vSphere のセキュリティ

Update 3
変更日：2022 年 11 月 23 日
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

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

ヴイ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

目次

vSphere セキュリティについて

vSphere のセキュリティでは、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。

VMware では、多様性の受け入れを尊重しています。お客様、パートナー企業、社内コミュニティとともにこの原則を推進することを目的として、多様性に配慮した言葉遣いでコンテンツを作成します。

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 のセキュリティ の概要

トピック	コンテンツの概要
権限とユーザーの管理	■ 権限モデル（ロール、グループ、オブジェクト） ■ カスタム ロールの作成 ■ 権限の設定 ■ グローバル権限の管理
ホストのセキュリティ機能	■ 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 ■ ホストのスマート カード認証 ■ vSphere Authentication Proxy ■ UEFI セキュア ブート ■ Trusted Platform Module (TPM) ■ VMware® vSphere Trust Authority™ ■ セキュアな ESXi 構成と構成のシーリング
仮想マシンの暗号化	■ VMware vSphere® Native Key Provider™。 ■ 仮想マシンの暗号化機能 ■ KMS の設定 ■ 仮想マシンの暗号化と復号化 ■ トラブルシューティングとベスト プラクティス
ゲスト OS のセキュリティ	■ 仮想 Trusted Platform Module (vTPM) ■ 仮想化ベースのセキュリティ (VBS)
TLS プロトコル構成の管理	コマンドライン ユーティリティを使用した TLS プロトコル構成の変更
セキュリティのベスト プラクティスおよび強化	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 ■ vCenter Server のセキュリティ ■ ホストのセキュリティ ■ 仮想マシンのセキュリティ ■ ネットワークのセキュリティ
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

付属ドキュメントの『vSphere の認証』では、vCenter Single Sign-On を使用した認証の管理や vSphere 環境での証明書の管理などに認証サービスを使用する方法について説明します。

これらのドキュメントに加え、VMware では vSphere のリリースごとに 『vSphere セキュリティ設定ガイド』（旧称 『セキュリティ強化ガイド』）を公開しており、https://core.vmware.com/security で参照できます。「vSphere Security Configuration Guide」 には、ユーザーが設定可能な、またはユーザーによる設定が必要なセキュリティ設定に関するガイドラインや、VMware 提供のセキュリティ設定をデフォルトで維持するかどうかをユーザーが確認するためのガイドラインが含まれます。

Platform Services Controller に対する変更点

vSphere 7.0 以降、新しい vCenter Server をデプロイする場合、または vCenter Server 7.0 にアップグレードする場合は、vCenter Server の実行用に最適化された事前構成済みの仮想マシンである、vCenter Server アプライアンスを使用する必要があります。新しい vCenter Server では、認証、証明書管理、タグ、ライセンスなどの機能とワークフローを保持するすべての Platform Services Controller サービスが提供されます。外部 Platform Services Controller をデプロイして使用する必要がなくなりました。これらの操作を行うこともできません。すべての Platform Services Controller サービスは vCenter Server に統合され、デプロイと管理が簡素化されました。

これらのサービスは vCenter Server に属するようになったため、Platform Services Controller の一部としては記載していません。vSphere 7.0 では、vSphere の認証 ドキュメントが Platform Services Controller の管理 ドキュメントに置き換わっています。新しいドキュメントには、認証と証明書の管理に関する詳細が記載されています。vCenter Server Appliance を使用して、既存の外部 Platform Services Controller を使用する vSphere 6.5 および 6.7 環境から vSphere 7.0 にアップグレードまたは移行する方法については、『vSphere のアップグレード』を参照してください。

対象読者

この情報は、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想定しています。

認証

VMware は、Common Criteria 認証が完了した VMware 製品のリストを公開しています。特定の VMware 製品バージョンが認証されているかどうかを確認するには、「Common Criteria Evaluation and Validation」Web ページ (https://www.vmware.com/security/certifications/common-criteria.html) を参照してください。

更新情報

『vSphere のセキュリティ』ドキュメントは、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 のセキュリティ』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 11 月 23 日	■ vCenter Server システム ロールへのマイナー更新。 ■ vSphere Native Key Provider に関する情報を追加してキーの永続性の概要および ESXi ホストでのキーの永続性の有効化および無効化を更新しました。 ■ VLAN のセキュリティ強化へのマイナー更新。
2022 年 10 月 13 日	■ ESXi 監査レコードの管理へのマイナー更新。 ■ vSphere Native Key Provider の更新の誤記を修正。 ■ 仮想化ベース セキュリティのベスト プラクティス、仮想マシンでの仮想化ベースのセキュリティの有効化、および 既存の仮想マシンでの仮想化ベース セキュリティの有効化 に対するマイナー更新。 ■ `vifs` コマンドに対する参照を削除しました。詳細については、VMware のナレッジベースの記事 (https://kb.vmware.com/article/78473) を参照してください。
2022 年 8 月 22 日	■ ESXi 証明書の更新へのマイナー更新。 ■ vSphere Native Key Provider の削除へのマイナー更新。 ■ 信頼機関クラスタでのキー プロバイダの作成の例を修正しました。 ■ vCenter Server 管理対象オブジェクト ブラウザ (MOB) を使用するように API を使用したホスト暗号化モードの無効化を記述し直しました。 ■ VMware vSphere Lifecycle Manager 権限に関する複数のトピックにマイナー更新を行いました。
2022 年 7 月 28 日	■ ESXi 証明書署名要求の要件へのマイナー更新。 ■ 仮想 Trusted Platform Module の概要へのマイナー更新。 ■ MAC アドレス変更へのマイナー更新。 ■ 複数のトピックを更新して、URL を受け入れる VMware vSphere Lifecycle Manager API の使用権限の割り当て先を管理者または信頼できるユーザーに限定する必要があることを明記しました。
2022 年 7 月 12 日	■ ユーザー検証設定の変更へのマイナー更新。 ■ ESXi 証明書の更新へのマイナー更新。 ■ Fault Tolerance 暗号化の有効化へのマイナー更新。 ■ セキュアな ESXi 構成の execInstalledOnly の適用の有効化/無効化 の ESXCLI コマンドのフォーマットに関する問題を修正しました。 ■ 未使用の表示機能の無効化へのマイナー更新。 ■ 非公開機能の無効化 から、現在は TRUE に設定されているパラメータを削除しました。 ■ 暗号化ストレージ ポリシーの作成内の手順を修正しました。

リビジョン	説明
2022 年 6 月 15 日	■ 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に、vCenter Server と暗号化された通信に関する情報を追加しました。 ■ 権限の階層的な継承に、vSphere Distributed Switch での権限の割り当てに関する情報を追加しました。 ■ ESXi ホストの UEFI セキュア ブートへのマイナー更新。 ■ 仮想マシンの暗号化のベスト プラクティスに、暗号化の考慮事項に関する情報を追加しました。 ■ vSphere Native Key Provider の概要へのマイナー更新。 ■ API を使用したホスト暗号化モードの無効化に、`HostCryptoState` に関する情報を追加しました。 ■ 仮想 Trusted Platform Module を使用した仮想マシンの作成および仮想 Trusted Platform Module の既存の仮想マシンでの有効化に、必須の権限、暗号化操作.移行を追加しました。この権限により、DRS が別のホストで仮想マシンを起動した場合に仮想マシンをパワーオンにできます。 ■ 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へのマイナー更新。 ■ ESXi ホストでの TLS バージョンの有効化または無効化へのマイナー更新。 ■ コンテンツ ライブラリの権限に、権限の設定に関する情報を追加しました。 ■ vSphere タギングの権限の誤記を修正。
2022 年 4 月 29 日	■ ESXi 監査レコードの管理では、`auditLogReader` プログラムは vSphere 7.0 Update 3d の時点で `viewAudit` プログラムに置き換えられます。 ■ セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化とセキュアな ESXi 構成の execInstalledOnly の適用の有効化/無効化へのマイナー更新。 ■ vSphere 仮想マシンの暗号化で環境を保護する方法へのマイナー更新。 ■ キーの永続性の概要、vSphere Native Key Provider のバックアップ、および ESXi ホストでのキーの永続性の有効化および無効化の vSphere Native Key Provider とキー パーシステンスに関する情報を更新しました。 ■ vSphere Native Key Provider の概要へのマイナー更新。 ■ vSphere Native Key Provider の更新のコマンドを修正しました。 ■ ファイアウォールを介した ESXi ホストの接続へのマイナー更新。 ■ ストレージ ビュー権限へのマイナー更新。
2022 年 3 月 10 日	■ ホストのアップグレードと証明書へのマイナー更新。 ■ Auto Deploy でのカスタム証明書の使用の手順 4 の不正コマンドを修正しました。 ■ vSphere Client を使用した仮想マシンへの AMD Secure Encrypted Virtualization-Encrypted State の追加、仮想マシンへの AMD Secure Encrypted Virtualization-Encrypted State の追加、vSphere Client を使用した既存の仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の有効化、および既存の仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の有効化の前提条件を更新しました。 ■ 仮想マシンの暗号化の相互運用性へのマイナー更新。 ■ vSphere Native Key Provider の概要を更新し、vSphere Native Key Provider に TPM 2.0 が必要ないことを記載しました。 ■ vSphere Client を使用した信頼済みホストの信頼済みキー プロバイダの構成とコマンドラインを使用した信頼済みホストの信頼済みキー プロバイダの構成で、vSphere Trust Authority キー プロバイダを追加すると、キー プロバイダが使用できるまでに少し時間がかかることを明記しました。 ■ 仮想 Trusted Platform Module を使用した仮想マシンの作成、仮想 Trusted Platform Module の既存の仮想マシンでの有効化、および仮想マシンからの仮想 Trusted Platform Module の削除に必要な権限を追加しました。
2022 年 1 月 19 日	■ vSphere での認可についてへのマイナー更新。 ■ ESXi 証明書とキー ファイルのリストアへのマイナー更新。 ■ スタンドアローン ESXi ホストの場合、ESXi ホストでの TLS バージョンの有効化または無効化 の vCenter Server システムから `reconfigureEsx ESXiHost` コマンドを実行する必要があることを明確にしました。 ■ FIPS を使用する場合の考慮事項ファイルベースのバックアップとリストアに関する情報を使用して vCenter Server を更新しました。

リビジョン	説明
2021 年 12 月 21 日	■ vifs コマンドを使用した SSH 鍵のアップロードの誤記を訂正しました。 ■ TPM シーリング ポリシーの概要へのマイナー更新。 ■ セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化へのマイナー更新。 ■ ESXi ホストの暗号化モードの問題の解決へのマイナー更新。 ■ 暗号化された vSphere vMotion へのマイナー更新。
2021 年 12 月 7 日	■ vSphere キー プロバイダの比較へのマイナー更新。 ■ 拡張リンク モード構成での vSphere Native Key Provider のインポートという新しいトピックを追加しました。 ■ vSphere 信頼機関 のベスト プラクティス、注意事項、相互運用性へのマイナー更新。 ■ vSphere Client を使用した暗号化された仮想マシンの再キー化という新しいトピックを追加しました。 ■ 新しい権限を追加してコンテンツ ライブラリの権限を更新しました。 ■ 新しい権限を追加して vSphere with Tanzu の権限を更新しました。
2021 年 11 月 3 日	■ 仮想ネットワーク レイヤーの保護へのマイナー更新。 ■ セキュアな ESXi 構成の execInstalledOnly の適用の有効化/無効化へのマイナー更新。 ■ 列の表示/非表示の切り替え方法を含むユーザー インターフェイスのマイナーな変更が反映されるように、複数の ESXi ホストの証明書有効期限情報の表示、Virtual Trusted Platform Module 対応の仮想マシンの特定、仮想 Trusted Platform Module デバイス証明書の表示、および VBS 対応仮想マシンの特定を更新しました。 ■ ユーザー インターフェイスに関するマイナーな変更が反映されるように、ESXi ファイアウォール設定の管理と ESXi ホストで許可される IP アドレスの追加を更新しました。 ■ 仮想マシンの暗号化の相互運用性に暗号化関連の情報を追加しました。 ■ 両方のオプションのデフォルトを [承諾] から [拒否] に変更したことが反映されるように、MAC アドレス変更と偽装転送を更新しました。 ■ 仮想マシンのプロビジョニングの権限に記載されている権限を訂正しました。 ■ Single Sign-On 監査イベントへのマイナー更新。
2021 年 10 月 05 日	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、認証、認可、各 ESXi ホストでのファイアウォール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 Server 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。vCenter Server オブジェクト階層では、vCenter Server システム、ESXi ホスト、仮想マシン、ネットワーク オブジェクトやストレージ オブジェクトなど、さまざまなオブジェクトにセキュリティ対策を講じることができます。

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と、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 ホストを保護するため、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。一貫性を維持するには、リファレンス ホストを設定して、このホストのホスト プロファイルにすべてのホストを同期させることができます。また、スクリプトによる管理を実行し、確実にすべてのホストに変更を適用することで、使用環境を保護することもできます。

次のアクションを実施すると、vCenter Server が管理する ESXi ホストの保護を強化できます。背景や詳細については、『Security of the VMware vSphere Hypervisor』のホワイト ペーパーを参照してください。

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、root 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 アクセスを有効にする場合は、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、ホストを管理する権限が必要です。ホスト オブジェクトに対する権限は、ホストを管理する vCenter Server システムから設定します。

特定ユーザーと最小限の権限の使用

デフォルトで、root ユーザーは多くのタスクを実行できます。管理者が root ユーザー アカウントを使用して ESXi ホストにログインすることを許可しないようにしてください。代わりに、vCenter Server から特定の管理者ユーザーを作成し、それらのユーザーに管理者ロールを割り当てます。これらのユーザーに、カスタム ロールを割り当てることもできます。「vCenter Server カスタム ロールの作成」を参照してください。

ホスト上で直接ユーザーを管理している場合は、ロール管理オプションは制限されます。『vSphere の単一ホスト管理：VMware Host Client』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

デフォルトで ESXi ホストのファイアウォール ポートは、対応するサービスを開始するときにのみ開かれます。vSphere 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さまざまなホストが同期されていることが重要です。これを実現するには、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。ホスト プロファイルは、スクリプトによる管理の代替となる機能です。リファレンス 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すべての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『vCenter Server 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 モードでは、ESXi ホストはデフォルトで、vCenter Server を介してのみアクセスできます。厳密なロックダウン モードまたは通常のロックダウン モードを選択できます。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ように例外ユーザーを定義できます。

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、VIB 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せん。

ホストと VIB の許容レベルの管理を参照してください。

ESXi 証明書の管理

VMware Certificate Authority (VMCA) は、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、サードパーティまたはエンタープライズ認証局 (CA) によって署名された証明書で、既存の証明書を置き換えることができます。

ESXi ホストの証明書管理を参照してください。

スマート カード認証の検討

ESXi では、ユーザー名とパスワードの認証の代わりにスマート カード認証の使用がサポートされます。セキュリティ強化のために、スマート カード認証を設定できます。vCenter Server 用に 2 要素認証もサポートされます。ユーザー名およびパスワードによる認証と同時に、スマート カード認証も設定できます。

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 ロックアウトの検討

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。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 回許容されています。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。

注： 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。

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。

スタンドアローン ホストのセキュリティの考慮事項と類似していますが、管理タスクは若干異なります。『vSphere の単一ホスト管理：VMware Host Client』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制限するための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 インスタンスを保護する場合があります。

vCenter Server と暗号化された通信

デフォルト（「out of the box」の状態）、vCenter Server と他の vSphere コンポーネント間のすべてのデータ通信は暗号化されます。状況によっては、環境の構成により、トラフィックの一部が暗号化されない場合があります。たとえば、メール アラートに暗号化されていない SMTP を構成し、監視に暗号化されていない SNMP を構成できます。DNS トラフィックも暗号化されません。vCenter Server は、ポート 80 (TCP) とポート 443 (TCP) で待機します。ポート 443 (TCP) は業界標準の HTTPS（セキュア HTTP）ポートで、保護には TLS 1.2 暗号化を使用します。ポート 80 (TCP) は業界標準の HTTP ポートで、暗号化を使用しません。ポート 80 の目的は、要求をポート 80 から安全なポート 443 にリダイレクトすることです。

すべての vCenter Server のホスト マシンを強化する

vCenter Server 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 Server の証明書モデルについて

VMware Certificate Authority は、デフォルトでは、VMCA 署名付き証明書を持つ各 ESXi ホストおよび環境内の各マシンをプロビジョニングします。会社のポリシーで要求されている場合は、デフォルトの動作を変更できます。詳細については、ドキュメント『vSphere の認証』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。最初にソフトウェアをインストールする際に、vCenter Single Sign-On ドメインの管理者パスワード（デフォルトで administrator@vsphere.local）を指定します。最初は、アイデンティティ ソースとして、このドメインのみ使用できます。フェデレーション認証のために Microsoft Active Directory Federation Services (AD FS) などの外部 ID プロバイダを追加できます。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。これらの ID ソースのいずれかを認証できるユーザーが、オブジェクトを表示したり、タスクを実行したりすることができます（そのような権限がある場合）。詳細については、『vSphere の認証』を参照してください。

名前付き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権限を、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 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、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。

PTP または NTP の設定

環境内の各ノードに PTP または 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刻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 プラクティスに従う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の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 の仮想マシン管理ドキュメント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 コンソールにアクセス可能なユーザーは、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によって、仮想マシンに悪意のある攻撃がが発生する可能性があります。

UEFI セキュア ブートの検討

UEFI ブートを使用するよう仮想マシンを設定できます。オペレーティング システムがセキュア UEFI ブートをサポートしている場合は、このオプションを仮想マシンに対して選択し、セキュリティを強化できます。仮想マシンの UEFI セキュア ブートを有効または無効にするを参照してください。

Carbon Black Cloud Workload の検討

Carbon Black Cloud Workload をインストールして使用することで、リスクの特定、攻撃の防止、異常なアクティビティの検出が可能になります。Carbon Black Cloud プラットフォームに組み込まれた AppDefense 機能により、Carbon Black Cloud Workload は AppDefense の後継製品です。

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 レイヤーに依存して、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、および仮想ネットワーク 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、13 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。管理ネットワークには、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だけがアクセスできるようにします。

ESXi のネットワーク 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。ESXi ホストでは、ファイアウォール ルールを使用すれば、対応するファイアウォールをサービスと関連付け、サービスのステータスに応じてファイアウォールを開閉できます。

また、vCenter Server インスタンス上でポートを明示的に開くこともできます。

vSphere、vSAN を含む VMware 製品でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。VMware 製品別のポート検索、ポートのカスタマイズ リストの作成、およびポート リストの出力または保存を行うことができます。

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 のネットワーク』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 ネットワークを保護するためにどの方法を使用するかは、次のようないくつかの要因によって決まります。

- インストールされているゲスト OS
- 仮想マシンが信頼される環境で運用されるかどうか。

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、強力な防御を実現できます。

13 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 をサポートします。VLAN によって物理ネットワークをセグメント化できます。仮想マシン ネットワークまたはストレージ構成の保護を強化するために、VLAN を使用できます。VLAN を使用すると、同じ物理ネットワーク上の 2 台の仮想マシンは同じ VLAN 上にない限り、相互にパケットを送受信することはできません。

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、アプリケーション 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、仮想ディスクがある 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、Virtual Volumes 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 を使用するように環境を設定できます。会社のポリシーで必要な場合は、相互 CHAP を設定することができます。vSphere Client または CLI を使用して CHAP を設定します。

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。

vSphere 環境のパスワード

vSphere 環境のパスワードの制限、パスワードの有効期限、およびアカウントのロックアウトは、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、特定の要件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 Server 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 Server 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、パスワードの有効期限、およびアカウントのロックアウトは、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。

vCenter Single Sign-On 管理者

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。詳細については、vSphere の認証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 ナレッジベースの記事で検索してください。リセットには、vCenter Server システムへの root アクセスなどその他の権限が必要です。

vCenter Single Sign-On ドメインの他のユーザー

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ドメインのユーザーのパスワードは、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を守る必要があります。詳細については、vSphere の認証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、パスワードの有効期限、およびアカウントのロックアウトは、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 ID ソースがサポートされます。ユーザーは自分のユーザー名を使用して vSphere Client で対応するドメインにログインできます。デフォルト以外のドメインに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。ドメイン パスワード パラメータは、各ドメインに対して適用されます。

vCenter Server 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 アプライアンスは事前に構成された仮想マシンであり、vCenter Server 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 をデプロイするときに、これらのパスワードを指定します。

- root ユーザーのパスワード。
- vCenter Single Sign-On ドメインの管理者のパスワード。デフォルトは administrator@vsphere.local　です。

vCenter Server 管理インターフェイスから、root ユーザーのパスワードの変更と、その他の vCenter Server ローカル ユーザー管理タスクを実行できます。vCenter Server 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

ESXi および vCenter Server は、ベスト プラクティスに従うことで、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。

本書では、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	3 章 ESXi ホストのセキュリティ強化
vCenter Server システム	vCenter Server のセキュリティのベスト プラクティス
仮想マシン	仮想マシンのセキュリティのベスト プラクティス
vSphere のネットワーク	vSphere ネットワークのセキュリティのベスト プラクティス

本書は、セキュアな環境の確保に使用する必要な情報の 1 つに過ぎません。

VMware のセキュリティ 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. VMware セキュリティ リソース (Web)

テクニカル ノート	リソース
安全な構成とハイパーバイザーのセキュリティなど、ESXi および vCenter Server のセキュリティと運用に関する情報を提供します。	https://core.vmware.com/security
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 トピックを中心に説明します。	http://www.vmware.com/go/security
企業セキュリティ対策ポリシー	http://www.vmware.com/support/policies/security_response.html VMware は、お客様がセキュアな環境を維持できるように支援します。セキュリティ上の問題は迅速に解決します。VMware セキュリティ対策ポリシーでは、VMware 製品において起こりうる脆弱性を解決するための取り組みを文書化しています。
サードパーティのソフトウェア サポート ポリシー	http://www.vmware.com/support/policies/ 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、http://www.vmware.com/vmtn/resources/ で ESXi の互換性ガイドを参照してください。 業界には、まだ VMware が検証していない製品や構成が数多く提供されています。互換性ガイドに製品や構成が掲載されていない場合、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	https://core.vmware.com/compliance
異なるバージョンの vSphere コンポーネントの、CCEVS や FIPS などのセキュリティ認証と検証についての情報。	https://www.vmware.com/support/support-resources/certifications.html

表 1-2. VMware セキュリティ リソース (Web) （続き）

テクニカル ノート	リソース
vSphere などの VMware 製品の各バージョンのセキュリティ構成ガイド（旧称「セキュリティ強化ガイド」）。	https://core.vmware.com/security
『Security of the VMware vSphere Hypervisor』ホワイト ペーパー	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere のアクセス許可とユーザー管理タスク

2

アクセスは認証と認可によって制御されます。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 コンポーネントにログインできるかどうかを全面的に決定します。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 のユーザー権限モデルおよびユーザー管理タスクの実行方法について説明します。

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。

初期状態で vCenter Server システムにログオンできるのは、vCenter Single Sign-On ドメイン管理者だけです。デフォルト ドメインは vsphere.local で、デフォルトの管理者は administrator@vsphere.local です。デフォルトのドメインは、vSphere のインストール中に変更できます。

管理者は、次の手順を実行できます。

1 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。『vSphere の認証』ドキュメント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またはグループに割り当てます。

 (vSphere Client を使用したロールと権限の割り当て)

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

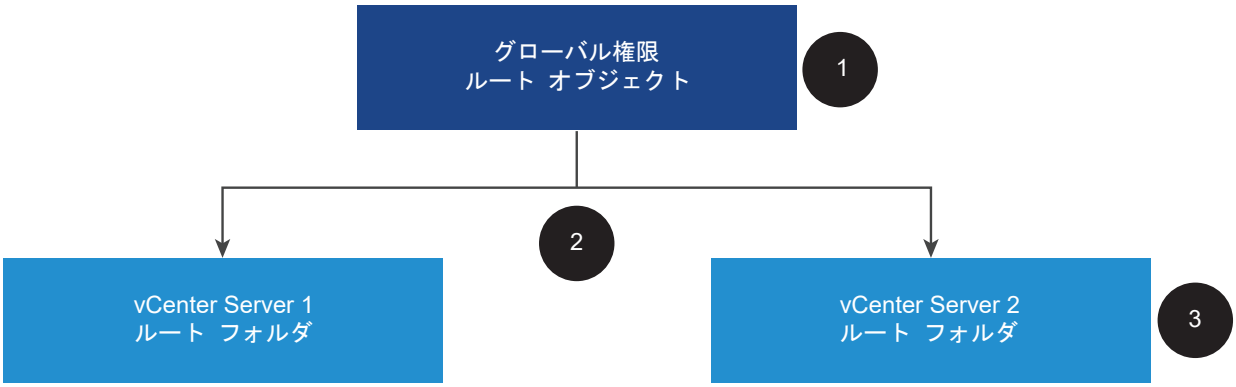
vSphere では、複数のモデルがサポートされており、ユーザーがタスクを実行できるかどうかを決定できます。vCenter Single Sign-On グループのメンバーシップを使用して、ユーザーが実行できる機能を決定します。オブジェクトでのロールまたはグローバル権限によって、他のタスクを実行てきるかどうかが決定されます。

認可の概要

vSphere では、権限を持つユーザーが他のユーザーにタスクを実行する権限を付与できます。グローバル権限またはローカルの vCenter Server 権限を使用して、それぞれの vCenter Server インスタンスに対して他のユーザーを認証できます。

次の図は、グローバル権限とローカル権限の動作を示しています。

図 2-1. グローバル権限とローカル権限



図の中の要素

1 ルート オブジェクト レベルでグローバル権限を割り当て、[子へ伝達] を選択します。

2 vCenter Server は、環境内の vCenter Server 1 および vCenter Server 2 のオブジェクト階層に権限を伝達します。

3 vCenter Server 2 のルート フォルダに対するローカル権限は、グローバル権限をオーバーライドします。

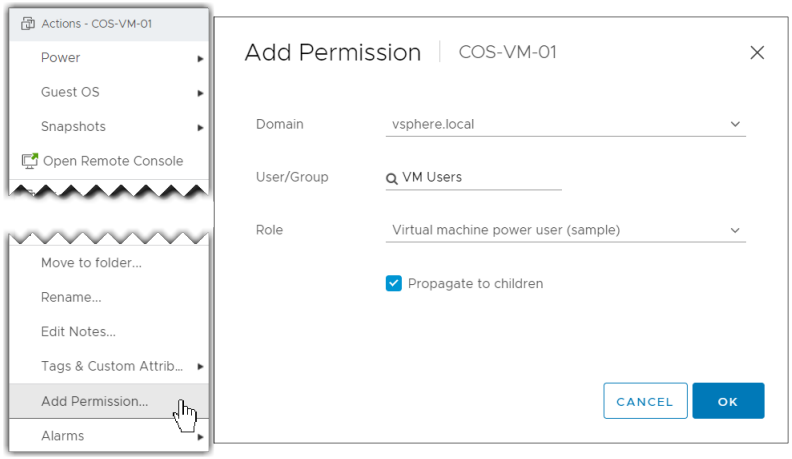
vCenter Server のアクセス許可

vCenter Server システムの権限モデルは、オブジェクト階層内のオブジェクトに権限を割り当てることによって成立しています。ユーザーは次の方法で権限を取得します。

- ユーザーの特定の権限、またはユーザーがメンバーであるグループから
- オブジェクトに対する権限または親オブジェクトからの権限の継承

各権限によって、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。権限を追加するには、vSphere Client を使用します。たとえば、仮想マシンを右クリックし、[権限の追加] を選択し、ダイアログ ボックスに入力してユーザーのグループにロールを割り当てできます。そのロールによって、仮想マシン上の対応する権限がユーザーに付与されます。

図 2-2. vSphere Client を使用した仮想マシンへのアクセス許可の追加



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、デプロイ内ソリューション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。つまり、グローバル権限は、ソリューション インベントリ階層にまたがるグローバル ルート オブジェクトに適用されます。（ソリューションには vCenter Server、vRealize Orchestrator などが含まれます）グローバル権限は、タグやコンテンツ ライブラリなどのグローバル オブジェクトにも適用されます。たとえば、2 つのソリューションで構成される vCenter Server デプロイと vRealize Orchestrator を検討します。グローバル権限を使用して、読み取り専用権限を持つユーザーのグループにロールを割り当て、vCenter Server オブジェクト階層と vRealize Orchestrator オブジェクト階層の両方のすべてのオブジェクトに割り当てできます。

グローバル権限は、vCenter Single Sign-On ドメイン全体にレプリケートされます（デフォルトでは vsphere.local）。グローバル権限は、vCenter Single Sign-On ドメイン グループを介して管理されるサービスの認可を提供しません。グローバル権限を参照してください。

vCenter Single Sign-On グループにおけるグループ メンバーシップ

vCenter Single Sign-On ドメイン グループのメンバーは、特定の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 の認証』ドキュメント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 の単一ホスト管理：VMware Host Client』ドキュメントを参照してください。

