エージェントは仮想マシンまたはオプションの VIB となります。このエージェントは、ESXi ホストの機能を拡張して、NSX-v や vRealize Automation などの vSphere ソリューションで必要な追加のサービスを提供します。
15007	vService Manager (VSM)。このサービスは vCenter Server エクステンションの登録を行います。このポートは、使用するエクステンションに必要な場合にのみ開きます。
50100-60099	クライアント統合プラグインはローカル ループバック ホスト名を使用し、ポート 8093 と 50100 から 60099 の範囲のランダム ポートを使用します。クライアント統合プラグインは、ローカル通信の場合、このポート範囲のみを使用します。このポートは、ファイアウォールでブロックしたままにできます。

これらのポートに加え、必要に応じてその他のポートも構成できます。

## CIM ベースのハードウェア監視ツールのアクセス制御

CIM（Common Information Model）システムは、一連の標準 API を使用してリモート アプリケーションからハードウェア レベルで管理できるインターフェイスを提供します。CIM インターフェイスのセキュリティを確保するため、これらのアプリケーションには必要最小限のアクセス権のみを付与します。アプリケーションが root または完全な管理者アカウントでプロビジョニングされていて、そのアプリケーションが侵害された場合、仮想環境全体が侵害される可能性があります。

CIM はオープンな標準で、ESXi でエージェントレス、標準ベースのハードウェア リソース監視を行うフレームワークを定義します。このフレームワークは、CIM オブジェクト マネージャ（通常は CIM ブローカーと呼ばれます）と一連の CIM プロバイダで構成されます。

CIM プロバイダは、デバイス ドライバおよび基盤となるハードウェアへのアクセスを管理するメカニズムとして使用されます。サーバのメーカーや特定のハードウェア デバイス ベンダーを含むハードウェア ベンダーは、特定のデバイスの監視と管理を行うようにプロバイダを記述できます。また、VMware もサーバ ハードウェア、ESXi ストレージ インフラストラクチャ、および仮想化固有のリソースの監視を実装するプロバイダを記述します。これらのプロバイダは ESXi システム内で実行されるため、非常に軽量で特定の管理タスクに重点を置くように設計されています。CIM ブローカーはすべての CIM プロバイダから情報を取得し、標準 API（最も一般的な API は WS-MAN）を使用してその情報を外部に表示します。

CIM インターフェイスにアクセスするリモート アプリケーションには root 認証情報を提供しないでください。代わりに、それらのアプリケーションに固有のサービス アカウントを作成し、ESXi システムで定義されたローカル アカウント、および vCenter Server で定義されたロールに対して CIM 情報への読み取り専用アクセス権を付与します。

## 手順

- 1 CIM アプリケーションに固有のサービス アカウントを作成します。
- 2 ESXi システムで定義されたローカル アカウント、および vCenter Server で定義されたロールに対して CIM 情報への読み取り専用アクセス権を付与します。
- 3 (オプション) アプリケーションで CIM インターフェイスへの書き込みアクセス権が必要な場合は、次の 2 つの権限のみをサービス アカウントに適用するロールを作成します。
  - ホスト.構成.SystemManagement
  - ホスト.CIM.CIMInteraction

監視アプリケーションの用途に応じて、このロールはホストのローカルとして作成するか、vCenter Server で一元的に定義することができます。

## 結果

CIM アプリケーション用に作成されたサービス アカウントでユーザーがホストにログインした場合、ユーザーには SystemManagement および CIMInteraction、または読み取り専用アクセス権のみが付与されます。

# 仮想マシンのセキュリティ

# 7

仮想マシンで実行するゲスト OS は、物理システムと同じセキュリティ リスクにさらされます。物理マシンと同様に仮想マシンをセキュリティで保護します。

この章には、次のトピックが含まれています。

- 仮想マシンから VMX ファイルへの情報メッセージの制限
- 仮想ディスクの圧縮の防止
- 仮想マシンのセキュリティのベスト プラクティス

## 仮想マシンから VMX ファイルへの情報メッセージの制限

仮想マシンから VMX ファイルへの情報メッセージを制限して、データストアがいっぱいになりサービス拒否 (DoS) が発生することを防ぎます。サービス拒否は、仮想マシンの VMX ファイルのサイズが管理されておらず、情報量がデータストアの容量を超えた場合に発生します。

情報としての名前と値のペアを含む構成ファイルのサイズは、デフォルトでは 1MB に制限されています。ほとんどの場合この容量で十分ですが、必要に応じてこの値を変更できます。たとえば、構成ファイルに大量のカスタム情報が格納されている場合、この制限値を増やすことができます。

---

**注：** 必要な情報の量を慎重に検討してください。情報の量がデータストアの容量を超えると、サービス拒否が発生する可能性があります。

---

デフォルト制限値の 1 MB は、詳細オプションのリストに `tools.setInfo.sizeLimit` パラメータが含まれていない場合でも適用されます。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 `tools.setInfo.sizeLimit` パラメータを追加または編集します。

## 仮想ディスクの圧縮の防止

ゲスト OS の管理者以外のユーザーは、仮想ディスクを圧縮できます。仮想ディスクを圧縮すると、未使用のディスク領域が解放されます。ただし、仮想ディスクを繰り返し圧縮した場合、ディスクが使用できなくなりサービス拒否が発生する可能性があります。これを防ぐには、仮想ディスクの圧縮機能を無効にします。

### 前提条件

- 仮想マシンをパワーオフします。
- 仮想マシンでの root または管理者権限を持っていることを確認します。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 以下のパラメータを追加または編集します。

名前	値
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

- 6 [OK] をクリックします。

### 結果

この機能を無効にすると、データストアの容量が足りなくなったときに仮想マシンのディスクを圧縮できません。

## 仮想マシンのセキュリティのベスト プラクティス

仮想マシンのセキュリティのベスト プラクティスに従うことで、vSphere デプロイの整合性を確保できます。

### ■ 仮想マシンの全般的な保護

仮想マシンは、あらゆる点で物理サーバと同等です。物理システムと同じセキュリティ対策を仮想マシンで講じます。

### ■ 仮想マシンをデプロイするためのテンプレートの使用

仮想マシンにゲスト OS およびアプリケーションを手動でインストールする場合、誤って構成する可能性があります。テンプレートを使用して、アプリケーションをインストールしていない堅牢な基本オペレーティングシステム イメージをキャプチャすることで、既知のベース ライン レベルのセキュリティですべての仮想マシンを作成できます。

#### ■ 仮想マシン コンソールの使用の最小化

仮想マシンのコンソールには、物理サーバーで行う監視と同じように、仮想マシンで監視を行う機能があります。仮想マシンのコンソールにアクセス権があるユーザーには、仮想マシンの電力管理とリムーバブル デバイス接続コントロールへのアクセス権があります。これにより、仮想マシンは悪意のある攻撃を受ける可能性があります。

#### ■ 仮想マシンのリソースの引き継ぎの防止

1つの仮想マシンによるホスト リソースの消費量が多すぎるため、ホスト上のほかの仮想マシンが機能を実行できなくなる場合、サービス拒否（DoS）が発生する可能性があります。仮想マシンが DoS の原因となるのを防止するには、共有の設定やリソース プールの使用などのホストのリソース管理機能を使用します。

#### ■ 仮想マシン内の不必要な機能の無効化

仮想マシンで実行されるすべてのサービスは攻撃の対象になる可能性があります。システムで実行するアプリケーションまたはサービスをサポートする必要のない、不要なシステム コンポーネントを無効にすることで、攻撃を受ける可能性のあるコンポーネント数を減らします。

## 仮想マシンの全般的な保護

仮想マシンは、あらゆる点で物理サーバと同等です。物理システムと同じセキュリティ対策を仮想マシンで講じます。

次のベスト プラクティスに従い、仮想マシンを保護します。

### パッチおよびその他の保護

適切なパッチの適用を含む、すべてのセキュリティ対策を最新の状態に保ちます。パワーオフされた休止仮想マシンは見過ごしやすいため、休止仮想マシンの更新を常に確認することが特に重要です。たとえば、アンチウイルス ソフトウェア、アンチスパイウェア、侵入検知、その他の保護が仮想インフラストラクチャ内のすべての仮想マシンで有効になっていることを確認します。仮想マシンのログ用に十分な容量があることも確認する必要があります。

### アンチウィルス スキャン

各仮想マシンは標準的なオペレーティング システムをホストしているため、アンチウイルス ソフトウェアをインストールして、ウイルスから仮想マシンを保護する必要があります。仮想マシンの利用方法によっては、ソフトウェア ファイアウォールのインストールも必要になる場合があります。

特に、多数の仮想マシンをデプロイするときは、ウイルス スキャンのスケジュールを調整してください。すべての仮想マシンを同時にスキャンすると、使用している環境内のシステムのパフォーマンスが大幅に低下します。ソフトウェア ファイアウォールとアンチウイルス ソフトウェアは仮想化に負荷をかけることがあるため、特に仮想マシンが完全に信頼できる環境にあることが確実な場合は、この 2 つのセキュリティ対策の必要性和仮想マシンのパフォーマンスのバランスをとることができます。

### シリアル ポート

シリアル ポートは、周辺機器を仮想マシンに接続するためのインターフェイスです。多くの場合、サーバのコンソールへの低レベルでの直接接続のために物理システムで使用されます。仮想シリアル ポートでは、1つの仮想マシンへの同じアクセスが許可されます。シリアル ポートでは低レベルのアクセスを行うことができ、多くの場合、ログまたは権限のように高レベルでの制御は行われません。

## 仮想マシンをデプロイするためのテンプレートの使用

仮想マシンにゲスト OS およびアプリケーションを手動でインストールする場合、誤って構成する可能性があります。テンプレートを使用して、アプリケーションをインストールしていない堅牢な基本オペレーティング システム イメージをキャプチャすることで、既知のベース ライン レベルのセキュリティですべての仮想マシンを作成できます。

堅牢でパッチ適用済みの適切に構成された OS を含むテンプレートを使用してアプリケーション固有の他のテンプレートを作成したり、アプリケーション テンプレートを使用して仮想マシンをデプロイすることができます。

### 手順

- ◆ 堅牢でパッチ処理済みの適切に構成されたオペレーティング システム デプロイを含む、仮想マシン作成用のテンプレートを指定します。

可能な場合は、テンプレートでアプリケーションもデプロイします。デプロイされる仮想マシンに固有の情報にアプリケーションが依存していないことを確認します。

### 次のステップ

テンプレートに関する詳細は、『vSphere 仮想マシン管理』ドキュメントを参照してください。

## 仮想マシン コンソールの使用の最小化

仮想マシンのコンソールには、物理サーバーで行う監視と同じように、仮想マシンで監視を行う機能があります。仮想マシンのコンソールにアクセス権があるユーザーには、仮想マシンの電力管理とリムーバブル デバイス接続コントロールへのアクセス権があります。これにより、仮想マシンは悪意のある攻撃を受ける可能性があります。

### 手順

- 1 ターミナル サービスや SSH のようなネイティブのリモート管理サービスを使用して、仮想マシンと通信してください。

必要な場合に限り、仮想マシン コンソールへのアクセス権を付与してください。

- 2 コンソールへの接続を必要な数に制限します。

たとえば、安全性の高い環境では、接続を 1 つに制限します。一部の環境では、通常のタスクを実行するために必要な同時接続数に応じて、その制限を増やすことができます。

## 仮想マシンのリソースの引き継ぎの防止

1 つの仮想マシンによるホスト リソースの消費量が多すぎるため、ホスト上のほかの仮想マシンが機能を実行できなくなる場合、サービス拒否（DoS）が発生する可能性があります。仮想マシンが DoS の原因となるのを防止するには、共有の設定やリソース プールの使用などのホストのリソース管理機能を使用します。

デフォルトでは、ESXi ホストのすべての仮想マシンがリソースを均等に共有します。共有およびリソース プールを使用して、サービス拒否攻撃を防止します。この攻撃では、1 つの仮想マシンがホストのリソースの大半を消費して、同じホストの別の仮想マシンが目的の機能を実行できなくなります。

影響について十分理解するまでは、制限の機能を使用しないでください。

**手順**

- 1 各仮想マシンは、正常に機能するために必要なだけのリソース（CPU およびメモリ）を使用してプロビジョニングします。
- 2 共有を使用して、重要な仮想マシンに対してリソースを保証します。
- 3 要件が似ている仮想マシンをグループ化し、リソース プールを作成します。
- 4 各リソース プールで、共有の設定をデフォルトのままにし、プール内の各仮想マシンにおおよそ同じリソース優先度が設定されるようにします。

この設定では、1つの仮想マシンが同じリソース プールの他の仮想マシンより多くを使用することはできなくなります。

**次のステップ**

共有および制限の詳細については、『vSphere リソース管理』ドキュメントを参照してください。

**仮想マシン内の不必要な機能の無効化**

仮想マシンで実行されるすべてのサービスは攻撃の対象になる可能性があります。システムで実行するアプリケーションまたはサービスをサポートする必要のない、不要なシステム コンポーネントを無効にすることで、攻撃を受ける可能性のあるコンポーネント数を減らします。

通常、仮想マシンは物理サーバと同数のサービスや機能は必要ありません。システムを仮想化するときに、特定のサービスまたは機能が必要であるかどうかを評価します。

**手順**

- ◆ オペレーティング システムで未使用のサービスを無効にします。  
たとえば、システムでファイル サーバを実行している場合は Web サービスをオフにします。
- ◆ CD/DVD ドライブ、フロッピー ドライブ、USB アダプタなどの未使用の物理デバイスを切断します。
- ◆ 未使用の機能（未使用の表示機能、HGFS (Host Guest File System) など）を無効にします。
- ◆ スクリーン セーバーをオフにします。
- ◆ Linux、BSD、または Solaris ゲスト OS で X Window システムが不要な場合、X Window システムは実行しないでください。

**不要なハードウェア デバイスの削除**

すべての有効になっているデバイスや接続されているデバイスは、攻撃チャネルになる可能性があります。仮想マシン上で権限のないユーザーおよびプロセスは、ネットワーク アダプタや CD-ROM ドライブなどのハードウェア デバイスを接続または切断できます。攻撃者は、仮想マシンのセキュリティを侵害するためにこの機能を利用できます。不要なハードウェア デバイスを削除しておくことで攻撃の防止に役立ちます。



仮想マシンにアクセスした攻撃者は、切断されたハードウェア デバイスを接続し、ドライブ内に残されたメディアにある機密情報にアクセスしたり、ネットワーク アダプタを切断して仮想マシンをネットワークから隔離し、結果的にサービス拒否状態にすることができます。

- 承認されていないデバイスが接続されていないことを確認し、不要または未使用のハードウェア デバイスを削除します。
- 仮想マシン内から不要な仮想デバイスを無効にします。
- 必須ではないデバイスが仮想マシンに接続されていないことを確認します。シリアル ポートとパラレル ポートはデータセンターの仮想マシンではほとんど使用されず、CD/DVD ドライブは通常はソフトウェアのインストール時にのみ一時的に接続されます。

#### 手順

- 1 vSphere Web Client を使用して vCenter Server システムにログインします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 各ハードウェア デバイスをチェックして、接続すべきデバイスかどうかを確認します。

次のようなデバイスをチェックします。

- フロッピー ドライブ
- シリアル ポート
- パラレル ポート
- USB コントローラ
- CD-ROM ドライブ

### 未使用の表示機能の無効化

未使用の表示機能は、悪意のあるコードを使用環境に挿入するための媒介として攻撃者に利用される可能性があります。使用環境で使用されていない機能は無効にしてください。

#### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。

- 5 必要に応じて、次のパラメータを追加または編集して設定します。

オプション	説明
<code>svga.vgaonly</code>	このパラメータを TRUE に設定すると、高度なグラフィック機能が動作しなくなります。文字セル コンソール モードのみを使用できます。この設定を使用する場合、 <code>mks.enable3d</code> は無効になります。  <b>注：</b> 仮想化ビデオ カードを必要としない仮想マシンにのみこの設定を適用します。
<code>mks.enable3d</code>	3D 機能を必要としない仮想マシンでこのパラメータを FALSE に設定します。

## 非公開機能の無効化

VMware 仮想マシンは、vSphere システムおよびホストされている仮想化プラットフォーム（Workstation や Fusion など）の両方で使用できるように設計されています。vSphere システムで仮想マシンを実行する場合、特定の仮想マシン パラメータは有効である必要はありません。これらのパラメータを無効にし、脆弱性を引き起こす可能性を軽減します。

### 前提条件

仮想マシンをパワーオフします。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 次のパラメータを追加または編集して TRUE に設定します。
  - `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 [OK] をクリックします。

## HGFS ファイル転送の無効化

自動化された Tools のアップグレードなどの特定の操作では、Host Guest File System (HGFS) と呼ばれるハイパーバイザー内のコンポーネントを使用します。高セキュリティ環境では、攻撃者が HGFS を使用してゲスト OS 内のファイルを転送するリスクを最小限に抑えるために、このコンポーネントを無効にすることができます。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 `isolation.tools.hgfsServerSet.disable` パラメータが TRUE に設定されていることを確認します。

### 結果

この変更を行うと、VMX プロセスは、Tools プロセスからのコマンドに応答しなくなります。ゲスト OS とのファイルの転送に HGFS を使用する API（一部の VIX コマンドや VMware Tools 自動アップグレード ユーティリティなど）は機能しなくなります。

## ゲスト OS システムとリモート コンソール間のコピー アンド ペースト操作の無効化

ゲスト OS とリモート コンソール間のコピー アンド ペースト操作はデフォルトで無効です。安全な環境のためには、デフォルト設定を保持してください。コピー アンド ペースト操作が必要な場合は、vSphere Web Client を使用して操作を有効にする必要があります。

これらのオプションはデフォルトで推奨値に設定されています。ただし、監査ツールで設定が正しいかどうか確認できるようにする場合は、明示的に true に設定する必要があります。

### 前提条件

仮想マシンをパワーオフします。

### 手順

- 1 vSphere Web Client を使用して vCenter Server システムにログインします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] をクリックし、[構成の編集] をクリックします。

- 4 名前と値の各列に次の値が入力されていることを確認するか、[行の追加] をクリックして値を入力します。

名前	推奨値
isolation.tools.copy.disable	真
isolation.tools.paste.disable	真
isolation.tools.setGUIOptions.enable	false

ゲスト OS の VMware Tools コントロール パネルで行なった設定は、これらのオプションによってすべてオーバーライドされます。

- 5 [OK] をクリックします。
- 6 (オプション) 構成パラメータに変更を加えた場合、仮想マシンを再起動してください。

### クリップボードにコピーされた機密データの漏えい制限

ホストでは、クリップボードにコピーされた機密データの漏えいを防ぐため、コピー アンド ペーストの操作がデフォルトで無効になっています。

VMware Tools を実行している仮想マシンでコピー アンド ペーストが有効になっている場合、ゲスト OS とリモート コンソールとの間でコピー アンド ペースト操作が可能です。コンソール ウィンドウにフォーカスが移るとすぐに、仮想マシンを操作している権限のないユーザーおよび実行中のプロセスは、仮想マシン コンソールのクリップボードにアクセスできます。ユーザーがコンソールを使用する前に機密情報をクリップボードにコピーすると、ユーザーが気付かない間に、機密データが仮想マシンにさらされています。この問題を防ぐため、ゲスト OS のコピー アンド ペースト操作はデフォルトで無効になっています。

必要な場合は、仮想マシンのコピー アンド ペースト操作を有効にできます。

### ユーザーによる仮想マシン内のコマンドの実行を制限

vCenter Server 管理者ロールのユーザーは、デフォルトで、仮想マシンのゲスト OS 内のファイルおよびプログラムを操作できます。ゲストの機密性、可用性、または整合性が損なわれるリスクを軽減するため、ゲスト操作権限を持たない非ゲスト アクセス ロールを作成します。

セキュリティを考慮して、物理データセンターの場合と同様に仮想データセンターへのアクセス許可を制限します。ユーザーに完全な管理者アクセス権限が付与されないようにするには、ゲスト アクセス権限を無効化するカスタムロールを作成し、管理者権限が必要ではあっても、ゲスト OS 内のファイルおよびプログラムを操作することを許可されないユーザーにそのロールを適用します。

たとえば、機密情報を含むインフラストラクチャ上にある仮想マシンが構成に含まれる場合があります。vMotion や Storage vMotion での移行などのタスクでは、IT ロールに仮想マシンへのアクセス権が必要です。この場合、ゲスト OS 内のいくつかのリモート操作を無効化して、IT ロールが機密情報にアクセスできないようにする必要があります。

#### 前提条件

ロールを作成する vCenter Server システムで管理者権限を持っていることを確認します。

## 手順

- 1 ロールを作成する vCenter Server システムの管理者権限を持つユーザーとして vSphere Web Client にログインします。
- 2 [管理] をクリックし、[ロール] を選択します。
- 3 [ロールの作成アクション] アイコンをクリックし、ロールの名前を入力します。  
たとえば、「**ゲスト アクセス不可の管理者**」と入力します。
- 4 [すべての権限] を選択します。
- 5 すべての権限、仮想マシン、ゲスト操作 を選択解除して、ゲスト操作の権限セットを削除します。
- 6 [OK] をクリックします。

## 次のステップ

vCenter Server システムまたはホストを選択し、新規権限を持つユーザーまたはグループをペアにするアクセス許可を、新規作成されたロールに割り当てます。デフォルトの管理者ロールからそれらのユーザーを削除します。

## 仮想マシンのユーザーまたはプロセスによるデバイスの切断防止

仮想マシン上でルートまたはシステム管理者の権限のないユーザーおよびプロセスは、ネットワーク アダプタや CD-ROM ドライブなどのデバイスを接続または切断したり、デバイス設定を変更したりできます。仮想マシンのセキュリティを向上させるには、これらのデバイスを削除してください。デバイスを永久に削除するのが好ましくない場合は、仮想マシンのユーザーまたはプロセスがゲスト OS からデバイスを接続または切断するのを防ぐことができます。

## 前提条件

仮想マシンがパワーオフされている。

## 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 名前と値の各列に次の値が入力されていることを確認するか、[行の追加] をクリックして値を入力します。

名前	値
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

ゲスト OS の VMware Tools コントロール パネルで行なった設定より、これらのオプションが優先されます。

- 6 [OK] をクリックして [構成パラメータ] ダイアログ ボックスを閉じ、再度 [OK] をクリックします。

## ゲスト OS の可変メモリ制限の変更

構成ファイルに大量のカスタム情報が格納されている場合は、ゲスト OS の可変メモリ制限を増やすことができます。

### 前提条件

仮想マシンをパワーオフします。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] - [詳細] を選択し、[構成の編集] をクリックします。
- 4 パラメータ `tools.setInfo.sizeLimit` を追加または編集し、値をバイト数に設定します。
- 5 [OK] をクリックします。

## ゲスト OS のプロセスによるホストへの構成メッセージの送信防止

ゲストが構成ファイルに対して名前と値のペアを書き込むことを禁止できます。これは、ゲスト OS による構成設定の変更を禁止する必要がある場合に適切です。

### 前提条件

仮想マシンをパワーオフします。

### 手順

- 1 vSphere Web Client インベントリで仮想マシンを検索します。
  - a データセンター、フォルダ、クラスタ、リソース プール、またはホストを選択します。
  - b [関連オブジェクト] タブで、[仮想マシン] をクリックします。
- 2 仮想マシンを右クリックし、[設定の編集] をクリックします。
- 3 [仮想マシン オプション] を選択します。
- 4 [詳細] をクリックして、[構成の編集...] をクリックします。
- 5 [行の追加] をクリックし、次の値を名前と値の各列に入力します。
  - 名前の列: **`isolation.tools.setinfo.disable`**
  - 値の列: **`true`**
- 6 [OK] をクリックして [構成パラメータ] ダイアログ ボックスを閉じ、再度 [OK] をクリックします。