管理対象ホストの場合、vCenter Server インベントリ内の ESXi ホスト オブジェクトにロールを割り当てます。

オブジェクトレベルの権限モデルについて理解する

ユーザーまたはグループが vCenter Server オブジェクトに対してタスクを実行することを許可するには、オブジェクトに対する権限を使用します。プログラムの観点から、ユーザーが操作を実行しようとすると、API メソッドが実行されます。vCenter Server は、そのメソッドのアクセス許可をチェックして、ユーザーが操作の実行を許可されているかどうかを確認します。たとえば、ユーザーがホストを追加しようとすると、`AddStandaloneHost_Task` メソッドが呼び出されます。このメソッドでは、ユーザーのロールに Host.Inventory.Add standalone host 権限が必要です。この権限がチェックで見つからない場合、ユーザーはホストを追加する権限を拒否されます。

以下の概念が重要です。

権限

vCenter Server オブジェクト階層内のオブジェクトは、それぞれが関連する権限を持ちます。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。権限は子オブジェクトへ伝達できます。

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ユーザー グループに対してのみ権限を付与することができます。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には、vCenter Single Sign-On の認証に使用する ID ソースが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。

権限

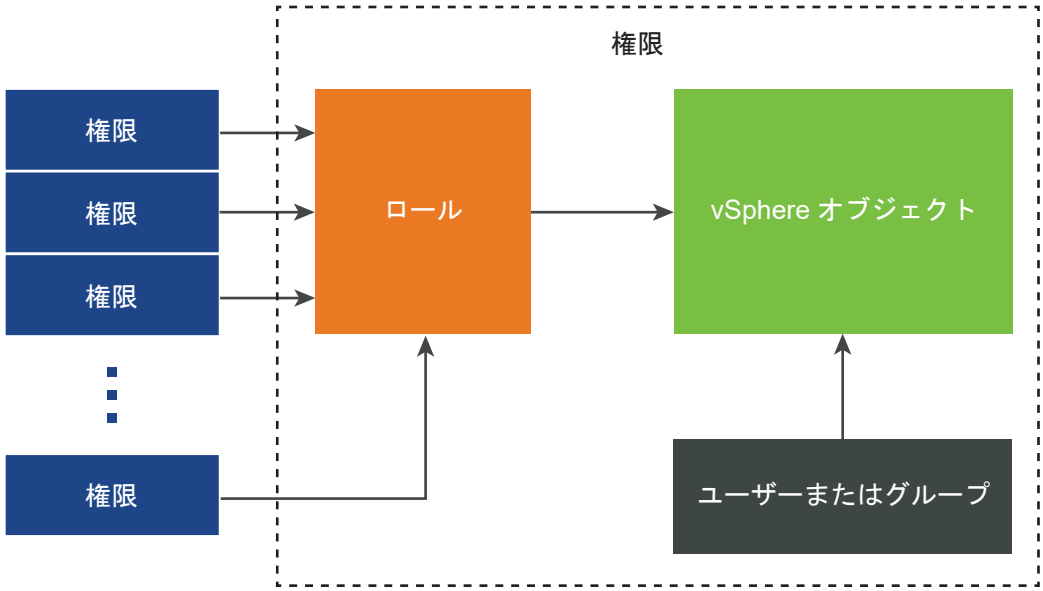
権限とは、細かな設定が可能なアクセス制御です。これらの権限をロールとしてグループ化することで、ユーザーやグループにマッピングできるようになります。

ロール

ロールは権限のセットです。ロールにより、ユーザーが実行する標準的なタスク ベースのオブジェクトに、権限を割り当てることができます。管理者などのシステム ロールは vCenter Server で事前に定義されており、変更できません。vCenter Server には、リソース プール管理者など、変更可能なデフォルトのサンプル ロールもいくつか提供されています。カスタム ロールは、一から作成するか、サンプル ロールをクローン作成し、変更することで作成できます。vCenter Server カスタム ロールの作成を参照してください。

次の図は、権限とロールから権限が構築され、vSphere オブジェクトのユーザーまたはグループに割り当てられる方法を示しています。

図 2-3. vSphere の権限



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 権限を適用するオブジェクトを、vCenter Server オブジェクト階層の中で選択します。

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個別の権限、または権限のセットであるロールを選択します。

デフォルトでは、[子へ伝達] は選択されていません。選択したオブジェクトとその子オブジェクトで選択したロールを使用するには、グループまたはユーザーのチェックボックスを選択する必要があります。

vCenter Server は、頻繁に使用される権限セットを組み合わせたサンプル ロールを提供します。また、一連のロールを組み合わせて、カスタム ロールを作成することもできます。

アクセス許可をソース 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ことが必要な場合があります。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。

次の情報を参照してください。

目的の情報	参照先
カスタム ロールの作成	vCenter Server カスタム ロールの作成
すべての権限と、各権限を適用できるオブジェクト	16 章 事前定義された権限
さまざまなオブジェクトでさまざまなタスク向けに必要な権限のセット	一般的なタスクに必要な権限

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。 ESXi ホストの権限の割り当てを参照してください。

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、いくつかのオブジェクトに対するロールを Smith というユーザーに割り当てたとします。ドメイン管理者が名前を Smith2 に変更します。ホストでは、Smith は存在しなくなったと判断され、このユーザーに関する権限は次回の検証時に vSphere オブジェクトから削除されます。

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、次回の検証時に、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。次回の検証前に 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 で置換されます。

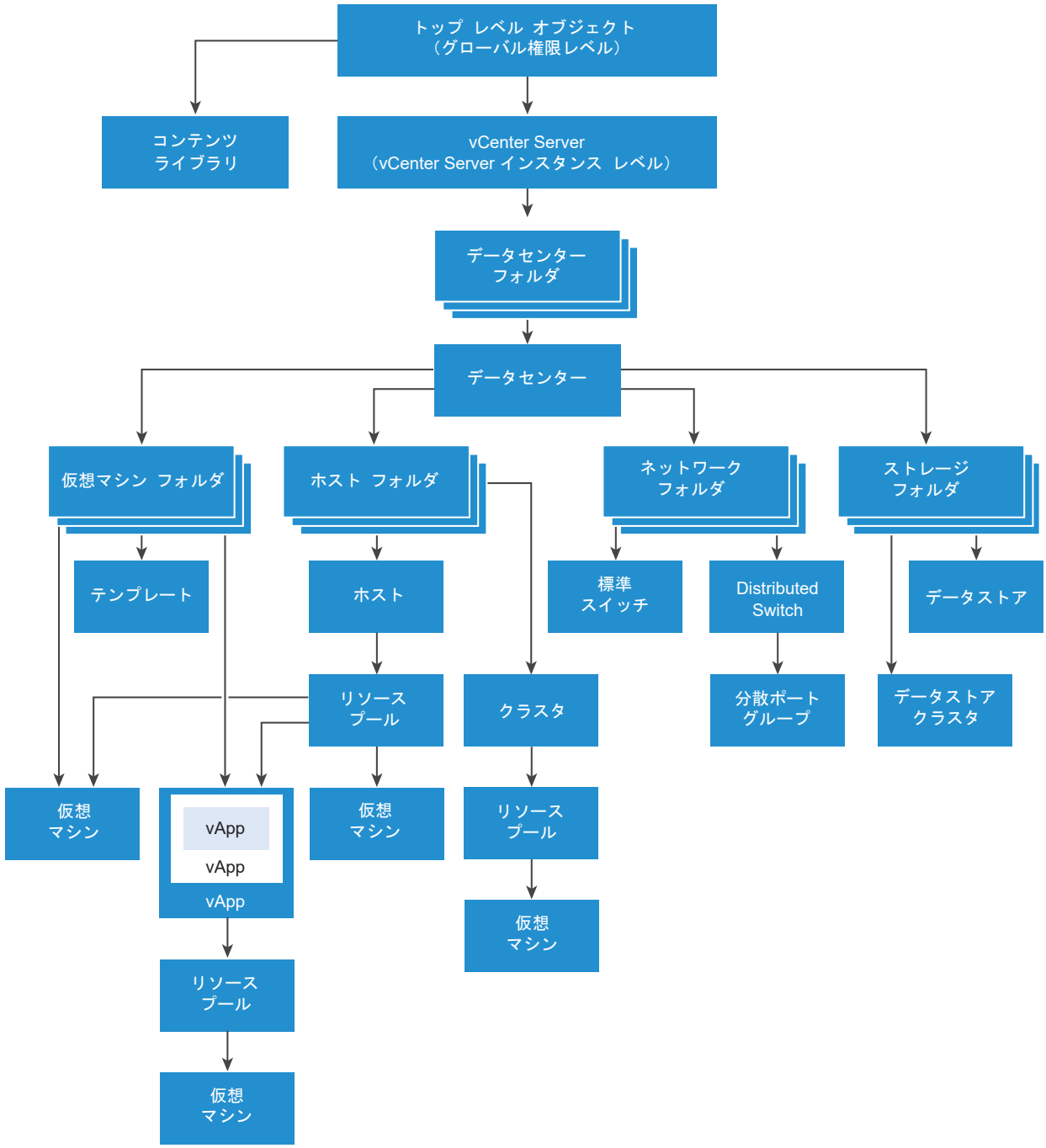
権限の階層的な継承

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 2-4. vSphere のインベントリ階層



この図について：

- 仮想マシン、ホスト、ネットワーク、およびストレージ フォルダに直接権限を設定することはできません。つまり、これらのフォルダはコンテナとして機能し、ユーザーには表示されません。
- 標準スイッチに権限を設定することはできません。

注： vSphere Distributed Switch (VDS) の子に権限を設定して伝達できるようにするには、データセンターに作成されたネットワーク フォルダにスイッチ オブジェクトが存在する必要があります。

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、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

管理対象エンティティは、次の vSphere オブジェクトを参照します。管理対象エンティティでは、エンティティ タイプに応じて特定の操作を実行できます。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。vSphere オブジェクト、プロパティ、方法の詳細については、vSphere API のドキュメントを参照してください。

- 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、ある権限で、GroupAdmin にあるオブジェクトの管理者ロールを割り当てるように指定し、別の権限で、GroupVMAdmin に同じオブジェクトの仮想マシン管理者ロールを割り当てるように指定できます。ただし、GroupVMAdmin グループに、このオブジェクトの同じ GroupVMAdmin に別の権限を割り当てることはできません。

親の伝達プロパティが true に設定されている場合、子オブジェクトはその親の権限を継承します。子オブジェクトに直接設定された権限は、親オブジェクトの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。

同じオブジェクトに複数のグループ ロールが定義されており、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。

- オブジェクトに対し、ユーザーの権限が直接定義されていない。この場合は、ユーザーは所属するグループがオブジェクトに対して持っている権限の集合を取得します。
- オブジェクトに対し、ユーザーの権限が直接定義されている。この場合は、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：複数のグループからの権限の継承

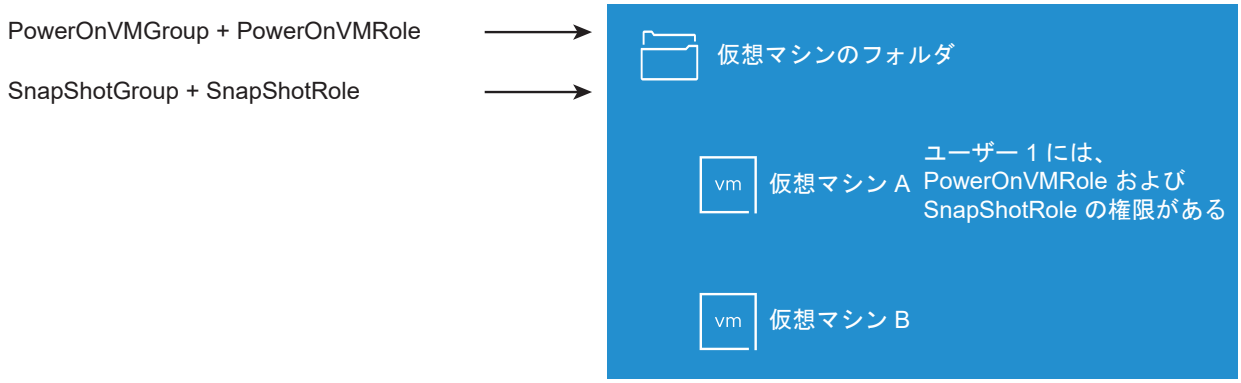
この例では、親オブジェクトで権限が付与されているグループから、オブジェクトが複数の権限を継承する方法を示します。

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。

- PowerOnVMRole は、仮想マシンをパワーオンできる。
- SnapShotRole は、仮想マシンのスナップショットを作成できる。
- PowerOnVMGroup は、仮想マシン フォルダで PowerOnVMRole 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。
- SnapShotGroup は、仮想マシン フォルダで SnapShotRole 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。

PowerOnVMGroup と SnapShotGroup の両方に属するユーザー 1 がログインします。ユーザー 1 は、仮想マシン A と仮想マシン B の両方のパワーオンとスナップショットの作成を実行できます。

図 2-5. 例 1：複数のグループからの権限の継承



例 2： 子の権限による親の権限のオーバーライド

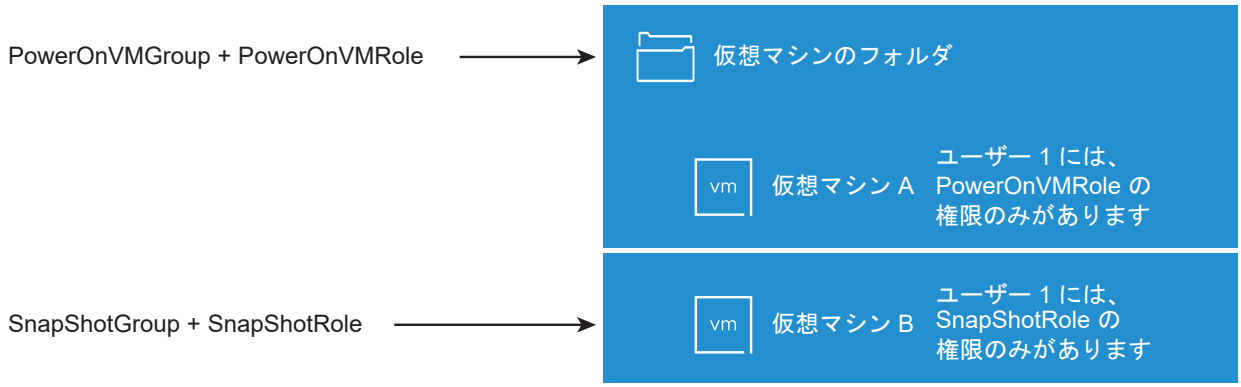
この例では、子オブジェクトに割り当てられた権限が、親オブジェクトに割り当てられている権限をオーバーライドする方法を示します。このオーバーライド機能によって、ユーザーのアクセスをインベントリの特定の領域に制限できます。

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。

- PowerOnVMRole は、仮想マシンをパワーオンできる。
- SnapShotRole は、仮想マシンのスナップショットを作成できる。
- PowerOnVMGroup は、仮想マシン フォルダで PowerOnVMRole 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。
- SnapShotGroup は、仮想マシン B で SnapShotRole を付与されている。

PowerOnVMGroup と SnapShotGroup の両方に属するユーザー 1 がログインします。SnapShotRole は、PowerOnVMRole 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 PowerOnVMRole 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 2-6. 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

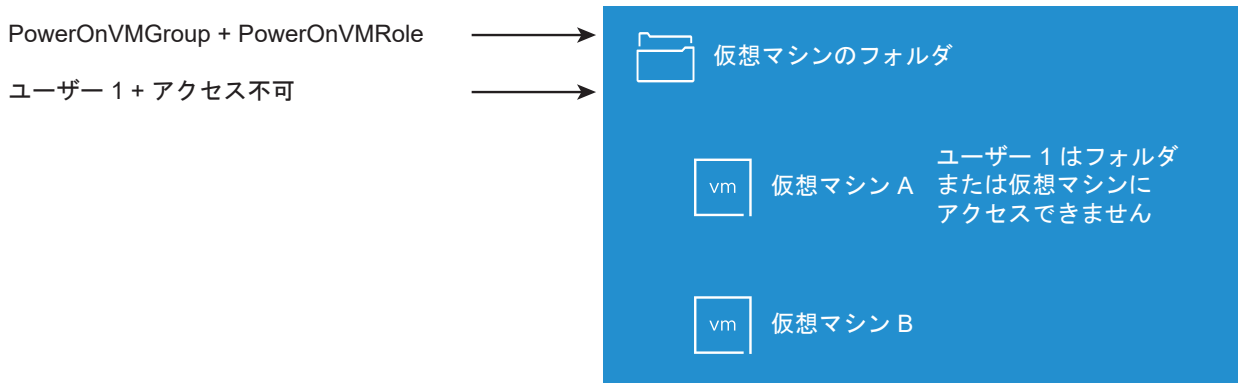
この例では、個々のユーザーに直接ロールを割り当てることによって、グループに割り当てられたロールに関連付けられた権限をオーバーライドする方法を示します。

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。

- PowerOnVMRole は、仮想マシンをパワーオンできる。
- PowerOnVMGroup は、仮想マシン フォルダで PowerOnVMRole 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 NoAccess ロールを割り当てられている。

PowerOnVMGroup に属するユーザー 1 がログインします。仮想マシン フォルダでユーザー 1 に割り当てられている NoAccess 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 フォルダや仮想マシン A および B にアクセスできません。仮想マシン A および B は、ユーザー 1 の階層には表示されません。

図 2-7. 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

権限は、vCenter オブジェクト階層内のオブジェクトに設定されます。各権限によって、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権限を追加し、ユーザー 2 に管理者ロールを与える別の権限を追加できます。

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.メモリ構成特権を含むロールをグループに付与する権限を追加します。

権限の概念については、オブジェクトレベルの権限モデルについて理解するの説明を参照してください。

権限は、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 オブジェクトや、すべてのホスト オブジェクトが格納されたフォルダ オブジェクトに権限を設定できます。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 オブジェクトに伝達される権限を割り当てることで、すべてのソリューションのあらゆるオブジェクトに権限を適用できます。「グローバル権限」を参照してください。

インベントリ オブジェクトへの権限の追加

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 オブジェクトにユーザーとグループおよびこれら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、そのフォルダに権限を設定することで、複数のオブジェクトに同じ伝達される権限を同時に割り当てることができます。

権限を割り当てるには、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

オブジェクトの権限を変更するには、権限.権限の変更 権限を含むロールが必要です。

手順

1 vSphere Client オブジェクト ナビゲータで、権限の割り当て先オブジェクトを探します。

2 [権限] タブをクリックします。

3 [追加] をクリックします。

4 （オプション）外部 ID プロバイダをフェデレーション認証用に構成してある場合、その ID プロバイダのドメインは [ドメイン] ドロップダウン メニューで選択できます。

5 選択したロールに定義された権限を付与するユーザーまたはグループを選択します。

   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のドメインを選択します。

   b [検索] ボックスに名前を入力します。

      ユーザー名およびグループ名が検索されます。

   c ユーザーまたはグループを選択します。

6 [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。

7 （オプション） 権限を伝達するには、[子へ伝達] チェック ボックスを選択します。

   ロールは選択したオブジェクトにのみ適用され、子オブジェクトに伝達されます。

8 [OK] をクリックします。

権限の変更または削除

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 [子へ伝達] 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 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 [権限] タブをクリックします。

3 行をクリックして権限を選択します。

タスク	手順
権限の変更	a [ロールの変更] アイコンをクリックします。 b [ロール] ドロップダウン メニューでユーザーまたはグループのロールを選択します。 c [子へ伝達] チェック ボックスを切り替えて、権限の継承を変更します。 d [OK] をクリックします。
権限の削除	[権限の削除] アイコンをクリックします。

ユーザー検証設定の変更

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 Server5.0 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。同じ方法で ESXi のユーザー リストを検索することはできません。

手順

1 vSphere 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 [設定] を選択して、[設定] - [全般] の順にクリックします。

3 [編集] をクリックし、[ユーザー ディレクトリ] を選択します。

4 必要に応じて値を変更し、[保存] をクリックします。

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 サーバー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	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する場合は有効に切り替えます。
クエリ制限サイズ	vCenter Server が、[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から表示するユーザーおよびグループの最大数。「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。

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。オンプレミスの SDDC では、グローバル権限が vCenter Server と vRealize Orchestrator の両方におよぶ場合がありま

す。ただし、vSphere SDDC の場合、グローバル権限は、タグやコンテンツ ライブラリなどのグローバル オブジェクトに適用されます。

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、ユーザーまたはグループが階層内のすべてのオブジェクトに対して持つ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

通常、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でロール（権限セット）を持つように指定します。

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。グローバル権限は、タグやコンテンツ ライブラリなどのグローバル オブジェクトにも適用されます。タグ オブジェクトに対する権限を参照してください。

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。

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。

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 ルート 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. vSphere Client を使用して、vCenter Server にログインします。
2. [管理] を選択し、[アクセス コントロール] 領域で [グローバル権限] をクリックします。
3. [権限プロバイダ] ドロップダウン メニューでドメインを選択します。
4. （オプション）外部 ID プロバイダをフェデレーション認証用に構成してある場合、その ID プロバイダのドメインは [ドメイン] ドロップダウン メニューで選択できます。
5. [追加] をクリックします。

6 選択したロールに定義された権限を付与するユーザーまたはグループを選択します。

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のドメインを選択します。

b [検索] ボックスに名前を入力します。

ユーザー名およびグループ名が検索されます。

c ユーザーまたはグループを選択します。

7 [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。

8 [子へ伝達] チェック ボックスを選択して、権限を伝達するかどうかを指定します。

グローバル権限を割り当てて [子へ伝達] 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。

9 [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 のトップ 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

仮想マシンなどの vCenter Server インベントリ オブジェクト上のユーザーに権限を付与すると、そのユーザーは権限に関連付けられたタスクを実行できるようになります。ただし、ユーザーはオブジェクト上の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トップ 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 2-1. 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トップ レベル 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、トップ 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ち、トップレベルから伝播されるため、タグ Production に対して権限を持ちます。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 2-2. 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。

注： この動作は、vCenter Server 権限の継承方法とは異なります。子オブジェクトに定義された vCenter Server 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。

表 2-3. 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を持つユーザーには、仮想マシン属性の読み取りや変更が許可されます。

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、Sales グループに、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、Sales グループ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、削除することができます。

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 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 VMware Host 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 の単一ホスト管理：VMware Host Client』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 から管理する場合は、ホストと vCenter Server の両方でカスタム ロールを保持しないでください。ロールは vCenter Server レベルで定義します。

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、System.Read という 3 つのシステム定義権限が付与されます。これらの権限は vSphere Client には表示されませんが、一部の管理対象オブジェクトの特定のプロパティを読み取るために使用されます。vCenter Server のすべての事前定義されたロールには、これらの 3 つのシステム定義の権限が含まれています。詳細については、『vSphere Web Services API』ドキュメントを参照してください。

vCenter Server カスタム ロールの作成

環境のアクセス コントロールのニーズに合わせて、vCenter Server カスタム ロールを作成できます。ロールを作成するか、既存のロールのクローンを作成することができます。

他の vCenter Server システムと同じ vCenter Single Sign-On ドメインに参加する vCenter Server システムでロールを作成または編集できます。VMware Directory Service (vmdir) により、ロールに加えた変更がグループ内のほかのすべての vCenter Server システムに伝播されます。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 Client を使用して、vCenter Server にログインします。

2 [管理] を選択し、[アクセス コントロール] 領域で [ロール] をクリックします。

3 次のようにロールを作成します。

オプション	説明
ロールを作成するには	[新規] をクリックします。
ロールをクローン作成する場合	ロールを選択し、[クローン作成] をクリックします。

詳細については vCenter Server システム ロールを参照してください。

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および選択解除します。

権限カテゴリをスクロールし、そのカテゴリのすべての権限または権限のサブセットを選択します。すべてのカテゴリ、選択したカテゴリ、または選択解除されたカテゴリを表示できます。すべての権限、選択された権限、または選択解除された権限を表示することもできます。

詳細については 16 章 事前定義された権限を参照してください。

注： ロールのクローン作成中は、権限を変更できません。権限を変更するには、クローン作成されたロールを選択し、[編集] をクリックします。

6 [追加] をクリックします。

次のステップ

これで、オブジェクトを選択し、そのオブジェクトのユーザーまたはグループにロールを割り当てることによって、権限を作成できます。

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。オブジェクトに権限を追加する場合は、ユーザーまたはグループとロールをペアリングします。vCenter Server には、変更できないデフォルトのシステムロールがいくつか含まれています。

vCenter Server には、いくつかのデフォルト 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。

デフォルト ロールに関連付けられている権限を表示するには、vSphere Client（[メニュー] - [管理] - [ロール]）のロールに移動し、[権限] タブをクリックします。

すべての vSphere の権限と説明を表示するには、16 章 事前定義された権限を参照してください。

vCenter Server ロール階層には、複数のサンプル ロールも含まれます。サンプル ロールのクローンを作成して、同様のロールを作成することができます。

ロールを作成する場合、システム ロールのいずれからも権限は継承されません。

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の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が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。サポート対象の ID サービスについては、『vSphere の認証』のドキュメントを参照してください。

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。

読み取り専用ロール

オブジェクトに対する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。たとえば、このロールを持つユーザーは、仮想マシン、ホスト、およびリソース プールの属性を表示できますが、ホストのリモート コンソールを表示することはできません。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。

アクセスなしロール

オブジェクトに対する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。

vCenter Single Sign-On ドメインの管理者（デフォルトで administrator@vsphere.local）、root ユーザー、および vpxuser には、デフォルトで管理者ロールが割り当てられます。その他のユーザーには、デフォルトでアクセスなしロールが割り当てられます。

ベスト プラクティスは、ルート レベルにユーザーを作成し、このユーザーに管理者ロールを割り当てることです。管理者権限を持つ名前付きユーザーを作成した後は、root ユーザーを権限から削除することも、そのロールを「アクセスなし」に変更することもできます。

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限に高めるため、ロールと権限のベスト プラクティスに準拠してください。

vCenter Server 環境のロールと権限を設定するときは、次のベスト プラクティスを実施してください。

- 可能であれば、個々のユーザーではなく、グループにロールを割り当てます。
- 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、権限が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る可能性があります。
- 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。
- オブジェクトに権限を割り当てるときに伝達を有効にすることを検討してください。伝達により、オブジェクト階層内の新規オブジェクトで権限が確実に継承されます。たとえば、仮想マシン フォルダに権限を割り当てて、伝達を有効にすると、権限がフォルダ内のすべての仮想マシンに確実に適用されます。
- 階層内の特定の領域をマスクするには、アクセスなしロールを使用します。アクセスなしロールは、そのロールを持つユーザーまたはグループに対し、アクセスを制限します。
- ライセンスへの変更は、同じ vCenter Single Sign-On ドメイン内のリンクされたすべての vCenter Server システムに伝達されます。
- ライセンスの伝達は、すべての vCenter Server システムでユーザーが権限を持っていない場合にも発生します。

一般的なタスクに必要な権限

多くのタスクには、インベントリ内の複数のオブジェクトに対する権限が必要です。1 つのオブジェクトに対するユーザー権限でタスクを実行しても、タスクは正常に完了できません。

次の表は、複数の権限を必要とする一般的なタスクです。インベントリ オブジェクトに権限を追加するには、事前定義済みのロールの 1 つまたは複数の権限をユーザーに割り当てます。権限セットを複数回割り当てる場合は、カスタム ロールを作成します。

vSphere Client ユーザー インターフェイスでの操作が API 呼び出しにどのようにマップされるか、および操作を実行するために必要な権限については、『vSphere Web Services API リファレンス』ドキュメントを参照してください。たとえば、`AddHost_Task(addHost)` メソッドの API ドキュメントでは、ホストをクラスタに追加するために Host.Inventory.AddHostToCluster 権限が必要と指定されています。

以下の表で、実行するタスクが見つからない場合は、次のルールに基づいて、特定の操作を許可するための権限を割り当てる必要があります。

- ストレージ容量が必要となる操作には、ターゲット データストアでのデータストア.容量の割り当て権限と、操作自体を実行する権限が必要です。仮想ディスクやスナップショットを作成する場合などでは、これらの権限が必要です。
- 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 2-4. 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： ■ 仮想マシン.インベントリ.新規作成 ■ 仮想マシン.設定.新規ディスクの追加（新規仮想ディスクを作成する場合） ■ 仮想マシン.設定.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） ■ 仮想マシン.設定.Raw デバイスの設定（RDM または SCSI パススルー デバイスを使用している場合）	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
	移行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.容量の割り当て	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
仮想マシンのパワーオン	仮想マシンがデプロイされているデータセンター： 仮想マシン.相互作用.パワーオン	仮想マシンのパワー ユーザーまたは管理者
	仮想マシンまたは仮想マシンのフォルダ 仮想マシン.相互作用.パワーオン	
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： ■ 仮想マシン.インベントリ.既存のものから作成 ■ 仮想マシン.設定.新規ディスクの追加	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 ■ vApp.インポート	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.容量の割り当て	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