## 独立型の読み取り専用ディスクの使用の回避

独立型読み取り専用ディスクを使用する場合、侵入に成功した攻撃者は、システムのシャットダウンまたは再起動によってマシンが侵害されたことの証拠をすべて削除することができます。仮想マシンでのアクティビティの通常の記録がなければ、管理者は攻撃に気づかない可能性があります。したがって、独立型読み取り専用ディスクは使用しないでください。

### 手順

- ◆ syslog サーバや同等の Windows ベースのイベント コレクタなどの別個のサーバに、仮想マシンのアクティビティがリモートで確実にログに記録されるようにします。

ゲストでイベントとアクティビティのリモート ログが構成されていない場合は、scsiX:Y.mode を次のいずれかの設定にする必要があります。

- なし
- 独立型読み取り専用に設定しない

### 結果

読み取り専用モードが有効になっていない場合は、システムの再起動時に仮想マシンを既知の状態にロールバックすることはできません。

# vSphere ネットワークのセキュリティ強化

# 8

vSphere ネットワークの保護は、環境を保護するために不可欠です。各種の vSphere コンポーネントをさまざまな方法で保護します。vSphere 環境のネットワークの詳細については、vSphere ネットワークドキュメントを参照してください。

この章には、次のトピックが含まれています。

- vSphere ネットワーク セキュリティの概要
- ファイアウォールによるネットワークのセキュリティ強化
- 物理スイッチのセキュリティ強化
- セキュリティ ポリシーによる標準スイッチ ポートのセキュリティ強化
- vSphere 標準スイッチのセキュリティ強化
- vSphere 分散スイッチおよび分散ポート グループのセキュリティ強化
- VLAN を使用した仮想マシンのセキュリティ強化
- 単一の ESXi ホストでのネットワーク DMZ の作成
- 単一の ESXi ホスト内での複数のネットワークの作成
- インターネット プロトコル セキュリティ
- SNMP 構成が適切であることの確認
- 必要なときにのみ vSphere Network Appliance API で仮想スイッチを使用
- vSphere ネットワークのセキュリティのベスト プラクティス

## vSphere ネットワーク セキュリティの概要

vSphere 環境のネットワーク セキュリティには、物理ネットワーク環境の保護と多くの点で共通した特徴がありますが、仮想マシンにのみあてはまる特徴も含まれています。

### ファイアウォール

仮想ネットワークの一部またはすべての仮想マシンにホスト ベースのファイアウォールをインストールおよび構成することで、仮想ネットワークにファイアウォール保護を追加します。



効率を高くするために、プライベート仮想マシン イーサネット ネットワーク（仮想ネットワーク）を設定できます。仮想ネットワークの場合、仮想ネットワークの入口にある仮想マシンにホスト ベースのファイアウォールをインストールします。ファイアウォールは、物理ネットワーク アダプタと仮想ネットワークの残りの仮想マシンとの間で、保護バッファとして機能します。

ホスト ベースのファイアウォールをインストールするとパフォーマンスが低下することがあるので、仮想ネットワーク上の別の仮想マシンにホスト ベースのファイアウォールをインストールする前に、セキュリティ要件とパフォーマンス目標のバランスを考慮してください。

[ファイアウォールによるネットワークのセキュリティ強化](#) を参照してください。

## セグメント化

ホスト内の異なる仮想マシン ゾーンを異なるネットワーク セグメントに置きます。各仮想マシン ゾーンをそれ自身のネットワーク セグメントで隔離すると、仮想マシン ゾーン間でデータ漏れのリスクを最小限に抑えることができます。セグメント化により、攻撃者が ARP テーブルを操作して MAC および IP アドレスのマッピングを変え、ホストとのネットワーク トラフィックのアクセスを取得するアドレス解決プロトコル（ARP）スプーフィングなどのさまざまな脅威を防止できます。攻撃者は ARP スプーフィングを使用して、中間者攻撃（MTM）、サービス拒否（DoS）攻撃、対象システムのハイジャック、または仮想ネットワークの崩壊を行います。

セグメント化を綿密に計画して、仮想マシン ゾーン間のパケット転送機会を減らすことで、被害者にネットワーク トラフィックの送信が要求される傍受攻撃を防ぐことができます。さらに、攻撃者は特定の仮想マシン ゾーンでセキュリティ保護されていないサービスを使用して、ホスト内の別の仮想マシン ゾーンにアクセスすることができません。次の 2 つの方法のうちいずれかを使用してセグメント化を実装できます。各方法のメリットは異なります。

- 仮想マシン ゾーンに個別の物理ネットワーク アダプタを使用して、ゾーンを隔離させる。仮想マシン ゾーンに個別の物理ネットワーク アダプタを設定する方法は、おそらく最も安全で、最初に作成したセグメントをあとから不正に構成されにくい方法です。
- ネットワークを保護するように、仮想ローカル エリア ネットワーク（VLAN）を設定する。VLAN は、物理的に分離したネットワークを実装する場合のセキュリティのメリットをハードウェア オーバーヘッドなしにほとんどすべて利用できるので、追加デバイスや配線などの導入および保守にかかるコストを節約できる、実行可能なソリューションを提供します。[VLAN を使用した仮想マシンのセキュリティ強化](#) を参照してください。

## 不正アクセスの防止

仮想マシン ネットワークが物理ネットワークに接続されている場合、物理マシンで構成されたネットワークのように侵害を受けやすくなります。仮想マシン ネットワークが物理ネットワークから隔離されている場合でも、ネットワークの仮想マシンは、ネットワークのほかの仮想マシンから攻撃を受けやすくなります。仮想マシンのセキュリティ要件は通常、物理マシンのセキュリティ要件と同じになります。

仮想マシンはそれぞれ隔離されています。仮想マシンは、別の仮想マシンに対して、メモリを読み取ったり書き込んだり、データへアクセスしたり、アプリケーションを使用したりすることはできません。ただしネットワーク内で、どの仮想マシンも仮想マシン グループも、ほかの仮想マシンから不正にアクセスされる可能性があるため、体外的な保護がさらに必要になることがあります。

## ファイアウォールによるネットワークのセキュリティ強化

セキュリティ システム管理者は、ファイアウォールを使用して、ネットワークまたはネットワーク内で選択したコンポーネントを侵入から保護します。

ファイアウォールは、システム管理者が明示的または暗黙的に許可したポート以外のすべてのポートを閉じ、その範囲内のデバイスへのアクセスを制御します。管理者が開くポートは、ファイアウォールの内側と外側のデバイス間のトラフィックを許可します。

---

**重要：** ESXi 5.5 以降の ESXi ファイアウォールは、ネットワーク単位での vMotion トラフィックのフィルタリングを許可しません。そのため、vMotion ソケットへの受信接続が行われないように、外部ファイアウォールにルールをインストールする必要があります。

---

仮想マシン環境では、コンポーネント間で、ファイアウォールのレイアウトを計画できます。

- vCenter Server システムなどの物理マシンと ESXi ホスト間のファイアウォール。
- 仮想マシン間（たとえば、外部 Web サーバとして機能している仮想マシンと、企業の内部ネットワークに接続されている仮想マシン間）のファイアウォール。
- 物理ネットワーク アダプタ カードと仮想マシン間にファイアウォールを配置する場合などの物理マシンと仮想マシン間のファイアウォール。

ESXi 構成の中でファイアウォールをどのように使用するかは、ネットワークをどのように使用するか、特定のコンポーネントでどの程度のセキュリティが必要か、によって異なります。たとえば、各マシンが同じ部署の異なるベンチマーク テスト スイートを実行することだけを目的としている仮想ネットワークを作成すると、仮想マシン間で不必要なアクセスが生じる可能性が最小になります。したがって、ファイアウォールが仮想マシン間に存在する構成は必要ありません。ただし、外部ホストからのテスト実行の割り込みを防ぐために、仮想ネットワークのエントリ ポイントでファイアウォールを構成して、仮想マシンの全体のセットを保護することができます。

ファイアウォールのポートの図については、VMware ナレッジベースの記事 [2131180](#) を参照してください。

### vCenter Server を使用した構成でのファイアウォール

vCenter Server を介して ESXi ホストにアクセスする場合、通常はファイアウォールを使用して vCenter Server を保護します。このファイアウォールは、ネットワークに基本的な保護を提供します。

ファイアウォールは、クライアントと vCenter Server との間に配置されていることがあります。または、導入環境によっては、vCenter Server とクライアントがファイアウォールの内側に配置されている場合があります。ここで確認する主要な点は、システムのエントリー ポイントとなる場所にファイアウォールがあるということです。

vSphere vMotion™ や vSphere フォールト トレランスなどの TCP および UDP ポートの包括的なリストは、[vCenter Server の TCP および UDP ポート](#) を参照してください。

vCenter Server で構成されたネットワークは、vSphere Web Client、またはホストとのインターフェイスに SDK を使用するサードパーティ製ネットワーク管理クライアントを介して、通信を受信できます。通常の操作中、vCenter Server は、指定ポートで管理されるホストとクライアントからのデータを待機します。また、vCenter Server は、管理ホストが指定ポートで vCenter Server からのデータを待機することを前提としています。これらの構成要素のいずれかの間にファイアウォールがある場合、データ転送をサポートするため、ファイアウォールに開いているポートがあることを確認する必要があります。

また、ネットワークの使用方法や、さまざまなデバイスに必要なセキュリティ レベルの程度により、ネットワークのさまざまなアクセス ポイントにファイアウォールを追加することもできます。ファイアウォールの配置場所は、ネットワーク構成から特定したセキュリティ リスクに基づいて選択します。次のリストに、ESXi の実装に共通するファイアウォールの配置場所を示します。

- vSphere Web Client またはサードパーティ製ネットワーク管理クライアントと vCenter Server の間。
- ユーザーが Web ブラウザを介して仮想マシンにアクセスする場合は、Web ブラウザと ESXi ホストの間。
- vSphere Web Client を介して仮想マシンにアクセスする場合は、vSphere Web Client と ESXi ホストの間。この接続は、vSphere Web Client と vCenter Server の間の追加接続で、別のポートが必要です。
- vCenter Server と ESXi ホストの間。
- ネットワーク内の ESXi ホスト間。通常、ホスト間のトラフィックは信頼できると考えられますが、マシン間でのセキュリティ違反を考慮する場合は、ホスト間にファイアウォールを追加することもできます。

ESXi ホスト間にファイアウォールを追加してサーバ間で仮想マシンを移行したり、クローン作成を実行したり、vMotion を使用したりする場合、ソース ホストとターゲット ホストが通信できるように、ソースとターゲット を分ける任意のファイアウォールのポートを開く必要があります。

- ESXi ホストと、NFS や iSCSI ストレージなどネットワーク ストレージとの間。これらのポートは、VMware に固有のものではありません。ネットワークの仕様に従って構成してください。

## ファイアウォールを介した vCenter Server への接続

vCenter Server は、TCP ポート 443 を使用してクライアントからのデータ転送を待機します。vCenter Server とそのクライアント間にファイアウォールがある場合、vCenter Server がクライアントからデータを受信できる接続を構成する必要があります。

vCenter Server が vSphere Web Client からデータを受信できるようにするには、ファイアウォールで TCP ポート 443 を開きます。ファイアウォールの構成は、サイトで何が使用されているかによって異なります。詳細については、ローカルのファイアウォールのシステム管理者に問い合わせてください。

vSphere Web Client から vCenter Server の通信用のポートとして、ポート 443 を使用しない場合は、vSphere Web Client から vCenter Server の設定を変更して別のポートに切り替えることができます。『vCenter Server およびホスト管理』ドキュメントを参照してください。

まだ vSphere Client を使用している場合は、『vSphere Client による vSphere の管理』ドキュメントを参照してください。

## vCenter Server を使用しない構成でのファイアウォール

vCenter Server を使用せずに、クライアントを ESXi ネットワークに直接接続できます。

vCenter Server を使用せずに構成したネットワークは、vSphere Client、いずれかの vSphere コマンドライン インターフェイス、vSphere Web Services SDK、またはサードパーティ クライアントを介して通信を受信します。ほとんどの箇所では、ファイアウォールの必要性は vCenter Server が存在する場合と同じですが、重要な相違点がいくつかあります。

- vCenter Server が含まれている構成と同様に、ESXi レイヤー、または構成によっては、クライアントと ESXi レイヤーを保護するようにファイアウォールを設定する必要があります。このファイアウォールは、ネットワークに基本的な保護を提供します。
- このような構成でのライセンスは、各ホストにインストールする ESXi パッケージの一部です。ライセンスはサーバに常駐するので、個別のライセンス サーバは必要はありません。このため、ライセンス サーバと ESXi ネットワーク間にファイアウォールは必要ありません。

ファイアウォールのポートは、ESXCLI を使用するか、vSphere Client を使用するか、またはファイアウォール ルールを使用して構成できます。[ESXi ファイアウォールの構成](#) を参照してください。

## ファイアウォールを介した ESXi ホストの接続

2 つの ESXi ホスト間にファイアウォールがある場合に、ホスト間でトランザクションを許可したり、vCenter Server を使用して、vSphere HA (High Availability) トラフィック、移行、クローン作成、vMotion などのソース アクティビティまたはターゲット アクティビティを実行したりするには、管理対象のホストがデータを受信できる接続を構成する必要があります。

データ受信のための接続を構成するには、vSphere High Availability、vMotion、vSphere Fault Tolerance などのサービスからのトラフィック用のポートを開きます。構成ファイル、vSphere Web Client のアクセス、およびファイアウォール コマンドについては、[ESXi ファイアウォールの構成](#) を参照してください。ポートの一覧については、[ESXi ホストの送受信ファイアウォール ポート](#) を参照してください。ポート構成の詳細については、ファイアウォール システム管理者にお問い合わせください。

## ファイアウォールを介した仮想マシン コンソールへの接続

ユーザーおよび管理者が仮想マシン コンソールと通信するには、特定のポートを開く必要があります。どのポートを開くかは、仮想マシン コンソールのタイプ、および vSphere Web Client を使用して vCenter Server を介して接続するか vSphere Client から直接 ESXi ホストに接続するかによって異なります。

### vSphere Web Client を介してブラウザベースの仮想マシン コンソールに接続

vSphere Web Client を使用して接続すると、ESXi ホストを管理する vCenter Server システムに必ず接続し、そこから仮想マシン コンソールにアクセスします。

vSphere Web Client を使用していて、ブラウザベースの仮想マシン コンソールに接続する場合、次のアクセスが可能である必要があります。

- ファイアウォールは、ポート 9443 での vSphere Web Client の vCenter Server へのアクセスを許可する必要があります。
- ファイアウォールは、ポート 902 での vCenter Server の ESXi ホストへのアクセスを許可する必要があります。

## vSphere Web Client を介してスタンドアロンの仮想マシン コンソールに接続

vSphere Web Client を使用して、スタンドアロンの仮想マシン コンソールに接続する場合、次のアクセスが可能である必要があります。

- ファイアウォールは、ポート 9443 での vSphere Web Client の vCenter Server へのアクセスを許可する必要があります。
- ファイアウォールは、スタンドアロン仮想マシン コンソールのポート 9443 での vCenter Server へのアクセス、およびポート 902 での ESXi ホストへのアクセスを許可する必要があります。

## ESXi ホストへの vSphere Client を使用した直接接続

ESXi ホストに直接接続する場合は、vSphere Client 仮想マシン コンソールを使用できます。

**注：** vSphere Client を使用して vCenter Server システムによって管理されているホストに直接接続しないでください。このようなホストに vSphere Client から変更を行うと、使用中の環境が不安定になります。

ファイアウォールは、ポート 443 および 902 での ESXi ホストへのアクセスを許可する必要があります。

vSphere Client は、ポート 902 を使用して仮想マシンのゲスト OS の MKS（マウス、キーボード、スクリーン）アクティビティの接続を提供します。ユーザーが仮想マシンのゲスト OS およびアプリケーションと通信するときは、このポートを使用します。この機能に異なるポートを構成することはできません。

## 物理スイッチのセキュリティ強化

各 ESXi ホストで物理スイッチをセキュリティ強化して、ホストおよびその仮想マシンに攻撃者がアクセスできないようにします。

ホストを確実に保護するには、スパニング ツリーを無効にして物理スイッチ ポートを構成し、外部物理スイッチと仮想スイッチ タギング（VST）モードの仮想スイッチ間のトランク リンクに非ネゴシエーション オプションを構成します。

### 手順

- 1 物理スイッチにログインし、スパニング ツリー プロトコルが無効になっているか、ESXi ホストに接続されているすべての物理スイッチ ポートにポート ファストが構成されていることを確認します。
- 2 ブリッジまたはルーティングを実行する仮想マシンの場合は、BPDU ガードと Port Fast を無効にし、スパニング ツリー プロトコルを有効にして、最初のアップストリーム物理スイッチ ポートが構成されていることを定期的に確認します。

Sphere 5.1 以降では、潜在的なサービス拒否（DoS）攻撃から物理スイッチを保護するため、ESXi ホストでゲスト BPDU フィルタをオンにすることができます。

- 3 物理スイッチにログインし、ESXi ホストに接続されている物理スイッチ ポートで動的トランク プロトコル（DTP）が有効になっていないことを確認します。
- 4 物理スイッチ ポートを定期的に調べ、仮想スイッチの VLAN トランク ポートに接続されている場合は、トランク ポートとして正しく構成されていることを確認します。

## セキュリティ ポリシーによる標準スイッチ ポートのセキュリティ強化

物理ネットワーク アダプタと同様に、仮想マシン ネットワーク アダプタは、異なるマシンから発信されたように見えるフレームを送信したり、別のマシンになりすまし、そのマシンに送信されるように意図されたネットワーク フレームを受信したりできます。また、物理ネットワーク アダプタと同様に、仮想マシン ネットワーク アダプタは、他のマシンが送信先に設定されているフレームを受信するように構成できます。このような設定は、両方ともセキュリティ リスクを生じます。

ネットワークの標準スイッチを作成する場合、vSphere Web Client にポート グループを追加して、スイッチに接続されるシステム トラフィック用の仮想マシンと VMkernel アダプタにポリシーを強制します。

VMkernel ポート グループまたは仮想マシン ポート グループを標準スイッチに追加する作業の一環として、ESXi はグループ内のポート用にセキュリティ ポリシーを構成します。このセキュリティ ポリシーを使用すると、ホストの仮想マシンのゲスト OS がネットワーク上の他のマシンになりすますことを、ホストで確実に防止できます。このセキュリティ機能は、なりすましを行うゲスト OS が、なりすましが阻止されたことを検知できないように、実装されます。

セキュリティ ポリシーによって、仮想マシンでのなりすましや傍受攻撃に対する保護をどの程度強化するかが決定されます。セキュリティ プロファイルの設定を正しく使用するには、仮想マシン ネットワーク アダプタが転送をどのように制御するか、および攻撃がこのレベルでどのように開始されるかについて理解する必要があります。資料『vSphere ネットワーク』のセキュリティ ポリシーに関するセクションを参照してください。

.

## vSphere 標準スイッチのセキュリティ強化

標準スイッチのトラフィックは、スイッチのセキュリティ設定を使用して、MAC アドレス モードの一部を制限することによって、レイヤー 2 攻撃から保護することができます。

各仮想マシン ネットワーク アダプタには、初期 MAC アドレスと有効な MAC アドレスがあります。

### 初期 MAC アドレス

初期 MAC アドレスは、アダプタの作成時に割り当てられます。初期 MAC アドレスは、ゲスト OS の外部から再構成できますが、ゲスト OS により変更することはできません。

### 有効な MAC アドレス

各アダプタには有効な MAC アドレスがあります。これは、送信先 MAC アドレスが有効な MAC アドレスとは異なる着信ネットワーク トラフィックをフィルタリングするために使用します。ゲスト OS は、有効な MAC アドレスの設定に関与し、通常、有効な MAC アドレスを初期 MAC アドレスに一致させます。

仮想マシン ネットワーク アダプタの作成時、有効な MAC アドレスおよび初期 MAC アドレスは同じです。ゲスト OS は、有効な MAC アドレスの値をいつでも変更できます。オペレーティング システムが有効な MAC アドレスを変更すると、そのネットワーク アダプタは、新規 MAC アドレスに送信されるネットワーク トラフィックを受信します。

ネットワーク アダプタを通してパケットを送信する場合、ゲスト OS は通常、それ自身のアダプタの有効な MAC アドレスをイーサネット フレームの送信元 MAC アドレス フィールドに置きます。受信側ネットワーク アダプタの MAC アドレスは、送信先 MAC アドレス フィールドに置きます。受信側アダプタは、パケットの送信先 MAC アドレスがそれ自身の有効な MAC アドレスに一致する場合だけパケットを受け付けます。

オペレーティング システムは、なりすまししている送信元 MAC アドレスを持つフレームを送信できます。つまり、オペレーティング システムは、受信側ネットワークにより許可されているネットワーク アダプタになります。ことで、ネットワークのデバイスに対して、悪意のある攻撃を実行する可能性があります。

ポート グループまたはポートでセキュリティ ポリシーを構成して、なりすましやレイヤー 2 傍受攻撃に対して仮想トラフィックを保護します。

分散ポート グループおよびポートのセキュリティ ポリシーには、次のオプションがあります。

- プロミスカス モード ([無差別モード操作](#) を参照)
- MAC アドレス変更 ([MAC アドレス変更](#) を参照)
- 偽装転送 ([偽装転送](#) を参照)

デフォルトの設定は、ホストに関連付けられている仮想スイッチを vSphere Web Client から選択することにより、表示および変更することができます。『vSphere ネットワーク』ドキュメントを参照してください。

## MAC アドレス変更

仮想スイッチのセキュリティ ポリシーには [MAC アドレス変更] オプションが含まれています。このオプションは、仮想マシンが受け取るトラフィックに影響を及ぼします。

[Mac アドレスの変更] オプションが [承諾] に設定されている場合、ESXi は有効な MAC アドレスを初期 MAC アドレスとは異なるアドレスに変更する要求を受け入れます。

[Mac アドレスの変更] オプションが [拒否] に設定されている場合、ESXi は有効な MAC アドレスを、初期 MAC アドレスとは異なるアドレスに変更する要求を拒否します。この設定により、MAC のなりすましに対してホストが保護されます。仮想マシン アダプタが要求の送信に使用したポートは無効になります。仮想マシン アダプタは、有効な MAC アドレスが初期 MAC アドレスと一致しない限り、それ以上のフレームを受け取りません。ゲスト OS は、MAC アドレスの変更要求が拒否されたことを検知しません。

---

**注：** iSCSI イニシエータは、特定のタイプのストレージから MAC アドレスを変更できることに依存しています。ESXi iSCSI を iSCSI ストレージとともに使用している場合、[MAC アドレス変更] オプションを [承諾] に設定します。

---

場合によっては、複数のアダプタがネットワーク上で同じ MAC アドレスを使用することが適切な場合もあります。たとえば、Microsoft Network Load Balancing をユニキャスト モードで使用している場合です。Microsoft Network Load Balancing が標準マルチキャスト モードで利用される場合、アダプタは MAC アドレスを共有しません。

## 偽装転送

[偽装転送] オプションは、仮想マシンから転送されるトラフィックに影響を及ぼします。

[偽造転送] オプションが [承諾] に設定されている場合、ESXi はソースと有効な MAC アドレスを比較しません。



[偽装転送] オプションを [拒否] に設定して、MAC のなりすましに対して保護できます。このように設定すると、ホストはゲスト OS から転送されるソース MAC アドレスと、その仮想マシン アダプタの有効な MAC アドレスを比較して、それらが一致するかどうかを確認します。アドレスが一致しない場合、ESXi ホストはパケットをドロップします。