表 2-4. 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 ■ リソース.仮想マシンのリソース プールへの割り当て ■ 仮想マシン.インベントリ.移動	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
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 ■ 仮想マシン.相互作用.質問への回答 ■ 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.相互作用.デバイス接続 ■ 仮想マシン.相互作用.パワーオフ ■ 仮想マシン.相互作用.パワーオン ■ 仮想マシン.相互作用.リセット ■ 仮想マシン.相互作用.CD メディアの設定（CD からインストールする場合） ■ 仮想マシン.相互作用.フロッピー メディアの設定（フロッピー ディスクからインストールする場合） ■ 仮想マシン.相互作用.VMware Tools のインストール	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： ■ データストア.データストアの参照 ■ データストア.低レベルのファイル操作	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 ■ リソース.パワーオン状態の仮想マシンの移行 ■ 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）	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 ■ リソース.パワーオフ状態の仮想マシンの移行 ■ 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）	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.容量の割り当て	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

表 2-4. 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
	移行先のデータストア データストア.容量の割り当て	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 ■ ホスト.インベントリ.クラスタの変更	管理者
vSphere Client を使用して単一のホストをデータセンターに追加するか、PowerCLI または API を使用して（addHost API を利用して）単一のホストをクラスタに追加します。	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
	クラスタ： ■ ホスト.インベントリ.クラスタの変更 ■ 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
	データセンター： ホスト.インベントリ.スタンドアロン ホストの追加	システム管理者
クラスタに複数のホストを追加	クラスタ： ■ ホスト.インベントリ.クラスタの変更 ■ 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
	クラスタの親データセンター（伝達が有効）： ■ ホスト.インベントリ.スタンドアロン ホストの追加 ■ ホスト.インベントリ.ホストの移動 ■ ホスト.インベントリ.クラスタの変更 ■ ホスト.構成.メンテナンス	システム管理者
仮想マシンの暗号化	暗号化タスクは、vCenter Server を含む環境でのみ実行することができます。加えて、ESXi ホストでは、ほとんどの暗号化タスクについて、暗号化モードが有効になっている必要があります。このタスクを実行するユーザーには、適切な権限が与えられている必要があります。一連の暗号化操作権限によって、きめ細かな制御が可能となります。暗号化タスクの前提条件と必要な権限を参照してください。	システム管理者

ESXi ホストのセキュリティ強化

3

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送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。ESXi ホストは証明書インフラストラクチャに参加します。ホストは、デフォルトで VMware Certificate Authority (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。

注： ESXi は、Linux カーネルまたは市販の Linux ディストリビューション上に構築されていません。自己完結型のユニットとして提供される独自の VMware 専用のカーネルおよびソフトウェア ツールを使用しており、Linux ディストリビューションのアプリケーションやコンポーネントは含まれていません。

この章には、次のトピックが含まれています。

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。その場合は、信頼できる環境で作業していることを確認し、他のセキュリティ対策を講じるようにします。

組み込みのセキュリティ機能

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 インターフェイスはデフォルトで無効になっています。トラブルシューティングまたはサポート アクティビティを実行する場合以外は、これらのインターフェイスは無効のままにしてください。日常のアクティビティでは、vSphere Client を使用します。そのため、アクティビティはロールベースのアクセス制御および最新のアクセス制御方法の影響を受けます。
- 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。追加のサービスが必要な場合は、ポートを開きます。
- 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。
- Web クライアントによるアクセスをサポートするため、ESXi によって内部 Web サービスが使用されています。このサービスは、管理と監視のために Web クライアントで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 Web サービス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。「VMware Security Advisories」およびセキュリティ アラートのメーリング リストを購読して、セキュリティ関連の警告を受け取ることができます。http://lists.vmware.com/mailman/listinfo/security-announce の Web ページを参照してください。
- 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。
- 暗号で署名されていないドライバやアプリケーションがホストでロードされないようにするには、UEFI セキュア ブートを使用します。セキュア ブートの有効化は、システム BIOS で実行します。ESXi ホストで、ディスク パーティションなどに対して追加の設定変更を行う必要はありません。ESXi ホストの UEFI セキュア ブートを参照してください。
- ESXi ホストに TPM 2.0 チップが搭載されている場合は、システム BIOS でチップを有効にして設定します。TPM 2.0 は、セキュア ブートと連携することでセキュリティを強化し、ハードウェア内のルートに信頼保証を配置します。Trusted Platform Module による ESXi ホストの保護を参照してください。

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 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。VMware Host Client を使用して管理対象ホストに直接アクセスせず、DCUI から管理対象ホストを変更しないようにします。

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。

トラブルシューティングを行う場合にのみ DCUI を使用する

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 ホストを管理するには、GUI クライアントのいずれか、または VMware CLI や API のいずれかを使用します。ESXCLI の概念と範例(https://code.vmware.com/) を参照してください。ESXi Shell または SSH を使用する場合は、アクセス権を持つアカウントを制限し、タイムアウト時間を設定します。

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、いくつかのサードパーティ製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のあるタスクをサポートします。VMware では、VMware ソースから提供されたこれらのパッケージへのアップグレードのみをサポートします。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 のナレッジベースの記事を確認してください。

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。

システムの詳細設定

システムの詳細設定は、ログ作成、システム リソース、セキュリティなど、ESXi 動作の特性を制御します。

次の表に、セキュリティにとって重要な ESXi システムの詳細設定の一部を示します。システムの詳細設定をすべて表示するには、vSphere Client（[ホスト] - [設定] - [システム] - [システムの詳細設定]）または特定のリリースの API を参照してください。

表 3-1. セキュリティに関するシステム詳細設定のリストの一部

システムの詳細設定	説明	デフォルト値
Annotations.WelcomeMessage	ログイン前の Host Client またはデフォルト画面の DCUI に、ようこそメッセージを表示します。DCUI では、ようこそメッセージが一部のテキスト（ホスト IP アドレスなど）を置き換えます。	（空）
Config.Etc.issue	SSH ログイン セッション中にバナーを表示します。最適な結果を得るには、末尾に改行を使用します。	（空）
Config.Etc.motd	SSH ログイン時に今日のメッセージを表示します。	（空）
Config.HostAgent.vmacore.soap.sessionTimeout	システムが VIM API を自動的にログアウトさせるまでのアイドル時間を分単位で設定します。ゼロ (0) の値を指定すると、アイドル時間は無効になります。この設定は、新しいセッションにのみ適用されます。	30（分）
Mem.MemEagerZero	仮想マシンの終了後に、VMkernel オペレーティング システム（VMM プロセスを含む）のユーザー ワールド ページおよびゲスト メモリ ページのゼロクリアを有効にします。デフォルト値 (0) を指定すると、Lazy Zero が使用されます。値 1 を指定すると、Eager Zero が使用されます。	0（無効）
Security.AccountLockFailures	システムがユーザーのアカウントをロックするまでのログイン試行の最大失敗回数を設定します。たとえば、5 回目のログインに失敗したときにアカウントをロックするには、この値を 4 に設定します。ゼロ (0) の値を指定すると、アカウントのロックは無効になります。 実装上の理由から、一部のログイン メカニズムでは予期せずにカウントされることがあります。 ■ VIM ログイン（VMware Host Client を含む）と ESXCLI には、正確なログイン失敗回数が反映されます。 ■ SSH 接続では、1 回のパスワード プロンプトの表示が 1 回のログイン試行としてカウントされ、ログインに成功するとカウントは取り消されます。この動作は、チャレンジ/レスポンス通信では通常の動作です。 ■ CGI ログインではログイン失敗の数が二重にカウントされます。 **注意：** この問題により、CGI インターフェイスを使用している場合は、ログイン失敗回数よりも早くユーザーがロックアウトされることがあります。	5

表 3-1. セキュリティに関するシステム詳細設定のリストの一部 （続き）

システムの詳細設定	説明	デフォルト値
Security.AccountUnlockTime	ユーザーがロックアウトされる秒数を設定します。指定したロック タイムアウト内にログインを試行すると、ロック タイムアウトが再開されます。	900（15 分）
Security.PasswordHistory	ユーザーごとに記憶するパスワードの数を設定します。この設定により、重複するパスワードや類似するパスワードの使用を防止できます。	0
Security.PasswordMaxDays	パスワード変更までの最大日数を設定します。	99999

Security.PasswordQualityControl	`Pam_passwdqc` 構成で必要な長さと文字クラスの要件を変更するか、パスフレーズを許可します。パスワード内で特殊文字を使用できます。パスワードの長さは 15 文字以上にすることができます。デフォルト設定では、3 種類の文字と 7 文字以上が必要です。
	DoD Annex を実装する場合は、`similar=deny` オプションと最小パスワード長を組み合わせて、パスワードが十分に異なるという要件を満たすことができます。パスワードの履歴設定は、VIM `LocalAccountManager.changePassword` API を介して変更されたパスワードにのみ適用されます。パスワードを変更するには、ユーザーに管理者権限が必要です。PasswordQualityControl 設定と PasswordMaxDays 設定の組み合わせは、DoD Annex の要件を満たします。
	`min=disabled,disabled,disabled,disabled,15`
	`similar=deny`
		retry=3
		min=disabled,disabled,disabled,7,7

UserVars.DcuiTimeOut	システムが DCUI を自動的にログアウトさせるまでのアイドル時間を秒単位で設定します。ゼロ (0) の値を指定すると、タイムアウトは無効になります。	600（10 分）
UserVars.ESXiShellInteractiveTimeOut	システムが対話型シェルを自動的にログアウトさせるまでのアイドル時間を秒単位で設定します。この設定は、新しいセッションでのみ有効になります。ゼロ (0) の値を指定すると、アイドル時間は無効になります。DCUI と SSH シェルの両方に適用されます。	0
UserVars.ESXiShellTimeOut	ログイン シェルがログインを待機する時間を秒単位で設定します。ゼロ (0) の値を指定すると、タイムアウトは無効になります。DCUI と SSH シェルの両方に適用されます。	0

表 3-1. セキュリティに関するシステム詳細設定のリストの一部 （続き）

システムの詳細設定	説明	デフォルト値
UserVars.HostClientSessionTimeout	システムが Host Client を自動的にログアウトさせるまでのアイドル時間を秒単位で設定します。ゼロ (0) の値を指定すると、アイドル時間は無効になります。	900（15 分）
UserVars.HostClientWelcomeMessage	ログイン時に Host Client にようこそメッセージを表示します。このメッセージは、以降のログイン時に「ヒント」として表示されます。	（空）

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 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 のホスト プロファイル』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。

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 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。リファレンス情報およびプログラミングのヒントについては、『ESXCLI 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 Client を使用する方法について主に説明されています。

VMware PowerCLI

VMware PowerCLI は、vSphere API への Windows PowerShell インターフェイスです。VMware 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。

VMware PowerCLI には、数百の 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。https://developer.vmware.com/powercli を参照してください。

ESXCLI

ESXCLI 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。『ESXCLI のドキュメント』を参照してください。

vSphere Automation SDK for Python などの vSphere Automation 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 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

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

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

4 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。

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。Security.PasswordHistory の詳細オプションを使用して、ユーザーごとに記憶するパスワードの数を設定することもできます。

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 VMware Host Client を使用してアクセスするためのパスワード要件があります。

- 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 種類の文字のうち 3 つ以上を混在させる必要があります。
- デフォルトでは、パスワードの長さは 7 文字以上 40 文字未満です。
- パスワードに、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。

注： パスワードの先頭に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。辞書にある語をパスワードに使用すると、パスワード全体の強度が低下します。

ESXi のパスワードの例

次にパスワードの候補を示し、オプションが以下のように設定されている場合のパスワードについて説明します。

```
retry=3 min=disabled,disabled,disabled,7,7
```

この設定では、新しいパスワードが十分に強力ではない場合、またはパスワードが 2 回正しく入力されなかった場合、ユーザーは最大 3 回 (retry=3) 入力を要求されます。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。max、passphrase など、その他のオプションの詳細については、pam_passwdqc のメイン 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が 2 に減っています。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が 2 に減っています。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。デフォルト設定やその他の設定を変更するには、vSphere 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、最小で 3 つの単語を含むパスフレーズを許可しています。

レガシー ホストで `/etc/pam.d/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、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 およびホストの管理』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 (`passphrase=4`) 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 man ページを参照してください。

注： パスワードのオプションは、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、テストを実行します。

この例では、パスワードの複雑性の要件で、大きなパスワードの違い、5 つのパスワードの記憶履歴、および 90 日間のローテーション ポリシーを実施する 4 種類の文字から 8 文字が要求されるように設定します。

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

`Security.PasswordHistory` オプションを 5 に設定し、`Security.PasswordMaxDays` オプションを 90 に設定します。

ESXi のアカウント ロックアウトの動作

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 5 回許容されています。デフォルトでは 15 分後に、アカウントのロックが解除されます。

ログイン動作の設定

ESXi ホストのログイン動作を設定するには、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。
- `Security.PasswordHistory`。ユーザーごとに記憶するパスワードの数。ゼロを指定すると、パスワード履歴は無効になります。

ESXi 詳細オプションの設定の詳細については、『vCenter Server およびホストの管理』ドキュメントを参照してください。

暗号化キーの生成

ESXi では、通常の操作に対しいくつかの非対称キーが生成されます。トランスポート レイヤー セキュリティ (TLS) キーにより、TLS プロトコルを使用した ESXi ホストとの通信が保護されます。SSH キーは、SSH プロトコルを使用して、ESXi ホストとの通信を保護します。

トランスポート レイヤー セキュリティ キー

トランスポート レイヤー セキュリティ (TLS) キーは、TLS プロトコルを使用してホストとの通信を保護します。最初の起動時に、ESXi ホストでは TLS キーが 2048 ビット RSA キーとして生成されます。現在、ESXi は TLS 用 ECDSA キーの自動生成を実装していません。TLS プライベート キーは、管理者が処理するものではありません。

TLS キーは、以下の読み取り専用の場所にあります。

```
/etc/vmware/ssl/rui.key
```

TLS パブリック キー（中間認証局を含む）は、次の読み取り専用の場所に X.509 v3 証明書として配置されます。

```
/etc/vmware/ssl/rui.crt
```

vCenter Server を ESXi ホストで使用する場合、vCenter Server では CSR が自動的に生成され、VMware Certificate Authority (VMCA) を使用して署名され、証明書が生成されます。ESXi ホストを vCenter Server に追加すると、vCenter Server では結果の証明書が ESXi ホストにインストールされます。

デフォルトの TLS 証明書は自己署名されます。subjectAltName フィールドは、インストール時のホスト名と一致します。別の証明書をインストールして、たとえば、別の subjectAltName を使用したり、特定の認証局 (CA) を検証チェーンに含めることができます。ESXi SSL 証明書とキーの置き換えを参照してください。

VMware Host Client を使用して、証明書を置き換えることもできます。vSphere の単一ホスト管理：VMware Host Client を参照してください。

SSH キー

SSH キーは、SSH プロトコルを使用して、ESXi ホストとの通信を保護します。最初の起動時に、nistp256 ECDSA キーが生成され、SSH キーが 2048 ビット RSA キーとして生成されます。SSH サーバはデフォルトで無効になっています。SSH アクセスは、主にトラブルシューティングを目的としています。SSH キーは、管理者によるサービス提供の対象外です。SSH を使用してログインするには、完全なホスト制御と同等の管理者権限が必要になります。SSH アクセスを有効にする手順については、ESXi Shell へのアクセスの有効化を参照してください。

SSH パブリック キーは次の場所に配置されます。

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

SSH プライベート キーは次の場所に配置されます。

```
/etc/ssh/ssh_host_rsa_key
```

```
/etc/ssh/ssh_host_ecdsa_key
```

TLS 暗号化キー確立

TLS 暗号化キー確立の構成は、RSA ベース キー転送（NIST Special Publication 800-56B で指定）、または短期的な Ecliptic Curve Diffie Hellman (ECDH)（NIST Special Publication 800-56A で指定）を使用した ECC ベース キー契約のいずれかを選択する TLS 暗号化スイートの選択によって管理されます。

SSH 暗号化キー確立

SSH 暗号化キー確立の構成は、SSHD 構成によって管理されます。ESXi では、RSA ベース キー転送（NIST Special Publication 800-56B で指定）、短期的な Diffie Hellman (DH)（NIST Special Publication 800-56A で指定）キー契約、および短期的な Ecliptic Curve Diffie Hellman (ECHD)（NIST Special Publication 800-56A で指定）を許可するデフォルトの構成が提供されます。SSHD 構成は、管理者によるサービス提供の対象外です。

SSH セキュリティ

ESXi Shell および SSH インターフェイスはデフォルトで無効になっています。トラブルシューティングまたはサポート アクティビティを実行する場合以外は、これらのインターフェイスは無効のままにしてください。日常のアクティビティでは、vSphere Client を使用します。そのため、アクティビティはロールベースのアクセス制御および最新のアクセス制御方法の影響を受けます。

ESXi の SSH 設定では、次の設定が使用されます。

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。

ESXi SSH キー

SSH キーは、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 キーにより、信頼されたユーザーまたはスクリプトがパスワードを入力せずにホストにログインすることを許可できます。

vifs コマンドを使用して、SSH キーをホストにコピーできます。HTTPS PUT を使用して SSK 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。詳細については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/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ことには固有のリスクが存在します。ユーザー名とパスワードを公開することの潜在的なリスクと信頼されるキーを持つユーザーによる侵入のリスクとを比較してください。

vifs コマンドを使用した 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する場合は、vifs コマンドで認証済み鍵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ファイル
- 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。このファイルを変更すると、ホスト デーモン (hostd) が認識しない変更を加えることになります。

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`
RSA 鍵	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
RSA 公開鍵	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

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。脆弱性があると、デバイス ドライバなどのバグの多いコードまたは悪意のあるコードがゲスト OS の特権モードで実行されてしまいます。業界標準のハードウェアとファームウェアには現在、ESXi ホストを脆弱性から保護するための十分なエラー抑制サポートがありません。

仮想マシンに対する PCI または PCIe のパススルーは、信頼できるエンティティが仮想マシンを所有し、管理している場合にのみ使用してください。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い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 デバイスのバグや非互換性が原因で発生する場合があります。他のエラー原因には、ゲスト OS でのドライバの問題があります。

- ゲスト OS は、ESXi ホストで IOMMU ページ障害を引き起こす Direct Memory Access (DMA) を生成する場合があります。この処理は、仮想マシン メモリ外のアドレスを対象とする DMA 操作が原因となっている場合があります。一部のマシンでは、ホストのファームウェアが、マスク不可能な割り込み (NMI) による致命的なエラーを報告するように IOMMU 障害を設定します。この致命的なエラーが、ESXi ホストのクラッシュを引き起こします。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。間違った割り込みにより、ESXi ホストがクラッシュすることがあります。理論上、これらの間違った割り込みを悪用する方法はあり得るのです。

管理対象オブジェクトブラウザの無効化

管理対象オブジェクト ブラウザ (MOB) 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、MOB 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。MOB 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。

MOB はデフォルトでは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。MOB は次のように有効および無効にできます。

手順

1. vSphere Client インベントリで、ホストに移動して参照します。
2. [構成] 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] をクリックします。
4. [Config.HostAgent.plugins.solo.enableMob] の値を確認し、必要に応じて [編集] をクリックして値を変更します。

   `vim-cmd` を ESXi Shell から使用しないでください。

ESXi のネットワーク 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 VMware 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、別個のネットワークを使用することも推奨されます。

- vSphere vMotion、VMware vSphere Fault Tolerance、VMware vSAN、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。それぞれの機能用にネットワークを分離します。多くの場合、単一の物理サーバ ラックの外部にこれらのネットワークをルーティングさせる必要はありません。

- 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 トラフィックを他のトラフィックから隔離します。通常、管理ネットワークには、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ます。管理ネットワークへのアクセスを保護するには、Bastion ホストまたは仮想プライベート ネットワーク (VPN) を使用します。このネットワーク内のアクセスを厳密に管理します。
- 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。

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

vSphere Auto Deploy を使用する場合は、使用環境を保護するために、ネットワーク セキュリティ、起動イメージ セキュリティ、およびホスト プロファイルを介したパスワードの漏洩の可能性に十分に注意してください。

ネットワーク セキュリティ

PXE ベースのほかのデプロイの場合と同様に、ネットワークをセキュリティ保護します。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 ブートの間は、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、SHA-512 でハッシュ化されます。
  - 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ために、vSphere Authentication Proxy 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。

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、これらのリモート 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。root または管理者アカウントを使用してリモート アプリケーションをプロビジョニングした場合に、アプリケーションが侵害されると、仮想環境も侵害される恐れがあります。

CIM はオープンな標準で、ESXi ホスト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 ドライバと基盤となるハードウェアへの管理アクセスをサポートします。サーバ メーカーやハードウェア デバイス ベンダーなどのハードウェア ベンダーは、自社のデバイスを監視および管理するプロバイダを作成できます。VMware は、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を監視するプロバイダを作成します。これらのプロバイダは軽量で、特定の管理タスクに特化して ESXi ホスト内で実行されます。CIM ブローカはすべての CIM プロバイダから情報を取得し、標準 API を使用してその情報を外部に開示します。最も一般的な API は WS-MAN です。

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、これらのアプリケーション用に権限の小さな vSphere ユーザー アカウントを作成し、VIM API チケット関数を使用して、この権限の小さなユーザー アカウントに CIM を認証するためのセッション ID（「チケット」）を発行します。このアカウントに CIM チケットを取得するための権限が付与されている場合、VIM API はチケットを CIM に提供できます。これらのチケットは、任意の CIM-XML API 呼び出しに対するユーザー ID とパスワードの両方として提供されます。詳細については、`AcquireCimServicesTicket()`メソッドを参照してください。

サードパーティの CIM VIB をインストールすると（`esxcli software vib install -n` *`VIBname`* コマンドを実行した場合など）、CIM サービスが開始します。

CIM サービスを手動で有効にする必要がある場合は、次のコマンドを実行します。

```
esxcli system wbem set -e true
```

必要に応じて、CIM サービスのみが実行されるように wsman（WSManagement サービス）を無効にできます。

```
esxcli system wbem set -W false
```

wsman が無効になっていることを確認するには、次のコマンドを実行します。

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

ESXCLI コマンドの詳細については、「ESXCLI のドキュメント」を参照してください。CIM サービスを有効にする方法の詳細については、https://kb.vmware.com/kb/1025757 にある VMware ナレッジベースの記事を参照してください。

手順

1 CIM アプリケーション用に root 以外の vSphere ユーザー アカウントを作成します。

『vSphere の認証』で、vCenter Single Sign-On ユーザーを追加する方法のトピックを参照してください。ユーザー アカウントに必要な vSphere の権限は、Host.CIM.Interaction です。

2 選択した vSphere API SDK を使用して、vCenter Server に対してユーザー アカウントを認証します。次に、CIM-XML ポート 5989 または WS-Man ポート 433 の API を使用して管理者レベル アカウントとして `AcquireCimServicesTicket()`を呼び出し、ESXi を認証するためのチケットを返します。

詳細については、『vSphere Web Services API リファレンス』を参照してください。

3 必要に応じて、2 分ごとにチケットを更新します。

ESXi ホストの証明書管理

VMware Certificate Authority (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、新しい各 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。

ESXi の証明書は、vSphere 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 6.0 以降の証明書

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 TLS を使用します。

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 3-2. 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）	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。 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。 このモードでは、vSphere Client から証明書を更新することができます。
カスタム認証局	このモードは、サードパーティ CA またはエンタープライズ 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。 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 Client から証明書を更新することはできません。 **注：** 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 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。
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.x 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。 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.x 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。

証明書有効期限

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 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す。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または vCenter Server システムの一部です。

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、最初に接続を試みます。接続できない場合、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。

ESXi の証明書管理に必要な権限

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 Client から設定できます。

ホスト名と IP アドレスの変更

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 3-3. 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。

ホストのアップグレードと証明書

ESXi ホストを ESXi 6.5 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（サムプリント）証明書が VMware 認証局 (VMCA) 署名付き証明書に置き換えられます。ESXi ホストがカスタムの証明書を使用している場合は、証明書が期限切れまたは無効であっても、アップグレード プロセスではその証明書が保持されます。

推奨されるアップグレード ワークフローは、使用している証明書によって異なります。

サムプリント証明書を使用してプロビジョニングされたホスト

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。これらのホストは ESXi 6.5 以降にアップグレードする必要があります。

カスタムの証明書を使用してプロビジョニングされたホスト

カスタムの証明書（通常はサードパーティの 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、アップグレード プロセスでこれらの証明書は維持されます。証明書の更新時に誤って置き換えられないように、証明書モードを [カスタム] に変更してください。

注： VMCA モードの環境の場合、vSphere 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 Client に表示されます。

Auto Deploy でプロビジョニングされたホスト

Auto Deploy でプロビジョニングされるホストでは、ESXi 6.5 以降のソフトウェアを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。

Auto Deploy でのカスタム証明書の使用を参照してください。

証明書モード切り替えワークフロー

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従来のサムプリント 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、切り替える必要もありません。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。

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 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 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。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 を使用する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。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。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。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。

ESXi 証明書のデフォルト設定

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。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。

デフォルト設定の多くは、vSphere Client を使用して変更できます。組織および場所の情報を変更することを検討します。証明書のデフォルト設定の変更を参照してください。

表 3-4. ESXi 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
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.daysValid
証明書有効期限のハードしきい値。このしきい値に達すると、vCenter Server は赤いアラームを生成します。	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 3-4. ESXi CSR 設定 （続き）

パラメータ	デフォルト値	詳細オプション
証明書有効期限のソフトしきい値。このしきい値に達すると、vCenter Server はイベントを生成します。	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。ホストのアップグレードと証明書を参照してください。	vmca サムプリントまたはカスタムを指定することもできます。証明書モードの変更を参照してください。	vpxd.certmgmt.mode

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 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。

デフォルト設定のリストについては、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 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 [構成] をクリックし、[詳細設定] をクリックします。

3 [設定の編集] をクリックします。

4 [名前] 列で [フィルタ] アイコンをクリックし、[フィルタ] ボックスに **`vpxd.certmgmt`** と入力して、証明書管理パラメータのみを表示します。

5 企業のポリシーに合わせて既存のパラメータの値を変更し、[保存] 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 に送信される証明書署名要求 (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は、ホストを切断してから再接続するか、または証明書を更新します。

複数の ESXi ホストの証明書有効期限情報の表示

ESXi6.0 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 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。サムプリント 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 Client を使用して、vCenter Server にログインします。

2 インベントリ リストを参照し、vCenter Server インスタンスを選択します。

3 [ホストおよびクラスタ] - [ホスト] の順に選択します。

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。

4 列を表示または非表示にするには、左下隅にある 3 バーの [列セレクタ] をクリックします。

5 [証明書の有効期限] チェック ボックスを選択し、必要に応じて右にスクロールして追加された列を表示します。

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。

6 （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。

単一の ESXi ホスト用証明書の詳細の表示

ESXi 6.0 以降のホストで、VMCA モードまたはカスタム モードの場合は、vSphere Client で証明書の詳細を表示できます。証明書に関する情報は、デバッグなどに役立ちます。

手順

1 vSphere Client インベントリで、ホストに移動して参照します。

2 [構成] をクリックします。

3 [システム] で、[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。

フィールド	説明
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。 **良好** 通常動作 **期限切れ** 証明書はまもなく期限切れになります。 **間もなく期限切れ** 証明書は 8 か月以内に期限切れになります（デフォルト）。 **期限切れ間近** 証明書は 2 か月以内に期限切れになります（デフォルト）。 **期限切れ** 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、VMware 認証局 (VMCA) によって証明書が割り当てられている場合は、vSphere Client からそれらの証明書を更新できます。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、期限が近づいている場合、またはそれ以外の理由で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。期限切れになる前に証明書を更新しなかった場合、ホストを切断して再接続した際に vCenter Server 証明書が更新されます。vCenter Server にホストを再度追加すると、信頼が再確立され、vCenter Server は無条件に更新された証明書を発行できるようになります。

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 [間もなく期限切れ] になっている証明書を更新します。

前提条件

以下を確認します。

- ESXi ホストが vCenter Server システムに接続されている。
- vCenter Server システムと ESXi ホスト間に適切な時刻同期がある。
- DNS 解決が vCenter Server システムと ESXi ホスト間で動作する。
- vCenter Server システムの MACHINE_SSL_CERT および Trusted_Root 証明書が有効であり、期限切れでない。VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/2111411) を参照してください。
- ESXi ホストがメンテナンス モードではない。

手順

1 vSphere Client インベントリで、ホストに移動して参照します。

2 [構成] をクリックします。

3 [システム] で、[証明書] をクリックします。

選択したホストの証明書の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、ホスト用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 VMware Endpoint Certificate Store (VECS) 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。

証明書モードの変更

企業ポリシーでカスタム証明書を使用する必要がある場合を除き、VMCA を使用して環境内に ESXi ホストをプロビジョニングします。カスタム証明書を別のルート CA と一緒に使用するには、vCenter Server `vpxd.certmgmt.mode` 詳細オプションを編集できます。変更後に証明書を更新すると、ホストは VMCA 証明書で自動的にはプロビジョニングされなくなります。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 vSphere 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 [構成] をクリックし、[設定] で [詳細設定] をクリックします。

3 [設定の編集] をクリックします。

4 [名前] 列で [フィルタ] アイコンをクリックし、[フィルタ] ボックスに **`vpxd.certmgmt`** と入力して、証明書管理パラメータのみを表示します。

5 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、[保存] をクリックします。

6 vCenter Server サービスを再起動します。

サービスの再起動の詳細については、vCenter Server の構成のドキュメントを参照してください。

ESXi SSL 証明書とキーの置き換え

企業のセキュリティ ポリシーによっては、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。

企業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されている認証局 (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、さまざまな方法で信頼されてい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 ホストの CA 署名付き証明書の使用に関する詳細な手順については、証明書モード切り替えワークフローを参照してください。

注： vSAN クラスタの一部である ESXi ホストで SSL 証明書を置き換える場合は、https://kb.vmware.com/s/article/56441 にある VMware ナレッジベースの記事に記載されている手順に従ってください。

- ESXi 証明書署名要求の要件

  エンタープライズまたはサードパーティ CA 署名付き証明書を使用するか、従属 CA 署名付き証明書を使用する場合は、証明書署名リクエスト (CSR) を認証局 (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` コマンドを使用して、デフォルトの VMware 認証局 (VMCA) の署名付き 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

エンタープライズまたはサードパーティ CA 署名付き証明書を使用するか、従属 CA 署名付き証明書を使用する場合は、証明書署名リクエスト (CSR) を認証局 (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。

- キー サイズ：2,048 ビット（最小）から 16,384 ビット（最大）（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、否認防止、キー暗号化が含まれている必要があります。
- 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）

vSphere 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。
- アルゴリズム md2WithRSAEncryption、md5WithRSAEncryption、RSASSA-PSS、dsaWithSHA1、ecdsa_with_SHA1、sha1WithRSAEncryption はサポートされていません。

CSR の生成の詳細については、https://kb.vmware.com/s/article/2113926 にある VMware ナレッジベースの記事を参照してください。

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、vSphere Client からの SSH トラフィックを有効にします。
- 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。

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` コマンドを使用して、デフォルトの VMware 認証局 (VMCA) の署名付き 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、vSphere Client からの SSH トラフィックを有効にします。
- 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。

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。

ESXi 証明書署名要求の要件を参照してください。

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。

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 ServerTRUSTED_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、vSphere Client からの SSH トラフィックを有効にします。
- 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。

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

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。

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 ServerTRUSTED_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。

注： vCenter Server システムが ESXi ホストにインストールされている認証局 (CA) と同じ認証局 (CA) によって発行されたカスタム証明書を使用して実行されている場合、この手順は必要ありません。

手順

1. ESXi ホストを管理する vCenter Server システムの vCenter Server シェルにログインします。
2. たとえば次のように、`dir-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/dir-cli trustedcert publish --cert path_to_RootCA
   ```

3. プロンプトが表示されたら、Single Sign-On 管理者の認証情報を入力します。
4. カスタム証明書が中間 CA によって発行されている場合は、次のようなコマンドを実行して vCenter Server の `TRUSTED_ROOTS` ストアに中間 CA を追加する必要もあります。

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

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

- 認証局に証明書を要求します。証明書は以下の要件を満たす必要があります。
  - キー サイズ：2,048 ビット（最小）から 16,384 ビット（最大）（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、否認防止、キー暗号化が含まれている必要があります。
  - 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）
- 証明書ファイルに `rbd-ca.crt`、キー ファイルに `rbd-ca.key` という名前を付けます。

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/` ディレクトリ内にあります。

2 vSphere Authentication Proxy サービスを停止します。

ツール	手順
vCenter Server 管理インターフェイス	a Web ブラウザで、vCenter Server 管理インターフェイス (https://*vcenter-IP-address-or-FQDN*:5480) に移動します。 b root としてログインします。 デフォルトの root パスワードは、vCenter Server のデプロイ時に設定したパスワードです。 c [サービス] をクリックし、[VMware vSphere Authentication Proxy サービス] をクリックします。 d [停止] をクリックします。
CLI	`service-control --stop vmcam`

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 サービスを稼動しているシステムで次のコマンドを実行し、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。

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

5 TRUSTED_ROOTS ストアの内容を含む `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 ESXi 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

次回、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、Auto Deploy サーバによって証明書が生成されます。Auto Deploy サーバでは、TRUSTED_ROOTS ストアに追加したルート証明書が使用されます。

注： 証明書の置き換え後に Auto Deploy で問題が発生した場合は、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2000988) を参照してください。

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 ESXi 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、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。

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 Client の [セキュリティ プロファイル]、[サービス]、[ファイアウォール] の各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設定してリスクを低減します。

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 Client 内の各ホストに対して、[設定] - [ファイアウォール] 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。

  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。

  注： CommunitySupported VIB がインストールされている ESXi ホストの問題の調査を依頼すると、VMware テクニカル サポートから、この VIB をアンインストールするよう求められることがあります。要求された手順を実行し、調査中の問題がこの VIB に関連しているかどうかを判別するためのトラブルシューティングを行います。

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 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受信および送信ファイアウォール接続を構成できます。

このタスクでは、vSphere Client を使用して ESXi ファイアウォールを設定する方法について説明します。ESXi Shell または ESXCLI 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コマンドラインで ESXi を設定できます。概要については『ESXCLI スタート ガイド』を、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『ESXCLI の概念と範例』を参照してください。

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 Client を使用して、vCenter Server にログインします。

2 インベントリで、ホストに移動して参照します。

3 [構成] をクリックし、[システム] の [ファイアウォール] をクリックします。

[受信] と [送信] をクリックして、受信接続と送信接続を切り替えることができます。

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。

5 [グループ化解除済み]、[SSH]、[簡易ネットワーク管理プロトコル]の 3 つのサービス グループのいずれかから選択します。

6 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。

7 一部のサービスでは、[システム] で [設定] - [サービス] の順に移動してサービスの詳細を管理できます。

サービスの起動、停止、および再起動の詳細については、サービスの有効化または無効化を参照してください。

8 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。

9 [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。

サービスに対して許可された IP アドレス リストを更新するには、vSphere Client、ESXCLI、または PowerCLI を使用します。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。このタスクでは、vSphere Client の使用方法について説明します。ESXCLI の使用手順については、https://code.vmware.com/にあるファイアウォールの管理のトピック「ESXCLI Concepts and Examples」を参照してください。

手順

1 vSphere Client を使用して、vCenter Server にログインします。

2 ESXi ホストに移動して参照します。

3 [構成] をクリックし、[システム] の [ファイアウォール] をクリックします。

[受信] と [送信] をクリックして、受信接続と送信接続を切り替えることができます。

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。

5 [グループ化解除済み]、[SSH]、[簡易ネットワーク管理プロトコル]の 3 つのサービス グループのいずれかから選択します。

6 [許可された IP アドレス] セクションを表示するには、サービスを展開します。

7 [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

8 サービス自体が選択されていることを確認します。

9 [OK] をクリックします。

10 サービスの [許可された IP アドレス] 列で変更を確認します。

ESXi ホストの送受信ファイアウォール ポート

vSphere Client および VMware Host Client では、各サービスのファイアウォール ポートを開閉したり、選択した IP アドレスからのトラフィックを許可したりできます。

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。ESXi ファイアウォールでサポートされているポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。

VMware Ports and Protocols Tool では、デフォルトでインストールされているサービスのポート情報が一覧表示されます。他の VIB をホストにインストールすると、追加のサービスおよびファイアウォール ポートが使用可能になる場合があります。この情報は、主に vSphere Client に表示されるサービスに関するものですが、VMware Ports and Protocols Tool にはそれ以外のポートも含まれています。

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します。

ファイアウォール コマンド リファレンス

コマンド ラインで ESXi Shell または ESXCLI 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。ファイアウォールおよびファイアウォール ルールを操作するには、概要について ESXCLI スタート ガイドを参照し、ESXCLI の使用例について「ESXCLI の概念と範例」を参照してください。

ESXi 7.0 以降では、カスタム ファイアウォール ルールの作成に使用される `service.xml` ファイルへのアクセスが制限されます。`/etc/rc.local.d/local.sh` ファイルを使用してカスタム ファイアウォール ルールを作成する方法については、VMware ナレッジベースの記事 KB2008226 を参照してください。

表 3-5. 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	デフォルトのアクションをパスに設定するには、true に設定します。デフォルトのアクションをドロップに設定するには、false に設定します。
esxcli network firewall set --enabled	ESXi のファイアウォールを有効または無効にします。
esxcli network firewall load	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。
esxcli network firewall refresh	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。
esxcli network firewall unload	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。
esxcli network firewall ruleset list	ルール セット情報を一覧表示します。
esxcli network firewall ruleset set --allowed-all	すべての IP アドレス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。
esxcli network firewall ruleset set --enabled --ruleset-id=<string>	指定したルールセットを有効にするには、有効を true に設定します。指定したルールセットを無効にするには、有効を false に設定します。
esxcli network firewall ruleset allowedip list	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。
esxcli network firewall ruleset allowedip add	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。
esxcli network firewall ruleset allowedip remove	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。
esxcli network firewall ruleset rule list	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。会社のポリシーで許可されている場合は、セキュリティ プロファイルからサービスを無効にしたり有効にしたりできます。

サービスの有効化または無効化 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 Client から次のサービスのステータスを変更できます。

表 3-6. 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 デーモン	実行中	負荷に基づくチーミング。
attestd	停止	vSphere 信頼機関 証明サービス。
kmxd	停止	vSphere 信頼機関 キー プロバイダ サービス。
Active Directory サービス	停止	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 デーモン	停止	ネットワーク時間プロトコル デーモン。
PC/SC スマート カード デーモン	停止	ホストのスマート カード認証を有効にすると、このサービスが開始されます。ESXi のスマート カード認証の構成を参照してください。
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 デーモン。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 デーモン。Syslog は、vSphere 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。vCenter Server のインストールとセットアップ を参照してください。
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 デー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。

サービスの有効化または無効化

vSphere Client から、サービスを有効または無効にすることができます。

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。ユーザー インターフェイス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 Client を使用して vCenter Server に接続します。

手順

1 インベントリでホストを参照します。

2 [構成] をクリックし、[システム] の [サービス] をクリックします。

3 変更するサービスを選択します。

a ホストのステータスを 1 回だけ変更する場合は、[再起動]、[起動]、または[停止] を選択します。

b 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、[起動ポリシーの編集] をクリックしてポリシーを選択します。

- [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。[ポートに連動して開始および停止] と同様に、このオプションで、サービスは定期的にタスクの完了を試行します (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 サービスを起動した際に、ホストがパワーオン状態の場合、サービスは実行を続けます。サービスが開始されているときにホストがパワーオフされると、シャットダウン プロセスの一部としてサービスが停止します。ホストがパワーオンされると、サービスが再起動され、ユーザーが定義した状態が保持されます。
- [ポートに連動して開始および停止]: 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。

注： これらの設定は、ユーザー インターフェイス、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。

4 [OK] をクリックします。

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。

通常ロックダウン モードまたは厳密なロックダウン モードを選択して、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。例外ユーザー リストを使用することもできます。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。

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 Client を通じて、vCenter Server から、または vSphere Web Services SDK を使用することによっ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。
  - 通常のロックダウン モードの場合、例外ユーザー リストのアカウントは ダイレクト コンソール ユーザー インターフェイス (DCUI) にアクセスできます（管理者権限がある場合）。さらに、`DCUI.Access` 詳細システム設定で指定されているすべてのユーザーは、ダイレクト コンソール ユーザー インターフェイス (DCUI) にアクセスできます。
- ESXi Shell または SSH が有効で、ホストがロックダウン モードの場合、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。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 3-7. 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	権限に基づくすべてのユーザー	vCenter (vpxuser) 権限に基づく例外ユーザー vCloud Director（vslauser、使用可能な場合）	vCenter (vpxuser) 権限に基づく例外ユーザー vCloud Director（vslauser、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) 権限に基づく例外ユーザー vCloud Director（vslauser、使用可能な場合）	vCenter (vpxuser) 権限に基づく例外ユーザー vCloud Director（vslauser、使用可能な場合）

表 3-7. ロックダウン モードの動作 （続き）

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
ダイレクト コンソール ユーザー インターフェイス (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）および 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

ユーザーは、ロックダウン モードが有効になる前に、ESXi Shell にログインするか、SSH を介してホストにアクセスすることがあります。その場合、例外ユーザー リストに含まれ、ホストの管理者権限を持つユーザーは、ログインしたままになります。他のすべてのユーザーに対しては、セッションが閉じられます。この動作は、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。

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。

ホストへのすべての直接アクセスを完全に許可しないようにする場合は、厳密なロックダウン モードを選択できます。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 Client インベントリで、ホストに移動して参照します。

2 [構成] 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] 選択します。

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
標準	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 が有効な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 が有効であれば、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。

ロックダウン モードの無効化

ロックダウン モードを無効にすることで、ESXi ホストに直接接続して構成を変更できるようになります。ロックダウン モードを有効にした方が、環境の安全性は高まります。

ロックダウン モードは次のようにして無効にできます。

グラフィカル ユーザー インターフェイスを使用する

vSphere 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にできます。

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 モードを無効にできます。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 Client インベントリでホストを参照します。

2 [構成] 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] 選択します。

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、[無効] を選択してロックダウン モードを無効にします。

6 [OK] をクリックします。

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 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、致命的な障害の際にアクセスを有効にするために使用します。

ロックダウン モードを有効にすると、ユーザー権限は保持されます。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 モードを無効にすると、ユーザー権限はリストアされます。

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権限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 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 キー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 キーを押します。

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 の致命的な障害が発生したときに 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 モードが有効な場合に各アカウントでデフォルトで行える動作と、デフォルト動作を変更する方法は、vSphere バージョンによって決まります。

- vSphere 5.0 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 で致命的なエラーが発生した場合のために用意されています。通常、企業は、このアクセス権を持つユーザーのパスワードを安全な場所に保管しておくようにします。`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 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

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場合、`DCUI.Access` 詳細オプションを使用すると、ロックダウン モードを終了できます。ユーザーをリストに追加するには、vSphere Client からホストの [詳細設定] を編集します。

注： DCUI.Access リストに登録されているユーザーは、付与さ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。ロックダウン モードを変更できるようにすると、ホストのセキュリティに影響が及ぶ可能性があります。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 Client インベントリで、ホストに移動して参照します。
2. [構成] 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] をクリックし、[編集] をクリックします。
4. DCUI のフィルタ。
5. [DCUI.Access] テキスト ボックスに、ローカル ESXi 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 ユーザー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。
6. [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 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権を失いません。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 Client インベントリで、ホストに移動して参照します。
2. [構成] 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] 選択します。

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、[ユーザーの追加] アイコンをクリックして例外ユーザーを追加します。

VIB を使用したセキュアなアップデートの実行

ESXCLI を使用して ESXi をアップグレードするには、VIB、イメージ プロファイル、およびソフトウェア デポについて理解している必要があります。

ESXi は、実際のソフトウェアを含む一連の vSphere インストールバンドル（VIB）を示すイメージ プロファイルで構成されます。VIB は、システムのコンポーネントを表す署名付き RAM ディスクで、Linux システムの RPM または DEB とほぼ同じです。イメージ プロファイルは、VIB の集合体です。ソフトウェア デポは、VIB とイメージ プロファイルの集合体です。ESXi パッチおよびデポには、VIB の共通セットから構成されるアップデートされたイメージ プロファイルが含まれています。

`esxcli software` コマンドを使用して、ESXi のアップデートをスタンド アローン ホストにインストールできます。詳細については、『ESXi のアップグレード』を参照してください。

注： 通常、vSphere 7.0 以降の環境では、ESXi ホストのライフサイクル管理に VMware vSphere® vSphere Lifecycle Manager を使用します。

インストールされているすべての VIB とその現在のバージョン、または現在のイメージ プロファイルをリストするには、次の ESXCLI コマンドを使用します。

- `esxcli software vib list`
- `esxcli software profile get`

通常、ESXi を安全にアップグレードするための手順の概要は、次のとおりです。

- ESXi ホストをメンテナンス モードにする
- `esxcli software profile update` コマンドを実行する。このコマンドでは SSH を介してホストに転送された URL または ZIP ファイルにポイントします
- ESXi ホストの再起動

VMware では VIB が暗号で署名されるため、VIB またはデポ全体のセキュアな転送は不要で、アップデート プロセスによってこれらの署名が検証されます。

ホストと VIB の許容レベルの管理

VIB の許容レベルは、その VIB の認定の度合いによって異なります。最も低い VIB のレベルによってホストの許容レベルが決まります。レベルの低い VIB を許可する場合は、ホストの許容レベルを変更できます。ホストの許容レベルを変更できるようにするためには、CommunitySupported VIB を削除してください。

VIB は、VMware またはそのパートナーからの署名を含んだソフトウェア パッケージです。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。

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。たとえば、ホストの許容レベルが VMwareAccepted である場合、PartnerSupported レベルの VIB をインストールすることはできません。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。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。

ESXi ホストの許容レベルは、vSphere Client の[セキュリティ プロファイル]に表示されます。

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の詳細なテストが行われます。現在このレベルでは、I/O Vendor Program (IOVP) プログラム ドライバのみが公開されています。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 では、ユーザーがこの許容レベルの VIB に関してサポート コールを行った場合、パートナーのサポート組織に問い合わせるように案内しています。

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。現在このレベルでは、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 テクノロジーが公開されています。VMware では、ユーザーがこの許容レベルの VIB に関してサポート コールを行った場合、パートナーのサポート組織に問い合わせるように案内しています。

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、VMwareAccepted、PartnerSupported 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 CommunitySupported である場合は、次のコマンドを実行して、CommunitySupported レベルの 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 次のコマンドを実行して CommunitySupported VIB をすべて削除します。

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

4 次の方法のいずれかを使用して、ホストの許容レベルを変更します。

オプション	説明
CLI コマンド	`esxcli software acceptance set --level level` `level` パラメータは必須で、設定する許容レベルを指定します。**VMwareCertified**、**VMwareAccepted**、**PartnerSupported**、または **CommunitySupported** のいずれかにする必要があります。詳細については ESXCLI のリファレンスを参照してください。
vSphere Client	a インベントリでホストを選択します。 b [構成] をクリックします。 c [システム] で、[セキュリティ プロファイル] 選択します。 d [ホスト イメージ プロファイル許容レベル] の [編集] をクリックし、許容レベルを選択します。

結果

新しい許容レベルが有効になります。

注： ESXi は、許容レベルによって管理される VIB の整合性チェックを実行します。`VMkernel.Boot.execInstalledOnly` 設定を使用して、ホストにインストールされている有効な VIB から発信されたバイナリのみを実行するように ESXi に指示できます。この設定をセキュア ブートと組み合わせると、ESXi ホストで実行されるすべてのプロセスが署名され、許可され、想定されるようになります。デフォルトでは、vSphere 7 のパートナーとの互換性のために、`VMkernel.Boot.execInstalledOnly` 設定は無効になっています。この設定を有効にすると（可能な場合）、セキュリティが向上します。ESXi の詳細オプションの構成の詳細については、https://kb.vmware.com/kb/1038578 の VMware のナレッジベースの記事を参照してください。

ESXi ホストの権限の割り当て

通常、vCenter Server システムで管理される 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。スタンドアローンの 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 Client を使用して管理タスクを実行します。

vCenter Server オブジェクト階層内の ESXi ホスト オブジェクトを選択して、限ら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。これらのユーザーは、ESXi ホスト上で直接管理を実行できます。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 アカウントに非常に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。

スタンドアローン ESXi ホストへの権限の割り当て

VMware Host 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。『vSphere の単一ホスト管理：VMware Host Client』ドキュメントを参照してください。

ESXi のすべてのバージョンにおいて、事前定義済みのユーザーを `/etc/passwd` ファイルで確認できます。

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。

システム管理者

管理者ロール。

アクセスなし

アクセスなし。これがデフォルトのロールです。デフォルトのロールはオーバーライドできます。

ESXi ホストに直接接続された VMware Host 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、ローカルのカスタム ロールを ESXi ホストに追加できます。『vSphere の単一ホスト管理：VMware Host Client』ドキュメントを参照してください。

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。ESXi ユーザーにロールを割り当てた場合、vCenter Server ユーザーに同じロールは割り当てられません。

事前定義された権限

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

デフォルトでは、各 ESXi ホストに、管理者ロールを持つ単一の root ユーザー アカウントがあります。この root 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。

root ユーザーは権限を持つユーザーとして一般的に知られているため、悪用されて、ESXi ホストに容易に侵入される可能性があります。また、汎用的な root アカウントを使用すると、実施に実行したユーザーを特定することが難しくなります。

管理状況を追跡するには、管理者権限を持つ個人アカウントを作成してください。root アカウントには非常に複雑なパスワードを設定し、root 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。root アカウントは削除しないでください。ESXi ホストのユーザーへの権限割り当ての詳細については、『vSphere の単一ホスト管理：VMware Host Client』を参照してください。

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に専用のアカウントを指定し、特定のユーザーに割り当てることです。ESXi Active Directory 機能を使用して、Active Directory 認証情報を管理します。

重要： root ユーザーのアクセス権限は削除できます。ただし、最初に root レベルの別の権限を持つ別のユーザーを作成し、管理者ロールに割り当てる必要があります。

vpxuser ユーザー

vCenter Server では、vpxuser の権限を使用して、ホストに対するアクティビティを管理します。

vCenter Server の管理者は、root ユーザーとほぼ同様の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も可能です。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。管理者権限を持つユーザーのみが、ホストで直接これらのタスクを実行することができます。

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

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。このユーザーは主に、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場合に使用します。

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。ユーザーが直接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。

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設定します。

ESXi ホストを Active Directory に追加する際には、ドメイン グループ ESX Admins にホストに対する完全な管理者権限を割り当てます（ホストが存在する場合）。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 KB1025569 の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. 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 の時刻の同期または 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 Client インベントリで、ホストに移動して参照します。
   b. [構成] をクリックします。
   c. [ネットワーク] で、[TCP/IP 構成] をクリックします。
   d. [TCP/IP スタック] のデフォルトで、[DNS] をクリックし、ホスト名およびホストの DNS サーバ情報が正しいことを確認します。

次のステップ

ホストをディレクトリ サービス ドメインに参加させます。ディレクトリ サービス ドメインへのホストの追加を参照してください。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。権限を設定して、Active Directory ドメインに参加したユーザーおよびグループが vCenter Server コンポーネントにアクセスできるようにします。権限の管理方法については、インベントリ オブジェクトへの権限の追加 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

ホストでディレクトリ サービスを利用するには、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 Client インベントリでホストを参照します。
2. [構成] 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。

次のステップ

参加した Active Directory ドメインのユーザーおよびグループが vCenter Server コンポーネントにアクセスできるように権限を設定することができます。権限の管理方法については、インベントリ オブジェクトへの権限の追加を参照してください。

ディレクトリ サービス設定の確認

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 サーバの設定を確認できます。

手順

1 vSphere Client インベントリで、ホストに移動して参照します。

2 [構成] 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。

次のステップ

参加した Active Directory ドメインのユーザーおよびグループが vCenter Server コンポーネントにアクセスできるように権限を設定することができます。権限の管理方法については、インベントリ オブジェクトへの権限の追加を参照してください。

vSphere Authentication Proxy の使用

ESXi ホストを Active Directory ドメインに明示的に追加する代わりに、vSphere Authentication Proxy を使用して Active Directory ドメインに追加することができます。

Active Directory サーバのドメイン名と vSphere Authentication Proxy の IP アドレスを特定できるようにホストを設定するだけです。vSphere Authentication Proxy が有効な場合、Auto Deploy によってプロビジョニングされるホストは自動的に Active Directory ドメインに追加されます。Auto Deploy を使用してプロビジョニングされないホストでも、vSphere Authentication Proxy を使用できます。

vSphere Authentication Proxy が使用する TCP ポートについては、vCenter Server に必要なポート を参照してください。

Auto Deploy

Auto Deploy でホストをプロビジョニングする場合は、Authentication Proxy をポイントするリファレンス ホストをセットアップできます。その後、Auto Deploy でプロビジョニングされるすべての ESXi ホストにリファレンス ホストのプロファイルを適用するルールを設定します。vSphere Authentication Proxy のアクセス コントロール リストには、Auto Deploy が PXE を使用してプロビジョニングするすべてのホストの IP アドレスが格納されます。ホストを起動すると、ホストは vSphere Authentication Proxy と通信を行います。vSphere Authentication Proxy は、アクセス コントロール リストに含まれているホストを Active Directory ドメインに追加します。

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 を使用する場合でも、Auto Deploy でカスタム証明書を使用する場合と同じ手順を実行すれば、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。

その他の ESXi ホスト

他のホストを vSphere Authentication Proxy を使用するようにセットアップすることで、Active Directory 認証を使用することなくドメインに参加できます。Active Directory 認証をホストに送信する必要も、Active Directory 認証をホスト プロファイルに保存する必要もありません。

ホストの IP アドレスを vSphere Authentication Proxy アクセス コントロール リストに追加すれば、vSphere Authentication Proxy はデフォルトで、IP アドレスに基づいてホストを認証します。クライアント認証を有効にすると、ホストの証明書が vSphere Authentication Proxy によってチェックされます。

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 を有効にする

vSphere Authentication Proxy サービスは、各 vCenter Server システムで利用できます。デフォルトでは、このサービスが実行されていません。ご利用の環境内で vSphere Authentication Proxy を使用する場合は、vCenter Server 管理インターフェイスから、またはコマンド ラインからサービスを開始してください。

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 のみまたは IPv4/IPv6 混在モードのネットワーク環境内のホスト マシンにインストールしてください。ただし、vSphere Authentication Proxy のアドレスを指定する場合は、IPv4 アドレスを指定する必要があります。

前提条件

ご使用の vCenter Server が 6.5 以降であることを確認します。それより前のバージョンの vSphere では、vSphere Authentication Proxy を別途インストールします。必要な手順については、以前のバージョンのドキュメントを参照してください。

手順

1 VMware vSphere Authentication Proxy サービスを起動します。

オプション	説明
vCenter Server 管理インターフェイス	a Web ブラウザで、vCenter Server 管理インターフェイス (https://*vcenter-IP-address-or-FQDN*:5480) に移動します。 b root としてログインします。 デフォルトの root パスワードは、vCenter Server のデプロイ時に設定したパスワードです。 c [サービス] をクリックし、[VMware vSphere Authentication Proxy] サービスをします。 d [開始] をクリックします。 e （オプション） サービスが開始されたら、[起動タイプの設定] をクリックし、[自動] をクリックして、自動的に起動されるように設定します。
CLI	`service-control --start vmcam`

2 サービスが正常に開始されたことを確認します。

結果

これで vSphere Authentication Proxy ドメインを設定する準備ができました。その後は、Auto Deploy でプロビジョニングされたすべてのホストが vSphere Authentication Proxy によって処理されます。vSphere Authentication Proxy には、明示的にホストを追加することもできます。

vSphere Client での vSphere Authentication Proxy へのドメインの追加

vSphere Authentication Proxy には、vSphere Client から、または `camconfig` コマンドを使用してドメインを追加することができます。

vSphere Authentication Proxy にドメインを追加できるのは、プロキシを有効にした後のみです。ドメインを追加すると、vSphere Authentication Proxy は Auto Deploy を使用してプロビジョニングしたすべてのホストをそのドメインに追加します。それ以外のホストにドメイン権限を付与しないようにする場合も、vSphere Authentication Proxy を使用できます。

手順

1. vSphere Client を使用して vCenter Server システムに接続します。
2. vCenter Server を選択し、[設定] をクリックします。
3. [Authentication Proxy] をクリックし、[編集] をクリックします。
4. vSphere Authentication Proxy からのホストの追加先となるドメインの名前を入力し、さらに、ドメインにホストを追加するための Active Directory 権限を持ったユーザーの名前とパスワードを入力します。
5. [保存] をクリックします。

camconfig コマンドでの vSphere Authentication Proxy へのドメインの追加

`camconfig` コマンドを使用して vSphere Authentication にドメインを追加することができます。

vSphere Authentication Proxy にドメインを追加できるのは、プロキシを有効にした後のみです。ドメインを追加すると、vSphere Authentication Proxy は Auto Deploy を使用してプロビジョニングしたすべてのホストをそのドメインに追加します。それ以外のホストにドメイン権限を付与しないようにする場合も、vSphere Authentication Proxy を使用できます。

手順

1. vCenter Server システムに、管理者権限を持つユーザーでログインします。
2. コマンドを実行して、Bash シェルへのアクセスを有効にします。

   ```
   shell
   ```

3. [camconfig] スクリプトが保存されている `/usr/lib/vmware-vmcam/bin/` ディレクトリに移動します。
4. ドメインおよびユーザーの Active Directory 認証情報を Authentication Proxy の構成に追加するには、次のコマンドを実行します。

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

   パスワードを求められます。

このユーザー名とパスワードは、vSphere Authentication Proxy によってキャッシュされます。必要に応じてユーザーを削除してから作成し直すことができます。ドメインは DNS 経由で到達できる必要がありますが、vCenter Single Sign-On の ID ソースにする必要はありません。

vSphere Authentication Proxy は、*ユーザー*が指定したユーザー名を使用して、ESXi ホストのアカウントを Active Directory に作成します。ユーザーには、ホストを追加する Active Directory ドメインにアカウントを作成する権限が必要です。この情報の執筆時点では、Microsoft サポート技術情報の記事 932455 にアカウント作成権限の背景情報が記載されています。

5 後で vSphere Authentication Proxy からドメインとユーザー情報を削除する必要が生じた場合は、次のコマンドを実行します。

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

vSphere Authentication Proxy を使用した、ドメインへのホストの追加

Auto Deploy サーバがプロビジョニングするすべてのホストは、vSphere Authentication Proxy に追加され、vSphere Authentication Proxy によってドメインに追加されます。vSphere Authentication Proxy を使用するドメインに他のホストを追加する場合は、vSphere Authentication Proxy に明示的に追加します。その後、vSphere Authentication Proxy サーバがそれらのホストをドメインに追加します。これにより、ユーザーが指定する認証を vCenter Server システムに送信する必要はなくなります。

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。

前提条件

- ESXi ホストで 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。追加されていないと、Authentication Proxy サービスは ESXi ホストを信頼できません。
- ESXi ホストでルート CA 署名付き証明書が使用されている場合は、適切なルート CA 署名付き証明書が vCenter Server システムに追加されていることを確認してください。 ESXi ホストの証明書管理を参照してください。

手順

1 vSphere Client インベントリで、ホストに移動して参照します。

2 [構成] 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。

mydomain.com のような **name.tld** 形式、または **mydomain.com/organizational_unit1/organizational_unit2**.のような **name.tld/container/path** 形式を使用します。

6 [プロキシ サーバの使用] を選択します。

7 Authentication Proxy サーバの IP アドレスを入力します。これは常に vCenter Server システムの IP アドレスと同じです。

8 [OK] をクリックします。

vSphere Authentication Proxy のクライアント認証を有効にする

vSphere Authentication Proxy は、そのアクセス コントロール リストに IP アドレスが存在するすべてのホストをデフォルトで追加します。セキュリティを強化するために、クライアント認証を有効にすることができます。クライアント認証が有効になっている場合、vSphere Authentication Proxy によってホストの証明書も併せて確認されます。

前提条件

- vCenter Server システムがホストを信頼していることを確認します。デフォルトでは、ホストを vCenter Server に追加すると、vCenter Server が信頼するルート CA によって署名された証明書がそのホストに割り当てられます。vSphere Authentication Proxy は、vCenter Server が信頼するルート CA を信頼します。
- ご利用の環境内で ESXi の証明書を交換する予定がある場合は、vSphere Authentication Proxy を有効にする前に交換作業を実施してください。ESXi ホスト上の証明書は、そのホストの登録側と一致している必要があります。

手順

1 vCenter Server システムに、管理者権限を持つユーザーでログインします。

2 コマンドを実行して、Bash シェルへのアクセスを有効にします。