ゲスト OS は、仮想マシン アダプタが、なりすましている MAC アドレスを使用したパケットの送信を実行できないことは検知しません。ESXi ホストは、なりすましているアドレスのパケットが配信される前に、そのパケットを遮断します。ゲスト OS は、そのパケットがドロップされたとみなす可能性があります。

## 無差別モード操作

無差別モードでは、仮想マシン アダプタが実行するすべての受信フィルタリングが除去されるため、ゲスト OS は回線で監視されるすべてのトラフィックを受信します。デフォルトでは、仮想マシン アダプタは無差別モードで操作できません。

無差別モードは、ネットワーク アクティビティのトラッキングに便利ですが、無差別モードのアダプタは、いくつかのパケットが特定のネットワーク アダプタのみに受信される場合でもパケットにアクセスできるため、この操作は安全ではありません。つまり、仮想マシン内のシステム管理者または root ユーザーは、ほかのゲスト OS またはホスト OS に送信されるトラフィックを参照できます。

---

**注：** 場合によっては、標準または分散仮想スイッチを無差別モードで実行するように構成することが適切なこともあります。たとえば、ネットワーク侵入検知ソフトウェアやパケット スニファアを実行している場合などです。

---

## vSphere 分散スイッチおよび分散ポート グループのセキュリティ強化

システム管理者は、vSphere 環境でいくつかの方法で vSphere Distributed Switch をセキュリティ強化することができます。

### 手順

- 1 静的バインドを使用した分散ポート グループの場合、自動展開機能が無効になっていることを確認します。

vSphere 5.1 以降では、自動展開はデフォルトで有効になっています。

自動展開を無効にするには、vSphere Web Services SDK またはコマンドライン インターフェイスを使用して、分散ポート グループで `autoExpand` プロパティを構成します。vSphere Web Services SDK のドキュメントを参照してください。

- 2 vSphere Distributed Switch のすべてのプライベート VLAN ID が完全に文書化されていることを確認します。
- 3 dvPortgroup で VLAN タギングを使用する場合、VLAN ID は外部 VLAN 対応アップストリーム スイッチの ID に対応している必要があります。VLAN ID が完全に追跡されていない場合、ID が誤って再利用され、不適切な物理マシンと仮想マシン間のトラフィックが妨げられることがあります。同様に、VLAN ID が誤っていたり欠落していたりすると、物理マシンと仮想マシンの間をトラフィックが行き来しないことがあります。
- 4 vSphere Distributed Switch に関連付けられている仮想ポート グループに未使用のポートが存在しないことを確認します。



## 5 すべての vSphere Distributed Switch にラベルを付けます。

ESXi ホストに関連付けられている vSphere Distributed Switch には、スイッチ名のフィールドが必要です。このラベルは、物理スイッチに関連付けられているホスト名と同じように、スイッチの機能記述子の役割を果たします。vSphere Distributed Switch のラベルは、スイッチの機能または IP サブネットを示します。たとえば、スイッチに内部用のラベルを付けて、スイッチが仮想マシンのプライベート仮想スイッチ（物理ネットワークアダプタがバインドされていないスイッチ）間の内部ネットワーク専用であることを示すことができます。

## 6 vSphere Distributed Switch のネットワーク健全性チェックがアクティブに使用されていない場合、これを無効にします。

ネットワーク健全性チェックは、デフォルトで無効になっています。有効にすると、攻撃者に使用される可能性のあるホスト、スイッチ、およびポートに関する情報が健全性チェック パケットに含まれるようになります。ネットワーク健全性チェックはトラブルシューティングにのみ使用し、トラブルシューティングが終了したらオフにします。

## 7 ポート グループまたはポートでセキュリティ ポリシーを構成して、なりすましやレイヤー 2 傍受攻撃に対して仮想トラフィックを保護します。

分散ポート グループおよびポートのセキュリティ ポリシーには、次のオプションがあります。

- プロミスカス モード（[無差別モード操作](#) を参照）
- MAC アドレス変更（[MAC アドレス変更](#) を参照）
- 偽装転送（[偽装転送](#) を参照）

Distributed Switch の右ボタン メニューから [分散ポート グループの管理] を選択し、ウィザードで [セキュリティ] を選択すると、現在の設定を表示および変更できます。『vSphere ネットワーク』ドキュメントを参照してください。

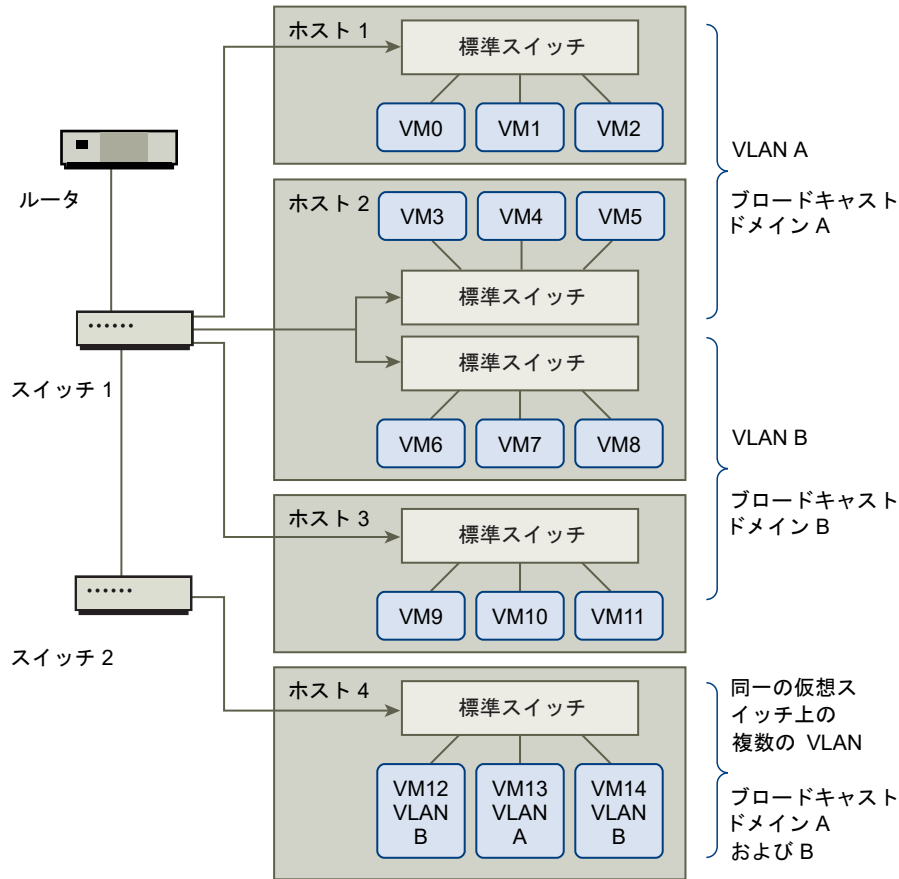
# VLAN を使用した仮想マシンのセキュリティ強化

ネットワークは、システムで最も脆弱性の大きい部分になる可能性があります。仮想マシン ネットワークには、物理ネットワークと同じ程度の保護が必要です。VLAN を使用すると、環境のネットワーク セキュリティを高めることができます。

VLAN は、VLAN の一部のポートだけにパケット ルーティングを許可する特定のタグ付け方法を使用した IEEE 標準ネットワーク スキームです。VLAN は、正しく構成されている場合、偶発的または悪意のある侵入から仮想マシンを保護できる、信頼性の高い方法です。

VLAN では、ネットワークの 2 台のマシンが同じ VLAN にないかぎり、パケットを送受信できないように、物理ネットワークをセグメント化できます。たとえば、会計記録や報告書は、企業が機密事項として扱う最も重要な内部情報です。販売部、出荷部、会計部の各従業員がすべて、同じ物理ネットワークの仮想マシンを使用している企業では、VLAN を設定して、会計部の仮想マシンを保護できます。

図 8-1. サンプル VLAN レイアウト



この構成では、会計部のすべての従業員は VLAN A の仮想マシンを使用し、販売部の従業員は VLAN B の仮想マシンを使用します。

ルータは、会計データを含むパケットをスイッチに転送します。これらのパケットは、VLAN A のみに配布されるようにタグが付けられます。したがって、このデータはブロードキャスト ドメイン A に制限され、ルータで構成されていないかぎり、ブロードキャスト ドメイン B に経路選択されません。

この VLAN 構成では、会計部あてに送信されるパケットを販売部が取得できないようにします。また、販売グループに送信されるパケットを会計部が受信しないようにもします。単一の仮想スイッチでサービスが提供される仮想マシンは、別の VLAN に置くことができます。

## VLAN のセキュリティの考慮事項

ネットワークの一部のセキュリティに VLAN を設定する方法は、ゲスト OS やネットワーク設備の構成方法などの要素により異なります。

ESXi は、IEEE 802.1q に完全に準拠した VLAN 実装を提供します。VLAN の設定方法について、特定の方法をお勧めすることはできませんが、セキュリティ実施ポリシーの一部として VLAN 導入を使用する場合に考慮すべき要素はあります。

## VLAN のセキュリティ強化

管理者には、vSphere 環境で VLAN を保護するオプションがいくつかあります。

### 手順

- 1 ポート グループが、アップストリームの物理スイッチによって予約されている VLAN の値に構成されていないことを確認します。

VLAN ID を物理スイッチのために予約された値に設定しないでください。

- 2 仮想ゲスト タギング (VGT) に使用する場合を除き、ポート グループが VLAN 4095 に構成されていないことを確認します。

vSphere には次の 3 種類の VLAN タギングがあります。

- 外部スイッチ タギング (EST)
- 仮想スイッチ タギング (VST) - 仮想スイッチが、接続した仮想マシンの受信トラフィックを構成された VLAN ID でタグ付けし、送信トラフィックからは VLAN タグを削除します。VST モードを設定するには、1 から 4095 までの VLAN ID を割り当てます。
- 仮想ゲスト タギング (VGT) - 仮想マシンが VLAN トラフィックを処理します。VGT モードを有効にするには、VLAN ID を 4095 に設定します。Distributed Switch 上で、[VLAN トランク] オプションを使用して VLAN に基づいた仮想マシン トラフィックを許可することもできます。

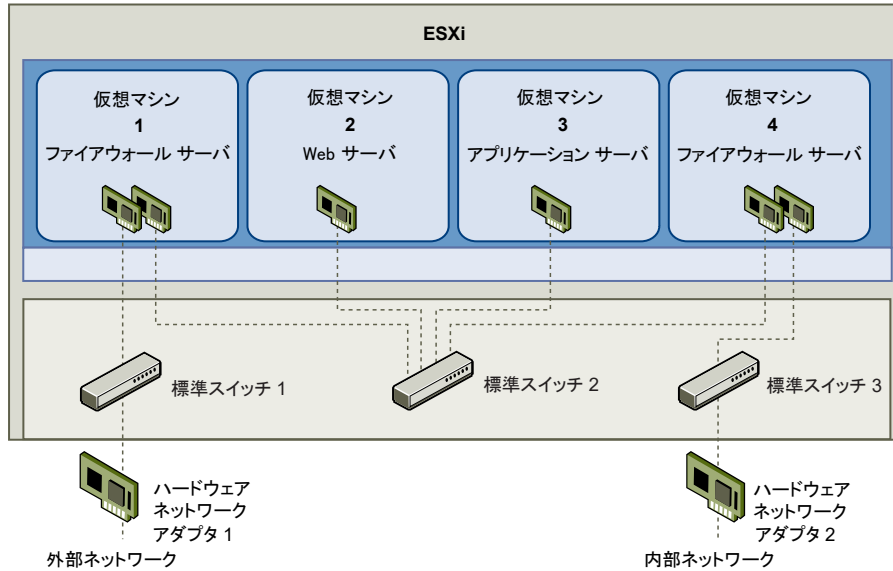
標準スイッチでは、VLAN ネットワーク モードをスイッチ レベルまたはポート グループ レベルで構成できます。Distributed Switch では、VLAN ネットワーク モードを分散ポート グループ レベルまたはポート レベルで構成できます。

- 3 各仮想スイッチのすべての VLAN が完全にドキュメント化されていること、各仮想スイッチに必要なすべての VLAN があり、かつ必要な VLAN のみがあることを確認してください。

## 単一の ESXi ホストでのネットワーク DMZ の作成

ESXi の隔離機能および仮想ネットワークの機能を使用して安全な環境を構成する 1 つの方法として、単一ホスト上にネットワーク非武装地帯 (DMZ) を作成するという例があります。

図 8-2. 単一の ESXi ホストに構成された DMZ



この例では、標準スイッチ 2 に仮想 DMZ を作成するよう、4 台の仮想マシンが構成されています。

- 仮想マシン 1 および仮想マシン 4 は、ファイアウォールを実行し、標準スイッチを介して物理ネットワーク アダプタに接続されています。これら両方の仮想マシンは、複数のスイッチを使用しています。
- 仮想マシン 2 は Web サーバを実行し、仮想マシン 3 はアプリケーション サーバとして動作しています。これら両方の仮想マシンは、1 つの仮想スイッチに接続されています。

Web サーバおよびアプリケーション サーバは、2 つのファイアウォール間の DMZ に置かれています。これらの要素間のルートは、ファイアウォールとサーバを接続する標準スイッチ 2 です。このスイッチは、DMZ 外の要素とは直接接続されていないので、2 つのファイアウォールによって外部トラフィックから隔離されています。

操作の観点から、インターネットからの外部トラフィックは、ハードウェア ネットワーク アダプタ 1 (標準スイッチ 1 を経由) を介して仮想マシン 1 に入り、このマシン上にインストールされているファイアウォールによって検査されます。ファイアウォールがトラフィックを許可すると、DMZ 内の標準スイッチ (標準スイッチ 2) を経由します。Web サーバおよびアプリケーション サーバもこのスイッチに接続されているため、外部要求に対応できます。

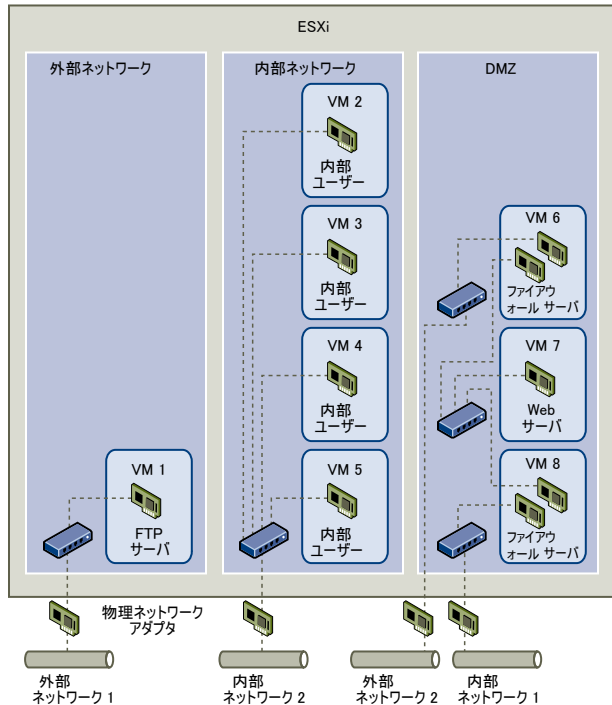
標準スイッチ 2 も仮想マシン 4 に接続されています。この仮想マシンは、DMZ と企業の内部ネットワーク間にファイアウォールを提供します。このファイアウォールは、Web サーバおよびアプリケーション サーバからのパケットをフィルタリングします。パケットが検証されると、標準スイッチ 3 を介してハードウェア ネットワーク アダプタ 2 に送信されます。ハードウェア ネットワーク アダプタ 2 は、企業の内部ネットワークに接続されています。

単一のホストに DMZ を作成する場合には、非常に軽量のファイアウォールを使用できます。この構成の仮想マシンは、別の仮想マシンを直接制御したり、そのメモリにアクセスしたりできませんが、すべての仮想マシンが仮想ネットワークを介して接続されています。このネットワークはウイルスの伝播に使用されたり、ほかの脅威のターゲットにされる可能性があります。DMZ の仮想マシンのセキュリティは、同じネットワークに接続された個別の物理マシンと同程度です。

## 単一の ESXi ホスト内での複数のネットワークの作成

ESXi システムでは、同一のホスト上で、ある仮想マシン グループを内部ネットワークに接続する一方で別のグループを外部ネットワークに接続し、さらにその他のグループを両方に接続する、といったことができるよう設計されています。これは、仮想マシンの隔離という基本に、仮想ネットワークの計画と使用を加えた機能です。

図 8-3. 単一の ESXi ホストに構成された外部ネットワーク、内部ネットワーク、および DMZ



図では、システム管理者が FTP サーバ、内部仮想マシン、DMZ という 3 つの異なる仮想マシンのゾーンにホストを構成しています。各ゾーンのサーバには固有の機能があります。

### FTP サーバ

仮想マシン 1 は、FTP ソフトウェアで構成され、ベンダーによりローカライズされたフォームやコラテラルなど、外部リソースとの間で送受信されるデータの保存エリアとして機能します。

この仮想マシンは、外部ネットワークのみと関連付けられています。このマシンには、外部ネットワーク 1 に接続する、独自の仮想スイッチおよび物理ネットワーク アダプタがあります。このネットワークは、企業が外部リソースからデータを受信するときに使用するサーバ専用のネットワークです。たとえば、企業が外部ネットワーク 1 を使用してベンダーから FTP トラフィックを受信し、FTP を介して外部で使用可能なサーバに保存されているデータに、ベンダーがアクセスできるようにします。仮想マシン 1 にサービスを提供するほか、外部ネットワーク 1 は、サイト中の異なる ESXi ホストで構成されている FTP サーバにサービスを提供します。

仮想マシン 1 は、仮想スイッチまたは物理ネットワーク アダプタをホスト内のどの仮想マシンとも共有しないので、ほかの常駐の仮想マシンは、仮想マシン 1 のネットワークに対してパケットを送受信できません。この制限により、被害者への送信ネットワーク トラフィックが必要なスニフィング攻撃を防ぎます。さらに重要なことに、攻撃者は、ホストのほかの仮想マシンにアクセスするために FTP の持つ脆弱性を使用できなくなります。

### 内部仮想マシン

仮想マシン 2 ～ 5 は、内部での使用のために予約されています。これらの仮想マシンは、医療記録、訴訟和解金、詐欺行為調査などの企業のプライベート データを処理および保存します。そのため、システム管理者は、これらの仮想マシンの保護レベルを最高にする必要があります。

これらの仮想マシンは、独自の仮想スイッチおよびネットワーク アダプタを介して内部ネットワーク 2 に接続します。内部ネットワーク 2 は、クレーム処理、企業内弁護士、調停人など、人事課による内部使用のために予約されています。

仮想マシン 2 ～ 5 は、仮想スイッチを介して相互に通信したり、物理ネットワーク アダプタを介して内部ネットワーク 2 の任意の内部仮想マシンと通信したりできます。これらの仮想マシンは、外部と接しているマシンとは通信できません。FTP サーバの場合と同様、これらの仮想マシンは、ほかの仮想マシンのネットワークとの間でパケットを送受信できません。同様に、ホストのほかの仮想マシンは、仮想マシン 2 ～ 5 との間でパケットを送受信できません。

## DMZ

仮想マシン 6 ～ 8 は、マーケティング グループが企業の外部 Web サイトを公開するときに使用する DMZ として構成されています。

この仮想マシンのグループは、外部ネットワーク 2 および内部ネットワーク 1 に関連付けられています。企業は外部ネットワーク 2 を使用して、マーケティングおよび財務部が企業 Web サイトや外部ユーザーに提供するその他の Web 機能をホスティングするために使用する Web サーバをサポートします。内部ネットワーク 1 は、マーケティング部が、企業 Web サイトにコンテンツを公開したり、ダウンロードを掲載したり、ユーザーフォーラムなどのサービスを保守したりするときに使用するルートです。

これらのネットワークは外部ネットワーク 1 および内部ネットワーク 2 から分離されていて、仮想マシンが接続点（スイッチやアダプタ）を共有していないため、FTP サーバまたは内部の仮想マシン グループとの間での攻撃リスクがありません。

仮想マシンの隔離を利用して、仮想スイッチを正しく構成し、ネットワーク分離を保持すると、システム管理者は同じ ESXi ホスト内に仮想マシンのゾーン 3 つをすべて収容でき、データやリソースの漏出をなくすことができます。

企業は、複数の内部および外部ネットワークを使用し、各グループの仮想スイッチや物理ネットワーク アダプタをほかのグループのものと完全に隔離することで、仮想マシン グループの分離を強化できます。

仮想スイッチが仮想マシンのゾーンにまたがることはないため、システム管理者は、ゾーン間でのパケット漏洩のリスクを削減できます。仮想スイッチは、設計上、別の仮想スイッチにパケットを直接漏洩することはできません。パケットが仮想スイッチ間で送受信されるのは、次の場合だけです。

- 仮想スイッチが、同じ物理 LAN に接続されている。
- 仮想スイッチが、パケットの送受信に使用できる共通の仮想マシンに接続されている。

サンプル構成では、このいずれの条件も発生しません。システム管理者が共通の仮想スイッチ パスが存在しないことを検証する場合は、vSphere Web Client のネットワーク スイッチ レイアウトを確認すると、可能性のある共有接続点を確認できます。

仮想マシンのリソースを保護するため、システム管理者は、仮想マシンごとにリソース予約および制限を構成し、DoS および DDoS 攻撃のリスクを低減します。システム管理者は、DMZ の前後にソフトウェア ファイアウォールをインストールし、ESXi ホストが物理ファイアウォールの内側に配置されるようにし、ネットワーク ストレージ リソースを構成してそれぞれが独自の仮想スイッチ持つようにすることで、このホストおよび仮想マシンの保護を強化します。

## インターネット プロトコル セキュリティ

IPsec（インターネット プロトコル セキュリティ）は、ホストで送受信される IP 通信を保護します。ESXi ホストでは、IPv6 を使用した IPsec がサポートされています。

ホストで IPsec を設定すると、送受信されるパケットの認証と暗号化が可能になります。IP トラフィックがいつ、どのように暗号化されるかは、システムのセキュリティ アソシエーションとセキュリティ ポリシーを設定する方法によって異なります。

セキュリティ アソシエーションは、システムでのトラフィックの暗号化方法を決定します。セキュリティ アソシエーションを作成するときは、ソースとターゲット、暗号化パラメータ、およびセキュリティ アソシエーションの名前を指定します。

セキュリティ ポリシーは、システムでトラフィックを暗号化するタイミングを決定します。セキュリティ ポリシーには、ソースとターゲットの情報、プロトコルと暗号化するトラフィックの方向、モード（トランスポートまたはトンネル）、および使用するセキュリティ アソシエーションが含まれます。

### 使用可能なセキュリティ アソシエーションの一覧表示

ESXi では、セキュリティ ポリシーで使用できるすべてのセキュリティ アソシエーションを一覧表示できます。この一覧には、ユーザーが作成したセキュリティ アソシエーションと、IKE（Internet Key Exchange）を使用して VMkernel がインストールしたセキュリティ アソシエーションの両方が含まれます。