```
shell
```

3 [camconfig] スクリプトが保存されている `/usr/lib/vmware-vmcam/bin/` ディレクトリに移動します。

4 次のコマンドを実行してクライアント認証を有効にします。

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

以後、追加対象となる各ホストの証明書が vSphere Authentication Proxy によって確認されます。

5 後で再びクライアント認証を無効にする場合は、次のコマンドを実行します。

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

ESXi ホストへの vSphere Authentication Proxy 証明書のインポート

デフォルトでは、vSphere Authentication Proxy 証明書の検証を ESXi ホストに対して明示的に行う必要があります。vSphere Auto Deploy を使用している場合、プロビジョニング対象となるホストに証明書を追加する処理が Auto Deploy サービスによって行われます。それ以外のホストについては、証明書を明示的に追加する必要があります。

前提条件

- ESXi ホストからアクセス可能なデータストアに vSphere Authentication Proxy 証明書をアップロードします。証明書は、WinSCP などの SFTP アプリケーションを使用して次の場所にある vCenter Server ホストからダウンロードできます。

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

- `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi 詳細設定が 1（デフォルト）に設定されていることを確認します。

手順

1. ESXi ホストを選択し、[構成] をクリックします。
2. [システム] で、[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. 証明書ファイルのパスを `[datatstore]/path/certname.crt` 形式で入力し、[OK] をクリックします。

vSphere Authentication Proxy 用の新しい証明書の生成

VMCA によってプロビジョニングされた新しい証明書を生成することや、VMCA を従属証明書として含んだ新しい証明書を生成することができます。

サード パーティ CA またはエンタープライズ CA によって署名されたカスタム証明書を使用する場合は、vSphere Authentication Proxy でカスタム証明書を使用するための設定を参照してください。

前提条件

vSphere Authentication Proxy が動作しているシステムの root 権限または管理者権限が必要です。

手順

1. `certool.cfg` のコピーを作成します。

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

2. 所属する組織の情報に合わせてコピーを編集します。次の例を参考にしてください。

   ```
   Country = IE
   Name = vmcam
   Organization = VMware
   ```

```
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3 新しいプライベート キーを /var/lib/vmware/vmcam/ssl/ に生成します。

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

localhost には、vCenter Server の FQDN を指定してください。

4 手順 1 と手順 2 で作成したキーおよび vmcam.cfg ファイルを使用して、/var/lib/vmware/vmcam/ssl/ に新しい証明書を生成します。

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

localhost には、vCenter Server の FQDN を指定してください。

vSphere Authentication Proxy でカスタム証明書を使用するための設定

vSphere Authentication Proxy でのカスタム証明書の使用は、いくつかの手順で構成されます。まず CSR を生成し、署名のために認証局 (CA) に送信します。次に、署名済みの証明書とキー ファイルを、vSphere Authentication Proxy がアクセスできる場所に配置します。

デフォルトでは、vSphere Authentication Proxy が初回起動時に CSR を生成し、それに対する署名を VMCA に依頼します。その証明書を使用して、vSphere Authentication Proxy は、vCenter Server に対する登録を行います。カスタム証明書を vCenter Server に追加すれば、ご利用の環境内でカスタム証明書を使用することができます。

手順

1 vSphere Authentication Proxy の証明書署名要求の生成

a 次の例に従って構成ファイル (/var/lib/vmware/vmcam/ssl/vmcam.cfg) を作成します。

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

b openssl を実行して CSR ファイルとキー ファイルを生成し、構成ファイルに渡します。

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

2 rui.crt 証明書と rui.key ファイルをバックアップし、次の場所に保管します。

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

3 vSphere Authentication Proxy の登録を解除します。

a camregister スクリプトが保存されている /usr/lib/vmware-vmcam/bin ディレクトリに移動します。

b 次のコマンドを実行します。

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

user には、vCenter Server に対する管理者権限を持った vCenter Single Sign-On ユーザーを指定してください。

4 vSphere Authentication Proxy サービスを停止します。

ツール	手順
vCenter Server 設定管理インターフェイス	a Web ブラウザで、vCenter Server 設定管理インターフェイス (https://*vcenter-IP-address-or-FQDN*:5480) に移動します。 b root としてログインします。 デフォルトの root パスワードは、vCenter Server のデプロイ時に設定したパスワードです。 c [サービス] をクリックし、[VMware vSphere Authentication Proxy サービス] をクリックします。 d [停止] をクリックします。
CLI	`service-control --stop vmcam`

5 既存の `rui.crt` 証明書と `rui.key` ファイルを、CA から受け取ったファイルに置き換えます。

6 vSphere Authentication Proxy サービスを再起動します。

7 新しい証明書とキーを使用して、vSphere Authentication Proxy を vCenter Server に明示的に再登録します。

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

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指定する代わりに、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規模企業では、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、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 カード認証の有効化

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 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 Client インベントリで、ホストに移動して参照します。
2. [構成] 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。

   証明書は PEM 形式である必要があります。
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 Client インベントリで、ホストに移動して参照します。
2. [構成] 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] 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。

接続の問題が発生した場合のユーザー名とパスワードを使用した認証

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。その場合は、ローカル ESXi 管理者ユーザーの認証情報で ESXi DCUI にログインすることができます。ログイン後、診断や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になります。

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権を持つホスト 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 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権は失われず、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 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。

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。

- ESXi Shell へのアクセスの有効化

  ESXi Shell および SSH インターフェイスはデフォルトで無効になっています。トラブルシューティングまたはサポート アクティビティを実行する場合以外は、これらのインターフェイスは無効のままにしてください。日常のアクティビティでは、vSphere Client を使用します。そのため、アクティビティはロールベースのアクセス制御および最新のアクセス制御方法の影響を受けます。

- 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 Client、ESXCLI、または VMware PowerCLI を使用して ESXi 設定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。

ESXi Shell へのアクセスの有効化

ESXi Shell および SSH インターフェイスはデフォルトで無効になっています。トラブルシューティングまたはサポート アクティビティを実行する場合以外は、これらのインターフェイスは無効のままにしてください。日常のアクティビティでは、vSphere Client を使用します。そのため、アクティビティはロールベースのアクセス制御および最新のアクセス制御方法の影響を受けます。

注： vSphere Client、リモートのコマンド ライン ツール（ESXCLI 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 インベントリで、ホストに移動して参照します。

2 [構成] をクリックし、[システム] の [サービス] をクリックします。

3 ESXi、SSH、またはダイレクト コンソール ユーザー インターフェイス サービスを管理します。

   a [サービス] ペインで、サービスを選択します。

   b [起動ポリシーを編集] 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。

   c サービスを有効にするには、[起動] をクリックします。

[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、[ホストと連動して起動および停止] を選択します。

次のステップ

ESXi Shell の可用性とアイドルのタイムアウトを設定します。 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。

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 Client インベントリで、ホストに移動して参照します。

2 [構成] 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 [編集] をクリックし、`UserVars.ESXiShellTimeOut` を選択します。

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 サービスの再起動が必要です。

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。

アイドル ESXi Shell セッションのタイムアウトの作成

ホストで ESXi Shell を有効にしていて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、他のユーザーがホストに対するアクセス権を取得する可能性が高くなります。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 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 Client インベントリで、ホストに移動して参照します。

2 [構成] 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 [編集] をクリックし、UserVars.ESXiShellInteractiveTimeOut を選択して、タイムアウト設定を入力します。

ゼロ (0) の値を指定すると、アイドル時間が無効になります。

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 (DCUI) 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。ダイレクト コンソール ユーザー インターフェイスには、ホストに接続されている物理コンソールからアクセスします。ホストが再起動して ESXi がロードされたら、F2 キーを押して DCUI にログインします。ESXi のインストール時に作成した認証情報を入力します。

注： ダイレクト コンソール ユーザー インターフェイス、vSphere 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。変更がコミットされる前にホストに障害が発生すると、ホストが失われる可能性があります。

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 キーを押します。

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 キー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のタイムアウトを設定します。ESXi Shell での可用性タイムアウトまたはアイドル タイムアウトの設定を参照してください。

ESXi Shell での可用性タイムアウトまたはアイドル タイムアウトの設定

ESXi Shell はデフォルトでは無効になっています。シェルを有効にする際にセキュリティを強化するため、可用性タイムアウトとアイドルのタイムアウトのどちらか一方、または両方を設定できます。

この 2 つのタイプのタイムアウトは、それぞれ異なる状況に適用されます。

アイドル タイムアウト

ユーザーがホストで ESXi Shell を有効にしていて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、この状況を防止できます。

可用性タイムアウト

可用性タイムアウトは、最初にこのシェルを有効にした後、ログインするまでの許容される時間を決定します。この時間を超えると、サービスは無効になり、ESXi Shell にログインすることはできません。

前提条件

ESXi Shell を有効にします。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た ESXi Shell へのアクセスの有効化を参照してください。

手順

1 ESXi Shell にログインします。

2 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。

3 アイドル タイムアウト（秒単位）、または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 サービスの再起動が必要です。

4 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。

5 [OK] をクリックします。

結果

- アイドル タイムアウトを設定した場合、指定された時間アイドル状態が続くとユーザーはログアウトされます。
- 可用性タイムアウトを設定した場合、このタイムアウト時間が経過する前にログインしないと、ログインできなくなります。

トラブルシューティングのために ESXi Shell にログイン

vSphere Client、ESXCLI、または VMware PowerCLI を使用して ESXi 設定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 ホストの UEFI セキュア ブート

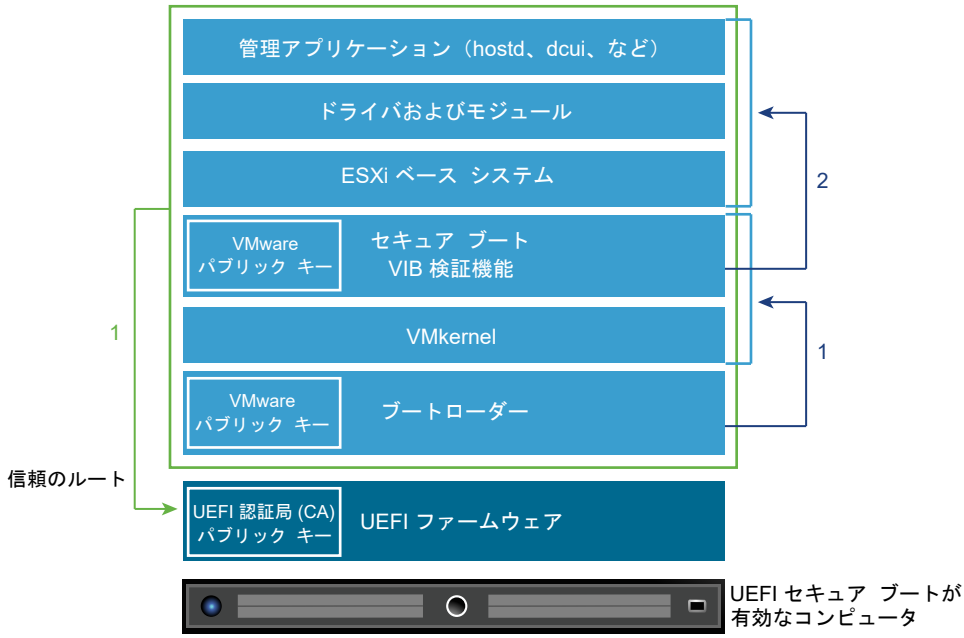
セキュア ブートは、UEFI ファームウェア標準の一部です。セキュア ブートが有効な場合、オペレーティング システムのブートローダーが暗号で署名されていない限り、マシンに UEFI ドライバまたはアプリケーションはロードされません。vSphere 6.5 以降、ESXi は、ハードウェアでセキュア ブートが有効な場合にこれをサポートします。

ESXi での UEFI セキュア ブートの使用方法

ESXi バージョン 6.5 以降では、ブート スタックの各レベルで UEFI セキュア ブートをサポートしています。

注： アップグレードされたホストで UEFI セキュア ブートを使用する前に、アップグレード後の ESXi ホストでのセキュア ブート検証スクリプトの実行 の手順に従って互換性を確認してください。

図 3-1. UEFI セキュア ブート



セキュア ブートが有効な場合、ブート シーケンスは次のようになります。

1 vSphere 6.5 以降、ESXi ブートローダーには VMware パブリック キーが含まれます。ブートローダーは、このキーを使用して、カーネルの署名と、セキュア ブート VIB 検証機能を含むシステムの小さなサブセットを検証します。

2 VIB 検証機能は、システムにインストールされているすべての VIB パッケージを検証します。

この時点で、UEFI ファームウェアの一部である証明書の信頼のルートを使用して、システム全体が起動されます。

注： vSphere 7.0 Update 2 以降をインストールまたはアップグレードするときに、ESXi ホストに TPM がある場合、TPM は UEFI セキュア ブートの PCR 値に基づいて TPM ポリシーを使用して機密情報をシーリングします。この値は、ポリシーが true として満たされている場合、その後の再起動時にロードされます。vSphere 7.0 Update 2 以降で UEFI セキュア ブートを無効または有効にするには、セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化を参照してください。

UEFI セキュア ブートのトラブルシューティング

セキュア ブートがブート シーケンスのいずれかのレベルで成功しない場合、エラーとなります。

エラー メッセージは、ハードウェア ベンダーによって、および検証が成功しなかったレベルによって異なります。

- 署名のないブートローダーまたは改ざんされているブートローダーでブートすると、ブート シーケンスでエラーとなります。表示されるメッセージは、ハードウェア ベンダーによって異なります。次のようなエラーが表示される場合もあれば、別のエラーが表示される場合もあります。

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

- カーネルが改ざんされている場合、次のようなエラーが表示されます。

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

- パッケージ（VIB またはドライバ）が改ざんされている場合、パープル スクリーンに次のメッセージが表示されます。

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

セキュア ブートの問題を解決するには、次の手順に従います。

1 セキュア ブートを無効にしてホストを再起動します。

2 セキュア ブート検証スクリプトを実行します（アップグレード後の ESXi ホストでのセキュア ブート検証スクリプトの実行を参照してください）。

3 `/var/log/esxupdate.log` ファイル内の情報を確認します。

アップグレード後の ESXi ホストでのセキュア ブート検証スクリプトの実行

UEFI セキュア ブートをサポートしていない ESXi の以前のバージョンから ESXi ホストをアップグレードした後は、セキュア ブートを有効にできる場合があります。セキュア ブートを有効にできるかどうかは、アップグレードの実行方法と、アップグレードによってすべての既存の VIB が置換されたか、一部の VIB が変更されないまま残されたかによって異なります。アップグレード後に検証スクリプトを実行して、アップグレード後のインストールがセキュア ブートをサポートするかどうかを判断できます。

セキュア ブートを正常に行うためには、インストールされているすべての VIB の署名がシステムで使用できる必要があります。ESXi の以前のバージョンは、VIB のインストール時に署名を保存できません。

- esxcli コマンドを使用してアップグレードすると、古いバージョンの ESXi は新しい VIB のインストールを実行するため、署名が保存されず、セキュア ブートは実行できません。
- ISO を使用してアップグレードすると、新しい VIB は署名を保存できます。これは、ISO を使用した vSphere Lifecycle Manager のアップグレードにもあてはまります。
- 以前の VIB がシステムに残っている場合、それらの VIB の署名は使用できず、セキュア ブートは実行できません。
  - システムがサードパーティ製ドライバを使用しており、VMware のアップグレードにドライバ VIB の新しいバージョンが含まれていない場合、アップグレード後に以前のバージョンの VIB がシステムに残ります。
  - まれに、VMware は特定の VIB の開発を継続せず、古い VIB を置き換える新しい VIB を提供しない場合があります。その際は、アップグレード後に古い VIB がシステムに残ることがあります。

注： UEFI セキュア ブートには、最新のブートローダーも必要です。このスクリプトは、最新のブートローダーをチェックしません。

前提条件

- ハードウェアで UEFI セキュア ブートがサポートされることを確認します。
- すべての VIB が、最低でも許容レベル PartnerSupported で署名されていることを確認します。CommunitySupported レベルの VIB を含めると、セキュア ブートを使用できません。

手順

1 ESXi をアップグレードして、次のコマンドを実行します。

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

2 出力を確認します。

`Secure boot can be enabled` または `Secure boot CANNOT be enabled` のいずれかが出力されます。

Trusted Platform Module による ESXi ホストの保護

ESXi ホストでは Trusted Platform Module (TPM) チップを使用できます。TPM は、ソフトウェアではなくハードウェアに基づく信頼保証を提供することでホストのセキュリティを強化するセキュアな暗号プロセッサです。

TPM は、セキュアな暗号プロセッサに関する業界全体の標準です。TPM チップは、ラップトップ、デスクトップ、サーバなど、現在使用されているほとんどのコンピュータに搭載されています。vSphere 6.7 以降は TPM バージョン 2.0 をサポートします。

TPM 2.0 チップは ESXi ホストの ID を証明します。ホストの証明は、指定時刻におけるホストのソフトウェアの状態を認証して、証明するプロセスのことです。署名されたソフトウェアのみが起動時にロードされるようにする UEFI セキュア ブートは、正常な証明の要件です。システム内で起動されたソフトウェア モジュールの測定値は TPM 2.0 チップに記録され、安全に保存されて、vCenter Server によってリモートに検証されます。

次に、リモート証明プロセスの手順の概要を示します。

1 リモート TPM の信頼性を確立して、リモート TPM の証明キー (AK) を作成します。

vCenter Server で ESXi ホストの追加、再起動、再接続が実行されると、vCenter Server はホストに対して認証キー (AK) を要求します。AK 作成プロセスでは TPM ハードウェア自体の検証も行われ、既知の（信頼できる）ベンダーがハードウェアを製造したことを確認できます。

2 ホストから、証明レポートを取得します。

vCenter Server を使用するには、TPM によって署名された Platform Configuration Register (PCR) の引用、およびその他のホストの署名付きバイナリ メタデータを含む証明レポートをホストから送信する必要があります。vCenter Server は信頼できると見なされている構成に情報が対応していることを確認することで、以前は信頼されていなかったホストのプラットフォームを識別します。

3 ホストの信頼性を確認します。

vCenter Server は署名付き引用の信頼性を検証し、ソフトウェアのバージョンを推測し、上記ソフトウェア バージョンの信頼性を判断します。vCenter Server によって署名付き引用が無効であると判断された場合は、リモート証明に失敗し、ホストは信頼されません。

TPM 2.0 チップを使用するには、vCenter Server 環境が次に示す要件を満たす必要があります。

- vCenter Server 6.7 以降
- TPM 2.0 チップを搭載していて、UEFI で有効になっている ESXi 6.7 以降のホスト
- 有効な UEFI セキュア ブート

ESXi ホストの BIOS で、TPM が SHA 256 ハッシュ アルゴリズムおよび TIS/FIFO (First-In, First-Out) インターフェイスを使用し、CRB (Command Response Buffer) は使用しないように構成されていることを確認します。これらの必要な BIOS オプションの設定方法については、ベンダーのドキュメントを参照してください。

次の場所で、VMware 認定の TPM 2.0 チップを確認します。

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

TPM 2.0 チップが搭載された ESXi ホストを起動するときに、vCenter Server はホストの証明ステータスを監視します。vSphere Client の vCenter Server の [サマリ] タブの [セキュリティ] に、ハードウェアの信頼ステータスが次のアラームと共に表示されます。

- 緑：完全に信頼されていることを示す通常のステータスです。
- 赤：証明に失敗しました。

注： すでに vCenter Server を管理している ESXi ホストに TPM 2.0 チップを追加する場合、ホストを切断してから、再度接続する必要があります。ホストの切断と再接続の詳細については、『vCenter Server およびホストの管理』ドキュメントを参照してください。

(ESXi と Trusted Platform Module 2.0 機能のデモ)

ESXi ホスト証明ステータスの表示

Trusted Platform Module 2.0 と互換性のあるチップは、ESXi ホストに追加されるとプラットフォームの整合性を証明します。vSphere Client でホストの証明ステータスを表示できます。Intel Trusted Execution Technology (TXT) のステータスを表示することもできます。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 データセンターに移動し、[監視] タブをクリックします。

3 [セキュリティ] をクリックします。

4 [証明] 列でホストのステータスを確認し、[メッセージ] 列で付随するメッセージを参照します。

5 このホストが信頼済みホストの場合は、詳細について信頼済みクラスタの証明ステータスの表示を参照してください。

次のステップ

失敗または警告の証明ステータスについては、ESXi ホスト証明の問題のトラブルシューティングを参照してください。信頼済みホストについては、信頼済みホスト証明の問題のトラブルシューティングを参照してください。

ESXi ホスト証明の問題のトラブルシューティング

ESXi ホストに Trusted Platform Module (TPM) デバイスをインストールするときに、ホストが証明を渡せないことがあります。この問題について考えられる原因をトラブルシューティングすることができます。

手順

1 ESXi ホストのアラームのステータスおよび付随するエラー メッセージを表示します。ESXi ホスト証明ステータスの表示を参照してください。

2 エラー メッセージが「`Host secure boot was disabled`」と表示される場合、セキュア ブートを再度有効にしてこの問題を解決する必要があります。

3 ホストの証明ステータスが失敗した場合は、vCenter Server `vpxd.log` ファイルで次のメッセージを確認します。

```
No cached identity key, loading from DB
```

このメッセージは、vCenter Server がすでに管理している ESXi ホストに TPM 2.0 チップを追加していることを示します。ホストを切断してから、再度接続する必要があります。ホストの切断と再接続の詳細については、『vCenter Server およびホストの管理』ドキュメントを参照してください。

vCenter Server ログ ファイルの詳細（場所、ログのローテーションを含む）については、https://kb.vmware.com/s/article/1021804 にある VMware のナレッジベースの記事を参照してください。

4 その他のすべてのエラー メッセージについては、カスタマ サポートにお問い合わせください。

ESXi ログ ファイル

ログ ファイルは、攻撃のトラブルシューティング、および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には、次の対策を講じてください。

- 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、ホストでアクティビティ専用のログが記録されます。
- ログを中央ホストにリモートで記録し、中央にログ ファイルを収集することができます。そのホストから 1 つのツールを使用してホストを監視し、分析を集約し、ログ データを検索できます。この方法により、監視が容易になり、複数のホストに対する組織的攻撃の情報が明らかになります。
- ESXi ホストでセキュアなリモート Syslog を構成するには、ESXCLI や PowerCLI を使用するか、API クライアントを使用します。
- Syslog 構成を照会し、Syslog サーバとポートが有効であることを確認します。

Syslog の設定および ESXi ログ ファイルの詳細については、vSphere の監視とパフォーマンス のドキュメントを参照してください。

ESXi ホストでの Syslog の構成

vSphere Client または `esxcli system syslog` コマンドを使用して syslog サービスを構成できます。

`esxcli system syslog` コマンドや他の ESXCLI コマンドの使用方法の詳細については、『ESXCLI スタート ガイド』を参照してください。

手順

1. vSphere Client インベントリで、ホストに移動して参照します。
2. [構成] 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] をクリックします。
4. [編集] をクリックします。
5. **`syslog`** でフィルタリングします。
6. ログをグローバルに設定するには、変更する設定を選択して、値を入力します。

オプション	説明
Syslog.global.defaultRotate	保持するアーカイブの最大数です。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。
Syslog.global.defaultSize	システムのログ ローテーションを行う前のログのデフォルト サイズ (KB 単位) です。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。

オプション	説明
Syslog.global.LogDir	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 ボリュームに配置できます。リブート後も変わらないのは、ローカル ファイル システムの `/scratch` ディレクトリのみです。ディレクトリを [*datastorename*] *path_to_file* と指定します。ここで、パスはデータストアをバッキングするボリュームのルートへの相対パスです。例えば、パスの `[storage1] /systemlogs` はパスの `/vmfs/volumes/storage1/systemlogs` にマッピングします。
Syslog.global.logDirUnique	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 [Syslog.global.LogDir] 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 ホストによって使用される場合、固有のディレクトリを作成しておくと便利です。
Syslog.global.LogHost	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。`ssl://hostName1:1514` のように、プロトコルとポートを含めることができます。UDP（ポート 514 でのみ）、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設定されている必要があります。リモート ホストの構成の詳細については、リモート ホストにインストールされている Syslog サービスのドキュメントを参照してください。 Syslog メッセージの受信に使用できるリモート ホストの数に制限はありません。

7 （オプション） 任意のログで、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 ローテーション数とログ サイズを入力します。

8 [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。

表 3-8. ESXi ログ ファイルの場所

コンポーネント	場所	目的
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。
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。
シェル ログ	`/var/log/shell.log`	ESXi シェル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。
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。

表 3-8. ESXi ログ ファイルの場所 （続き）

コンポーネント	場所	目的
vCenter Server 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）。
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/datastore/virtual machine/vwmare.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。
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 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）。
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。
クイック ブート	/var/log/loadESX.log	Quick Boot を使用した ESXi ホストの再起動に関連するすべてのイベントが含まれます。
信頼済みのインフラストラクチャ エージェント	/var/run/log/kmxa.log	ESXi 信頼済みホスト上のクライアント サービスに関連するアクティビティが記録されます。
キー プロバイダ サービス	/var/run/log/kmxd.log	vSphere 信頼機関 キー プロバイダ サービスに関連するアクティビティが記録されます。
証明サービス	/var/run/log/attestd.log	vSphere 信頼機関 の証明サービスに関連するアクティビティが記録されます。
ESX Token Service	/var/run/log/esxtokend.log	vSphere 信頼機関 ESX Token Service に関連するアクティビティが記録されます。
ESX API フォワーダ	/var/run/log/esxapiadapter.log	vSphere 信頼機関 API フォワーダに関連するアクティビティが記録されます。