使用可能なセキュリティ アソシエーションの一覧は、vSphere CLI コマンドの `esxcli` を使用して表示できます。

#### 手順

- ◆ コマンド プロンプトから、**`esxcli network ip ipsec sa list`** コマンドを入力します。

#### 結果

ESXi は、使用可能なすべてのセキュリティ アソシエーションを一覧表示します。

### IPsec セキュリティ アソシエーションの追加

セキュリティ アソシエーションを追加して、関連する IP トラフィックの暗号化パラメータを指定します。

セキュリティ アソシエーションは、vSphere CLI コマンドの `esxcli` を使用して追加できます。

#### 手順

- ◆ コマンド プロンプトで、**`esxcli network ip ipsec sa add`** コマンドを入力します。その際、次のオプションを 1 つ以上指定します。

オプション	説明
<code>--sa-source= <i>source address</i></code>	必須。ソース アドレスを指定します。
<code>--sa-destination= <i>destination address</i></code>	必須。ターゲット アドレスを指定します。
<code>--sa-mode= <i>mode</i></code>	必須。transport か tunnel、どちらかのモードを指定します。

オプション	説明
<b>--sa-spi= <i>security parameter index</i></b>	必須。セキュリティ パラメータ インデックスを指定します。セキュリティ パラメータ インデックスは、ホストへのセキュリティ アソシエーションを識別します。0x のプリフィックスを付けた 16 進数である必要があります。作成するセキュリティ アソシエーションは、それぞれプロトコルとセキュリティ パラメータ インデックスの組み合わせが一意である必要があります。
<b>--encryption-algorithm= <i>encryption algorithm</i></b>	必須。次のパラメータの 1 つを使用して、暗号化アルゴリズムを指定します。 <ul style="list-style-type: none"> <li>■ 3des-cbc</li> <li>■ aes128-cbc</li> <li>■ null (暗号化なし)</li> </ul>
<b>--encryption-key= <i>encryption key</i></b>	暗号化アルゴリズムの指定時に必須。暗号化キーを指定します。キーは、ASCII テキストとして、または 0x のプリフィックスを付けた 16 進数として入力できます。
<b>--integrity-algorithm= <i>authentication algorithm</i></b>	必須。認証アルゴリズムとして、hmac-sha1 か hmac-sha2-256 のどちらかを指定します。
<b>--integrity-key= <i>authentication key</i></b>	必須。認証キーを指定します。キーは、ASCII テキストとして、または 0x のプリフィックスを付けた 16 進数として入力できます。
<b>--sa-name= <i>name</i></b>	必須。セキュリティ アソシエーションの名前を入力します。

## 例：新規セキュリティ アソシエーション コマンド

次の例は、わかりやすいように余分な改行が挿入されています。

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

## IPsec セキュリティ アソシエーションの削除

ESXCLI vSphere CLI コマンドを使用して、セキュリティ アソシエーションを削除できます。

### 前提条件

削除するセキュリティ アソシエーションが使用中でないことを確認します。使用中のセキュリティ アソシエーションを削除しようとすると、削除に失敗します。

### 手順

- ◆ コマンド プロンプトで、  
**esxcli network ip ipsec sa remove --sa-name *security\_association\_name*** コマンドを入力します。



## 使用可能な IPsec セキュリティ ポリシーの一覧表示

ESXCLI vSphere CLI コマンドを使用して、使用可能なセキュリティ ポリシーを一覧表示できます。

### 手順

- ◆ コマンド プロンプトで、コマンド **esxcli network ip ipsec sp list** を入力します

### 結果

ホストは、使用可能なすべてのセキュリティ ポリシーを一覧表示します。

## IPsec セキュリティ ポリシーの作成

セキュリティ ポリシーを作成して、セキュリティ アソシエーションで設定されている認証と暗号化のパラメータを使用するタイミングを指定します。ESXCLI vSphere CLI コマンドを使用して、セキュリティ ポリシーを追加できます。

### 前提条件

セキュリティ ポリシーを作成する前に、[IPsec セキュリティ アソシエーションの追加](#) の説明に従って、適切な認証と暗号化のパラメータを指定してセキュリティ アソシエーションを追加します。

### 手順

- ◆ コマンド プロンプトで、**esxcli network ip ipsec sp add** コマンドを入力します。その際、次のオプションを 1 つ以上指定します。

オプション	説明
<b>--sp-source= <i>source address</i></b>	必須。ソース IP アドレスとブリフィックスの長さを指定します。
<b>--sp-destination= <i>destination address</i></b>	必須。ターゲット IP アドレスとブリフィックスの長さを指定します。
<b>--source-port= <i>port</i></b>	必須。ソース ポートを指定します。ソース ポートは、0 ～ 65535 の数値にする必要があります。
<b>--destination-port= <i>port</i></b>	必須。ターゲット ポートを指定します。ソース ポートは、0 ～ 65535 の数値にする必要があります。
<b>--upper-layer-protocol= <i>protocol</i></b>	次のパラメータのいずれかを使用して、上位レイヤー プロトコルを指定します。 <ul style="list-style-type: none"> <li>■ tcp</li> <li>■ udp</li> <li>■ icmp6</li> <li>■ any</li> </ul>
<b>--flow-direction= <i>direction</i></b>	in または out を使用して、トラフィックを監視する方向を指定します。
<b>--action= <i>action</i></b>	次のいずれかのパラメータを使用して、指定したパラメータを持つトラフィックが検出されたときの処理を指定します。 <ul style="list-style-type: none"> <li>■ none: 何も処理を行いません。</li> <li>■ discard: データの送受信を許可しません。</li> <li>■ ipsec: セキュリティ アソシエーションで指定されている認証と暗号化の情報を使用して、データが信頼できるソースから送信されたものかどうかを判別します。</li> </ul>

オプション	説明
<code>--sp-mode= <i>mode</i></code>	tunnel か transport の、どちらかのモードを指定します。
<code>--sa-name= <i>security association name</i></code>	必須。使用するセキュリティ ポリシーのセキュリティ アソシエーションの名前を入力します。
<code>--sp-name= <i>name</i></code>	必須。セキュリティ ポリシーの名前を入力します。

## 例：新規セキュリティ ポリシー コマンド

次の例は、わかりやすいように余分な改行が挿入されています。

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sal
--sp-name=sp1
```

## IPsec セキュリティ ポリシーの削除

ESXCLI vSphere CLI コマンドを使用して、ESXi ホストからセキュリティ ポリシーを削除できます。

### 前提条件

削除するセキュリティ ポリシーが使用中でないことを確認します。使用中のセキュリティ ポリシーを削除しようとすると、削除に失敗します。

### 手順

- ◆ コマンド プロンプトで、  
**esxcli network ip ipsec sp remove --sa-name *security policy name*** コマンドを入力します。

すべてのセキュリティ ポリシーを削除するには、

**esxcli network ip ipsec sp remove --remove-all** コマンドを入力します。

## SNMP 構成が適切であることの確認

SNMP が適切に構成されていないと、監視情報が不正なホストに送信される可能性があります。不正なホストは、この情報を攻撃を企てるために使用できます。

### 手順

- 1 **esxcli system snmp get** を実行して、SNMP が現在使用されているかどうかを判断します。

- 2 システムが SNMP を必要とする場合、`esxcli system snmp set --enable true` コマンドを実行して SNMP が実行されていることを確認します。
- 3 システムが SNMP を使用する場合、SNMP 3 のセットアップ情報について『監視およびパフォーマンス』ドキュメントを参照してください。

SNMP は、ESXi ホストごとに構成する必要があります。構成には vCLI、PowerCLI または vSphere Web Services SDK が使用できます。

## 必要なときにのみ vSphere Network Appliance API で仮想スイッチを使用

vSphere Network Appliance API (DvFilter) を使用する製品を使用していない場合は、ネットワーク情報を仮想マシンに送信するようにホストを構成しないでください。vSphere Network Appliance API が有効になっていると、攻撃者が仮想マシンをフィルタに接続しようとする可能性があります。この接続により、ホストの他の仮想マシンのネットワークにアクセスできるようになることがあります。

この API を使用する製品を使用している場合は、ホストが正しく構成されていることを確認します。『Sphere ソリューション、vService および ESX エージェントの配置および開発』の DvFilter のセクションを参照してください。API を使用するようにホストが設定されている場合は、`Net.DVFilterBindIpAddress` パラメータの値が API を使用する製品と一致することを確認します。

### 手順

- 1 `Net.DVFilterBindIpAddress` カーネル パラメータの値が正しいことを確認するには、vSphere Web Client を使用してパラメータを見つけます。
  - a ホストを選択し、[管理] タブをクリックします。
  - b [システム] の下で [システムの詳細設定] を選択します。
  - c `Net.DVFilterBindIpAddress` までスクロール ダウンし、パラメータの値が空であることを確認します。

パラメータは必ずしもアルファベット順ではありません。[フィルタ] フィールドに **DVFilter** と入力して、関連するパラメータすべてを表示します。
- 2 DvFilter 設定を使用していない場合は、値が空であることを確認します。
- 3 DvFilter 設定を使用している場合は、パラメータの値が DvFilter を使用する製品で使用している値と一致することを確認します。

## vSphere ネットワークのセキュリティのベスト プラクティス

ネットワーキング セキュリティのベスト プラクティスに従うことで、vSphere デプロイの整合性を確保できます。

## ネットワークのセキュリティに関する一般的推奨事項

一般的なネットワークのセキュリティ推奨事項に従うことは、ネットワーク環境のセキュリティを強化するための最初のステップです。その後、ファイアウォールや IPsec を使用したネットワークのセキュリティ強化などの特殊な領域に進むことができます。

- スパニング ツリーが有効化されている場合は、物理スイッチのポートが Portfast を使用して構成されるようにします。VMware の仮想スイッチは STP をサポートしていないため、ESXi ホストに接続されている物理スイッチ ポートでは、スパニング ツリーが有効化されている場合には Portfast が構成されており、物理スイッチ ネットワーク内でのループを回避するようになっている必要があります。Portfast が設定されていない場合には、潜在的なパフォーマンスと接続性の問題が発生する可能性があります。
- 分散仮想スイッチの Netflow トラフィックは、許可されたコレクタ IP アドレスに対してのみ送信されるようにします。Netflow エクスポートは暗号化されず、仮想ネットワークに関する情報を含めることができるため、連続的な中間者攻撃にさらされる危険性が増します。Netflow エクスポートが必要な場合は、すべての Netflow ターゲット IP アドレスが正しいことを確認してください。
- 必ず、ロールベースのアクセス制御を使用することにより、許可された管理者のみが仮想ネットワーク コンポーネントにアクセスできるようにします。たとえば、仮想マシン管理者は、管理する仮想マシンが存在するポートグループに対してのみアクセス権を持っている必要があります。ネットワーク管理者には、すべてのネットワーク コンポーネントに対するアクセス許可が必要ですが、仮想マシンへのアクセス権は不要です。アクセスを制限すると、偶発的であれ悪意のあるものであれ誤って構成するリスクが軽減され、責務の分離と最小限の権限という主要なセキュリティ概念が適用されます。
- ポート グループをネイティブ VLAN の値に構成しないようにします。物理スイッチは VLAN 1 をネイティブ VLAN として使用します。ネイティブ VLAN 上のフレームに 1 というタグは付いていません。ESXi にはネイティブ VLAN がありません。ポート グループで VLAN が指定されているフレームにはタグがありますが、ポート グループで VLAN が指定されていないフレームにタグは付いていません。この場合、1 というタグが付いている仮想マシンは結果的に物理スイッチのネイティブ VLAN に所属することになるので、問題が生じる可能性があります。

たとえば、Cisco 物理スイッチから届く VLAN 1 上のフレームには、VLAN 1 がこの物理スイッチ上のネイティブ VLAN であるため、タグが付けられていません。しかし、VLAN 1 として指定された ESXi ホストからのフレームには 1 というタグが付けられています。そのため、ネイティブ VLAN に向かう ESXi ホストからのトラフィックは、タグなしではなく 1 というタグが付いているので正しくルーティングされません。ネイティブ VLAN から届く物理スイッチからのトラフィックは、タグが付いていないので認識されません。ESXi 仮想スイッチのポート グループでネイティブ VLAN ID を使用している場合、このスイッチはタグなしのトラフィックを想定しているので、そのポート上の仮想マシンからのトラフィックはスイッチ上のネイティブ VLAN では認識されません。

- ポート グループをアップストリームの物理スイッチで予約された VLAN 値に構成しないようにします。物理スイッチは、特定の VLAN ID を内部的な目的で予約しており、多くの場合、これらの値に構成されているトラフィックは許可されません。たとえば、Cisco Catalyst スイッチでは通常、VLAN 1001 ~ 1024 および 4094 が予約されています。予約されている VLAN を使用すると、ネットワーク上でのサービスの拒否につながる可能性があります。

- Virtual Guest Tagging (VGT) の場合を除き、ポート グループを VLAN 4095 に構成しないようにします。ポート グループを VLAN 4095 に設定すると、VGT モードが有効になります。このモードでは、仮想スイッチが VLAN タグを変更することなくすべてのネットワーク フレームを仮想マシンに渡し、そうしたフレームの処理は仮想マシンに委ねられます。
- 分散仮想スイッチ上でポートレベルの構成オーバーライドを禁止します。ポートレベルの構成オーバーライドは、デフォルトで無効になっています。有効にすると、オーバーライドにより、仮想マシン用のセキュリティ設定をポートグループ レベルでの設定とは異なるものにすることが可能になります。ある種の仮想マシンには固有の構成が必要ですが、監視は必要不可欠です。オーバーライドが監視されていない場合は、セキュリティ性の低い分散仮想スイッチ構成へのアクセス権を持つだれもがそのアクセス権を悪用できる可能性があります。
- 分散仮想スイッチのポート ミラー トラフィックが認証済みのコレクター ポートまたは VLAN のみに送信されるようにします。vSphere Distributed Switch は、パケット キャプチャ デバイスが特定のトラフィック フローを収集できるように、トラフィックをあるポートから別のポートにミラーリングできます。ポート ミラーリングでは、すべての指定トラフィックのコピーが非暗号化形式で送信されます。ミラーリングされたこうしたトラフィックには、キャプチャされたパケット内の完全なデータが含まれています。そのため、宛先を誤るとそのデータ全体がセキュリティ侵害の危険にさらされる可能性があります。ポート ミラーリングが必要な場合は、ポート ミラー先の VLAN、ポート、およびアップリンク ID がすべて正しいことを確認してください。

## ネットワーク コンポーネントのラベル付け

ネットワーキング アーキテクチャのさまざまなコンポーネントを識別することは重要であり、ネットワークが拡大するにつれ、エラーが発生しないようにするのに役立ちます。

次のベスト・プラクティスに従います。

- ポート グループをクリアなネットワーク ラベルで構成します。これらのラベルは、ポート グループの機能記述子の役割を果たし、ネットワークがより複雑になるにつれ、各ポート グループの機能を識別するのに役立ちます。
- vSphere Distributed Switch ごとに、スイッチの機能や IP サブネットを示すクリアなネットワーク ラベルがあることを確認します。このラベルは、物理スイッチにホスト名が必要なように、スイッチの機能記述子の役割を果たします。たとえば、スイッチに内部というラベルを付けて、内部ネットワーキング用であることを示すことができます。標準の仮想スイッチのラベルは変更できません。

## vSphere VLAN 環境の文書化と確認

アドレスの問題を回避するため、VLAN 環境を定期的に確認します。VLAN 環境を完全に文書化し、VLAN ID が 1 回のみ使用されるようにします。文書化はトラブルシューティングに役立ち、環境を拡張するときには不可欠です。

### 手順

- 1 すべての vSwitch および VLAN ID が完全に文書化されていることを確認します。

仮想スイッチで VLAN タギングを使用する場合、ID は外部 VLAN 対応アップストリーム スwitch の ID に対応している必要があります。VLAN ID が完全に追跡されていない場合、ID が誤って再利用され、正しくない物理マシンと仮想マシン間でトラフィックが許可される可能性があります。同様に、VLAN ID が正しくない場合や欠落している場合、物理マシンと仮想マシン間で通過させるトラフィックがブロックされる可能性があります。

- 2 すべての分散仮想ポート グループ (dvPortgroup インスタンス) の VLAN ID が完全に文書化されるようにします。

dvPortgroup で VLAN タギングを使用する場合、ID は外部 VLAN 対応アップストリーム スイッチの ID に対応している必要があります。VLAN ID が完全に追跡されていない場合、ID が誤って再利用され、正しくない物理マシンと仮想マシン間でトラフィックが許可される可能性があります。同様に、VLAN ID が正しくない場合や欠落している場合、物理マシンと仮想マシン間で通過させるトラフィックがブロックされる可能性があります。

- 3 すべての分散仮想スイッチのプライベート VLAN ID が完全に文書化されるようにします。

分散仮想スイッチのプライベート VLAN (PVLAN) には、プライマリおよびセカンダリ VLAN ID が必要です。これらの ID は、外部 PVLAN 対応アップストリーム スイッチの ID に対応している必要があります。VLAN ID が完全に追跡されていない場合、ID が誤って再利用され、正しくない物理マシンと仮想マシン間でトラフィックが許可される可能性があります。同様に、PVLAN ID が正しくない場合や欠落している場合、物理マシンと仮想マシン間で通過させるトラフィックがブロックされる可能性があります。

- 4 VLAN トランク リンクが、トランク リンクとして機能する物理スイッチ ポートにのみ接続されていることを確認します。

仮想スイッチを VLAN トランク ポートに接続している場合は、アップリンク ポートの仮想スイッチと物理スイッチの両方を正しく構成する必要があります。物理スイッチが正しく構成されていない場合、VLAN 802.1q ヘッッドを持つフレームが、そのようなフレームの到着を予期していないスイッチに転送されます。

## 徹底したネットワーク隔離プラクティスの採用

徹底したネットワーク隔離プラクティスを採用すると、vSphere 環境におけるネットワークの安全性が大幅に強化されます。

### 管理ネットワークの隔離

vSphere 管理ネットワークでは、各コンポーネントの vSphere 管理インターフェイスにアクセスできます。管理インターフェイス上で動作するサービスは、攻撃者がシステムへの特権アクセスを取得するきっかけになります。このネットワークへのアクセスの取得から、リモート攻撃が始まる可能性があります。攻撃者は、管理ネットワークへのアクセスを取得すると、それがさらなる侵入のための足場となります。

ESXi ホストまたはクラスタ上で動作する最も安全性の高い仮想マシンのセキュリティ レベルで管理ネットワークを保護して、管理ネットワークへのアクセスを厳密に管理します。管理ネットワークがどんなに制限されていても、管理者は、この管理ネットワークにアクセスして、ESXi ホストと vCenter Server システムを構成する必要があります。

vSphere 管理ポート グループを共有 vSwitch 上の専用 VLAN に 配置します。vSphere 管理ポート グループの VLAN が本番環境の仮想マシンによって使用されない限り、vSwitch は本番環境 (仮想マシン) トラフィックと共有できます。他の管理関連エンティティが検出されるネットワークヘルレーティングされる可能性を除き (vSphere Replication と併用している場合など)、ネットワーク セグメントがルーティングされていないことを確認します。特に、本番環境の仮想マシン トラフィックがこのネットワークにルーティングできないことを必ず確認してください。

次のいずれかの方法を使用して、厳しく制御された管理機能へのアクセスを有効化します。

- 特に慎重に扱う必要のある環境では、管理ネットワークにアクセスするために、制御されたゲートウェイや他の制御された方法を構成します。たとえば、管理者に対して VPN 経由で管理ネットワークに接続することを要求したり、信頼できる管理者に対してのみアクセスを許可するようにします。
- 管理クライアントを実行するジャンプ ボックスを構成します。

## ストレージ トラフィックの隔離

IP ベースのストレージ トラフィックが隔離されていることを確認します。IP ベースのストレージには、iSCSI と NFS があります。仮想マシンは、仮想スイッチおよび VLAN を IP ベースのストレージ構成と共有することがあります。このタイプの構成は、IP ベースのストレージ トラフィックを承認されていない仮想マシン ユーザーに公開する可能性があります。

IP ベースのストレージは、暗号化されていないことが多いため、このネットワークにアクセスできるユーザーであれば、IP ベースのストレージを表示できます。承認されていないユーザーが IP ベースのストレージ トラフィックを表示できないようにするには、IP ベースのストレージ ネットワーク トラフィックを本番環境のトラフィックから論理的に分離します。承認されていないユーザーによるトラフィックの表示を制限するには、VMkernel 管理ネットワークから分離された VLAN またはネットワーク セグメントで、IP ベースのストレージ アダプタを構成します。

## VMotion トラフィックの隔離

VMotion 移行情報は、プレーン テキストで送信されます。この情報が通過するネットワークにアクセスできるユーザーであれば、誰でもこの情報を表示できます。攻撃者が VMotion トラフィックを傍受して、仮想マシンのメモリの内容を取得できる可能性があります。これにより、移行中にコンテンツが変更される MiTM 攻撃もステージングされる可能性があります。

隔離されたネットワーク上で、VMotion トラフィックを本番環境のトラフィックから切り離します。ネットワークをルーティングできないように設定します。つまり、レイヤー 3 ルータがこのネットワークと他のネットワークをスパンニングしないようにして、ネットワークへの外部アクセスを回避します。

VMotion ポート グループは、共有 vSwitch 上の専用 VLAN に配置する必要があります。VMotion ポート グループの VLAN が本番環境の仮想マシンによって使用されない限り、vSwitch は本番環境（仮想マシン）トラフィックと共有できます。

# 複数の vSphere コンポーネントが関係するベスト プラクティス

## 9

環境内の NTP の設定などの一部のセキュリティのベスト プラクティスは、複数の vSphere コンポーネントに影響します。環境を構成する場合は、次の推奨事項を考慮してください。

関連情報については、5 章 ESXi ホストのセキュリティ強化および 7 章 仮想マシンのセキュリティを参照してください。

この章には、次のトピックが含まれています。

- vSphere ネットワーク上の時計の同期
- ストレージのセキュリティのベスト プラクティス
- ホストのパフォーマンス データのゲストへの送信が無効化されていることを確認する
- ESXi Shell および vSphere Web Client のタイムアウトの設定

## vSphere ネットワーク上の時計の同期

vSphere ネットワーク上のすべてのコンポーネントの時計が同期されていることを確認します。vSphere ネットワーク内のマシンの時計が同期されていないと、ネットワーク マシン間の通信において、時間的な制約を受ける SSL 証明書が有効ではないと認識される場合があります。

時計が同期されていないと認証に問題が発生し、インストールが失敗したり、vCenter Server Appliance の vpxd サービスが起動しないことがあります。

vCenter コンポーネントが実行される Windows ホスト マシンが NTP サーバと同期していることを確認します。詳細は、ナレッジ ベースの記事 <http://kb.vmware.com/kb/1318> を参照してください。

- ネットワーク タイム サーバによる ESXi の時計の同期

vCenter Server のインストールまたは vCenter Server Appliance のデプロイの前に、vSphere ネットワーク上のすべてのマシンの時計を確実に同期させてください。

- vCenter Server Appliance の時刻同期設定の構成

デプロイ後、vCenter Server Appliance の時刻同期設定を変更できます。

## ネットワーク タイム サーバによる ESXi の時計の同期

vCenter Server のインストールまたは vCenter Server Appliance のデプロイの前に、vSphere ネットワーク上のすべてのマシンの時計を確実に同期させてください。



このタスクでは、vSphere Client から NTP をセットアップする方法を説明します。代わりに `vicfg-ntp` vCLI コマンドを使用できます。『vSphere Command-Line Interface Reference』を参照してください。

#### 手順

- 1 vSphere Client を起動し、ESXi ホストに接続します。
  - 2 [構成] タブで [時間の構成] をクリックします。
  - 3 [プロパティ] をクリックし、[オプション] をクリックします。
  - 4 [NTP 設定] を選択します。
  - 5 [追加] をクリックします。
  - 6 [NTP サーバの追加] ダイアログ ボックスで、同期する NTP サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
  - 7 [OK] をクリックします。
- ホスト時刻が NTP サーバと同期します。

## vCenter Server Appliance の時刻同期設定の構成

デプロイ後、vCenter Server Appliance の時刻同期設定を変更できます。

vCenter Server Appliance をデプロイする場合は、NTP サーバまたは VMware Tools を使用して、時刻同期方法を選択できます。vSphere ネットワークの時刻設定が変更された場合は、アプライアンス シェルのコマンドを使用して、vCenter Server Appliance を編集し、時刻同期設定を構成します。

定期的な時刻同期を有効にすると、VMware Tools はゲスト OS の時刻をホストの時刻と一致させます。

時刻同期が実行された後、VMware Tools は毎分、ゲスト OS の時計とホストの時計が一致しているかどうかを確認します。一致していない場合は、ゲスト OS の時計がホストの時計と一致するよう同期がとられます。

一般に、Network Time Protocol (NTP) などのネイティブの時刻同期ソフトウェアのほうが VMware Tools による定期的な時刻同期よりも正確であるため、NTP の使用が推奨されます。vCenter Server Appliance で使用できる定期的な時刻同期の形式は 1 つだけです。ネイティブの時刻同期ソフトウェアと vCenter Server Appliance VMware Tools による定期的な時刻同期のいずれか一方を選択すると、他方は無効化されます。

## VMware Tools の時刻同期の使用

VMware Tools の時刻同期を使用するように、vCenter Server Appliance を設定できます。

#### 手順

- 1 アプライアンス シェルにアクセスして、管理者ロールまたはスーパー管理者ロールを持つユーザーとしてログインします。
- スーパー管理者ロールが割り当てられているデフォルトのユーザーは `root` です。
- 2 次のコマンドを実行して、VMware Tools の時刻同期を有効にします。