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

VMware Fault Tolerance （FT） 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。

Fault Tolerance 暗号化の有効化

Fault Tolerance ログ トラフィックを暗号化できます。

vSphere Fault Tolerance はプライマリ仮想マシンとセカンダリ仮想マシン間のチェックを頻繁に実行するため、最後に成功したチェックポイントからセカンダリ仮想マシンをすばやくレジュームできます。チェックポイントには、前のチェックポイント以降に変更された仮想マシンの状態が含まれます。Fault Tolerance ログ トラフィックを暗号化できます。

Fault Tolerance を有効にした場合、FT 暗号化はデフォルトで [任意] に設定されます。つまり、プライマリ ホストとセカンダリ ホストの両方で暗号化が可能な場合にのみ、暗号化が有効になります。FT 暗号化モードを手動で変更する必要がある場合は、次の手順を実行します。

注： Fault Tolerance は、vSphere 7.0 Update 2 以降での vSphere 仮想マシンの暗号化をサポートします。ゲスト内およびアレイベースの暗号化は、仮想マシンの暗号化に依存したり、仮想マシンの暗号化に干渉したりすることはありません。複数の暗号化レイヤーを使用すると、コンピューティング リソースが追加で使用され、仮想マシンのパフォーマンスに影響を与える可能性があります。この影響は、ハードウェアのほか、I/O の量とタイプによって異なりますが、全体的なパフォーマンスへの影響は多くのワークロードで無視できます。重複排除、圧縮、レプリケーションなどのバックエンド ストレージ機能の有効性と互換性も仮想マシンの暗号化の影響を受けることがあります。

前提条件

FT 暗号化には SMP-FT が必須です。レガシー FT（記録/再生 FT）での暗号化はサポートされていません。

手順

1 仮想マシンを選択し、[設定の編集] を選択します。

2 [仮想マシン オプション] で [暗号化された Fault Tolerance] ドロップダウン メニューを選択します。

3 以下のいずれかのオプションを選択します。

オプション	説明
無効	暗号化された Fault Tolerance のログを有効にしないでください。
任意	暗号化は、双方が対応している場合にのみ有効にします。Fault Tolerance 仮想マシンは、暗号化された Fault Tolerance ログをサポートしていない ESXi ホストに移動できます。
必須	暗号化された FT ログをサポートするホストの中から、Fault Tolerance のプライマリ ホストとセカンダリ ホストを選択します。

注： 仮想マシンの暗号化が有効になっている場合、FT 暗号化モードはデフォルトで [必須] に設定され、変更できません。

FT 暗号化モードが [必須] に設定されている場合は、次のようになります。

- FT が有効な場合、FT 暗号化がサポートされているホストのみが、FT セカンダリを配置するホストのリストに表示されます。
- FT フェイルオーバーは、FT 暗号化がサポートされているホストでのみ実行されます。

4 [OK] をクリックします。

ESXi 監査レコードの管理

監査レコードは RFC 5424 に準拠しており、アイテムに関連するイベントに関する情報（時刻、ステータス、説明など）や ESXi ホストに対するアクションから発生したイベントのログに記録されるユーザー情報を含みます。ローカルとリモートの両方の監査レコードを保持できます。監査レコードの保持はデフォルトで無効になっています。ローカルとリモートの両方の監査モードを手動で有効にする必要があります。

ローカル ESXi 監査ログは、最新の監査メッセージの固定サイズ バッファとして動作します。メッセージでバッファがいっぱいになると、新しいレコードによって最も古いレコードが上書きされます。リモート監査ログは、標準 Syslog 形式 (RFC 3164) の監査レコードの同じストリームを暗号化されていない、または暗号化された (RFC 5425) フォームでリモート サーバに転送します。監査メッセージは RFC 5424 に準拠していますが、一般的な Syslog メッセージは RFC 3164 にのみ準拠しています。生成された監査メッセージは、ローカル ストアとリモート ストアに同時に送信されます。

ホストとリモート ストア間の接続が失われると、リモート ストアは生成された監査メッセージを破棄します。再接続時に、メッセージが失われる可能性があることを示す監査メッセージが生成されます。

監査レコードの構成

ESXCLI を使用して、ローカル監査レコードの保持を構成します。詳細については、『ESXCLI のリファレンス』(https://code.vmware.com/) を参照してください。

監査レコードの表示

監査レコードは次のように表示できます。

- ローカル：ESXi `/bin/viewAudit` アプリケーションを使用します。
- リモート：ESXCLI を使用して、リモート監査サーバを構成します。

FetchAuditRecords API（DiagnosticsManager 管理対象オブジェクト内）を使用して、監査レコードを表示することもできます。

ESXi 構成をセキュアにする

vSphere 7.0 Update 2 から、ESXi の構成は暗号化によって保護されます。オプションで ESXi ホストが TPM で保護されている場合、ESXi 構成の暗号化キーは TPM によってシールされます。

ESXi は、構成ファイルにシークレットを格納します。これらの構成は、アーカイブ ファイルとして ESXi ホストのブートバンクに保持されます。vSphere 7.0 Update 2 以降、このアーカイブ ファイルは暗号化されています。その結果、たとえ ESXi ホストのストレージに物理的にアクセスできたとしても、攻撃者はこのファイルを直接読み取ったり、変更したりすることはできません。

攻撃者によるシークレットへのアクセスを防ぐことができるだけでなく、TPM と併用することで、セキュアな ESXi 構成により、再起動時にも仮想マシンの暗号化キーを保存することができます。その結果、暗号化されたワークロードは、キー サーバが使用できない場合やアクセスできない場合に引き続き機能する可能性があります。キーの永続性の概要を参照してください。

セキュアな ESXi 構成の概要

ESXi 構成の暗号化を手動で有効にする必要はありません。vSphere 7.0 Update 2 以降をインストールまたはアップグレードすると、アーカイブされた ESXi 構成が暗号化されます。

vSphere 7.0 Update 2 以前では、アーカイブされた ESXi 構成ファイルは暗号化されません。vSphere 7.0 Update 2 以降 では、アーカイブされた構成ファイルが暗号化されます。ESXi ホストが Trusted Platform Module (TPM) で構成されている場合、TPM は構成をホストに「シーリング」するために使用され、強力なセキュリティ保証を提供します。

vSphere 7.0 Update 2 より前の ESXi 構成ファイルの概要

ESXi ホストの構成は、ホストで実行される各サービスの構成ファイルで構成されます。構成ファイルは通常、`/etc/` ディレクトリに存在しますが、他のネームスペースにも存在できます。構成ファイルには、サービスの状態に関する実行時情報が含まれています。時間の経過とともに、構成ファイルのデフォルト値が変更される可能性があります。たとえば、ESXi ホストの設定を変更した場合などです。cron ジョブは、ESXi 構成ファイルを定期的に、または ESXi が正常に、またはオンデマンドでシャットダウンしたときにバックアップし、ブート バンクにアーカイブ構成ファイルを作成します。ESXi が再起動すると、アーカイブされた構成ファイルが読み取られ、バックアップが作成されたときの ESXi の状態が再作成されます。vSphere 7.0 Update 2 以前では、アーカイブされた構成ファイルは暗号化されていません。その結果、物理的な ESXi ストレージにアクセスできる攻撃者が、システムがオフラインのときにこのファイルを読み取って変更する可能性があります。

セキュアな ESXi 構成の概要

ESXi ホストを vSphere 7.0 Update 2 以降にインストールまたはアップグレードした後の最初の起動時に、次のことが発生します。

- ESXi ホストに TPM があり、ファームウェアで有効になっている場合、アーカイブされた構成ファイルは、TPM に格納されている暗号化キーによって暗号化されます。この時点から、ホストの構成は TPM によってシーリングされます。
- ESXi ホストに TPM がない場合、ESXi は鍵導出関数 (KDF) を使用して、アーカイブされた構成ファイルのセキュアな構成暗号化鍵を生成します。KDF への入力は、ディスク内の `encryption.info` ファイルに保存されます。

注： ESXi ホストで有効な TPM デバイスがある場合、追加の保護が得られます

最初の起動後に ESXi ホストが再起動すると、次のことが発生します。

- ホストに ESXi TPM がある場合、ホストは、その特定のホストの TPM から暗号化キーを取得する必要があります。TPM 測定値が暗号化キーの作成時に使用されたシーリング ポリシーを満たす場合、ホストは TPM から暗号化キーを取得します。
- ESXi ホストに TPM がない場合、ESXi は `encryption.info` ファイルから情報を読み取り、セキュなな構成のロックを解除します。

セキュアな ESXi 構成の要件

- ESXi 7.0 Update 2 以降
- 構成の暗号化とシーリング ポリシーを使用する機能のための TPM 2.0

セキュアな ESXi 構成のリカバリ キー

セキュアな ESXi にはリカバリ キーが含まれています。セキュアな ESXi 構成をリカバリする必要がある場合は、コマンドライン ブート オプションとして入力した内容のリカバリ キーを使用します。リカバリ キーを一覧表示して、リカバリ キーのバックアップを作成できます。セキュリティ要件の一部としてリカバリ キーをローテーションできます。

リカバリーキーのバックアップを取ることは、セキュアな ESXi 構成を管理する上で重要な部分です。vCenter Server は、リカバリ キーのバックアップを通知するアラームを生成します。

リカバリ キー アラーム

リカバリーキーのバックアップを取ることは、セキュアな ESXi 構成を管理する上で重要な部分です。TPM モードの ESXi ホストが vCenter Server に接続または再接続されるたびに、vCenter Server はアラームを生成して、リカバリ キーをバックアップするように通知します。アラームをリセットすると、条件が変更されない限り、アラームは再び発生されません。

セキュアな ESXi 構成のベストプラクティス

リカバリ キーに関する以下のベスト プラクティスに従ってください。

- リカバリ キーを一覧表示すると、そのリカバリ キーは一時的に信頼されていない環境に表示され、メモリ内に保存されます。キーのトレースを削除します。
  - ホストを再起動すると、メモリに残ったキーが削除されます。
  - 保護を強化するには、ホストで暗号化モードを有効にします。ホスト暗号化モードを明示的に有効にするを参照してください。
- リカバリを実行する場合：
  - 信頼されていない環境でリカバリ キーのトレースを排除するには、ホストを再起動します。
  - セキュリティを強化するために、キーを 1 回リカバリした後に、リカバリ キーをローテーションして新しいキーを使用します。

TPM シーリング ポリシーの概要

vSphere 7.0 Update 2 以降で、ESXi ホストは TPM を使用して、プラットフォーム構成レジスタ (PCR) ポリシーに対してホストの構成をシールします。PCR ポリシーは、UEFI セキュア ブートなどの設定を強制するように構成できます。

TPM は、プラットフォーム構成レジスタ (PCR) 測定値を使用して、機密データへの不正アクセスを制限するポリシーを実装できます。TPM を使用する ESXi ホストを vSphere 7.0 Update 2 以降にインストールまたはアップグレードする場合、TPM はセキュア ブート設定を組み込んだポリシーを使用して機密情報をシールします。このポリシーは、データが TPM で最初にシーリングされた時にセキュア ブートが有効になっていた場合、後続のブートでデータをシーリングしようとするときにセキュアブートを有効にする必要があることを確認します。

セキュア ブートは、UEFI ファームウェア標準の一部です。UEFI セキュア ブートが有効な場合、オペレーティング システムのブートローダーに有効なデジタル署名がない限り、、ホストに UEFI ドライバまたはアプリケーションはロードされません。

UEFI セキュア ブートの強制適用を無効または有効にできます。セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化を参照してください。

注： vSphere 7.0 Update 2 以降をインストールまたは vSphere 7.0 Update 2 以降にアップグレードするときに TPM を有効にしない場合は、後で次のコマンドを使用して有効にできます。

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

TPM を有効化すると、設定を取り消すことはできません。

TPM がホストで有効な場合でも、一部の TPM で `esxcli system settings encryption set` コマンドが失敗します。

- vSphere 7.0 Update 2 の場合：NationZ (NTZ)、Infineon Technologies (IFX)、および Nuvoton Technologies Corporation (NTC) の特定の新しいモデル（NPCT75x など）からの TPM
- vSphere 7.0 Update 3 の場合：NationZ (NTZ) からの TPM

vSphere 7.0 Update 2 以降の最初の起動中に TPM を使用できない場合、このインストールまたはアップグレードは続行され、モードはデフォルトで「なし」(`--mode=NONE`) になります。その結果、TPM がアクティブ化されていない場合と同様に動作します。

TPM は、シーリング ポリシーの execInstalledOnly 起動オプションの設定を適用することもできます。execInstalledOnly の強制適用は、VMkernel が VIB の一部として適切にパッケージ化され署名されたバイナリのみを実行する高度な ESXi 起動オプションです。execInstalledOnly 起動オプションは、セキュア ブート オプションに依存します。シーリング ポリシーで execInstalledOnly 起動オプションを強制適用する前に、セキュア ブートの強制適用を有効にする必要があります。セキュアな ESXi 構成の execInstalledOnly の適用の有効化/無効化を参照してください。

セキュアな ESXi 構成の管理

ESXCLI コマンドを使用して、セキュアな ESXi 構成リカバリ キーの一覧表示、リカバリ キーのローテーション、および TPM ポリシーの変更（UEFI セキュア ブートの適用など）を実行できます。

セキュアな ESXi 構成リカバリ キーの内容の一覧表示

ESXCLI を使用して、セキュアな ESXi 構成リカバリ キーの内容を表示できます。

このタスクは、TPM がある ESXi ホストにのみ適用されます。通常、バックアップを作成する際、またはリカバリ キーのローテーションの一環として、セキュアな ESXi 構成リカバリ キーの内容を一覧表示します。

前提条件

- ESXCLI コマンド セットにアクセス可能であること。ESXCLI コマンドはリモートで実行することも、ESXi シェルで実行することもできます。
- ESXCLI スタンドアローン バージョンまたは PowerCLI を使用するために必要な権限：ホスト.構成.設定

手順

1 ESXi ホストで次のコマンドを実行します。

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

2 セキュアな構成をリカバリする必要がある場合に備えて、出力をバックアップとして安全なリモートの場所に保存します。

結果

リカバリ キー ID とキーが表示されます。

例： セキュアな ESXi 構成のリカバリ キーの一覧表示

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

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

セキュア な ESXi 構成のリカバリ キーのローテーション

ESXCLI を使用すると、セキュアな ESXi 構成のリカバリ キーをローテーションできます。

このタスクは、TPM がある ESXi ホストにのみ適用されます。セキュリティのベスト プラクティスの一環としてセキュアな ESXi 構成のリカバリ キーをローテーションできます。

前提条件

- ESXCLI コマンド セットにアクセス可能であること。ESXCLI コマンドはリモートで実行することも、ESXi シェルで実行することもできます。
- ESXCLI スタンドアローン バージョンまたは PowerCLI を使用するために必要な権限：ホスト.構成.設定

手順

1 リカバリ キーを一覧表示します。

セキュアな ESXi 構成リカバリ キーの内容の一覧表示を参照してください。

2 次のコマンドを実行します。

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

このコマンドでは、オプションの *keyID* は VMkernel キー キャッシュのキー ID、*uuid* はリカバリ ID（`esxcli system settings encryption recovery list` コマンドから取得）です。オプションのキー ID を指定しない場合、ESXi では古いリカバリ キーがランダムに生成される新しいリカバリ キーと置き換えられます。

結果

指定されている場合、リカバリ キーがキー ID によって参照されるキーの内容に設定されます。それ以外の場合、ESXi で新しいキー ID が指定されます。

セキュア な ESXi 構成のトラブルシューティングとリカバリ

セキュアな ESXi 構成で発生する可能性のあるブート問題をトラブルシューティングしてリカバリできます。

TPM をクリアした場合（TPM のシード値がリセットされる）、または TPM に障害が発生した場合は、セキュアな ESXi 構成をリストアするための手順を実行する必要があります。構成をリストアするには、リカバリ キーが必要です。ESXi 構成をリカバリするまで、ホストは起動できません。セキュアな ESXi 構成のリカバリを参照してください。

まれですが、ESXi ホストがセキュアな構成のリストアまたは復号化に失敗し、ホストが起動できなくなる可能性があります考えられる状況は次のとおりです。

- セキュア ブート設定（または他のポリシー）が変更された
- 改ざんが実際に行われた
- リカバリ キーが使用できない

これらの状態に対するトラブルシューティングを行うには、VMware ナレッジベースの記事 (https://kb.vmware.com/kb/81446) を参照してください。

セキュアな ESXi 構成のリカバリ

TPM に障害が発生した場合、または TPM をクリアする場合は、セキュアな ESXi 構成をリカバリする必要があります。ESXi 構成をリカバリするまで、ホストは起動できません。

セキュアな ESXi 構成をリカバリするこは、次の状況のことを指します。

- TPM をクリアした（TPM のシードがリセットされた）。
- TPM が失敗した。

他のセキュアな ESXi 構成の問題に対するトラブルシューティングについては、VMware ナレッジベースの記事 (https://kb.vmware.com/kb/81446) を参照してください。

リカバリを手動で実行します。インストールまたはアップグレード スクリプトの一部としてリカバリを実行しないでください。

前提条件

リカバリ キーを取得します。以前にリカバリ キーを一覧表示して保存している必要があります。セキュアな ESXi 構成リカバリ キーの内容の一覧表示を参照してください。

手順

1. （オプション） TPM に障害が発生した場合は、（ブート バンクで）ディスクを TPM がある別のホストに移動します。
2. ESXi ホストを起動します。
3. ESXi インストーラのウィンドウが表示されたら、Shift + O を押して起動オプションを編集します。

4 コマンド プロンプトで起動オプションを入力し、構成をリカバリします。

```
encryptionRecoveryKey=recovery_key
```

セキュアな ESXi 構成がリカバリされ、ESXi ホストが起動します。

5 変更を保持するには、次のコマンドを実行します。

```
/sbin/auto-backup.sh
```

次のステップ

リカバリ キーを入力すると、信頼できない環境に一時的に表示され、メモリに保存されます。必要ではありませんが、ベスト プラクティスとして、ホストを再起動すると、メモリ内のキーの残ったトレースを削除できます。または、キーをローテートさせることもできます。セキュア な ESXi 構成のリカバリ キーのローテーションを参照してください。

セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化

UEFI セキュア ブートの適用を有効にするか、以前に有効にした UEFI セキュア ブートの適用を無効にするかを選択できます。ESXi ホストの TPM の設定を変更するには、ESXCLI を使用する必要があります。

このタスクは、TPM を備えた ESXi ホストにのみ適用されます。UEFI セキュア ブートは、ファームウェアによって起動されたソフトウェアが信頼できることを保証するためのファームウェア設定です。UEFI セキュア ブートの有効化は、TPM を使用してすべてのブートで実行できます。

前提条件

- ESXCLI コマンド セットにアクセス可能であること。ESXCLI コマンドはリモートで実行することも、ESXi シェルで実行することもできます。
- ESXCLI スタンドアローン バージョンまたは PowerCLI を使用するために必要な権限：ホスト.構成.設定

手順

1 ESXi ホストの現在の設定を一覧表示します。

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

セキュア ブートの適用が有効になっている場合、[セキュア ブートが必要] には「true」と表示されます。セキュア ブートの適用が無効になっている場合、[セキュア ブートが必要] には「false」と表示されます。

モード が NONE と表示される場合は、ホストのファームウェアで TPM を有効にし、次のコマンドを実行してモードを設定する必要があります。

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

2 セキュア ブートの適用を有効または無効にする

オプション	説明

有効化	a ホストを正常にシャットダウンします。
	たとえば、vSphere Client の ESXi ホストを右クリックし、[電源] - [シャットダウン] を選択します。
	b ホストのファームウェアでセキュア ブートを有効にします。
	特定のベンダーのハードウェア ドキュメントを参照してください。
	c ホストを再起動します。
	d 次の ESXCLI コマンドを実行します。
	`esxcli system settings encryption set --require-secure-boot=T`
	e 変更を確認します。
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[セキュア ブートが必要] に「true」と表示されていることを確認します。
	f 設定を保存するには、次のコマンドを実行します。
	`/sbin/auto-backup.sh`

無効化	a 次の ESXCLI コマンドを実行します。
	`esxcli system settings encryption set --require-secure-boot=F`
	b 変更を確認します。
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	[セキュア ブートが必要] に「false」と表示されていることを確認します。
	c 設定を保存するには、次のコマンドを実行します。
	`/sbin/auto-backup.sh`
	ホストのファームウェアでセキュア ブートを無効にすることを選択できますが、この時点で、ファームウェア設定と TPM 適用の間の依存関係は設定されなくなります。

結果

ESXi ホストは、選択に応じて、セキュア ブートの適用を有効または無効にして実行されます。

注： vSphere 7.0 Update 2 以降をインストールまたは vSphere 7.0 Update 2 以降にアップグレードするときに TPM を有効にしない場合は、後で次のコマンドを使用して有効にできます。

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

TPM を有効化すると、設定を取り消すことはできません。

TPM がホストで有効な場合でも、一部の TPM で `esxcli system settings encryption set` コマンドが失敗します。

- vSphere 7.0 Update 2 の場合：NationZ (NTZ)、Infineon Technologies (IFX)、および Nuvoton Technologies Corporation (NTC) の特定の新しいモデル（NPCT75x など）からの TPM
- vSphere 7.0 Update 3 の場合：NationZ (NTZ) からの TPM

vSphere 7.0 Update 2 以降の最初の起動中に TPM を使用できない場合、このインストールまたはアップグレードは続行され、モードはデフォルトで「なし」(`--mode=NONE`) になります。その結果、TPM がアクティブ化されていない場合と同様に動作します。

セキュアな ESXi 構成の execInstalledOnly の適用の有効化/無効化

execInstalledOnly の適用を有効にするか、以前に有効にした execInstalledOnly の適用を無効にするかを選択できます。ESXi ホストの TPM の設定を変更するには、ESXCLI を使用する必要があります。execInstalledOnly の適用を有効にする前に、UEFI セキュア ブートの適用を有効にする必要があります。

このタスクは、TPM を備えた ESXi ホストにのみ適用されます。execInstalledOnly の高度な ESXi ブート オプションを TRUE に設定すると、VMkernel が VIB の一部としてパッケージ化および署名されたバイナリのみを実行することが保証されます。このブート オプションの有効化は、TPM を使用してすべてのブートで実行できます。

前提条件

- execInstalledOnly の適用を有効にするには、最初に UEFI セキュア ブートの適用を有効にする必要があります。execInstalledOnly の適用は、UEFI セキュア ブートの適用の上に構築されます。セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化を参照してください。
- ESXCLI コマンド セットにアクセス可能であること。ESXCLI コマンドはリモートで実行することも、ESXi シェルで実行することもできます。
- ESXCLI スタンドアローン バージョンまたは PowerCLI を使用するために必要な権限：ホスト.構成.設定

手順

1 ESXi ホストの現在の設定を一覧表示します。

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

execInstalledOnly の適用が有効になっている場合、[インストールされた VIB からのみ実行可能ファイルを要求する] に「true」と表示されます。execInstalledOnly の適用が無効になっている場合、[インストールされた VIB からのみ実行可能ファイルを要求する] に「false」と表示されます。execInstalledOnly の適用を有効にするには、セキュア ブートの適用を有効にする必要があります。この場合、[セキュア ブートが必要] には「true」と表示されます。

モード が NONE と表示される場合は、ホストのファームウェアで TPM を有効にし、次のコマンドを実行してモードを設定する必要があります。

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

また、[セキュア ブートが必要] に「False」と表示されている場合は、セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化を参照して適用を有効にします。

2 execInstalledOnly の適用を有効または無効にする

オプション	説明

有効化	a セキュア ブート オプションが適用されていることを確認します。
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[セキュア ブートが必要] に「true」と表示されていることを確認します。表示されていない場合は、セキュアな ESXi 構成のセキュア ブートの適用の有効化/無効化を参照してください。
	b execInstalledOnly ブート オプションの実行時の値を TRUE に構成するには、次の ESXCLI コマンドを実行します。
	`esxcli system settings kernel set -s execInstalledOnly -v TRUE`
	c ホストを正常にシャットダウンします。
	たとえば、vSphere Client の ESXi ホストを右クリックし、[電源] - [シャットダウン] を選択します。
	d ホストを再起動します。
	e execInstalledOnly の適用を設定するには、次の ESXCLI コマンドを実行します。
	`esxcli system settings encryption set --require-exec-installed-only=T`
	f 変更を確認します。
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	[インストールされた VIB からのみ実行可能ファイルを要求する] に「true」と表示されていることを確認します。
	g 設定を保存するには、次のコマンドを実行します。
	`/sbin/auto-backup.sh`

無効化	a 次の ESXCLI コマンドを実行します。
	`esxcli system settings encryption set --require-exec-installed-only=F`
	b 変更を確認します。
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[インストールされた VIB からのみ実行可能ファイルを要求する] に「false」と表示されていることを確認します。

オプション	説明
	c 設定を保存するには、次のコマンドを実行します。 `/sbin/auto-backup.sh` TPM は、execInstalledOnly ブート オプションを適用しなくなりました。

結果

ESXi ホストは、選択に応じて、execInstalledOnly の適用を有効または無効にして実行されます。

vCenter Server システムのセキュリティ

4

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

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

- 管理者ロールは、そのロールを必要とする管理者にのみ付与します。権限に制限のある管理者向けに、カスタム ロール作成したり、非暗号化管理者ロールを使用することができます。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、このロールを付与しないようにします。
- vCenter Server システムへの接続時に、アプリケーションが一意のサービス アカウントを使用するようにしてください。

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。

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 ホスト マシン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。これらのユーザーが、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 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。

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。vCenter Server のインストールまたはアップグレード後に、データベース管理者からこれらの権限を削除できます。

データストア ブラウザ アクセスの制限

データストア.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。この権限を持つユーザーは、Web ブラウザまたは vSphere Client を使用して、vSphere の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参照、アップロード、またはダウンロードできます。

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、カスタムの非ゲスト 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 ポリシー変更を検討

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。この設定が会社のポリシーに一致していることを確認し、一致していない場合は、vCenter Server のパスワード 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 フォルダに対する管理者ロールを持つユーザーまたはグループを再起動中に検証できない場合は、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。代わりに、vCenter Server は vCenter Single Sign-On 管理者（デフォルトでは administrator@vsphere.local）に管理者ロールを付与します。その後、このアカウントは vCenter Server 管理者の役割を果たすことができます。

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 vCenter Single Sign-On 管理者アカウント（デフォルトでは administrator@vsphere.local）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 Client 証明書の確認

vSphere Client または他のクライアント アプリケーションのユーザーに、証明書検証の警告に注意するよう喚起してください。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 Client から変更できます。

手順

1. vSphere Client を使用して、vCenter Server システムにログインします。
2. オブジェクト階層で、vCenter Server システムを選択します。
3. [構成] をクリックします。
4. [詳細設定] をクリックし、[設定の編集] をクリックします。
5. [フィルタ] アイコンをクリックし、「**VimPasswordExpirationInDays**」と入力します。
6. 要件を満たすように `VirtualCenter.VimPasswordExpirationInDays` を設定します。

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のと同時に 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 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。
- DNS、Active Directory、および PTP または 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 で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。

CLI と SDK を使用した Linux クライアントの使用の評価

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。

セキュリティ向上のため、vCenter Server システムと ESXi ホストにある VMware 認証局 (VMCA) の署名済み証明書を、エンタープライズまたはサードパーティ CA によって署名された証明書に置き換えることができます。ただし、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。

- ESXCLI 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に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。
- Bastion ホスト（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。

クライアント プラグインの調査

vSphere 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インストールを使用します。

vCenter Server のインストールには、vSphere Client の拡張フレームワークが含まれています。このフレームワークを使用すると、メニュー選択項目またはツールバーのアイコンでクライアントを拡張できます。拡張機能は、vCenter Server アドオン コンポーネントや外部の Web ベースの機能へのアクセスを提供できます。

拡張フレームワークを使用すると、意図しない機能が導入されるリスクがあります。たとえば、管理者が vSphere 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 Client を潜在的な危険性から保護するには、インストールされているすべてのプラグインを定期的に確認し、各プラグインは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 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 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ためのすべてのベスト プラクティスに従ってください。追加の手順を実行すると、お使いの vCenter Server のセキュリティを高めることができます。

PTP または NTP の設定

すべてのシステムで同じ相対時間ソースが使用されていることを確認します。この時間ソースは、協定世界時 (UTC) のような合意された時間標準と同期している必要があります。システムの同期は、証明書の検証を行うために不可欠です。PTP と 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、監査が不正確になります。vCenter Server と NTP サーバとの時刻同期を参照してください。

vCenter Server のネットワーク アクセスの制限

vCenter Server との通信に必要なコンポーネントへの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 システムに対する攻撃の可能性を軽減できます。

vSphere、vSAN を含む VMware 製品でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。VMware 製品別のポート検索、ポートのカスタマイズ リストの作成、およびポート リストの出力または保存を行うことができます。

Bastion ホストの構成

アセットを保護するため、Bastion ホスト（ジャンプ ボックスとも呼ばれます）で、引き上げられた管理タスクが実行されるよう構成します。Bastion ホストは、最小数の管理アプリケーションをホストする専用コンピュ

ータです。その他の不要なサービスはすべて削除されます。ホストは通常、管理ネットワーク上に配置されます。Bastion ホストでは、ログインを主要なユーザーに制限し、ログインするためのファイアウォール ルールを要求し、監査ツールによる監視を追加することで、アセットの保護が強化されます。

vCenter のパスワード要件とロックアウト動作

vSphere 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。

このセクションでは、vCenter Single Sign-On のパスワードについて説明します。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 の管理者パスワード

デフォルトで administrator@vsphere.local である vCenter Single Sign-On 管理者のパスワードは、vCenter Single Sign-On パスワード ポリシーによって指定されます。デフォルトでは、このパスワードは次の要件を満たす必要があります。

- 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

このユーザーのパスワードの長さは 20 文字までです。ASCII 以外の文字を使用できます。管理者はデフォルトのパスワード ポリシーを変更できます。『vSphere の認証』ドキュメントを参照してください。

vCenter Server のパスワード

vCenter Server では、パスワード要件は vCenter Single Sign-On、または Active Directory、OpenLDAP などの構成済み ID ソースによって決定されます。

vCenter Single Sign-On のロックアウト動作

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、vCenter Single Sign-On のロックアウト ポリシーを使用して変更できます。『vSphere の認証』を参照してください。

vCenter Single Sign-On 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。ユーザーはパスワード ポリシーの影響を受けます。

パスワードの変更

パスワードがわかっている場合は、`dir-cli password change` コマンドを使用してパスワードを変更できます。パスワードを忘れた場合は、vCenter Single Sign-On 管理者が `dir-cli password reset` コマンドを使用してユーザーのパスワードをリセットできます。

VMware のナレッジベースで、vSphere の各バージョンにおけるパスワードの有効期限とそれに関連するトピックを検索してください。

レガシー ESXi ホストのサムプリントの検証

vSphere 6.0 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 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 Client インベントリの vCenter Server を参照します。
2. [構成] をクリックします。
3. [設定] で、[全般] をクリックします。
4. [編集] をクリックします。
5. [SSL 設定] をクリックします。
6. ESXi 5.5 以前のホストのいずれかを手動で検証する場合、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。

   a. ダイレクト コンソールにログインし、F2 キーを押して [システムのカスタマイズ] メニューにアクセスします。

   b. [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。
7. 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。
8. [[保存]] をクリックします。

vCenter Server に必要なポート

vCenter Server システムは、すべての管理対象ホストへデータを送信可能であり、かつ vSphere Client からデータを受信できる必要があります。管理対象ホスト間での移行アクティビティやプロビジョニング アクティビティを有効にするには、事前に設定された TCP ポートおよび UDP ポートを経由して送信元ホストと送信先ホスト間でデータの送受信が可能である必要があります。

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。vSphere でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com の VMware Ports and Protocols Tool™ を参照してください。

インストール中、ポートが使用中であるか、拒否リストを使用してブロックされている場合は、vCenter Server インストーラによってエラー メッセージが表示されます。インストールを続行するには別のポート番号を使用する必要があります。プロセス間通信でのみ使用される内部ポートがあります。

VMware では、通信に指定のポートが使用されます。また、管理対象ホストでは、vCenter Server からのデータが指定ポートで監視されます。これらのいずれかの構成要素の間に組み込みのファイアウォールが存在する場合は、インストールまたはアップグレードのプロセスで、インストーラによってポートが開かれます。カスタマイズされたファイアウォールの場合は、必要なポートを手動で開く必要があります。管理対象ホスト 2 台の間にファイアウォールが存在し、移行、クローン作成など、送信元または送信先のアクティビティを実行する場合、管理対象ホストがデータを受信できるように構成する必要があります。

別のポートを使用して vSphere Client データを受信するように vCenter Server システムを構成するには、『vCenter Server およびホストの管理』を参照してください。

仮想マシンのセキュリティ

5

仮想マシンで実行するゲスト OS は、物理システムと同様のセキュリティ リスクにさらされます。仮想マシンを物理マシンと同様のセキュリティで保護し、本書と『セキュリティ設定ガイド』（旧称『セキュリティ強化ガイド』）に記載されているベスト プラクティスを実行します。

『セキュリティ設定ガイド』は、https://core.vmware.com/security から入手できます。

この章には、次のトピックが含まれています。

- 仮想マシンの UEFI セキュア ブートを有効または無効にする
- 仮想マシンから VMX ファイルへの情報メッセージの制限
- 仮想マシンのセキュリティのベスト プラクティス
- Intel Software Guard Extensions による仮想マシンのセキュリティ強化
- AMD の Secure Encrypted Virtualization -Encrypted State による仮想マシンの保護

仮想マシンの UEFI セキュア ブートを有効または無効にする

UEFI セキュア ブートは、PC の製造元が信頼するソフトウェアのみを使用して PC をブートするセキュリティ標準です。特定の仮想マシンのハードウェア バージョンとオペレーティング システムに対しては、物理マシンと同様にセキュア ブートを有効にできます。

UEFI セキュア ブートをサポートするオペレーティング システムでは、ブートローダー、オペレーティング システム カーネル、オペレーティング システムのドライバを含むブート ソフトウェアのそれぞれに署名が付与されています。仮想マシンのデフォルト構成には、いくつかのコード署名証明書が含まれます。

- Windows のブートにのみ使用される Microsoft 証明書。
- Linux ブートローダーなどのサードパーティ コードに使用する Microsoft によって署名された Microsoft 証明書。
- 仮想マシン内の ESXi のブートにのみ使用する VMware 証明書。

仮想マシンのデフォルト構成には、仮想マシン内からセキュア ブート構成の変更要求を認証するための証明書が 1 つ含まれます（セキュア ブート失効リストを含む）。これは Microsoft KEK (Key Exchange Key) 証明書です。

ほとんどの場合、既存の証明書を置き換える必要はありません。証明書を置き換える場合は、VMware ナレッジベースの記事を参照してください。

UEFI セキュア ブートを使用する仮想マシンには、VMware Tools バージョン 10.1 以降が必要です。VMware Tools の 10.1 をインストールしたら、仮想マシンをアップグレードできます。

Linux 仮想マシンのセキュア ブート モードでは、VMware のホスト/ゲスト ファイルシステムがサポートされません。VMware Tools から VMware のホスト/ゲスト ファイルシステムを削除してからセキュア ブートを有効にしてください。

注： 仮想マシンのセキュア ブートを有効にすると、その仮想マシンにロードできるのは、署名されたドライバのみになります。

このタスクでは、vSphere Client を使用して仮想マシンのセキュア ブートを有効にする方法と無効にする方法について説明します。スクリプトを記述して、マシンの設定の管理に使用することもできます。たとえば、次の PowerCLI コードを使用することで仮想マシンの BIOS から EFI へのファームウェアの変更を自動化できます。

```
$vm = Get-VM TestVM

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

詳細については、『VMware PowerCLI User's Guide』を参照してください。

前提条件

セキュア ブートは、すべての前提条件を満たしている場合にのみ有効にできます。前提条件を満たしていない場合、vSphere Client にチェック ボックスは表示されません。

- 仮想マシンのオペレーティング システムとファームウェアが UEFI ブートをサポートしていることを確認します。
  - EFI ファームウェア
  - 仮想ハードウェア バージョン 13 以降。
  - UEFI セキュア ブートをサポートするオペレーティング システム。

  注： 一部のゲスト OS では、ゲスト OS を変更せずに、BIOS ブートから UEFI ブートへの変更を行うことはサポートされません。UEFI ブートへの変更前に、ゲスト OS のドキュメントを参照してください。すでに UEFI ブートを使用している仮想マシンを UEFI セキュア ブートをサポートするオペレーティング システムにアップグレードすると、その仮想マシンのセキュア ブートを有効にできます。
- 仮想マシンをパワーオフします。仮想マシンが実行中の場合、チェック ボックスはグレーアウトされます。

手順

1. vSphere Client インベントリで、仮想マシンを参照します。
2. 仮想マシンを右クリックし、[設定の編集] を選択します。
3. [仮想マシン オプション] タブをクリックし、[起動オプション] を展開します。
4. [起動オプション] で、ファームウェアが [EFI] に設定されていることを確認します。

5 タスクを選択します。

- セキュア ブートを有効にするには、[セキュア ブート] チェック ボックスを選択します。
- セキュア ブートを無効にするには、[セキュア ブート] チェック ボックスを選択解除します。

6 [OK] をクリックします。

結果

仮想マシンの起動時には、有効な署名があるコンポーネントのみが許可されます。署名がないコンポーネントまたは署名が無効なコンポーネントがあると、起動プロセスはエラーで停止します。

仮想マシンから VMX ファイルへの情報メッセージの制限

仮想マシンから VMX ファイルへの情報メッセージを制限することで、データストアの容量がいっぱいになり、サービス拒否 （DoS） が発生することを防ぎます。DoS 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キャパシティを超えた場合に発生します。

仮想マシン構成ファイル（VMX ファイル）の制限は、デフォルトで 1 MB です。通常はこのキャパシティで十分ですが、必要に応じてこの値を変更できます。たとえば、ファイルにカスタム情報を大量に保存する場合は、上限を増やすこともできます。

注： 必要となる情報量を慎重に検討してください。情報量がデータストアのキャパシティを超えると、DoS 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 Client インベントリで、仮想マシンを参照します。

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 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。コンソールへアクセスできるということは、仮想マシンに対する悪意のある攻撃も可能になるということです。

- 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。システムで実行中のアプリケーションやサービスのサポートに必要ではないシステム コンポーネントを無効にすることで、攻撃の対象となる可能性を低減できます。

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。

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と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 の仮想マシン管理』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 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。コンソールへアクセスできるということは、仮想マシンに対する悪意のある攻撃も可能になるということです。

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. 仮想マシン コンソールへの接続を制限してください。

   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複数の同時接続が必要な場合に、接続を増やすことができます。

   a vSphere Client で仮想マシンをパワーオフします。

   b 仮想マシンを右クリックし、[設定の編集] を選択します。

   c [仮想マシン オプション] タブをクリックし、[VMware リモート コンソールのオプション] を展開します。

d　最大セッション数を入力します（**2** など）。

e　[OK] をクリックします。

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。

この影響を十分に理解するまで、制限を設定したり、リソース プールを使用したりしないでください。

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 のリソース管理』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。システムで実行中のアプリケーションやサービスのサポートに必要ではないシステム コンポーネントを無効にすることで、攻撃の対象となる可能性を低減できます。

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。

注：　可能であれば、「最小」または「コア」インストール モードでゲスト OS をインストールして、ゲスト OS のサイズ、複雑さ、および攻撃対象領域を縮小します。

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。

- 未使用の表示機能や、仮想マシンによるホスト ファイルの共有を可能にする VMware の共有フォルダ (Host Guest File System) など、未使用の機能を無効にします。
- 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がある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と攻撃の防止に役立ちます。

仮想マシンに攻撃者がアクセスすると、切断されたハードウェア デバイスに接続し、ハードウェア デバイスに残されたメディア上の機密情報にアクセスできます。攻撃者はまた、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、サービス拒否状態にすることもできます。

- 承認されていないデバイスを仮想マシンに接続しないでください。
- 不要なハードウェア デバイスや未使用のハードウェア デバイスは削除してください。
- 仮想マシン内から不要な仮想デバイスを無効にします。
- 必要なデバイスだけを仮想マシンに接続してください。仮想マシンがシリアル ポートやパラレル ポートを使用することはほとんどありません。原則として、ソフトウェアのインストール中、CD/DVD ドライブは一時的にのみ接続されます。

手順

1. vSphere Client インベントリで、仮想マシンを参照します。
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. 不要なハードウェア デバイスを無効にします。

   次のようなデバイスをチェックします。

   - 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

   注： vSphere 7.0 以降では、PowerCLI コマンドを使用してフロッピー ドライブ デバイスを管理する必要があります。

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。

前提条件

仮想マシンをパワーオフします。

手順

1 vSphere Client インベントリで、仮想マシンに移動して参照します。

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 該当する場合は、次のパラメータを追加または編集します。

オプション	説明
svga.vgaonly	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。このパラメータは、最新のゲスト OS では正しく動作しないため、TRUE に設定しないでください。`svga.vgaonly` を TRUE に設定すると、文字セル コンソール モードのみが使用可能になります。この設定を使用する場合、`mks.enable3d` は無効になります。 **注：** 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。
mks.enable3d	3D 機能を必要と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 環境と、ホストされる仮想化プラットフォーム（VMware Workstation や VMware Fusion など）の両方で使用できます。vSphere 環境で仮想マシンを実行する場合、特定の仮想マシン パラメータを有効にす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低減します。

前提条件

仮想マシンがパワーオフの状態である。

手順

1 vSphere Client インベントリで、仮想マシンを参照します。

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.memSchedFakeSampleStats.disable`
- `isolation.tools.getCreds.disable`
- `isolation.bios.bbs.disable`
- `isolation.tools.hgfsServerSet.disable`

6 [OK] をクリックします。

VMware の共有フォルダによる仮想マシンのホスト ファイル共有の無効化

高セキュリティ環境では、攻撃者が Host Guest File System (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、特定のコンポーネントを無効にすることができます。

このセクションで説明するパラメータを変更すると、共有フォルダ機能にのみ影響し、ゲスト仮想マシンでツールの一部として実行されている HGFS サーバには影響しません。また、これらのパラメータは、ツールのファイル転送を使用する自動アップグレードおよび VIX コマンドには影響しません。

手順

1. vSphere Client インベントリで、仮想マシンに移動して参照します。
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。

   TRUE に設定すると、HGFS サーバ機能の各ツールのサービス、デーモン、またはアップグレーダ プロセスからの通知を VMX プロセスが受信できなくなります。
6. （オプション）`isolation.tools.hgfs.disable` パラメータが TRUE に設定されていることを確認します。

   TRUE に設定すると、仮想マシンに対してホスト ファイルを共有するための未使用の VMware の共有フォルダ機能が無効になります。

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 Client を使用して操作を有効にする必要があります。

安全な環境を確保するために、これらのオプションのデフォルト値が設定されています。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

仮想マシンがパワーオフの状態である。

手順

1. vSphere Client インベントリで、仮想マシンに移動して参照します。
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] 列と [値] 列に次の値が入力されていることを確認するか、値を追加します。

名前	値
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
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。

6 [OK] をクリックします。

7 （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、仮想マシンで実行中のプロセスと、権限のないユーザーは、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、無意識に機密データを仮想マシンにさらす可能性があります。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 管理者ロールを持つユーザーは、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アプリケーションを操作できます。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。仮想マシンのファイルにアクセスする必要がない管理者にそのロールを割り当てます。

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権を制限します。管理者権限を付与する必要があるユーザーに、ゲスト OS のファイルとアプリケーションの操作を許可しない場合は、ゲスト アクセスを無効にするカスタム 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 による移行などのタスクで、データセンター管理者を仮想マシンにアクセスできるようにする必要がある場合は、リモート ゲスト OS の操作の一部を無効にして、そのような管理者が機密情報にアクセスできないようにします。

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 Client にログインします。

2 [管理] を選択して、[ロール] をクリックします。

3 管理者ロールをクリックして、[ロールのクローン作成アクション] をクリックします。

4 ロール名および説明を入力し、[OK] をクリックします。

たとえば、「**ゲスト アクセス不可の管理者**」と入力します。

5 クローン作成したロールを選択して、[ロールの編集アクション] アイコンをクリックします。

6 [仮想マシン] 権限で [ゲスト操作] を選択解除して、[次へ] をクリックします。

7 [終了] 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、新規作成したロールへのアクセス権をユーザーまたはグループに付与する権限を割り当てます。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 root 権限または管理者権限のないユーザーおよびプロセスが、ネットワーク アダプタや CD-ROM ドライブなどのデバイスの接続または切断や、デバイス設定の変更を行うことができます。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。

仮想マシンの詳細設定を変更することで、ゲスト OS の仮想マシン ユーザーと、ゲスト OS で実行されているプロセスによって、デバイスに変更が加えられるのを防止することができます。

前提条件

仮想マシンがパワーオフの状態である。

手順

1 vSphere Client インベントリで、仮想マシンを参照します。

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] 列と [値] 列に次の値が入力されていることを確認するか、値を追加します。

名前	値
isolation.device.connectable.disable	真
isolation.device.edit.disable	真

これらの設定は、仮想マシンに接続されているデバイスを接続および切断できる vSphere 管理者の機能には影響しません。

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 OS が構成を変更しないようにするため、これらのプロセスが構成ファイルに名前と値のペアを書き込めないようにすることができます。

前提条件

仮想マシンがパワーオフの状態である。

手順

1 vSphere Client インベントリで、仮想マシンを参照します。

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 [構成パラメータの追加] をクリックし、[名前] 列と [値] 列に次の値を各列に入力します。

列	値
名前	`isolation.tools.setinfo.disable`
値	`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。

Intel Software Guard Extensions による仮想マシンのセキュリティ強化

vSphere では、仮想マシンに Virtual Intel® Software Guard Extensions (vSGX) を設定できます。vSGX を使用すると、ワークロードのセキュリティを強化できます。

最近の Intel 製 CPU の一部には、Intel® Software Guard Extensions (Intel® SGX) と呼ばれるセキュリティ拡張機能が実装されています。Intel SGX は、特定のコードおよびデータを開示や変更から保護しようとするアプリケーション開発者が使用できる、プロセッサ固有のテクノロジーです。Intel SGX では、エンクレーブと呼ばれるメモリのプライベート領域をユーザーレベルのコードで定義できます。エンクレーブの内容は、エンクレーブの外部で実行されるコードからアクセスできないように保護されます。

ハードウェアで Intel SGX テクノロジーが使用可能な場合、vSGX により仮想マシンで SGX を使用できます。vSGX を使用するには、SGX 対応の CPU に ESXi ホストをインストールし、ESXi ホストの BIOS で SGX を有効にする必要があります。vSphere Client を使用して、仮想マシンで SGX を有効にすることができます。

vSGX の概要

ハードウェアで Intel SGX テクノロジーが使用可能な場合、仮想マシンでも SGX を使用できます。

vSGX の要件

vSGX を使用するには、vSphere 環境が以下の要件を満たす必要があります。

- 仮想マシンの要件：
  - EFI ファームウェア
  - ハードウェア バージョン 17 以降
- コンポーネントの要件：
  - vCenter Server 7.0 以降
  - ESXi 7.0 以降
- ゲスト OS のサポート：
  - Linux
  - Windows Server 2016（64 ビット）以降
  - Windows 10（64 ビット）以降

Intel 製ハードウェア

vSGX でサポートされている Intel 製ハードウェアについては、https://www.vmware.com/resources/compatibility/search.php の『vSphere 互換性ガイド』を参照してください。

特定の CPU では、ESXi ホストで SGX を有効にするためにハイパースレッディングをオフにする必要があります。詳細については、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/71367) を参照してください。

vSGX でサポートされない VMware の機能

vSGX を有効にした仮想マシンでは、次の機能はサポートされません。

- vMotion/DRS 移行
- 仮想マシンのサスペンドおよびレジューム
- 仮想マシンのスナップショット（仮想マシンのメモリのスナップショットを作成しない場合はサポートされます）
- フォールト トレランス
- ゲストの整合性 (GI)（VMware AppDefense™ 1.0 のプラットフォーム基盤）

注： Intel SGX アーキテクチャの機能上の理由により、これらの VMware 機能はサポートされません。VMware 側の欠陥によるものではありません。

仮想マシンでの vSGX の有効化

仮想マシンを作成するときに、その仮想マシンの vSGX を有効にすることができます。

前提条件

SGX 対応の CPU に ESXi ホストがインストールされ、ホストの BIOS で SGX が有効になっている必要があります。サポートされている Intel 製 CPU については、vSGX の概要を参照してください。

ハードウェア バージョン 17 以降および次のサポート対象ゲスト OS のいずれかを使用する仮想マシンを作成します。

- Linux
- Windows 10（64 ビット）以降
- Windows Server 2016（64 ビット）以降

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。
3. オブジェクトを右クリックして [新規仮想マシン] を選択し、表示される画面に沿って仮想マシンを作成します。

オプション	操作
作成タイプの選択	仮想マシンを作成します。
名前とフォルダの選択	名前とターゲットの場所を指定します。
コンピューティング リソースの選択	仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。
ストレージの選択	仮想マシン ストレージ ポリシーでストレージ ポリシーを選択します。互換データストアを選択します。
互換性の選択	[ESXi 7.0 以降] が選択されていることを確認します。
ゲスト OS を選択	Linux、Windows 10（64 ビット）、Windows Server 2016（64 ビット）のいずれかを選択します。

オプション	操作
ハードウェアのカスタマイズ	[セキュリティ デバイス] で、SGX の [有効化] チェックボックスをオンにします。[仮想マシン オプション] - [起動オプション] - [] で、EFI が選択されていることを確認します。隔離領域ページ キャッシュ (EPC) のサイズを入力し、必要に応じて柔軟な起動制御 (FLC) モードを選択します。
設定の確認	情報を確認し、[終了] をクリックします。

既存の仮想マシンでの vSGX の有効化

既存の仮想マシンで vSGX を有効にできます。

vSGX は、vSphere 7.0 以降で実行されている仮想マシンに対して有効にすることができます。

前提条件

- SGX 対応の CPU に ESXi ホストがインストールされ、ホストの BIOS で SGX が有効になっている必要があります。サポートされている Intel 製 CPU については、vSGX の概要を参照してください。
- 使用するゲスト OS は、Linux、Windows Server 2016（64 ビット）以降、または Windows 10（64 ビット）以降である必要があります。
- 環境内で実行されている ESXi ホストは、ESXi 7.0 以降である必要があります。
- 仮想マシンの電源がオフであることを確認します。
- 仮想マシンで EFI ファームウェアを使用する必要があります。
- 仮想マシンでは、ハードウェア バージョン 17 以降を使用している必要があります。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。
3. [設定の編集] ダイアログ ボックスの [セキュリティ デバイス] で、SGX の [有効化] チェックボックスを選択します。
4. 隔離領域ページ キャッシュ (EPC) のサイズを入力し、必要に応じて柔軟な起動制御 (FLC) モードを選択します。
5. [仮想マシン オプション] - [起動オプション] - [] で、EFI が選択されていることを確認します。
6. [OK] をクリックします。

仮想マシンからの vSGX の削除

仮想マシンから vSGX を削除できます。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。

3 [設定の編集] ダイアログ ボックスの [セキュリティ デバイス] で、SGX の [有効化] チェックボックスを選択解除します。

4 [OK] をクリックします。

vSGX エントリが、[仮想マシンのハードウェア] 表示枠にある仮想マシンの [サマリ] タブに表示されなくなったことを確認します。

AMD の Secure Encrypted Virtualization -Encrypted State による仮想マシンの保護

SEV-ES (Secure Encrypted Virtualization-Encrypted State) は、AMD の最新 CPU で利用できるハードウェア機能で、ゲスト OS のメモリおよびレジスタの状態を暗号化して保持することで、ハイパーバイザーからのアクセスから保護します。

SEV-ES は、追加のセキュリティ強化として仮想マシンに追加できます。SEV-ES により、CPU レジスタ内の情報がレジスタからハイパーバイザーなどのコンポーネントに漏洩することを防止できます。SEV-ES は、CPU レジスタの状態に対する悪意のある変更を検出することもできます。

AMD Secure Encrypted Virtualization-Encrypted State の概要

vSphere 7.0 Update 1 以降では、サポートされている AMD CPU およびゲスト OS で Secure Encrypted Virtualization-Encrypted State (SEV-ES) を有効にできます。

現在、SEV-ES でサポートされるのは、AMD EPYC 7xx2 CPU（コード ネーム「Rome」）以降の CPU と、SEV-ES の特定のサポート機能を備えたバージョンの Linux カーネルのみです。

SEV-ES のコンポーネントとアーキテクチャ

SEV-ES アーキテクチャは、次のコンポーネントで構成されています。

- AMD CPU、特に、暗号化キーを管理して暗号化を処理するプラットフォーム セキュリティ プロセッサ (PSP)。
- 対応オペレーティング システム。ゲストが開始したハイパーバイザーへの呼び出しを使用するオペレーティング システム。
- 仮想マシン モニタ (VMM) と仮想マシンの実行可能 (VMX) コンポーネント。仮想マシンのパワーオン時に暗号化された仮想マシンの状態を初期化し、ゲスト OS からの呼び出しも処理します。
- VMkernel ドライバ。ハイパーバイザーとゲスト OS の間で暗号化されていないデータを通信します。

ESXi 上での SEV-ES の実装と管理

まず、システムの BIOS 構成で SEV-ES を有効にする必要があります。BIOS 構成へのアクセスの詳細については、システムのドキュメントを参照してください。システムの BIOS で SEV-ES を有効にした後、仮想マシンに SEV-ES を追加できます。

仮想マシンの SEV-ES を有効または無効にするには、vSphere Client（vSphere 7.0 Update 2 以降の場合）、または PowerCLI コマンドを使用します。SEV-ES を使用して新しい仮想マシンを作成したり、既存の仮想マシンで SEV-ES を有効にしたりできます。SEV-ES が有効になっている仮想マシンを管理する権限は、通常の仮想マシンを管理する場合と同じです。

SEV-ES でサポートされていない VMware の機能

SEV-ES が有効な場合は、次の機能がサポートされません。

- システム管理モード
- vMotion
- パワーオン状態のスナップショット（ただし、非メモリ スナップショットはサポートされます）
- CPU またはメモリのホット アドまたはホット リムーブ
- サスペンド/レジューム
- VMware フォールト トレランス
- クローンとインスタント クローン
- ゲストの整合性
- UEFI セキュア ブート

vSphere Client を使用した仮想マシンへの AMD Secure Encrypted Virtualization-Encrypted State の追加

vSphere 7.0 Update 2 以降では、vSphere Client を使用して SEV-ES を仮想マシンに追加して、ゲスト OS のセキュリティを強化することができます。

SEV-ES は ESXi 7.0 Update 1 以降で実行されている仮想マシンに追加できます。

前提条件

- システムに AMD EPYC 7xx2（コード ネームは「Rome」）以降の CPU が搭載されていて、BIOS をサポートしている必要があります。
- SEV-ES は BIOS で有効にする必要があります。
- ESXi ホスト 1 台あたりの SEV-ES 仮想マシンの数は、BIOS によって制御されます。BIOS で SEV-ES を有効にするときに、SEV-ES 仮想マシンの数に 1 を加えた値を [Minimum SEV non-ES ASID] の設定に入力します。たとえば、同時に実行できる仮想マシンの数が 12 の場合は、**13** を入力します。

  注： vSphere 7.0 Update 1 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 16 台サポートされます。BIOS の設定を大きくしても SEV-ES の機能が停止することはありません。ただし、16 台という制限は引き続き適用されます。vSphere 7.0 Update 2 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 480 台サポートされます。

- 環境内で実行されている ESXi ホストは、ESXi 7.0 Update1 以降である必要があります。
- vCenter Server は、vSphere 7.0 Update 2 以降である必要があります。

- ゲスト OS は SEV-ES をサポートしている必要があります。

  現在、サポートされているのは、SEV-ES に対する特定のサポート機能を備えた Linux カーネルのみです。
- 仮想マシンのハードウェア バージョンが 18 以降である必要があります。
- 仮想マシンで [すべてのゲスト メモリを予約] オプションを有効にしておく必要があります。有効にしないと、パワーオンは失敗します。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 オブジェクトを右クリックして [新規仮想マシン] を選択し、表示される画面に沿って仮想マシンを作成します。

オプション	操作
作成タイプの選択	仮想マシンを作成します。
名前とフォルダの選択	名前とターゲットの場所を指定します。
コンピューティング リソースの選択	仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。
ストレージの選択	仮想マシン ストレージ ポリシーでストレージ ポリシーを選択します。互換データストアを選択します。
互換性の選択	[ESXi 7.0 以降] が選択されていることを確認します。
ゲスト OS を選択	Linux を選択し、SEV-ES が明確にサポートされている Linux のバージョンを選択します。
ハードウェアのカスタマイズ	[仮想マシン オプション] - [起動オプション] - [] で、EFI が選択されていることを確認します。[仮想マシン オプション] - [暗号化] の順に選択し、AMD SEV-ES の [有効化] チェックボックスを選択します。
設定の確認	情報を確認し、[終了] をクリックします。

結果

SEV-ES を使用する仮想マシンが作成されました。

仮想マシンへの AMD Secure Encrypted Virtualization-Encrypted State の追加

SEV-ES を仮想マシンに追加して、ゲスト OS のセキュリティを強化することができます。

SEV-ES は ESXi 7.0 Update 1 以降で実行されている仮想マシンに追加できます。

前提条件

- システムに AMD EPYC 7xx2（コード ネームは「Rome」）以降の CPU が搭載されていて、BIOS をサポートしている必要があります。
- SEV-ES は BIOS で有効にする必要があります。

- ESXi ホスト 1 台あたりの SEV-ES 仮想マシンの数は、BIOS によって制御されます。BIOS で SEV-ES を有効にするときに、SEV-ES 仮想マシンの数に 1 を加えた値を [Minimum SEV non-ES ASID] の設定に入力します。たとえば、同時に実行できる仮想マシンの数が 12 の場合は、**13** を入力します。

  注： vSphere 7.0 Update 1 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 16 台サポートされます。BIOS の設定を大きくしても SEV-ES の機能が停止することはありません。ただし、16 台という制限は引き続き適用されます。vSphere 7.0 Update 2 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 480 台サポートされます。

- 環境内で実行されている ESXi ホストは、ESXi 7.0 Update1 以降である必要があります。
- ゲスト OS は SEV-ES をサポートしている必要があります。

  現在、サポートされているのは、SEV-ES に対する特定のサポート機能を備えた Linux カーネルのみです。
- 仮想マシンのハードウェア バージョンが 18 以降である必要があります。
- 仮想マシンで [すべてのゲスト メモリを予約] オプションを有効にしておく必要があります。有効にしないと、パワーオンは失敗します。
- 環境にアクセスできるシステムに PowerCLI 12.1.0 以降がインストールされている必要があります。

手順

1 PowerCLI セッションで `Connect-VIServer` コマンドレットを実行して、SEV-ES が有効な仮想マシンを追加する ESXi ホストを管理する vCenter Server に、管理者として接続します。

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 `New-VM` コマンドレットを使用して仮想マシンを作成し、`-SEVEnabled $true` を指定します。

たとえば、最初にホスト情報を変数に割り当ててから、仮想マシンを作成します。

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

仮想ハードウェア バージョンを指定する必要がある場合は、`-HardwareVersion vmx-18` パラメータを指定して `New-VM` コマンドレットを実行します。例：

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
-HardwareVersion vmx-18
```