```
timesync.set --mode host
```

- 3 (オプション) 次のコマンドを実行して、VMware Tools の時刻同期が正常に適用されたことを確認します。

```
timesync.get
```

コマンドにより、時刻同期がホスト モードであることが返されます。

## 結果

アプライアンスの時刻は ESXi ホストの時刻と同期されます。

## vCenter Server Appliance 構成内の NTP サーバの追加または置換

NTP ベースの時刻同期を使用するように vCenter Server Appliance を設定するには、NTP サーバを vCenter Server Appliance 構成に追加する必要があります。

## 手順

- 1 アプライアンス シェルにアクセスして、管理者ロールまたはスーパー管理者ロールを持つユーザーとしてログインします。

スーパー管理者ロールが割り当てられているデフォルトのユーザーは root です。

- 2 `ntp.server.add` コマンドを実行して、NTP サーバを vCenter Server Appliance 構成に追加します。

たとえば、次のコマンドを実行します。

```
ntp.server.add --servers IP-addresses-or-host-names
```

ここで *IP-addresses-or-host-names* は、NTP サーバの IP アドレスまたはホスト名のコンマ区切りのリストです。

このコマンドにより、NTP サーバが構成に追加されます。時刻同期が NTP サーバに基づいている場合は、NTP デーモンが再起動され、新しい NTP サーバが再ロードされます。そうでない場合は、既存の NTP 構成に新しい NTP サーバが追加されるだけです。

- 3 (オプション) 古い NTP サーバを削除して、新しい NTP サーバを vCenter Server Appliance 構成に追加するには、`ntp.server.set` コマンドを実行します。

たとえば、次のコマンドを実行します。

```
ntp.server.set --servers IP-addresses-or-host-names
```

ここで *IP-addresses-or-host-names* は、NTP サーバの IP アドレスまたはホスト名のコンマ区切りのリストです。

このコマンドにより、古い NTP サーバが構成から削除され、入力された NTP サーバが構成内で設定されます。時刻同期が NTP サーバに基づいている場合は、NTP デーモンが再起動され、新しい NTP 構成が再ロードされます。そうでない場合は、NTP 構成内のサーバが、入力値として指定したサーバに置換されるだけです。

- 4 (オプション) 次のコマンドを実行し、NTP 構成の新しい設定が正常に適用されたことを確認します。

```
ntp.get
```

このコマンドは、NTP 同期が構成されているサーバの名前をスペースで区切ったリストを返します。NTP 同期が有効になっていると、このコマンドは [接続中] ステータスの NTP 構成を返します。NTP 同期が無効になっていると、このコマンドは [切断] ステータスの NTP 構成を返します。

#### 次のステップ

NTP 同期が無効になっている場合は、NTP サーバをベースにするように vCenter Server Appliance の時間同期設定を構成できます。 [vCenter Server Appliance と NTP サーバとの時刻同期](#) を参照してください。

## vCenter Server Appliance と NTP サーバとの時刻同期

NTP サーバを使用するように vCenter Server Appliance の時刻同期設定を構成できます。

#### 前提条件

vCenter Server Appliance 構成内に 1 つ以上の Network Time Protocol (NTP) サーバを設定します。 [vCenter Server Appliance 構成内の NTP サーバの追加または置換](#) を参照してください。

#### 手順

- 1 アプライアンス シェルにアクセスして、管理者ロールまたはスーパー管理者ロールを持つユーザーとしてログインします。

スーパー管理者ロールが割り当てられているデフォルトのユーザーは root です。

- 2 次のコマンドを実行して、NTP ベースの時刻同期を有効にします。

```
timesync.set --mode NTP
```

- 3 (オプション) 次のコマンドを実行して、NTP の同期が正常に適用されたことを確認します。

```
timesync.get
```

コマンドにより、時刻同期が NTP モードであることが返されます。

## ストレージのセキュリティのベスト プラクティス

ストレージのセキュリティ プロバイダによって概要が示されている、ストレージのセキュリティのベスト プラクティスに従います。CHAP と 相互 CHAP を利用して、iSCSI ストレージのセキュリティ強化、SAN リソースのマスクとゾーンニング、および NFS 4.1 の Kerberos 認証情報の構成を行うこともできます。

『VMware Virtual SAN の管理』ドキュメントも参照してください。

## iSCSI ストレージのセキュリティ

ホストで構成したストレージには、iSCSI を使用する 1 つ以上のストレージ エリア ネットワーク (SAN) を含めることができます。ホスト上に iSCSI を構成する場合は、いくつかの対策を講じて、セキュリティ リスクを最小にできます。

iSCSI とは、SCSI デバイスに直接接続するのではなく、ネットワーク ポート経由で TCP/IP を使用して、SCSI デバイスにアクセスしてデータ レコードを交換する方法です。iSCSI トランザクションでは、未処理の SCSI データ ブロックが iSCSI レコードでカプセル化され、要求側デバイスまたはユーザーに転送されます。

iSCSI SAN は、既存のイーサネット インフラストラクチャを効率的に使用できるようにし、ホストが動的に共有できるストレージ リソースにアクセスできるようにします。iSCSI SAN は、多くのユーザーにサービスを提供する、共通のストレージ プールに依存した環境に対して、経済的なストレージ ソリューションを提供します。任意のネットワーク システムと同様に、iSCSI SAN もセキュリティ違反の影響を受けます。

---

**注：** iSCSI SAN をセキュリティ強化するための要件および手順は、ホストで利用できるハードウェア iSCSI アダプタ、およびホストから直接構成された iSCSI の場合と似ています。

---

## iSCSI デバイスのセキュリティ強化

望ましくない侵入者から iSCSI デバイスを保護するために、ホストがターゲット LUN のデータにアクセスしようとしたときに、ホスト (イニシエータ) を iSCSI デバイス (ターゲット) で認証するよう要求する方法があります。

認証の目的は、イニシエータがターゲットへのアクセス権、つまり認証を構成するときに付与された権利を持っていることを立証することです。

ESXi は、iSCSI では、SRP (Secure Remote Protocol)、または公開鍵認証方法をサポートしていません。NFS 4.1 でのみ Kerberos を使用できます。

ESXi は、CHAP 認証と相互 CHAP 認証の両方をサポートしています。『vSphere ストレージ』ドキュメントでは、iSCSI デバイスに最適な認証方法を選択する方法と CHAP の設定方法を説明します。

CHAP シークレットが一意であることを確認します。相互認証シークレットはホストごとに別のものにする必要があります。可能であれば、サーバを認証するクライアントのシークレットもそれぞれ別のものにしてください。これにより、1つのホストがセキュリティ侵害されても、攻撃者は別の任意のホストを作成してストレージ デバイスを認証することができなくなります。単一の共有シークレットの場合は、1つのホストがセキュリティ侵害を受けると、攻撃者はストレージ デバイスを認証できるようになります。

## iSCSI SAN の保護

iSCSI 構成を計画するときは、iSCSI SAN の全体のセキュリティを向上させる方法を使用します。iSCSI 構成のセキュリティは IP ネットワーク程度なので、ネットワークを設定するときに優れたセキュリティ標準を適用して、iSCSI ストレージの安全性を高めてください。

次に、優れたセキュリティ標準を実装するための提案をいくつか示します。

### 転送データの保護

iSCSI SAN の第一のセキュリティ リスクは、転送されるストレージ データを攻撃者が傍受する可能性があることです。

攻撃者が iSCSI データを簡単に参照できないよう対策を強化してください。ハードウェア iSCSI アダプタおよび ESXi iSCSI イニシエータは、ターゲット間で受け渡しするデータを暗号化しないので、データはより傍受攻撃を受けやすくなります。

仮想マシンに iSCSI 構成を使用して標準スイッチと VLAN を共有できるように設定すると、iSCSI トラフィックが仮想マシン攻撃者により悪用される危険性があります。攻撃者が iSCSI 転送を受信できないようにするには、仮想マシンのいずれから iSCSI ストレージ ネットワークを参照できないようにしてください。

ハードウェア iSCSI アダプタを使用している場合、このようにするには、iSCSI アダプタおよび ESXi 物理ネットワーク アダプタがスイッチの共有やその他の方法によってホストの外部で不注意に接続されないようにします。ESXi ホストを直接介して iSCSI を構成する場合は、仮想マシンが使用する標準スイッチとは別の標準スイッチを介して iSCSI ストレージを構成することで、このようにできます。

専用標準スイッチを提供することで iSCSI SAN を保護するほかに、iSCSI SAN を独自の VLAN で構成して、パフォーマンスとセキュリティを向上させることができます。iSCSI 構成を個別の VLAN に置くと、iSCSI アダプタ以外のデバイスが iSCSI SAN 内の転送を参照できなくなります。また、ほかのソースからのネットワーク接続も、iSCSI トラフィックを妨害できなくなります。

## 安全な iSCSI ポート

iSCSI デバイスを実行する場合、ESXi ホストは、ネットワーク接続を待機するポートを開きません。これは、攻撃者がスピアポートを介して ESXi に侵入し、ホストの制御を取得する機会が減ることを意味しています。したがって、iSCSI を実行しても、接続の ESXi ホスト側で新たなセキュリティ リスクが生じることはありません。

実行する任意の iSCSI ターゲット デバイスには、iSCSI 接続を待機するために、1 つ以上のオープン TCP ポートが必要です。iSCSI デバイス ソフトウェアのセキュリティが脆弱である場合、ESXi に問題がなくても、データにはリスクが生じることがあります。このリスクを軽減するため、ストレージ メーカーが提供するすべてのセキュリティ パッチをインストールし、iSCSI ネットワークに接続されるデバイスを制限します。

## SAN リソースのマスキングおよびゾーニング

ゾーニングおよび LUN マスキングを使用して、SAN アクティビティを分割し、ストレージ デバイスへのアクセスを制限できます。

SAN リソースでゾーニングおよび LUN マスキングを使用することで、vSphere 環境におけるストレージへのアクセスを保護できます。たとえば、本番ゾーンでのアクティビティを妨げないようにするため、テスト用に定義されたゾーンを SAN 内で独立して管理できます。同様に、異なる部門に異なるゾーンを設定できます。

ゾーンを設定する場合、SAN デバイスで設定されているホスト グループを考慮してください。

各 SAN スwitch のゾーニングとマスキング機能および LUN マスキング管理用のディスク アレイとツールは、ベンダー固有です。

SAN ベンダーのマニュアルおよび vSphere ストレージ のドキュメントを参照してください。

## NFS 4.1 用 Kerberos 認証情報の使用

NFS バージョン 4.1 を使用する場合、ESXi は Kerberos 認証メカニズムをサポートします。

Kerberos は認証サービスの 1 つで、これにより ESXi にインストールされている NFS 4.1 クライアントは、NFS 共有をマウントする前に、NFS サーバに対してその ID を証明することができます。Kerberos では、セキュリティ保護のないネットワーク接続で使用できるよう暗号化を使用します。NFS 4.1 用の Kerberos の vSphere 実装では、クライアントおよびサーバの実在性認証のみをサポートしており、データの整合性サービスや機密保持サービスは提供しません。

Kerberos 認証を使用する場合は、次の考慮事項が適用されます。

- ESXi は、Active Directory ドメインおよび Key Distribution Center (KDC) で Kerberos バージョン 5 を使用します。

- vSphere 管理者として Active Directory 認証情報を指定し、NFS ユーザーが NFS 4.1 Kerberos データストアにアクセスできるようにします。認証情報の単一セットを使用して、そのホストにマウントされているすべての Kerberos データストアにアクセスします。
- 複数の ESXi ホストが同じ NFS 4.1 データストアを共有する場合は、共有データストアにアクセスするすべてのホストで同じ Active Directory 認証情報を使用する必要があります。この動作は、ホスト プロファイルでユーザーを設定し、すべての ESXi ホストにプロファイルを適用することによって、自動化することができます。
- NFS 4.1 は、AUTH\_SYS と Kerberos の同時マウントをサポートしていません。
- NFS 4.1 と Kerberos の組み合わせでは IPv6 がサポートされません。IPv4 のみがサポートされています。

## ホストのパフォーマンス データのゲストへの送信が無効化されていることを確認する

vSphere には、VMware Tools がインストールされている Windows オペレーティング システムの仮想マシン パフォーマンス カウンタが含まれています。パフォーマンス カウンタによって、仮想マシンの所有者はゲスト OS 内で正確にパフォーマンスを分析できます。デフォルトでは、vSphere はホスト情報をゲスト仮想マシンに公開しません。

ホストのパフォーマンス データのゲスト仮想マシンへの送信は、デフォルトで無効になっています。このデフォルト設定は、仮想マシンによる物理ホストの詳細情報の取得を防ぎます。また、仮想マシンのセキュリティ違反が生じた際にホスト データを利用できないようにします。

---

**注：** 次の手順は基本的なプロセスを示しています。このタスクをすべてのホストで同時に実行するには、vSphere または vSphere コマンドライン インターフェイス（vCLI、PowerCLI など）のいずれかを使用します。

---

### 手順

- 1 仮想マシンをホストする ESXi システムで、VMX ファイルを参照します。

仮想マシンの構成ファイルは、`/vmfs/volumes/データストアディレクトリ`にあります。`datastore`は、仮想マシン ファイルが保存されているストレージ デバイスの名前です。

- 2 VMX ファイルで、次のパラメータが設定されていることを確認します。

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 ファイルを保存して閉じます。

### 結果

ゲスト仮想マシン内から、ホストのパフォーマンス情報を取得できなくなります。

## ESXi Shell および vSphere Web Client のタイムアウトの設定

攻撃者がアイドル セッションを使用できないようにするには、ESXi Shell と vSphere Web Client のタイムアウトを確実に設定します。

## ESXi Shell のタイムアウト

ESXi Shell の場合は、vSphere Web Client およびダイレクト コンソール ユーザー インターフェイス (DCUI) から次のタイムアウトを設定できます。

### 可用性タイムアウト

可用性タイムアウト設定は、ESXi Shell を有効にしてからログインするまでの許容経過時間を示します。タイムアウト期間が過ぎると、サービスが無効となり、ユーザーはログインできなくなります。

### アイドル タイムアウト

アイドル タイムアウト設定は、ユーザーが対話形式のアイドル セッションからログアウトされるまでの許容経過時間を示します。アイドル タイムアウトの変更は、ユーザーが次に ESXi Shell にログインする際に適用されるため、既存のセッションは影響を受けません。

## vSphere Web Client のタイムアウト

vSphere Web Client のセッションは、デフォルトで 120 分後に終了します。このデフォルト設定は、『vCenter Server およびホスト管理』ドキュメントでの説明に従って、`webclient.properties` ファイルで変更できます。

# TLS 再構成ユーティリティでの TLS プロトコル構成の管理

# 10

TLS 再構成ユーティリティを使用して TLS プロトコルのバージョンを有効または無効にすることができます。  
vSphere 環境内で TLS 1.0 を無効にできるほか、TLS 1.0 と TLS 1.1 の両方を無効にすることも可能です。  
vSphere 6.5 以降、TLS プロトコル バージョン 1.0、1.1、および 1.2 はデフォルトで有効になります。

再構成では、環境内の vCenter Server、Platform Services Controller、vSphere Update Manager および ESXi ホストは、TLS を無効にできるバージョンのソフトウェアを実行する必要があります。TLS 1.0 を無効にできる VMware 製品のリストについては、VMware のナレッジベースの記事 [KB2145796](#) を参照してください。

TLS 1.0 を無効にする前に、その他の VMware 製品とサードパーティ製品が、有効になっている TLS プロトコルをサポートすることを確認してください。設定に応じて異なりますが、TLS 1.2、または TLS 1.1 と TLS 1.2 の両方をサポートするかどうか確認します。

この章には、次のトピックが含まれています。

- TLS バージョンの無効化をサポートするポート
- vSphere での TLS バージョンの無効化
- TLS 構成ユーティリティのインストール
- オプションの手動バックアップの実行
- vCenter Server システムでの TLS バージョンの無効化
- ESXi ホストでの TLS バージョンの無効化
- Platform Services Controller システムでの TLS バージョンの無効化
- TLS 構成の変更を元に戻す
- vSphere Update Manager での TLS バージョンの無効化

## TLS バージョンの無効化をサポートするポート

vSphere 環境で TLS Configurator ユーティリティを実行すると、vCenter Server、Platform Services Controller、および ESXi ホスト上で TLS を使用するポート間で TLS を無効にすることができます。TLS 1.0、または TLS 1.0 と TLS 1.1 の両方を無効にすることができます。

次の表に、ポートを一覧表示します。ポートが含まれていない場合、ユーティリティは影響しません。



表 10-1. TLS Configurator ユーティリティによって影響を受ける vCenter Server および Platform Services Controller

サービス	Windows での名前	Linux での名前	ポート
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMWareDirectoryService	vmldird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware Secure Token Service	VMwareSTS	vmware-stsd	7444
vSphere Update Manager サービス (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMWareDirectoryService	vmldird	11712

(\*) TLS は、これらのサービスの暗号リストで制御されます。高度な管理はできません。TLS 1.2 のみ、またはすべての TLS 1.x バージョンがサポートされます。

(\*\*) vCenter Server Appliance では、vSphere Update Manager は vCenter Server と同じシステムにあります。Windows の vCenter Server では、構成ファイルを編集することによって TLS を構成します。[vSphere Update Manager での TLS バージョンの無効化](#)を参照してください。

表 10-2. TLS Configurator ユーティリティによって影響を受ける ESXi ポート

サービス	サービス名	ポート
VMware HTTP Reverse Proxy とホストデーモン	Hostd	443
VMware vSAN VASA ベンダー プロバイダ	vSANVP	8080
VMware フォールト ドメイン マネージャ	FDM	8182
VMware vSphere API for IO Filters	ioFilterVPServer	9080
VMware 認証デーモン	vmware-authd	902

## メモと注意事項

- vCenter Server によって管理されているレガシー ESXi ホストが有効な TLS のバージョン (TLS 1.1 および TLS 1.2 または TLS 1.2 のみのいずれか) をサポートすることを確認します。vCenter Server 6.5 で TLS バージョンを無効にすると、vCenter Server はレガシー ESXi ホスト 5.x および 6.0 ホストを管理できなくなります。TLS 1.1 または TLS 1.2 をサポートするバージョンにこれらのホストをアップグレードします。
- 外部の Microsoft SQL Server または外部の Oracle データベースに対して TLS 1.2 のみの接続を使用することはできません。

- Windows Server 2008 で実行されている vCenter Server または Platform Services Controller インスタンスで TLS 1.0 を無効にしないでください。Windows 2008 は TLS 1.0 のみをサポートします。Microsoft TechNet の記事「TLS/SSL Settings」(『Server Roles and Technologies Guide』)を参照してください。
- 次の状況では、TLS 構成の変更を適用した後にホスト サービスを再起動する必要があります。
  - 直接 ESXi ホストに変更を適用する場合。
  - ホスト プロファイルを使用してクラスタ構成を通じて変更を適用する場合。

## vSphere での TLS バージョンの無効化

TLS バージョンを無効にするには、複数フェーズのプロセスがあります。正しい順序で TLS バージョンを無効にすることで、プロセスの間、環境はそのまま実行されるようにします。

- 1 Windows の環境内に vSphere Update Manager があり、vSphere Update Manager が別のシステム上にある場合は、構成ファイルを編集してプロトコルを明示的に無効にします。[vSphere Update Manager での TLS バージョンの無効化](#)を参照してください。

vCenter Server Appliance の vSphere Update Manager は常に vCenter Server システムに含まれており、スクリプトによって対応するポートが更新されます。

- 2 vCenter Server および Platform Services Controller に TLS 構成ユーティリティをインストールします。環境で組み込みの Platform Services Controller を使用する場合は、vCenter Server にのみユーティリティをインストールします。
- 3 vCenter Server 上でユーティリティを実行します。
- 4 vCenter Server によって管理されている各 ESXi ホスト上でユーティリティを実行します。各ホストまたはクラスタ内のすべてのホストに対してこのタスクを実行できます。
- 5 環境で、1 つ以上の Platform Services Controller インスタンスを使用する場合は、各インスタンス上でユーティリティを実行します。

### 前提条件

vSphere 6.0 U3 を実行するシステムおよび vSphere 6.5 を実行するシステムで、この設定を実行します。2 つの選択肢があります。

- TLS 1.0 を無効にし、TLS 1.1 と TLS 1.2 を有効にする。
- TLS 1.0 と TLS 1.1 を無効にし、TLS 1.2 を有効にする。

## TLS 構成ユーティリティのインストール

MyVMware.com から TLS 構成ユーティリティをダウンロードし、ローカル マシンにインストールできます。インストール後に、2 つのスクリプトを使用できます。1 つは、vCenter Server および Platform Services Controller 構成用、もう 1 つは ESXi 構成用です。

vCenter Server Appliance 上で、vSphere Update Manager のポートはスクリプトによって更新されます。vCenter Server 上で、vSphere Update Manager 構成ファイルを編集します。[vSphere Update Manager での TLS バージョンの無効化](#)を参照してください。

#### 前提条件

スクリプトをダウンロードするには MyVMware アカウントが必要です。

#### 手順

- 1 MyVMware アカウントにログインして、vSphere に移動します。
- 2 ライセンス供与されている製品および製品のバージョンを検索し、VMware vCenter Server を選択して、[ダウンロードに移動] をクリックします。
- 3 VMware vSphere の TLS 構成を選択し、次のファイルをダウンロードします。

OS	ファイル
Windows	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm

- 4 vCenter Server にファイルをアップロードし、スクリプトをインストールします。

また、外部 Platform Services Controller の環境で、Platform Services Controller にファイルをアップロードします。

OS	手順
Windows	<ol style="list-style-type: none"> <li>a 管理者権限を持つユーザーでログインします。</li> <li>b ダウンロードした VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi ファイルをコピーします。</li> <li>c MSI ファイルをインストールします。</li> </ol>
Linux	<ol style="list-style-type: none"> <li>a SSH を使用してアプライアンスに接続し、スクリプトを実行する権限を持つユーザーとしてログインします。</li> <li>b SCP クライアントを使用してアプライアンスに VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm ファイルをコピーします。</li> <li>c Bash シェルが有効でない場合は、次のコマンドを実行します。 <div data-bbox="681 1562 999 1612" data-label="Text"> <pre>shell.set --enabled true shell</pre> </div> </li> <li>d アップロードされた rpm ファイルが配置されているディレクトリに移動して、次のコマンドを実行します。 <div data-bbox="681 1732 1324 1785" data-label="Text"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre> </div> </li> </ol>

## 結果

インストールが完了したら、次の場所にあるスクリプトを検索します。

OS	場所
Windows	■ C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\VcTlsReconfigurator
	■ C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\EsxTlsReconfigurator
Linux	■ /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator
	■ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

## オプションの手動バックアップの実行

TLS 構成ユーティリティは、スクリプトが vCenter Server、Platform Services Controller、または vSphere Update Manager を変更するたびにバックアップを実行します。特定のディレクトリに対するバックアップが必要な場合は、手動バックアップを実行できます。

デフォルトのディレクトリは、Windows とアプライアンスで異なります。

OS	バックアップディレクトリ
Windows	c:\users\current_user\appdata\local\temp\yearmonthdayTtime
Linux	/tmp/yearmonthdayTtime

## 手順

- 1 ディレクトリを vSphereTlsReconfigurator、VcTlsReconfigurator サブディレクトリの順に変更します。

OS	コマンド
Windows	C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\ cd VcTlsReconfigurator
Linux	cd /usr/lib/vmware-vSphereTlsReconfigurator/ cd VcTlsReconfigurator

- 2 次のコマンドを実行して、特定のディレクトリにバックアップを作成します。

OS	コマンド
Windows	<i>directory_path</i> \VcTlsReconfigurator> reconfigureVc backup -d <i>backup_directory_path</i>
Linux	<i>directory_path</i> /VcTlsReconfigurator> ./ reconfigureVc backup -d <i>backup_directory_path</i>

### 3 バックアップが成功したことを確認します。

バックアップが成功すると、次の例のようになります。

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819"
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vmware\vSphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

### 4 (オプション) 後でリストアを実行する必要がある場合は、次のコマンドを実行できます。

```
reconfigure restore -d tmp directory or custom backup directory path
```

## vCenter Server システムでの TLS バージョンの無効化

TLS 構成ユーティリティを使用して vCenter Server システムの TLS バージョンを無効にできます。プロセスの一環として、TLS 1.1 と TLS 1.2 の両方を有効にするか、TLS 1.2 のみを有効にします。

#### 前提条件

vCenter Server が管理するホストおよびサービスが有効のままの TLS バージョンを使用して確実に通信できるようにします。TLS 1.0 のみを使用して通信する製品の場合、接続できなくなります。

#### 手順

- 1 スクリプトを実行できるユーザーとして vCenter Server システムにログインし、スクリプトが配置されているディレクトリに移動します。

OS	コマンド
Windows	cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator
Linux	cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator

- 2 オペレーティング システムおよび使用する TLS のバージョンに応じて、コマンドを実行します。

- TLS 1.0 を無効にし、TLS 1.1 および TLS 1.2 の両方を有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2
Linux	directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2

- TLS 1.0 と TLS 1.1 を無効にして、TLS 1.2 のみを有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.2</code>

- 3 環境内に他の vCenter Server システムが含まれている場合は、各 vCenter Server システムでプロセスを繰り返します。
- 4 各 ESXi ホストおよび各 Platform Services Controller 上で設定を繰り返します。

## ESXi ホストでの TLS バージョンの無効化

TLS 構成ユーティリティを使用して ESXi ホストの TLS バージョンを無効にできます。プロセスの一環として、TLS 1.1 と TLS 1.2 の両方を有効にするか、TLS 1.2 のみを有効にします。

ESXi ホストの場合は、vSphere 環境の他のコンポーネントとは別のスクリプトを使用します。

**注：** スクリプトは、`-p` オプションを指定しない限り、TLS 1.0 と TLS 1.1 の両方を無効にします。

### 前提条件

すべての製品または ESXi ホストに関連付けられたサービスが TLS 1.1 または TLS 1.2 を使用して確実に通信できるようにします。製品が TLS 1.0 のみを使用して通信する場合は、接続できなくなります。

### 手順

- 1 スクリプトを実行できるユーザーとして vCenter Server ホストにログインし、スクリプトが配置されているディレクトリに移動します。

OS	コマンド
Windows	<code>C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 クラスタ内のすべてのホストで TLS を無効にするには、次のいずれかのコマンドを実行します。
  - クラスタ内のすべてのホストで、TLS 1.0 を無効にして TLS 1.1 と TLS 1.2 の両方を有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- クラスタ内のすべてのホストで、TLS 1.0 と TLS 1.1 を無効にして TLS 1.2 のみを有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>

### 3 個々のホストで TLS を無効にするには、次のいずれかのコマンドを実行します。

- 個々のホストで TLS 1.0 を無効にして TLS 1.1 と TLS 1.2 の両方を有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 個々のホストで TLS 1.0 と TLS 1.1 を無効にして TLS 1.2 のみを有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h &lt;ESXi_Host_Name&gt; -u Administrative_User -p TLSv1.2</code>

### 4 ESXi ホストを再起動して、TLS プロトコルの変更を完了します。

## Platform Services Controller システムでの TLS バージョンの無効化

環境内に 1 台以上の Platform Services Controller システムが含まれている場合は、サポートされる TLS のバージョンを変更する TLS 構成ユーティリティを使用できます。

環境内で組み込みの Platform Services Controller のみを使用している場合、このタスクを実行する必要はありません。

**注：** 各 vCenter Server システムが TLS の互換性のあるバージョンを実行していることを確認した後にのみ、このタスクを続行します。vCenter Server 6.0.x または 5.5.x のインスタンスが vCenter Server に接続されている場合、それらのインスタンスは、TLS バージョンを無効にすると、Platform Services Controller との通信を停止します。

TLS 1.2 を有効にして、TLS 1.0 と TLS 1.1 を無効にすることができます。また、TLS 1.1 および TLS 1.2 を有効にして、TLS 1.0 のみを無効にすることもできます。

#### 前提条件

Platform Services Controller が接続するホストおよびサービスがサポートされるプロトコルを使用して確実に通信できるようにします。認証と証明書管理が Platform Services Controller によって処理されるため、影響を受ける可能性があるサービスについて慎重に検討してください。サポートされていないプロトコルのみを使用して通信するサービスの場合、接続できなくなります。

#### 手順

- 1 スクリプトを実行できるユーザーとして Platform Services Controller にログインし、スクリプトが配置されているディレクトリに移動します。

OS	コマンド
Windows	<code>cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 Windows の Platform Services Controller または Platform Services Controller アプライアンスでタスクを実行できます。

- TLS 1.0 を無効にし、TLS 1.1 および TLS 1.2 の両方を有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- TLS 1.0 と TLS 1.1 を無効にして、TLS 1.2 のみを有効にするには、次のコマンドを実行します。

OS	コマンド
Windows	<code>directory_path\VcTlsReconfigurator&gt; reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator&gt; ./reconfigureVc update -p TLSv1.2</code>

- 3 環境内にその他の Platform Services Controller システムが含まれている場合は、プロセスを繰り返します。



## TLS 構成の変更を元に戻す

TLS 構成ユーティリティを使用して、構成の変更を元に戻すことができます。変更を元に戻すとき、システムは、TLS Configurator ユーティリティを使用して無効にしたプロトコルを有効にします。

以前に構成をバックアップした場合にのみ、リカバリを実行できます。ESXi ホストでは変更を元に戻すことができません。

次の順序でリカバリを実行します。

### 1 vSphere Update Manager。

使用中の環境が Windows システムで個別の vSphere Update Manager インスタンスを実行している場合は、vSphere Update Manager を最初に更新する必要があります。

### 2 vCenter Server

### 3 Platform Services Controller

#### 手順

#### 1 Windows マシンまたはアプライアンスに接続します。

#### 2 変更を元に戻すシステムにログインします。

OS	手順
Windows	<ol style="list-style-type: none"> <li>1 管理者権限を持つユーザーでログインします。</li> <li>2 VcTlsReconfigurator ディレクトリに移動します。</li> </ol> <pre>cd C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator</pre>
Linux	<ol style="list-style-type: none"> <li>1 SSH を使用してアプライアンスに接続し、スクリプトを実行する権限を持つユーザーとしてログインします。</li> <li>2 Bash シェルが現在有効でない場合は、次のコマンドを実行します。</li> </ol> <pre>shell.set --enabled true shell</pre> <ol style="list-style-type: none"> <li>3 VcTlsReconfigurator ディレクトリに移動します。</li> </ol> <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre>

### 3 以前のバックアップを確認します。

OS	手順
Windows	<pre>C:\ProgramData\VMware\vCenterServer\logs\vsphere-TlsReconfigurator\VcTlsReconfigurator.log</pre> <p>出力は次の例ようになります。</p> <pre>c:\users\username\AppData\Local\Temp\20161108T161539 c:\users\username\AppData\Local\Temp\20161108T171539</pre>
Linux	<pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log</pre> <p>出力は次の例ようになります。</p> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre>

### 4 リストアを実行するには、次のいずれかのコマンドを実行します。

OS	手順
Windows	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例</p> <pre>reconfigureVc restore -d c:\users\username\AppData\Local\Temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

### 5 その他の vCenter Server インスタンスで手順を繰り返します。

### 6 その他の Platform Services Controller インスタンスで手順を繰り返します。

## vSphere Update Manager での TLS バージョンの無効化

vSphere Update Manager 6.0 Update 3 以降では、TLS プロトコルバージョン 1.0、1.1、および 1.2 がすべてデフォルトで有効になります。TLS バージョン 1.0 および TLS バージョン 1.1 は無効にできますが、TLS バージョン 1.2 を無効にすることはできません。

TLS 構成ユーティリティを使用して、その他のサービスの TLS プロトコル構成を管理できます。ただし、vSphere Update Manager では、TLS プロトコルを手動で再構成する必要があります。

TLS プロトコル構成の変更には、次のタスクのいずれかが含まれる可能性があります。

- TLS バージョン 1.1 および TLS バージョン 1.2 を有効にすると同時に、TLS バージョン 1.0 を無効にする。
- TLS バージョン 1.2 を有効にすると同時に、TLS バージョン 1.0 および TLS バージョン 1.1 を無効にする。

- 無効になっている TLS プロトコル バージョンを再度有効にする。

## Update Manager ポート 9087 の以前の TLS バージョンを無効にする

vci-integrity.xml 構成ファイルを変更することによって、ポート 9087 の TLS の以前のバージョンを無効にできます。プロセスはポート 8084 とは異なります。

**注：** TLS バージョンを無効にする前に、vSphere Update Manager と通信するサービスがそのバージョンを使用していないことを確認します。

### 前提条件

vSphere Update Manager サービスを停止します。『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

### 手順

- 1 vSphere Update Manager サービスを停止します。
- 2 Update Manager インストール ディレクトリに移動します。このディレクトリは、vSphere 6.0 と vSphere 6.5 でそれぞれ異なります。

バージョン	場所
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 jetty-vum-ssl.xml ファイルのバックアップを作成し、ファイルを開きます。
- 4 ファイルを変更することで、以前のバージョンの TLS を無効にします。

オプション	説明
TLS 1.0 を無効にします。TLS 1.1 および TLS 1.2 は有効のままにします。	<pre>&lt;Set name="ExcludeProtocols"&gt;   &lt;Array type="java.lang.String"&gt;     &lt;Item&gt;TLSv1&lt;/Item&gt;   &lt;/Array&gt; &lt;/Set&gt;</pre>
TLS 1.0 および TLS 1.1 を無効にします。TLS 1.2 は有効のままにします。	<pre>&lt;Set name="ExcludeProtocols"&gt;   &lt;Array type="java.lang.String"&gt;     &lt;Item&gt;TLSv1&lt;/Item&gt;     &lt;Item&gt;TLSv1.1&lt;/Item&gt;   &lt;/Array&gt; &lt;/Set&gt;</pre>

- 5 ファイルを保存します。
- 6 vSphere Update Manager サービスを再起動します。

## Update Manager ポート 8084 での以前の TLS バージョンの無効化

vci-integrity.xml 構成ファイルを変更することによって、ポート 8084 の TLS の以前のバージョンを無効にできます。このプロセスはポート 9087 の場合と異なります。

**注：** TLS バージョンを無効にする前に、vSphere Update Manager と通信するサービスがそのバージョンを使用していないことを確認します。

### 前提条件

vSphere Update Manager サービスを停止します。『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

### 手順

- 1 vSphere Update Manager サービスを停止します。
- 2 6.0 と 6.5 で異なる Update Manager インストール ディレクトリに移動します。

バージョン	場所
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 vci-integrity.xml ファイルのバックアップを作成し、ファイルを開きます。
- 4 vci-integrity.xml ファイルに <sslOptions> タグを追加します。

```
<ssl>
  <handshakeTimeoutMs>120000</handshakeTimeoutMS>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>

<ssl>
  <privateKey>ssl/rui.key</privateKey>
  <certificate>ssl/rui.crt</certificate>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

- 5 無効にする TLS バージョンに応じて、<sslOptions> タグの次の 10 進数の値のいずれかを使用します。
  - TLSv1.0 のみを無効にするには、10 進数の値 117587968 を使用します。
  - TLSv1.0 および TLSv1.1 を無効にするには、10 進数の値 386023424 を使用します。
- 6 ファイルを保存します。
- 7 vSphere Update Manager サービスを再起動します。

## Update Manager ポート 9087 での無効な TLS バージョンの再有効化

Update Manager ポート 9087 の TLS バージョンを無効にして問題が発生した場合、バージョンを再度有効にすることができます。このプロセスはポート 8084 を有効にする場合と異なります。

以前のバージョンの TLS を再度有効にすると、セキュリティに影響します。

#### 手順

- 1 vSphere Update Manager サービスを停止します。
- 2 6.0 と 6.5 で異なる Update Manager インストール ディレクトリに移動します。

バージョン	場所
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 jetty-vum-ssl.xml ファイルのバックアップを作成し、ファイルを開きます。
- 4 有効にする TLS プロトコルのバージョンに対応する TLS タグを削除します。  
たとえば、TLSv1.1 を有効にするには、jetty-vum-ssl.xml ファイルの <Item>TLSv1.1</Item> を削除します。
- 5 ファイルを保存します。
- 6 vSphere Update Manager サービスを再起動します。

## Update Manager ポート 8084 での無効な TLS バージョンの再有効化

Update Manager ポート 8084 の TLS バージョンを無効にして問題が発生した場合、バージョンを再度有効にすることができます。このプロセスはポート 9087 の場合と異なります。

以前のバージョンの TLS を再度有効にすると、セキュリティに影響があります。

#### 手順

- 1 vSphere Update Manager サービスを停止します。
- 2 6.0 と 6.5 で異なる Update Manager インストール ディレクトリに移動します。

バージョン	場所
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 vci-integrity.xml ファイルのバックアップを作成し、ファイルを開きます。
- 4 <sslOptions> タグで使用されている 10 進数の値を変更するか、タグを削除してすべてのバージョンの TLS を許可します。
  - TLS 1.1 を有効にして TLS 1.0 を無効なままにするには、10 進数の値 117587968 を使用します。
  - TLS 1.1 と TLS 1.0 の両方を再度有効にするには、タグを削除します。
- 5 ファイルを保存します。
- 6 vSphere Update Manager サービスを再起動します。

# 事前定義された権限

# 11

次の表は、デフォルトの権限の一覧表示です。ロールに対して選択するときに、ユーザーとペアにして、オブジェクトに割り当てることができます。この付録の表で使用されている VC は vCenter Server を指し、HC はホスト クライアントであるスタンドアロン ESXi またはワークステーション ホストを指します。

権限を設定するときは、特定の各操作に適切な権限が、すべてのオブジェクト タイプに設定されていることを確認してください。一部の操作では、ルート フォルダや親フォルダへのアクセス権が必要になったり、処理中のオブジェクトにアクセスする必要性が生じたりする場合があります。親フォルダおよび関連オブジェクトでのアクセス権またはパフォーマンス権限が必要な操作もあります。

vCenter Server の拡張機能は、ここに記載されていない権限を定義する場合があります。それらの権限の詳細については、拡張機能に関するドキュメントを参照してください。

この章には、次のトピックが含まれています。

- アラーム権限
- Auto Deploy およびイメージ プロファイルの権限
- 証明書権限
- コンテンツ ライブラリの権限
- データセンター権限
- データストアの権限
- データストア クラスターの権限
- Distributed Switch の権限
- ESX Agent Manager の権限
- 拡張機能権限
- フォルダの権限
- グローバル権限
- ホスト CIM 権限
- ホスト構成権限
- ホスト インベントリ
- ホストのローカル操作権限

- ホスト vSphere レプリケーションの権限
- ホスト プロファイル権限
- Inventory Service プロバイダの権限
- Inventory Service のタグ付けの権限
- ネットワーク権限
- パフォーマンス権限
- 特権
- プロファイル駆動型のストレージの権限
- リソース権限
- スケジュール設定タスクの権限
- セッションの権限
- ストレージ ビュー権限
- タスクの権限
- 転送サービス権限
- VRM ポリシー権限
- 仮想マシンの構成の権限
- 仮想マシン ゲストの操作権限
- 仮想マシン相互作用の権限
- 仮想マシンのインベントリ権限
- 仮想マシンのプロビジョニングの権限
- 仮想マシンのサービス構成権限
- 仮想マシンのスナップショット管理の権限
- 仮想マシンの vSphere Replication 権限
- dvPort グループの権限
- vApp 権限
- vService の権限

## アラーム権限

アラーム権限は、インベントリ オブジェクトに対するアラームの作成、変更、および応答を行えるかどうかを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-1. アラーム権限

権限名	説明	必要とするオブジェクト
アラーム.アラームの確認	起動されたすべてのアラームのアラーム アクションをすべて停止できるようにします。	アラームが起動されているオブジェクト
アラーム.アラームの作成	新しいアラームを作成できるようにします。 アラームをカスタム アクションを指定して作成すると、アラーム作成時にアクションの実行に必要な権限が確認されます。	アラームが起動されているオブジェクト
アラーム.アラーム アクションの無効化	アラームの起動後に発生したアラーム アクションを停止できるようにします。アラームを無効にするわけではありません。	アラームが起動されているオブジェクト
アラーム.アラームの変更	アラームのプロパティを変更できるようにします。	アラームが起動されているオブジェクト
アラーム.アラームの削除	アラームを削除できるようにします。	アラームが起動されているオブジェクト
アラーム.アラーム ステータスの設定	構成されているイベント アラームのステータスを変更できるようにします。The status can change to [Normal], [Warning], or [Alert].	アラームが起動されているオブジェクト

## Auto Deploy およびイメージ プロファイルの権限

Auto Deploy の権限により、Auto Deploy のルールでさまざまなタスクを実行できるユーザーと、ホストに関連付けることができるユーザーを制御します。Auto Deploy の権限により、イメージ プロファイルを作成または編集することができるユーザーを制御することもできます。

次の表では、Auto Deploy のルールおよびルール セットを管理できるユーザーおよびイメージ プロファイルを作成および編集できるユーザーを判別する権限について説明します。vSphere のインストールとセットアップ を参照してください。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。



表 11-2. Auto Deploy の権限

権限名	説明	必要とするオブジェクト
Auto Deploy.ホスト.マシンの関連付け	ユーザーがマシンとホストを関連付けることができます。	vCenter Server
Auto Deploy.イメージ プロファイル.作成	イメージ プロファイルを作成できます。	vCenter Server
Auto Deploy.イメージ プロファイル.編集	イメージ プロファイルを編集できます。	vCenter Server
Auto Deploy.ルール.作成	Auto Deploy のルールを作成できます。	vCenter Server
Auto Deploy.ルール.削除	Auto Deploy のルールを削除できます。	vCenter Server
Auto Deploy.ルール.編集	Auto Deploy のルールを編集できます。	vCenter Server
Auto Deploy.ルールセット.有効化	Auto Deploy のルール セットを有効にできます。	vCenter Server
Auto Deploy.ルールセット.編集	Auto Deploy のルール セットを編集できます。	vCenter Server

## 証明書権限

証明書権限により、ESXi の証明書を管理できるユーザーを制御します。

この権限により、ESXi ホストの証明書管理を実行できるユーザーが決まります。vCenter Server 証明書管理の詳細については、[証明書管理の操作に必要な権限](#)を参照してください。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-3. ホスト証明書権限

権限名	説明	必要とするオブジェクト
証明書.証明書を管理	ESXi ホストの証明書を管理できるようにします。	vCenter Server

## コンテンツ ライブラリの権限

コンテンツ ライブラリを使用すると、仮想マシン テンプレートと vApp を簡単かつ効率的に管理できます。コンテンツ ライブラリの権限で、コンテンツ ライブラリのさまざまな側面を表示または管理できるユーザーを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-4. コンテンツ ライブラリの権限

権限名	説明	必要とするオブジェクト
コンテンツ ライブラリ.ライブラリ アイテムの追加	ライブラリにアイテムを追加できるようにします。	ライブラリ
コンテンツ ライブラリ.ローカル ライブラリの作成	指定した vCenter Server システムでローカル ライブラリを作成できるようにします。	vCenter Server
コンテンツ ライブラリ.購読済みライブラリの作成	購読済みライブラリを作成できるようにします。	vCenter Server
コンテンツ ライブラリ.ライブラリ アイテムの削除	ライブラリ アイテムを削除できるようにします。	ライブラリ。すべてのライブラリ アイテムに伝達されるようにこの権限を設定します。
コンテンツ ライブラリ.ローカル ライブラリの削除	ローカル ライブラリを削除できるようにします。	ライブラリ
コンテンツ ライブラリ.購読済みライブラリの削除	購読済みライブラリを削除できるようにします。	ライブラリ
コンテンツ ライブラリ.ファイルのダウンロード	コンテンツ ライブラリからファイルをダウンロードできるようにします。	ライブラリ
コンテンツ ライブラリ.ライブラリ アイテムの消去	アイテムを消去できるようにします。購読済みライブラリのコンテンツは、キャッシュできる場合とキャッシュできない場合があります。コンテンツがキャッシュされた場合は、ライブラリ アイテムを消去するとライブラリ アイテムを解放できます（この権限がある場合）。	ライブラリ。すべてのライブラリ アイテムに伝達されるようにこの権限を設定します。
コンテンツ ライブラリ.購読済みライブラリの消去	購読済みライブラリを消去できるようにします。購読済みライブラリのコンテンツは、キャッシュできる場合とキャッシュできない場合があります。コンテンツがキャッシュされた場合は、ライブラリを消去するとライブラリを解放できます（この権限がある場合）。	ライブラリ

表 11-4. コンテンツ ライブラリの権限（続き）

権限名	説明	必要とするオブジェクト
コンテンツ ライブラリ.ストレージのインポート	ソース ファイル URL が ds:// または file:// から始まる場合、ユーザーがライブラリ アイテムをインポートできるようにします。デフォルトでは、この権限はコンテンツ ライブラリ管理者に対して無効になっています。ストレージ URL からのインポートはコンテンツのインポートを意味するため、必要な場合に限り、またインポートを実行するユーザーにセキュリティ上の問題がある場合に限り、この権限を有効にします。	ライブラリ
コンテンツ ライブラリ.購読情報の検知	この権限を使用すると、ソリューション ユーザーおよび API は、URL、SSL 証明書、およびパスワードを含むリモート ライブラリの購読情報をプロープできるようにします。表示される構造は、購読構成が成功したかどうか、SSL エラーなどの問題が発生していないかどうかを示します。	ライブラリ
コンテンツ ライブラリ.ストレージの読み込み	コンテンツ ライブラリ ストレージを読み込めるようにします。	ライブラリ
コンテンツ ライブラリ.ライブラリ アイテムの同期	ライブラリ アイテムを同期できるようにします。	ライブラリ。すべてのライブラリ アイテムに伝達されるようにこの権限を設定します。
コンテンツ ライブラリ.購読済みライブラリの同期	購読済みライブラリを同期できるようにします。	ライブラリ
コンテンツ ライブラリ.タイプのイントロスペクション	ソリューション ユーザーまたは API が、コンテンツ ライブラリ サービスにサポートされているプラグインをイントロスペクトできるようにします。	ライブラリ
コンテンツ ライブラリ.構成設定の更新	構成設定を更新できるようにします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	ライブラリ
コンテンツ ライブラリ.ファイルの更新	コンテンツをコンテンツ ライブラリにアップロードできるようにします。ライブラリ アイテムからファイルを削除できるようにします。	ライブラリ
コンテンツ ライブラリ.ライブラリの更新	コンテンツ ライブラリを更新できるようにします。	ライブラリ
コンテンツ ライブラリ.ライブラリ アイテムの更新	ライブラリ アイテムを更新できるようにします。	ライブラリ。すべてのライブラリ アイテムに伝達されるようにこの権限を設定します。
コンテンツ ライブラリ.ローカル ライブラリの更新	ローカル ライブラリを更新できるようにします。	ライブラリ
コンテンツ ライブラリ.購読済みライブラリの更新	購読済みライブラリのプロパティを更新できるようにします。	ライブラリ
コンテンツ ライブラリ.構成設定の表示	構成設定を表示できるようにします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	ライブラリ

## データセンター権限

データセンター権限は、vSphere Web Client インベントリ内のデータセンターを作成および編集する機能を制御します。

すべてのデータセンター権限は、vCenter Server 内でのみ使用されます。データセンターの作成権限は、データセンター フォルダまたはルート オブジェクトに対して定義されます。その他のデータセンター権限はすべて、データセンター、データセンター フォルダ、またはルート オブジェクトに割り当てられます。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-5. データセンター権限

権限名	説明	必要とするオブジェクト
データセンター.データセンターの作成	新規データセンターの作成を許可します。	データセンター フォルダ またはルート オブジェクト
データセンター.データセンターの移動	データセンターの移動を許可します。 移動元と移動先の両方に権限が必要です。	データセンター（ソースと ターゲットの両方）
データセンター.ネットワーク プロトコルのプロファイル構成	データセンターのネットワーク プロファイルの構成を許可します。	データセンター
データセンター.IP プール割り当てのクエリ	IP アドレスのプールを構成します。	データセンター
データセンター.データセンターの再構成	データセンターの再構成を許可します。	データセンター
データセンター.IP の割り当てのリリース	データセンターに割り当てられた IP の割り当て解除を許可します。	データセンター
データセンター.データセンターの削除	データセンターの削除を許可します。 この操作を行うための権限を取得するには、オブジェクトとその親オブジェクトに対する権限が必要です。	データセンターと親オブジェクト
データセンター.データセンター名の変更	データセンター名の変更を許可します。	データセンター

## データストアの権限

データストア権限は、データストアの参照、管理、領域の割り当ての機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-6. データストアの権限

権限名	説明	必要とするオブジェクト
データストア.領域の割り当て	仮想マシン、スナップショット、クローン、または仮想ディスク用に、データストアの領域を割り当てられるようにします。	データストア
データストア.データストアの参照	データストアのファイルを参照できるようにします。	データストア
データストア.データストアの構成	データストアを構成できるようにします。	データストア
データストア.低レベルのファイル操作	データストア ブラウザ内で、読み取り、書き込み、削除、および名前変更操作を実行できるようにします。	データストア

表 11-6. データストアの権限（続き）

権限名	説明	必要とするオブジェクト
データストア.データストアの移動	フォルダ間でデータストアを移動できるようにします。 移動元と移動先の両方に権限が必要です。	データストア、移動元と移動先
データストア.データストアの削除	データストアを削除できるようにします。 この権限は廃止されました。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	データストア
データストア.ファイルの削除	データストアのファイルを削除できるようにします。 この権限は廃止されました。低レベルのファイル操作権限を割り当てます。	データストア
データストア.データストア名の変更	データストア名を変更できるようにします。	データストア
データストア.仮想マシン ファイルの更新	データストアが再署名された後、そのデータストア上の仮想マシン ファイルへのファイル パスを更新できるようにします。	データストア
データストア.仮想マシン メタデータの更新	データストアに関連付けられた仮想マシン メタデータの更新を許可します。	データストア

## データストア クラスターの権限

データストア クラスターによって、ストレージ DRS のデータストア クラスターの構成を制御する権限が与えられます。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-7. データストア クラスターの権限

権限名	説明	必要とするオブジェクト
データストア クラスター.データストア クラスターの構成	ストレージ DRS のデータストア クラスター設定を作成および構成できるようにします。	データストア クラスター

## Distributed Switch の権限

Distributed Switch の権限により、Distributed Switch インスタンスの管理に関連したタスクを実行する権限を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-8. vSphere Distributed Switch の権限

権限名	説明	必要とするオブジェクト
Distributed Switch.作成	Distributed Switch を作成できるようにします。	データセンター、ネットワーク フォルダ
Distributed Switch.削除	Distributed Switch を削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	分散スイッチ
Distributed Switch.ホスト操作	Distributed Switch のホスト メンバーを変更できるようにします。	分散スイッチ
Distributed Switch.変更	Distributed Switch の構成を変更できるようにします。	分散スイッチ
Distributed Switch.移動	vSphere Distributed Switch を別のフォルダに移動できるようにします。	分散スイッチ
Distributed Switch.Network I/O Control の操作	vSphere Distributed Switch のリソース設定を変更できるようにします。	分散スイッチ
Distributed Switch.ポリシー操作	vSphere Distributed Switch のポリシーを変更できるようにします。	分散スイッチ
Distributed Switch.ポート構成の操作	vSphere Distributed Switch のポートの構成を変更できるようにします。	分散スイッチ
Distributed Switch.ポート設定の操作	vSphere Distributed Switch のポートの設定を変更できるようにします。	分散スイッチ
Distributed Switch.VSPAN 操作	vSphere Distributed Switch の VSPAN 構成を変更できるようにします。	分散スイッチ

## ESX Agent Manager の権限

ESX Agent Manager の権限は、ESX Agent Manager およびエージェント仮想マシンに関する操作を制御します。ESX Agent Manager は、管理仮想マシンをインストールできるサービスです。管理仮想マシンは 1 つのホストに結び付けられており、VMware DRS や仮想マシンを移行するその他のサービスの影響を受けません。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-9. ESX Agent Manager

権限名	説明	必要とするオブジェクト
ESX Agent Manager.構成	ホストまたはクラスタにエージェント仮想マシンをデプロイできるようにします。	仮想マシン
ESX Agent Manager.変更	仮想マシンのパワーオフや削除など、エージェント仮想マシンへの変更を可能にします。	仮想マシン
ESX Agent View.表示	エージェント仮想マシンの表示を可能にします。	仮想マシン

## 拡張機能権限

拡張機能権限は、拡張機能のインストールおよび管理の機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-10. 拡張機能権限

権限名	説明	必要とするオブジェクト
拡張機能.拡張機能の登録	拡張機能（プラグイン）を登録できるようにします。	ルート vCenter Server
拡張機能.拡張機能の登録解除	拡張機能（プラグイン）を登録解除できるようにします。	ルート vCenter Server
拡張機能.拡張機能の更新	拡張機能（プラグイン）を更新できるようにします。	ルート vCenter Server

## フォルダの権限

フォルダの権限は、フォルダの作成および管理の機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-11. フォルダの権限

権限名	説明	必要とするオブジェクト
フォルダ.フォルダの作成	新しいフォルダを作成できるようにします。	フォルダ
フォルダ.フォルダの削除	フォルダを削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	フォルダ
フォルダ.フォルダの移動	フォルダを移動できるようにします。 移動元と移動先の両方に権限が必要です。	フォルダ
フォルダ.フォルダ名の変更	フォルダの名前を変更できるようにします。	フォルダ

## グローバル権限

グローバル権限は、タスク、スクリプト、拡張機能に関するグローバル タスクを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-12. グローバル権限

権限名	説明	必要とするオブジェクト
グローバル.vCenter Server として機能	vMotion の送信操作または vMotion の受信操作を準備または開始できるようにします。	ルート vCenter Server
グローバル.タスクのキャンセル	実行中のタスクまたは待機中のタスクをキャンセルできるようにします。	タスクに関連するインベントリ オブジェクト
グローバル.キャパシティ プランニング	物理マシンから仮想マシンへの統合を計画する際にキャパシティ プランニングを使用できるようにします。	ルート vCenter Server
グローバル.診断	診断ファイル、ログ ヘッド、バイナリ ファイル、診断バンドルのリストを取得できるようにします。  潜在的なセキュリティ違反を防止するため、この権限は vCenter Server 管理者ロールに制限してください。	ルート vCenter Server
グローバル.メソッドの無効化	vCenter Server 拡張機能のサーバが、vCenter Server によって管理されるオブジェクトに対する特定の操作を無効にできるようにします。	ルート vCenter Server
グローバル.メソッドの有効化	vCenter Server 拡張機能のサーバが、vCenter Server が管理するオブジェクトの特定の操作を有効にできるようにします。	ルート vCenter Server
グローバル.グローバル タグ	グローバル タグを追加または削除できるようにします。	ルート ホストまたは vCenter Server
グローバル.健全性	vCenter Server コンポーネントの健全性を表示できるようにします。	ルート vCenter Server
グローバル.ライセンス	インストールされたライセンスを表示し、ライセンスの追加または削除を行えるようにします。	ルート ホストまたは vCenter Server
グローバル.ログ イベント	特定の管理対象エンティティに対して、ユーザー定義のイベントをログに記録できるようにします。	任意のオブジェクト
グローバル.カスタム属性の管理	カスタム フィールド定義を追加、削除、または名前変更できるようにします。	ルート vCenter Server
グローバル.プロキシ	プロキシとの間のエンドポイントを追加または削除するための、内部インターフェイスへのアクセスを可能にします。	ルート vCenter Server
グローバル.スクリプト アクション	アラームと組み合わせてスクリプト アクションをスケジュール設定できるようにします。	任意のオブジェクト
グローバル.サービス マネージャ	vSphere CLI で <code>resxtp</code> コマンドを使用できるようにします。	ルート ホストまたは vCenter Server
グローバル.カスタム属性の設定	管理対象オブジェクトのカスタム属性を表示、作成、または削除できるようにします。	任意のオブジェクト
グローバル.設定	ランタイム vCenter Server 構成設定を読み取りおよび変更できるようにします。	ルート vCenter Server
グローバル.システム タグ	システム タグを追加または削除できるようにします。	ルート vCenter Server

## ホスト CIM 権限

ホスト CIM 権限は、ホストの健全性を監視する CIM の使用を制御します。



この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-13. ホスト CIM 権限

権限名	説明	必要とするオブジェクト
ホスト.CIM.CIM 相互作用	クライアントが CIM サービスで使用するチケットを取得できるようにします。	ホスト

## ホスト構成権限

ホスト構成権限は、ホストを構成する機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-14. ホスト構成権限

権限名	説明	必要とするオブジェクト
ホスト.構成.詳細設定	詳細なホスト構成オプションを設定できるようにします。	ホスト
ホスト.構成.認証ストア	Active Directory 認証ストアを構成できるようにします。	ホスト
ホスト.構成.PCI バススルー設定の変更	ホストの PCI バススルー設定を変更できるようにします。	ホスト
ホスト.構成.SNMP 設定の変更	ホストの SNMP 設定を変更できるようにします。	ホスト
ホスト.構成.日付および時刻の設定の変更	ホストの日時設定を変更できるようにします。	ホスト
ホスト.構成.設定の変更	ESXi ホストでロックダウン モードを設定できるようにします。	ホスト
ホスト.構成.接続	ホストの接続状態（接続中または切断）を変更できるようにします。	ホスト
ホスト.構成.ファームウェア	ESXi ホストのファームウェアを更新できるようにします。	ホスト
ホスト.構成.ハイパースレッド	ホストの CPU スケジューラでハイパースレッドを有効化または無効化できるようにします。	ホスト
ホスト.構成.イメージ構成	ホストに関連付けられたイメージを変更できるようにします。	
ホスト.構成.メンテナンス	ホストのメンテナンス モードへの切り替えおよび終了と、ホストのシャットダウンおよび再起動を行えるようにします。	ホスト
ホスト.構成.メモリ構成	ホスト構成を変更できるようにします。	ホスト
ホスト.構成.ネットワークの構成	ネットワーク、ファイアウォール、vMotion ネットワークを構成できるようにします。	ホスト
ホスト.構成.電源	ホストの電力管理設定を構成できるようにします。	ホスト
ホスト.構成.パッチのクエリ	インストール可能なパッチを照会し、ホストにパッチをインストールできるようにします。	ホスト

表 11-14. ホスト構成権限（続き）

権限名	説明	必要とするオブジェクト
ホスト.構成.セキュリティ プロファイル およびファイアウォール	SSH、Telnet、SNMP などのインターネット サービスや、ホスト ファイアウォールを構成できるようにします。	ホスト
ホスト.構成.ストレージ パーティション 構成	VMFS データストアおよび診断パーティションを管理できるように します。この権限を持つユーザーは新しいストレージ デバイスをス キャンして iSCSI を管理できます。	ホスト
ホスト.構成.システム管理	ホスト上のファイル システムを操作する拡張機能を許可します。	ホスト
ホスト.構成.システム リソース	システム リソース階層の構成を更新できるようにします。	ホスト
ホスト.構成.仮想マシン自動起動構成	単一ホスト上の仮想マシンの自動起動および自動停止の順序を変更 できるようにします。	ホスト

## ホスト インベントリ

ホスト インベントリ権限は、インベントリへのホストの追加、クラスタへのホストの追加、インベントリ内でのホストの移動を制御します。

この表では、インベントリ内でのホストとクラスタの追加および移動に必要な権限について説明します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-15. ホスト インベントリ権限

権限名	説明	必要とするオブジェクト
ホスト.インベントリ.クラスタ へのホストの追加	既存クラスタにホストを追加できるようにします。	クラスタ
ホスト.インベントリ.スタンド アロン ホストの追加	スタンドアロン ホストを追加できるようにします。	ホスト フォルダ
ホスト.インベントリ.クラスタ の作成	新しいクラスタを作成できるようにします。	ホスト フォルダ
ホスト.インベントリ.クラスタ の変更	クラスタのプロパティを変更できるようにします。	クラスタ
ホスト.インベントリ.クラスタ またはスタンドアロン ホスト の移動	クラスタまたはスタンドアロン ホストをフォルダ間で移動できるようにしま す。 移動元と移動先の両方に権限が必要です。	クラスタ
ホスト.インベントリ.ホストの 移動	既存の一連のホストをクラスタに移動したり、クラスタから移動したりできる ようにします。 移動元と移動先の両方に権限が必要です。	クラスタ
ホスト.インベントリ.クラスタ の削除	クラスタまたはスタンドアロン ホストを削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの 両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	クラスタ、ホスト

表 11-15. ホスト インベントリ権限（続き）

権限名	説明	必要とするオブジェクト
ホスト.インベントリ.ホストの削除	ホストを削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	ホストと親オブジェクト
ホスト.インベントリ.クラスタ名の変更	クラスタの名前を変更できるようにします。	クラスタ

## ホストのローカル操作権限

ホストのローカル操作権限は、vSphere Client がホストに直接接続されているときに実行する操作を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-16. ホストのローカル操作権限

権限名	説明	必要とするオブジェクト
ホスト.ローカル操作.vCenter へのホストの追加	vpxa や aam などの vCenter エージェントのホストへのインストールおよびホストからの削除を許可します。	ルート ホスト
ホスト.ローカル操作.仮想マシンの作成	ホストに登録せずにディスク上で最初から新規仮想マシンを作成することを許可します。	ルート ホスト
ホスト.ローカル操作.仮想マシンの削除	ディスクで仮想マシンを削除できるようにします。登録および未登録の仮想マシンでサポートされます。	ルート ホスト
ホスト.ローカル操作.NVRAM コンテンツの抽出	ホストの NVRAM の内容の抽出を許可します。	
ホスト.ローカル操作権限.ユーザー グループの管理	ホストでのローカル アカウントの管理を許可します。	ルート ホスト
ホスト.ローカル操作.仮想マシンの再構成	仮想マシンの再構成を許可します。	ルート ホスト
ホスト.ローカル操作.スナップショットのレイアウト変更	仮想マシンのスナップショットのレイアウトに対する変更を許可します。	ルート ホスト

## ホスト vSphere レプリケーションの権限

ホスト vSphere レプリケーションの権限で、ホストの VMware vCenter Site Recovery Manager™ による仮想マシンのレプリケーションの使用を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-17. ホスト vSphere レプリケーションの権限

権限名	説明	必要とするオブジェクト
ホスト.vSphere Replication.レプリケーションの管理	このホストでの仮想マシンのレプリケーションの管理を許可します。	ホスト

## ホスト プロファイル権限

ホスト プロファイル権限は、ホスト プロファイルの作成と変更に関連する操作を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-18. ホスト プロファイル権限

権限名	説明	必要とするオブジェクト
ホスト プロファイル.クリア	プロファイル関連情報をクリアできるようにします。	ルート vCenter Server
ホスト プロファイル.作成	ホスト プロファイルを作成できるようにします。	ルート vCenter Server
ホスト プロファイル.削除	ホスト プロファイルを削除できるようにします。	ルート vCenter Server
ホスト プロファイル.編集	ホスト プロファイルを編集できるようにします。	ルート vCenter Server
ホスト プロファイル.エクスポート	ホスト プロファイルをエクスポートできるようにします。	ルート vCenter Server
ホスト プロファイル.表示	ホスト プロファイルを表示できるようにします。	ルート vCenter Server

## Inventory Service プロバイダの権限

Inventory Service の権限は内部でのみ使用されます。使用しません。

## Inventory Service のタグ付けの権限

Inventory Service のタグ付けの権限は、タグおよびタグ カテゴリの作成および削除、vSphere インベントリ オブジェクトに対するタグの割り当てと削除を行う機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-19. vCenter Inventory Service の権限

権限名	説明	必要とするオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグの割り当てまたは割り当て解除	vCenter Server インベントリ中のオブジェクトにタグを割り当てたり、その割り当てを解除できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグの作成	タグを作成できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ カテゴリの作成	タグ カテゴリを作成できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ スコアの作成	タグの範囲を作成できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグの削除	タグ カテゴリを削除できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ カテゴリの削除	タグ カテゴリの削除を許可します。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ スコアの削除	タグの範囲を削除できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグの編集	タグを編集できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ カテゴリの編集	タグ カテゴリを編集できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.vSphere タグ スコアの編集	タグの範囲を編集できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.カテゴリの UsedBy フィールドの変更	タグ カテゴリの UsedBy フィールドを変更できるようにします。	任意のオブジェクト
Inventory Service.vSphere のタグ付け.タグの UsedBy フィールドの変更	タグの UsedBy フィールドを変更できるようにします。	任意のオブジェクト

## ネットワーク権限

ネットワーク権限は、ネットワーク管理に関するタスクを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-20. ネットワーク権限

権限名	説明	必要とするオブジェクト
ネットワーク.ネットワークの割り当て	仮想マシンへのネットワークの割り当てを許可します。	ネットワーク、仮想マシン
ネットワーク.構成	ネットワークの構成を許可します。	ネットワーク、仮想マシン

表 11-20. ネットワーク権限（続き）

権限名	説明	必要とするオブジェクト
ネットワーク.ネットワークの移動	フォルダ間でのネットワークの移動を許可します。 移動元と移動先の両方に権限が必要です。	ネットワーク
ネットワーク.削除	ネットワークの削除を許可します。 この権限は廃止されました。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	ネットワーク

## パフォーマンス権限

パフォーマンス権限は、パフォーマンス統計情報の設定の変更を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-21. パフォーマンス権限

権限名	説明	必要とするオブジェクト
パフォーマンス.間隔の変更	パフォーマンス データの収集間隔を作成、削除、および更新できるようにします。	ルート vCenter Server

## 特権

特権は、ロールおよび権限の割り当てを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-22. 特権

権限名	説明	必要とするオブジェクト
権限.権限の変更	エンティティに対して 1 つ以上の権限ルールを定義したり、エンティティで特定のユーザーまたはグループに既存のルールがある場合はルールをアップデートできるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	任意のオブジェクトと親オブジェクト
権限.権限の変更	権限のグループまたは説明を変更できます。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	
権限.ロールの変更	ロールの名前と、そのロールに関連付けられた権限を更新できるようにします。	任意のオブジェクト
権限.ロール権限の再割り当て	ロールのすべての権限を別のロールに再割り当てできるようにします。	任意のオブジェクト

## プロファイル駆動型のストレージの権限

プロファイル駆動型のストレージの権限では、ストレージ プロファイル関連の操作が制御されます。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-23. プロファイル駆動型のストレージの権限

権限名	説明	必要とするオブジェクト
プロファイル駆動型ストレージ. プロファイル駆動型ストレージ更新	ストレージ機能および仮想マシンのストレージ プロファイルの作成および更新など、ストレージ プロファイルに変更を加えられるようにします。	ルート vCenter Server
プロファイル駆動型ストレージ. プロファイル駆動型ストレージ ビュー	定義されているストレージ機能およびストレージ プロファイルを表示できるようにします。	ルート vCenter Server

## リソース権限

リソース権限は、リソース プールの作成と管理、および仮想マシンの移行を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-24. リソース権限

権限名	説明	必要とするオブジェクト
リソース.推奨の適用	vMotion での移行を実行するためにサーバからの提案を受け入れられるようにします。	クラスタ
リソース.vApp のリソース プールへの割り当て	リソース プールに vApp を割り当てられるようにします。	リソース プール
リソース.仮想マシンのリソース プールへの割り当て	リソース プールに仮想マシンを割り当てられるようにします。	リソース プール
リソース.リソース プールの作成	リソース プールを作成できるようにします。	リソース プール、クラスタ
リソース.パワーオフ状態の仮想マシンの移行	別のリソース プールまたはホストにパワーオフ状態の仮想マシンを移行できるようにします。	仮想マシン
リソース.パワーオン状態の仮想マシンの移行	別のリソース プールまたはホストにパワーオン状態の仮想マシンを vMotion で移行できるようにします。	
リソース.リソース プールの変更	リソース プールの割り当てを変更できるようにします。	リソース プール
リソース.リソース プールの移動	リソース プールを移動できるようにします。移動元と移動先の両方に権限が必要です。	リソース プール
リソース.vMotion のクエリ	仮想マシンと一連のホストの一般的な vMotion 互換性を照会できるようにします。	ルート vCenter Server

表 11-24. リソース権限（続き）

権限名	説明	必要とするオブジェクト
リソース.リソース プールの削除	リソース プールを削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	リソース プール
リソース.リソース プール名の変更	リソース プールの名前を変更できるようにします。	リソース プール

## スケジュール設定タスクの権限

スケジュール設定タスクの権限は、スケジュール設定タスクの作成、編集、削除を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-25. スケジュール設定タスクの権限

権限名	説明	必要とするオブジェクト
スケジュール設定タスク.タスクの作成	タスクをスケジュール設定できるようにします。スケジュール設定時に、スケジュール設定操作を実行する権限に加えて必要な権限です。	任意のオブジェクト
スケジュール設定タスク.タスクの変更	スケジュール設定タスクのプロパティを再構成できるようにします。	任意のオブジェクト
スケジュール設定タスク.タスクの削除	待機中のスケジュール設定タスクを削除できるようにします。	任意のオブジェクト
スケジュール設定タスク.タスクの実行	スケジュール設定タスクをすぐに実行できるようにします。 スケジュール設定タスクの作成と実行には、関連するアクションを実行する権限も必要です。	任意のオブジェクト

## セッションの権限

セッションの権限は、vCenter Server システムのセッションを開くための拡張機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-26. セッションの権限

権限名	説明	必要とするオブジェクト
セッション.ユーザーへのなりすまし	別のユーザーのなりすましを実行できるようにします。この機能は拡張機能で使われます。	ルート vCenter Server
セッション.メッセージ	グローバル ログイン メッセージを設定できるようにします。	ルート vCenter Server



表 11-26. セッションの権限（続き）

権限名	説明	必要とするオブジェクト
セッション.セッションの確認	セッション有効性を確認できるようにします。	ルート vCenter Server
セッション.セッションの表示および停止	セッションの表示と、1 人以上のログオン ユーザーの強制ログアウトを可能にします。	ルート vCenter Server

## ストレージ ビュー権限

ストレージ ビュー権限は、ストレージ監視サービス API に対する権限を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-27. ストレージ ビュー権限

権限名	説明	必要とするオブジェクト
ストレージ ビュー.サービスの構成	権限のあるユーザーに対してすべてのストレージ監視サービス API の使用を許可します。読み取り専用のストレージ監視サービス API に対する権限では、ストレージ ビュー.表示 を使用します。	ルート vCenter Server
ストレージ ビュー.表示	権限のあるユーザーに対して読み取り専用のストレージ監視サービス API の使用を許可します。	ルート vCenter Server

## タスクの権限

タスクの権限は、vCenter Server のタスクを作成およびアップデートするための拡張機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-28. タスクの権限

権限名	説明	必要とするオブジェクト
タスク.タスクの作成	拡張機能でユーザー定義タスクを作成できるようにします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	ルート vCenter Server
タスク.タスクの更新	拡張機能でユーザー定義タスクを更新できるようにします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	ルート vCenter Server

## 転送サービス権限

転送サービス権限は VMware 内部で使用されます。これらの権限を使用しないでください。

## VRM ポリシー権限

VRM ポリシーの権限は VMware 内部で使用されます。これらの権限を使用しないでください。

## 仮想マシンの構成の権限

仮想マシンの構成権限は、仮想マシンのオプションおよびデバイスを構成する機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-29. 仮想マシンの構成の権限

権限名	説明	必要とするオブジェクト
仮想マシン.構成.既存ディスクの追加	既存の仮想ディスクを仮想マシンに追加できるようにします。	仮想マシン
仮想マシン.構成.新規ディスクの追加	仮想マシンに追加する仮想ディスクを新規作成できるようにします。	仮想マシン
仮想マシン.構成.デバイスの追加または削除	ディスク以外のデバイスを追加または削除できるようにします。	仮想マシン
仮想マシン.構成.詳細	仮想マシンの構成ファイルの詳細パラメータを追加または変更できるようにします。	仮想マシン
仮想マシン.構成.CPU カウン トの変更	仮想 CPU 数を変更できるようにします。	仮想マシン
仮想マシン.構成.リソースの変 更	特定のリソース プールで一連の仮想マシン ノードのリソース構成を変更できるようにします。	仮想マシン
仮想マシン.構成.managedBy の構成	エクステンションまたはソリューションが、そのエクステンションまたはソリューションが管理するものとして仮想マシンにマークを付けられるようにします。	仮想マシン
仮想マシン.構成.ディスク変更 の追跡	仮想マシンのディスクのトラッキング変更を有効または無効にできるようにします。	仮想マシン
仮想マシン.構成.ディスク リ ース	仮想マシンのディスク リース操作を行えるようにします。	仮想マシン
仮想マシン.構成.接続設定の表 示	仮想マシンのリモート コンソール オプションの構成を可能にします。	仮想マシン
仮想.構成.仮想ディスクの拡張	仮想ディスクのサイズを拡張できるようにします。	仮想マシン
仮想マシン.構成.ホストの USB デバイス	ホスト ベースの USB デバイスを仮想マシンに接続できるようにします。	仮想マシン
仮想マシン.構成.メモリ	仮想マシンに割り当てられているメモリのサイズを調整できるようにします。	仮想マシン
仮想マシン.構成.デバイス設定 の変更	既存のデバイスのプロパティを変更できるようにします。	仮想マシン
仮想マシン.構成.Fault Tolerance の互換性のクエリ	仮想マシンに Fault Tolerance との互換性があるかどうかを確認できるようにします。	仮想マシン

表 11-29. 仮想マシンの構成の権限（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.構成.所有していないファイルのクエリ	所有していないファイルを照会できるようにします。	仮想マシン
仮想マシン.構成.Raw デバイス	Raw ディスク マッピングや SCSI パススルー デバイスを追加または削除できるようにします。 このパラメータを設定すると、接続状態を含めて、Raw デバイスを変更する権限がすべてオーバーライドされます。	仮想マシン
仮想マシン.構成.バスからの再ロード	仮想マシンの ID を維持しながら、仮想マシンの構成バスを変更できるようにします。VMware vCenter Site Recovery Manager などのソリューションは、この操作を使用し、フェイルオーバーおよびフェイルバック時に仮想マシンの ID を維持します。	仮想マシン
仮想マシン.構成.ディスクの削除	仮想ディスク デバイスを削除できるようにします。	仮想マシン
仮想マシン.構成.名前の変更	仮想マシンの名前を変更するか、仮想マシンに関連する注釈を変更できるようにします。	仮想マシン
仮想マシン.構成.ゲスト情報のリセット	仮想マシンのゲスト OS 情報を編集できるようにします。	仮想マシン
仮想マシン.構成.注釈の設定	仮想マシンの注釈を追加または編集できるようにします。	仮想マシン
仮想マシン.構成.設定	仮想マシンの標準設定を変更できるようにします。	仮想マシン
仮想マシン.構成.スワップファイルの配置	仮想マシンのスワップファイル配置ポリシーを変更できるようにします。	仮想マシン
仮想マシン.構成.仮想マシンのロックを解除	仮想マシンを復号化できるようにします。	仮想マシン
仮想マシン.構成.仮想マシンの互換性のアップグレード	仮想マシンの互換性バージョンをアップグレードできるようにします。	仮想マシン

## 仮想マシン ゲストの操作権限

仮想マシン ゲストの操作権限により、仮想マシンのゲスト OS 内部のファイルおよびプログラムと API によって相互作用する機能を制御します。

これらの操作の詳細については、『VMware vSphere API リファレンス』ドキュメントを参照してください。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-30. 仮想マシン ゲストの操作

権限名	説明	適用されるオブジェクト
仮想マシン.ゲスト操作.ゲスト操作のエイリアス変更	仮想マシンのエイリアスの変更を伴う仮想マシン ゲストの操作を許可します。	仮想マシン
仮想マシン.ゲスト操作.ゲスト操作のエイリアス クエリ	仮想マシンのエイリアスの照会を伴う仮想マシン ゲストの操作を許可します。	仮想マシン

表 11-30. 仮想マシン ゲストの操作（続き）

権限名	説明	適用されるオブジェクト
仮想マシン.ゲスト操作.ゲスト操作の変更	仮想マシンへのファイルの転送など、仮想マシン内のゲスト OS への変更を伴う仮想マシンゲストの操作を可能にします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	仮想マシン
仮想マシン.ゲスト操作.ゲスト操作のプログラム実行	仮想マシン内でのプログラムの実行を伴う仮想マシン ゲストの操作を可能にします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	仮想マシン
仮想マシン.ゲスト操作.ゲスト操作のクエリ	ゲスト OS 内でのファイルの一覧表示など、ゲスト OS への照会を伴う仮想マシン ゲストの操作を可能にします。 この権限に関連する vSphere Web Client のユーザー インターフェイス要素はありません。	仮想マシン

## 仮想マシン相互作用の権限

仮想マシン相互作用の権限は、仮想マシンのコンソールとの通信、メディアの構成、電源操作の実行、および VMware Tools のインストールの機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-31. 仮想マシン相互作用

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.質問への回答	仮想マシンの状態遷移の問題またはランタイムエラーを解決できるようにします。	仮想マシン
仮想マシン.相互作用.仮想マシン上でのバックアップ操作	仮想マシン上でバックアップ操作を実行できるようにします。	仮想マシン

表 11-31. 仮想マシン相互作用（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.CD メディアの構成	仮想 DVD/CD-ROM デバイスを構成できるようにします。	仮想マシン
仮想マシン.相互作用.フロッピー メディアの構成	仮想フロッピー デバイスを構成できるようにします。	仮想マシン
仮想マシン.相互作用.コンソールでの相互作用	仮想マシンの仮想マウス、キーボード、画面を操作できるようにします。	仮想マシン
仮想マシン.相互作用.スクリーンショットの作成	仮想マシンのスクリーンショットを作成できるようにします。	仮想マシン
仮想マシン.相互作用.すべてのディスクの最適化	仮想マシンのすべてのディスクを最適化できるようにします。	仮想マシン

表 11-31. 仮想マシン相互作用（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.デバイス接続	仮想マシンの切断可能な仮想デバイスの接続状態を変更できるようにします。	仮想マシン
仮想マシン.相互作用.Fault Tolerance の無効化	Fault Tolerance を使用する仮想マシンのセカンダリ仮想マシンを無効化できるようにします。	仮想マシン
仮想マシン.相互作用.ドラッグ アンド ドロップ	仮想マシンとリモート クライアントの間でファイルをドラッグ アンド ドロップできるようにします。	仮想マシン

表 11-31. 仮想マシン相互作用 （続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.Fault Tolerance の有効化	Fault Tolerance を使用する仮想マシンのセカンダリ仮想マシンを有効化できるようにします。	仮想マシン
仮想マシン.相互作用.VIX API によるゲスト OS 管理	VIX API を介して仮想マシンのオペレーティングシステムを管理できるようにします。	仮想マシン
仮想マシン.相互作用.USB HID スキャン コードの挿入	USB HID スキャンコードを挿入できるようにします。	仮想マシン
仮想マシン.相互作用.一時停止/一時停止の解除	仮想マシンを一時停止または一時停止解除できるようにします。	仮想マシン

表 11-31. 仮想マシン相互作用（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.ワイプまたは圧縮操作の実行	仮想マシンのワイプまたは圧縮操作を実行できるようにします。	仮想マシン
仮想マシン.相互作用.パワーオフ	パワーオン状態の仮想マシンをパワーオフできるようにします。この操作でゲスト OS をパワーダウンできます。	仮想マシン
仮想マシン.相互作用.パワーオン	パワーオフ状態の仮想マシンをパワーオンしたり、サスペンド状態の仮想マシンをレジュームできるようにします。	仮想マシン



表 11-31. 仮想マシン相互作用 （続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.仮想マシン上でのセッション記録	仮想マシン上でのセッションを記録できるようにします。	仮想マシン
仮想マシン.相互作用.仮想マシン上での再生セッション	仮想マシンで記録されたセッションを再生できるようにします。	仮想マシン
仮想マシン.相互作用.リセット	仮想マシンをリセットしたり、ゲスト OS を再起動できるようにします。	仮想マシン
仮想マシン.相互作用.Fault Tolerance の再開	仮想マシンのフォールトトレランスの再開を可能にします。	仮想マシン

表 11-31. 仮想マシン相互作用（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.サスペンド	パワー オン状 態の仮 想マシ ンをサ スペン ドでき るよう にしま す。こ の操作 でゲストがス タンバ イ モー ドに切 り替わ ります。	仮想マシン
仮想マシン.相互作用.Fault Tolerance のサスペンド	仮想マ シンの フォー ルト ト レラン スの中 断を可 能にし ます。	仮想マシン
仮想マシン.相互作用.フェイルオーバーのテスト	セカン ダリの 仮想マ シンを プライ マリの 仮想マ シンに するこ とによ って、 Fault Tolera nce の フェイ ルオー バーを テスト できる ように します。	仮想マシン

表 11-31. 仮想マシン相互作用 （続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.セカンダリ仮想マシンの再起動テスト	Fault Tolerance を使用する仮想マシンのセカンダリ仮想マシンを終了できるようにします。	仮想マシン
仮想マシン.相互作用.Fault Tolerance をオフにする	仮想マシンの Fault Tolerance をオフにできるようにします。	仮想マシン

表 11-31. 仮想マシン相互作用（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.相互作用.Fault Tolerance をオンにする	仮想マシンの Fault Tolerance をオンにできるようにします。	仮想マシン
仮想マシン.相互作用.VMware Tools のインストール	ゲスト OS の CD-ROM として VMware Tools CD インスターをマウントまたはアンマウントできるようにします。	仮想マシン

## 仮想マシンのインベントリ権限

仮想マシンのインベントリ権限は、仮想マシンの追加、移動、および削除を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダレベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-32. 仮想マシンのインベントリ権限

権限名	説明	必要とするオブジェクト
仮想マシン.インベントリ.既存のものから作成	クローン作成やテンプレートからデプロイすることによって、既存の仮想マシンやテンプレートに基づいた仮想マシンを作成できるようにします。	クラスタ、ホスト、仮想マシン フォルダ
仮想マシン.インベントリ.新規作成	仮想マシンを作成し、その実行用にリソースを割り当てることができるようにします。	クラスタ、ホスト、仮想マシン フォルダ
仮想マシン.インベントリ.移動	階層内で仮想マシンを移動できるようにします。移動元と移動先の両方に権限が必要です。	仮想マシン

表 11-32. 仮想マシンのインベントリ権限（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.インベントリ.登録	既存の仮想マシンを、vCenter Server またはホスト インベントリに追加できるようにします。	クラスタ、ホスト、仮想マシン フォルダ
仮想マシン.インベントリ.削除	仮想マシンを削除できるようにします。削除すると、仮想マシンの基礎となるファイルがディスクから削除されます。  この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	仮想マシン
仮想マシン.インベントリ.登録解除	仮想マシンを vCenter Server またはホスト インベントリから登録解除できるようにします。  この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	仮想マシン

## 仮想マシンのプロビジョニングの権限

仮想マシンのプロビジョニングの権限は、仮想マシンのデプロイおよびカスタマイズに関するアクティビティを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-33. 仮想マシンのプロビジョニングの権限

権限名	説明	必要とするオブジェクト
仮想マシン.プロビジョニング.ディスク アクセスの許可	読み取りおよび書き込みのランダム アクセス用に仮想マシン上のディスクを開けるようにします。多くの場合、リモート ディスクのマウントに使用します。	仮想マシン
仮想マシン.プロビジョニング.読み取り専用ディスク アクセスの許可	読み取りのランダム アクセス用に仮想マシン上のディスクを開けるようにします。多くの場合、リモート ディスクのマウントに使用します。	仮想マシン
仮想マシン.プロビジョニング.仮想マシンのダウンロードの許可	仮想マシンに関連するファイル（vmx、ディスク、ログ、nvram など）の操作を読み取れるようにします。	ルート ホストまたは vCenter Server
仮想マシン.プロビジョニング.仮想マシン ファイルのアップロードの許可	仮想マシンに関連するファイル（vmx、ディスク、ログ、nvram など）への書き込み操作を可能にします。	ルート ホストまたは vCenter Server
仮想マシン.プロビジョニング.テンプレートのクローン作成	テンプレートのクローンを作成できるようにします。	テンプレート
仮想マシン.プロビジョニング.仮想マシンのクローン作成	既存の仮想マシンのクローン作成と、リソースの割り当てを行えるようにします。	仮想マシン
仮想マシン.プロビジョニング.仮想マシンからのテンプレートの作成	仮想マシンから新規テンプレートを作成できるようにします。	仮想マシン
仮想マシン.プロビジョニング.カスタマイズ	仮想マシンを移動せずに仮想マシンのゲスト OS をカスタマイズできるようにします。	仮想マシン

表 11-33. 仮想マシンのプロビジョニングの権限（続き）

権限名	説明	必要とするオブジェクト
仮想マシン.プロビジョニング.テンプレートのデプロイ	テンプレートから仮想マシンをデプロイできるようにします。	テンプレート
仮想マシン.プロビジョニング.テンプレートとしてマークを付ける	既存のパワーオフ状態の仮想マシンをテンプレートとしてマーキングできるようにします。	仮想マシン
仮想マシン.プロビジョニング.仮想マシンとしてマークを付ける	既存のテンプレートを仮想マシンとしてマーキングできるようにします。	テンプレート
仮想マシン.プロビジョニング.カスタマイズ仕様の変更	カスタマイズ仕様を作成、変更、削除できるようにします。	ルート vCenter Server
仮想マシン.プロビジョニング.ディスクの昇格	仮想マシンのディスクを昇格できるようにします。	仮想マシン
仮想マシン.プロビジョニング.カスタマイズ仕様の読み取り	カスタマイズ仕様を読み取れるようにします。	仮想マシン

## 仮想マシンのサービス構成権限

仮想マシンのサービス構成権限により、サービス構成で監視および管理タスクを実行できるユーザーを制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

**注：** vSphere 6.0 では、vSphere Web Client を使用してこの権限を割り当てまたは削除しないでください。

表 11-34. 仮想マシンのサービス構成権限

権限名	説明
仮想マシン.サービス構成.通知の許可	サービス ステータスに関する通知を生成および使用できるようにします。
仮想マシン.サービス構成.グローバル イベント通知のポーリングの許可	通知が存在するかどうか照会できるようにします。
仮想マシン.サービス構成.サービス構成の管理	仮想マシンのサービスを作成、変更、および削除できるようにします。
仮想マシン.サービス構成.サービス構成の変更	既存の仮想マシンのサービス構成を変更できるようにします。
仮想マシン.サービス構成.サービス構成の照会	仮想マシンのサービスのリストを取得できるようにします。
仮想マシン.サービス構成.サービス構成の読み取り	既存の仮想マシンのサービス構成を取得できるようにします。

## 仮想マシンのスナップショット管理の権限

仮想マシンのスナップショット管理の権限は、スナップショットの作成、削除、名前変更、復元の機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-35. 仮想マシンの状態の権限

権限名	説明	必要とするオブジェクト
仮想マシン.スナップショット管理.スナップショットの作成	仮想マシンの現在の状態からスナップショットを作成できるようにします。	仮想マシン
仮想マシン.スナップショット管理.スナップショットの削除	スナップショット履歴からスナップショットを削除できるようにします。	仮想マシン
仮想マシン.スナップショット管理.スナップショット名の変更	スナップショットの名前や説明を新しく変更できるようにします。	仮想マシン
仮想マシン.スナップショット管理.スナップショットまで戻る	仮想マシンを特定のスナップショットの状態に設定できるようにします。	仮想マシン

## 仮想マシンの vSphere Replication 権限

仮想マシンの vSphere レプリケーション権限により、仮想マシンの VMware vCenter Site Recovery Manager™ を使用してレプリケーションの使用を管理します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-36. 仮想マシン vSphere レプリケーション

権限名	説明	必要とするオブジェクト
仮想マシン.vSphere Replication.レプリケーションの構成	仮想マシンのレプリケーションを構成できるようにします。	仮想マシン
仮想マシン.vSphere Replication.レプリケーションの管理	完全な同期、オンライン同期、またはオフライン同期をレプリケーション上で起動できるようにします。	仮想マシン
仮想マシン.vSphere Replication.レプリケーションの監視	レプリケーションを監視できるようにします。	仮想マシン

## dvPort グループの権限

分散仮想ポート グループの権限は、分散仮想ポート グループの作成、削除、および変更機能を制御します。

この表では、分散仮想ポート グループの作成および構成に必要な権限について説明します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-37. 分散仮想ポート グループの権限

権限名	説明	必要とするオブジェクト
dvPort グループ.作成	分散仮想ポート グループを作成できるようにします。	仮想ポート グループ
dvPort グループ.削除	分散仮想ポート グループを削除できるようにします。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	仮想ポート グループ
dvPort グループ.変更	分散仮想ポート グループ構成を変更できるようにします。	仮想ポート グループ
dvPort グループ.ポリシー操作	分散仮想ポート グループのポリシーを設定できるようにします。	仮想ポート グループ
dvPort グループ.スコープ操作	分散仮想ポート グループの範囲を設定できるようにします。	仮想ポート グループ

## vApp 権限

vApp 権限は、vApp のデプロイと構成関連の操作を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-38. vApp 権限

権限名	説明	必要とするオブジェクト
vApp.仮想マシンの追加	vApp に仮想マシンを追加できます。	vApp
vApp.リソース プールの割り当て	リソース プールを vApp に割り当てることができます。	vApp
vApp.vApp の割り当て	vApp を別の vApp に割り当てることができます。	vApp
vApp.クローン作成	vApp のクローンを作成できます。	vApp
vApp.作成	vApp の作成ができます。	vApp
vApp.削除	vApp の削除ができます。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	vApp
vApp.エクスポート	vSphere から vApp をエクスポートできます。	vApp
vApp.インポート	vSphere に vApp をインポートできます。	vApp
vApp.移動	vApp をインベントリの新しい場所に移動できます。	vApp
vApp.パワーオフ	vApp をパワーオフにできます。	vApp
vApp.パワーオン	vApp をパワーオンにできます。	vApp



表 11-38. vApp 権限 (続き)

権限名	説明	必要とするオブジェクト
vApp.名前の変更	vApp の名前を変更できます。	vApp
vApp.サスペンド	vApp のサスペンドができます。	vApp
vApp.登録解除	vApp の登録解除ができます。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	vApp
vApp.OVF 環境の表示	vApp 内でパワーオンされている仮想マシンの OVF 環境を表示できます。	vApp
vApp.vApp アプリケーションの構成	製品情報やプロパティなど、vApp の内部構造を変更できます。	vApp
vApp.vApp インスタンスの構成	ポリシーなど、vApp のインスタンス構成を変更できます。	vApp
vApp.vApp managedBy 構成	エクステンションまたはソリューションが、そのエクステンションまたはソリューションが管理するものとして vApp にマークを付けられるようにします。 この権限に関連する vSphere Web Client のユーザーインターフェイス要素はありません。	vApp
vApp.vApp リソースの構成	vApp のリソース構成を変更できます。 この操作の実行を許可されるためには、オブジェクトとその親オブジェクトの両方でユーザーまたはグループにこの権限が割り当てられている必要があります。	vApp

## vService の権限

vService 権限は、仮想マシンおよび vApps に対する vService 依存関係の作成、構成、および更新のための機能を制御します。

この権限は、階層内の異なるレベルで設定できます。たとえば、フォルダ レベルで権限を設定した場合、その権限をフォルダ内の 1 つ以上のオブジェクトに伝達できます。[必要とするオブジェクト] 列に示されるオブジェクトには、直接または継承のいずれか方法で権限が設定されている必要があります。

表 11-39. vService

権限名	説明	必要とするオブジェクト
vService.依存関係の作成	仮想マシンまたは vApp から vService 依存関係を作成できるようにします。	vApp および仮想マシン
vService.依存関係の破棄	仮想マシンまたは vApp から vService 依存関係を削除できるようにします。	vApp および仮想マシン
vService.依存関係構成の再構成	プロバイダまたはバインドを更新するために依存関係を再構成できるようにします。	vApp および仮想マシン
vService.依存関係の更新	名前または説明を構成するために依存関係を更新できるようにします。	vApp および仮想マシン