結果

SEV-ES を使用する仮想マシンが作成されました。

vSphere Client を使用した既存の仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の有効化

vSphere 7.0 Update 2 以降では、vSphere Client を使用して SEV-ES を既存の仮想マシンに追加して、ゲスト OS のセキュリティを強化することができます。

SEV-ES は ESXi 7.0 Update 1 以降で実行されている仮想マシンに追加できます。

前提条件

- システムに AMD EPYC 7xx2（コード ネームは「Rome」）以降の CPU が搭載されていて、BIOS をサポートしている必要があります。
- SEV-ES は BIOS で有効にする必要があります。
- ESXi ホスト 1 台あたりの SEV-ES 仮想マシンの数は、BIOS によって制御されます。BIOS で SEV-ES を有効にするときに、SEV-ES 仮想マシンの数に 1 を加えた値を [Minimum SEV non-ES ASID] の設定に入力します。たとえば、同時に実行できる仮想マシンの数が 12 の場合は、**13** を入力します。

  注： vSphere 7.0 Update 1 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 16 台サポートされます。BIOS の設定を大きくしても SEV-ES の機能が停止することはありません。ただし、16 台という制限は引き続き適用されます。vSphere 7.0 Update 2 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 480 台サポートされます。

- 環境内で実行されている ESXi ホストは、ESXi 7.0 Update1 以降である必要があります。
- vCenter Server は、vSphere 7.0 Update 2 以降である必要があります。
- ゲスト OS は SEV-ES をサポートしている必要があります。

  現在、サポートされているのは、SEV-ES に対する特定のサポート機能を備えた Linux カーネルのみです。
- 仮想マシンのハードウェア バージョンが 18 以降である必要があります。
- 仮想マシンで [すべてのゲスト メモリを予約] オプションを有効にしておく必要があります。有効にしないと、パワーオンは失敗します。
- 仮想マシンがパワーオフ状態であることを確認します。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。
3. [仮想マシン オプション] - [起動オプション] - [] で、EFI が選択されていることを確認します。
4. [設定の編集] ダイアログ ボックスの [仮想マシン オプション] - [暗号化] で、AMD SEV-ES の [有効化] チェック ボックスを選択します。
5. [OK] をクリックします。

結果

仮想マシンに SEV-ES が追加されました。

既存の仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の有効化

SEV-ES を既存の仮想マシンに追加して、ゲスト OS のセキュリティを強化することができます。

SEV-ES は ESXi 7.0 Update 1 以降で実行されている仮想マシンに追加できます。

前提条件

- システムに AMD EPYC 7xx2（コード ネームは「Rome」）以降の CPU が搭載されていて、BIOS をサポートしている必要があります。
- SEV-ES は BIOS で有効にする必要があります。
- ESXi ホスト 1 台あたりの SEV-ES 仮想マシンの数は、BIOS によって制御されます。BIOS で SEV-ES を有効にするときに、SEV-ES 仮想マシンの数に 1 を加えた値を [Minimum SEV non-ES ASID] の設定に入力します。たとえば、同時に実行できる仮想マシンの数が 12 の場合は、**13** を入力します。

  注： vSphere 7.0 Update 1 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 16 台サポートされます。BIOS の設定を大きくしても SEV-ES の機能が停止することはありません。ただし、16 台という制限は引き続き適用されます。vSphere 7.0 Update 2 では、SEV-ES 対応の仮想マシンが ESXi ホスト 1 台あたり 480 台サポートされます。
- 環境内で実行されている ESXi ホストは、ESXi 7.0 Update1 以降である必要があります。
- ゲスト OS は SEV-ES をサポートしている必要があります。

  現在、サポートされているのは、SEV-ES に対する特定のサポート機能を備えた Linux カーネルのみです。
- 仮想マシンのハードウェア バージョンが 18 以降である必要があります。
- 仮想マシンで [すべてのゲスト メモリを予約] オプションを有効にしておく必要があります。有効にしないと、パワーオンは失敗します。
- 環境にアクセスできるシステムに PowerCLI 12.1.0 以降がインストールされている必要があります。
- 仮想マシンがパワーオフ状態であることを確認します。

手順

1 PowerCLI セッションで `Connect-VIServer` コマンドレットを実行して、SEV-ES を追加する仮想マシンが含まれている ESXi ホストを管理する vCenter Server に、管理者として接続します。

例：

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

2 `Set-VM` コマンドレットに `-SEVEnabled $true` を指定して実行し、仮想マシンに SEV-ES を追加します。

例：

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
```

仮想ハードウェア バージョンを指定する必要がある場合は、`-HardwareVersion vmx-18` パラメータを指定して `Set-VM` コマンドレットを実行します。例：

```
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
```

結果

仮想マシンに SEV-ES が追加されました。

vSphere Client を使用した仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の無効化

vSphere 7.0 Update 2 以降では、vSphere Client を使用して仮想マシンの SEV-ES を無効にできます。

前提条件

- 仮想マシンがパワーオフ状態であることを確認します。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。
3. [設定の編集] ダイアログ ボックスの [仮想マシン オプション] - [暗号化] で、AMD SEV-ES の [有効化] チェック ボックスを選択解除します。
4. [OK] をクリックします。

結果

仮想マシンで SEV-ES が無効になりました。

仮想マシンでの AMD Secure Encrypted Virtualization-Encrypted State の無効化

仮想マシンで SEV-ES を無効にできます。

前提条件

- 仮想マシンがパワーオフ状態であることを確認します。
- 環境にアクセスできるシステムに PowerCLI 12.1.0 以降がインストールされている必要があります。

手順

1. PowerCLI セッションで `Connect-VIServer` コマンドレットを実行して、SEV-ES を削除する仮想マシンが含まれている ESXi ホストを管理する vCenter Server に、管理者として接続します。

   例：

   ```
   Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
   ```

2. `Set-VM` コマンドレットに `-SEVEnabled $false` を指定して実行し、仮想マシン上で SEV-ES を無効にします。

   たとえば、最初にホスト情報を変数に割り当ててから、仮想マシンに対して SEV-ES を無効にします。

   ```
   $vmhost = Get-VMHost -Name 10.193.25.83
   Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
   ```

結果

仮想マシンで SEV-ES が無効になりました。

仮想マシンの暗号化

6

vSphere 仮想マシンの暗号化を使用すると、機密性の高いワークロードを安全性のより高い方法で暗号化できます。暗号化キーへのアクセスを、信頼された状態の ESXi ホストに基づいて設定できます。

仮想マシンの暗号化タスクを開始するためには、キー プロバイダを設定する必要があります。次の主要なプロバイダ タイプを使用できます。

表 6-1. vSphere キー プロバイダ

キー プロバイダ	説明	詳細
標準のキー プロバイダ	vSphere 6.5 以降で使用可能な標準キー プロバイダは、vCenter Server を使用して外部キー サーバからキーを要求します。キー サーバはキーを生成して保存し、配布のために vCenter Server に渡します。	7 章 標準キー プロバイダの構成と管理を参照してください。
信頼済みキー プロバイダ	vSphere 7.0 以降で使用可能な vSphere 信頼機関 信頼済みキー プロバイダは、ワークロード クラスタの証明状態に基いて暗号化キーにアクセスします。vSphere 信頼機関 は外部キー サーバが必要です。	9 章 vSphere 信頼機関を参照してください。
VMware vSphere® Native Key Provider™	vSphere 7.0 Update 2 以降で利用可能な vSphere Native Key Provider は、すべての vSphere エディションに組み込まれており、外部キー サーバは不要です。	8 章 vSphere Native Key Provider の構成と管理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 キー プロバイダの比較
- vSphere 仮想マシンの暗号化で環境を保護する方法
- vSphere 仮想マシンの暗号化のコンポーネント
- 暗号化プロセス フロー
- 仮想ディスクの暗号化
- 仮想マシンの暗号化のエラー
- 暗号化タスクの前提条件と必要な権限
- 暗号化された vSphere vMotion
- 暗号化のベスト プラクティス、注意事項、相互運用性

- キーの永続性の概要

vSphere キー プロバイダの比較

暗号化戦略の計画を立てる場合、vSphere キー プロバイダの機能の概要に注意を払う必要があります。

一般に、日常の操作の中で、キー プロバイダの違いによって機能または製品サポートに違いが生じることはほとんどありません。キー プロバイダの外観と動作はほとんど同じですが、次の表に示すように、キー プロバイダを選択する際には要件と規制についての検討が必要になる場合があります。

表 6-2. キー プロバイダについての検討事項

キー プロバイダ	外部キー サーバが必要?	クイック セットアップ?	vSphere でのみ動作?
標準のキー プロバイダ	はい	なし	なし
信頼済みキー プロバイダ	はい	なし	なし
vSphere Native Key Provider	なし	はい	はい

暗号化機能

次の暗号化機能は、キー プロバイダの各タイプでサポートされています。

- 同じキー プロバイダまたは別のキー プロバイダを使用して再キー化
- キーのローテーション
- 仮想 Trusted Platform Module (vTPM)
- ディスクの暗号化
- vSphere 仮想マシンの暗号化
- 他のキー プロバイダとの共存
- 別のキー プロバイダへのアップグレード

vSphere 機能

以下では、vSphere のいくつかの重要な機能に対するキー プロバイダのサポートについて説明します。

- 暗号化された vSphere vMotion: すべてのキー プロバイダ タイプでサポートされています。ターゲット ホストで同じキー プロバイダが使用可能である必要があります。暗号化された vSphere vMotion を参照してください。
- vCenter Server のファイルベースのバックアップとリストア：標準のキー プロバイダと vSphere Native Key Provider は、vCenter Server のファイルベースのバックアップとリストアをサポートします。ほとんどの vSphere 信頼機関 構成情報は ESXi ホストに格納されているため、vCenter Server のファイルベースのバックアップではこの情報のバックアップは行われません。vSphere 信頼機関 デプロイの構成情報が保存されていることを確認するには、vSphere 信頼機関構成のバックアップを参照してください。

VMware 製品

次の表は、一部の VMware 製品に対するキー プロバイダのサポートを比較したものです。

表 6-3. VMware 製品のサポートの比較

キー プロバイダ	vSAN	Site Recovery Manager	vSphere Replication
標準のキー プロバイダ	はい	はい	はい
信頼済みキー プロバイダ	はい	はい リカバリ側で同じ vSphere 信頼機関 サービス構成が使用可能な場合は、アレイ ベースのレプリケーションを伴う SRM がサポートされます。	いいえ
vSphere Native Key Provider	はい	はい	はい

必要なハードウェア

次の表は、キー プロバイダ ハードウェアのいくつかの最小要件を比較したものです。

表 6-4. 必要なハードウェアの比較

キー プロバイダ	ESXi ホスト上の TPM
標準のキー プロバイダ	必須ではない
信頼済みキー プロバイダ	信頼済みホスト（信頼済みクラスタ内のホスト）で必要です。 **注：** 現在、Trust Authority クラスタ内の ESXi ホストでは、TPM は必要ありません。ただし、ベスト プラクティスとして、TPM を使用して新しい ESXi ホストをインストールすることを検討してください。
vSphere Native Key Provider	必須ではない vSphere Native Key Provider の可用性は、オプションで TPM を備えたホストに制限できます。

キー プロバイダの名前の指定

vSphere では、キー プロバイダ名を使用して、キー識別子を検索します。2 つのキー プロバイダの名前が同じ場合、vSphere ではこれらのキー プロバイダは同等で、同じキーにアクセスできるとみなされます。各論理キー プロバイダには、そのタイプ（標準、信頼済み、ネイティブの各キー プロバイダ）に関係なく、すべての vCenter Server システムで一意の名前が付いている必要があります。

場合によっては、以下のような複数の vCenter Server システムで、同じキー プロバイダを構成します。

- vCenter Server システム間の暗号化された仮想マシンの移行
- vCenter Server をディザスタ リカバリ サイトとして設定

vSphere 仮想マシンの暗号化で環境を保護する方法

使用するキー プロバイダに関係なく、vSphere 仮想マシンの暗号化を使用して、暗号化された仮想マシンを作成し、既存の仮想マシンを暗号化できます。機密情報が含まれるすべての仮想マシン ファイルを暗号化することで、仮想マシンが保護されます。この暗号化および復号化タスクを実行できるのは、暗号化権限が付与されている管理者だけです。

vSphere 仮想マシンの暗号化でサポートされるストレージ

vSphere 仮想マシンの暗号化は、VMware vSAN を含む、サポートされているすべてのストレージ タイプ（NFS、iSCSI、ファイバ チャネル、直接接続されたストレージなど）で動作します。vSAN クラスタでの暗号化の使用の詳細については、『VMware vSAN の管理』ドキュメントを参照してください。

vSphere 仮想マシンの暗号化と vSAN では同じ暗号化ライブラリが使用されますが、プロファイルは異なります。仮想マシンの暗号化は仮想マシンごとの暗号化であり、vSAN はデータストア レベルでの暗号化です。

vSphere 暗号化キーとキー プロバイダ

vSphere では、キー暗号化キー (KEK) およびデータ暗号化キー (DEK) の形式の 2 つの暗号化レベルを使用します。簡単に言えば、ESXi ホストは仮想マシンとディスクを暗号化するための DEK を生成します。KEK はキー サーバによって提供され、DEK を暗号化（「ラップ」）します。KEK は AES256 アルゴリズムを使用して暗号化され、DEK は XTS-AES-256 アルゴリズムを使用して暗号化されます。キー プロバイダのタイプに応じて、DEK と KEK の作成および管理にはさまざまな方法が使用されます。

標準のキー プロバイダは次のように動作します。

1 ESXi ホストは内部キーを生成して使用し、仮想マシンとディスクを暗号化します。これらのキーは DEK として使用されます。

2 vCenter Server は、キー サーバ (KMS) からのキーの取得を要求します。これらのキーは KEK として使用されます。vCenter Server では各 KEK の ID のみが保存されます。キー自体は保存されません。

3 ESXi は、KEK を使用して内部キーを暗号化し、暗号化された内部キーをディスクに保存します。ESXi では KEK はディスクに保存されません。ホストが再起動されると、vCenter Server は、対応する ID を持つ KEK をキー サーバに要求して、ESXi で使用できるようにします。その後、ESXi は必要に応じて内部キーを復号化できます。

vSphere 信頼機関 の信頼済みキー プロバイダは次のように動作します。

1 暗号化された仮想マシンを作成する ESXi ホストにデフォルトの信頼済みキー プロバイダからアクセスできるかどうか、信頼済みクラスタの vCenter Server が確認します。

2 信頼済みクラスタの vCenter Server が、信頼済みキー プロバイダを仮想マシンの ConfigSpec に追加します。

3 仮想マシンの作成要求が ESXi ホストに送信されます。

4 証明トークンが ESXi ホストでまだ使用できない場合、ホストが証明サービスに対して要求します。

5 キー プロバイダ サービスが証明トークンを検証し、ESXi ホストに送信される KEK を作成します。KEK は、キー プロバイダで設定されたプライマリ キーでラップ（暗号化）されます。KEK 暗号文と KEK プレーンテキストの両方が信頼済みホストに返されます。

6 ESXi ホストが、仮想マシン ディスクを暗号化するための DEK を生成します。

7 ESXi ホストによって生成された DEK が KEK を使用してラップされ、キー プロバイダからの暗号文が暗号化されたデータとともに保存されます。

8 仮想マシンが暗号化され、ストレージに書き込まれます。

注： 暗号化された仮想マシンを削除または登録解除すると、ESXi ホストとクラスタでは、KEK がキャッシュから削除されます。ESXi ホストでは KEK を使用できなくなります。この動作は、標準のキー プロバイダでも信頼済みキー プロバイダでも同じです。

vSphere Native Key Provider は次のように動作します。

1 キー プロバイダを作成すると、vCenter Server がプライマリ キーを生成し、クラスタ内の ESXi ホストにプッシュします。（外部キー サーバは関与しません。）

2 ESXi ホストは、必要に応じて DEK を生成します。

3 暗号化アクティビティを実行すると、データが DEK で暗号化されます。

暗号化された DEK が、暗号化されたデータとともに保存されます。

4 データを復号化する場合は、プライマリ キーを使用して DEK を復号化し、次にデータを復号化します。

暗号化されるもの

vSphere 仮想マシンの暗号化機能は、仮想マシン ファイル、仮想ディスク ファイル、およびコア ダンプ ファイルの暗号化に対応しています。

仮想マシン ファイル

仮想マシンのほとんど、具体的には、VMDK ファイルに保存されていないゲスト データが暗号化されます。このファイル セットには、NVRAM、VSWP、および VMSN ファイルが含まれますが、これに限定されません。キー プロバイダから取得したキーにより、内部キーおよびその他のシークレットが含まれる VMX ファイル内の、暗号化されたバンドルのロックが解除されます。キーの取得は、キー プロバイダに応じて次のように機能します。

- 標準のキー プロバイダ：vCenter Server はキー サーバから取得したキーを管理し、ESXi ホストはキー プロバイダに直接アクセスできません。ホストは、vCenter Server がキーをプッシュするまで待ちます。
- 信頼済みキー プロバイダおよび vSphere Native Key Provider：ESXi ホストはキー プロバイダに直接アクセスし、要求されたキーを vSphere 信頼機関 サービスから直接取得するか、vSphere Native Key Provider から取得します。

vSphere Client を使用して暗号化された仮想マシンを作成する場合は、仮想マシンのファイルとは別に仮想ディスクの暗号化と復号化が可能になります。デフォルトでは、すべての仮想ディスクが暗号化されます。既存の仮想マシンの暗号化など、その他の暗号化タスクについては、仮想マシンのファイルとは別に仮想ディスクを暗号化および復号化できます。

注： 暗号化された仮想ディスクを、暗号化されていない仮想マシンに関連付けることはできません。

仮想ディスク ファイル

暗号化された仮想ディスク (VMDK) ファイルのデータが、クリアテキストでストレージや物理ディスクに書き込まれたり、ネットワーク経由で転送されたりすることはありません。VMDK 記述子ファイルは、ほとんどがクリアテキストですが、暗号化されたバンドルに KEK のキー ID と内部キー (DEK) が含まれます。

vSphere API を使用すると、新しい KEK で表層の再暗号化操作、または新しい内部キーで深層の再暗号化操作を行うことができます。

コア ダンプ

暗号化モードが有効になっている ESXi ホストのコア ダンプは常に暗号化されます。vSphere 仮想マシンの暗号化とコア ダンプを参照してください。vCenter Server システムのコア ダンプは暗号化されません。vCenter Server システムへのアクセスを保護してください。

注： vSphere 仮想マシンの暗号化と連携できるデバイスおよび機能に関する制限については、仮想マシンの暗号化の相互運用性を参照してください。

暗号化されないもの

仮想マシンに関連付けられているファイルの中には、暗号化されないもの、または部分的に暗号化されるものがあります。

ログ ファイル

ログ ファイルには機密データが含まれていないため、暗号化されません。

仮想マシン設定ファイル

VMX および VMSD ファイルに保存される仮想マシン構成情報のほとんどが暗号化されません。

仮想ディスク記述子ファイル

キーなしでディスクを管理できるように、仮想ディスク記述子ファイルのほとんどが暗号化されません。

暗号化操作を実行できるユーザー

暗号化操作権限が割り当てられているユーザーのみが、暗号化操作を行うことができます。権限セットは細かく設定されています。デフォルトの管理者システム ロールには、すべての暗号化操作権限が含まれています。非暗号化管理者ロールでは、暗号化操作権限を除くすべての管理者権限がサポートされます。

vSphere Native Key Provider は、Cryptographer.* 権限だけでなく、Cryptographer.ReadKeyServersInfo 権限を使用できます。この権限は、vSphere Native Key Provider に固有の権限です。

詳細については暗号化操作権限を参照してください。

追加のカスタム ロールを作成することで、たとえば、あるユーザー グループに対して仮想マシンの暗号化のみを許可し、復号化は禁止することができます。

暗号化操作の実行方法

vSphere Client では、多くの暗号化操作がサポートされています。他のタスクについては、vSphere API を使用できます。

表 6-5. 暗号化操作のインターフェイス

インターフェイス	操作	詳細情報
vSphere Client	暗号化された仮想マシンの作成 仮想マシンの暗号化および復号化	本書
PowerCLI	暗号化された仮想マシンの作成 仮想マシンの暗号化および復号化 vSphere 信頼機関 の構成	VMware PowerCLI コマンドレット リファレンス
vSphere Web Services SDK	暗号化された仮想マシンの作成 仮想マシンの暗号化および復号化 仮想マシンの再暗号化（深層）の実行（別の DEK を使用） 仮想マシンの再暗号化（表層）の実行（別の KEK を使用）	vSphere Web Services SDK プログラミング ガイド vSphere Web Services API リファレンス
`crypto-util`	暗号化されたコア ダンプの復号化 ファイルが暗号化されているかどうかの確認 ESXi ホスト上での他の管理タスクの直接実行	コマンドライン ヘルプ vSphere 仮想マシンの暗号化とコア ダンプ

仮想マシンの再暗号化

キーの有効期限が切れた場合や侵害された場合などに、新しいキーで仮想マシンを再暗号化できます。次のオプションを使用できます。

- 再暗号化（深層）。ディスク暗号化キー (DEK) とキー暗号化キー (KEK) の両方が置き換えられます。
- 再暗号化（表層）。KEK のみが置き換えられます。

仮想マシンの再暗号化は、API を使用して実行する必要があります。vSphere Web Services SDK プログラミング ガイド を参照してください。

再暗号化（深層）を行うには、仮想マシンがパワーオフされ、スナップショットが含まれていないことが必要です。再暗号化（表層）は、仮想マシンのスナップショットが作成済みであれば仮想マシンがパワーオン状態でも実行できます。スナップショットが作成済みの暗号化された仮想マシンの再暗号化（表層）は、単一のスナップショット分岐（ディスク チェーン）に対してのみ許可されます。複数のスナップショット分岐はサポートされていません。また、仮想マシンまたはディスクのリンク クローンでは再暗号化（表層）はサポートされません。チェーン内のすべてのリンクを新しい KEK で更新する前に再暗号化（表層）が失敗した場合でも、古い KEK と新しい KEK があれば暗号化された仮想マシンにアクセスできます。ただし、スナップショット操作を実行する前に、再暗号化（表層）操作を再実行することをお勧めします。

vSphere 仮想マシンの暗号化のコンポーネント

使用するキー プロバイダ、外部キー サーバ、vCenter Server システム、および ESXi ホストによって暗号化ソリューションが提供される可能性があります。

次のコンポーネントは、vSphere 仮想マシンの暗号化を構成します。

- KMS　とも呼ばれる外部キー サーバ（vSphere Native Key Provider では必要ありません）
- vCenter Server
- ESXi ホスト

キー サーバ

キー サーバは、キー プロバイダに関連付けられているキー管理相互運用性プロトコル (KMIP) の管理サーバです。標準キー プロバイダと信頼済みキー プロバイダには、キー サーバが必要です。vSphere Native Key Provider にはキー サーバは必要ではありません。次の表は、キー プロバイダとキー サーバの相互作用の違いについて説明します。

表 6-6. キー プロバイダとキー サーバの相互作用

キー プロバイダ	キー サーバとの相互作用
標準のキー プロバイダ	標準のキー プロバイダは、vCenter Server を使用してキー サーバにキーを要求します。キー サーバはキーを生成して保存し、ESXi ホストに配布するために vCenter Server に渡します。
信頼済みキー プロバイダ	信頼済みキー プロバイダはキー プロバイダ サービスを使用します。これにより、信頼できる ESXi ホストはキーを直接取得できます。vSphere 信頼機関 キー プロバイダ サービスについてを参照してください。
vSphere Native Key Provider	vSphere Native Key Provider にはキー サーバは必要ではありません。vCenter Server はプライマリ キーを生成し、ESXi ホストにプッシュします。次に、ESXi ホストは、データ暗号化キーを生成します（vCenter Server に接続されていない場合でも）。vSphere Native Key Provider の概要を参照してください。

vSphere Client または vSphere API を使用することで、キー プロバイダ インスタンスを vCenter Server システムに追加できます。複数のキー プロバイダ インスタンスを使用する場合は、すべてが同一ベンダーのインスタンスであることと、キーを複製することが必要です。

複数の環境で複数のキー サーバ ベンダーを使用する環境では、各キー サーバに 1 つのキー プロバイダを追加し、デフォルトのキー プロバイダを指定できます。最初に追加したキー プロバイダがデフォルトのキー プロバイダになります。後から明示的にデフォルトを指定できます。

KMIP クライアントである vCenter Server は、Key Management Interoperability Protocol (KMIP) を使用することで任意のキー サーバを簡単に使用することができます。

vCenter Server

次の表は、暗号化プロセスにおける vCenter Server の役割を示します。

表 6-7. キー プロバイダと vCenter Server

キー プロバイダ	vCenter Server の役割	権限の確認方法
標準のキー プロバイダ	キー サーバにログインするための資格情報を持っているのは vCenter Server だけです。ESXi ホストには、この認証情報がありません。vCenter Server はキー サーバからキーを取得し、ESXi ホストに渡します。vCenter Server はキー サーバのキーを格納しませんが、キー ID のリストは保持します。	vCenter Server は、暗号化操作を実行するユーザーの権限をチェックします。
信頼済みキー プロバイダ	vSphere 信頼機関 は、vCenter Server がキー サーバからキーを要求する必要をなくし、ワークロード クラスタの認証状態を条件として暗号化キーにアクセスできるようにします。信頼済みのクラスタと信頼機関クラスタには、別の vCenter Server システムを使用する必要があります。	vCenter Server は、暗号化操作を実行するユーザーの権限をチェックします。TrustedAdmins SSO グループのメンバーであるユーザーだけが管理操作を実行できます。
vSphere Native Key Provider	vCenter Server はキーを生成します。	vCenter Server は、暗号化操作を実行するユーザーの権限をチェックします。

vSphere Client を使用して、ユーザーのグループに暗号化操作権限を割り当てるか非暗号化管理者カスタム ロールを割り当てることができます。暗号化タスクの前提条件と必要な権限を参照してください。

vCenter Server は、vSphere Client イベント コンソールから表示、エクスポートできるイベントのリストに暗号化イベントを追加します。各イベントには、ユーザー、日時、キー ID、および暗号化操作が示されています。

キー サーバから取得するキーは、キー暗号化キー (KEK) として使用されます。

ESXi ホスト

ESXi ホストは、暗号化ワークフローのいくつかの場面で使用されます。

表 6-8. ESXi ホスト

キー プロバイダ	ESXi ホストの側面
標準のキー プロバイダ	■ vCenter Server は、キーが必要になった ESXi ホストにキーを渡します。ホストは、暗号化モードが有効になっている必要があります。現在のユーザーのロールに、暗号化操作権限が含まれている必要があります。暗号化タスクの前提条件と必要な権限および暗号化操作権限を参照してください。 ■ 暗号化された仮想マシンのゲスト データが、ディスクへの保存時に確実に暗号化されるようにします。 ■ 暗号化された仮想マシンのゲスト データが、暗号化されないままネットワークを通じて送信されないようにします。
信頼済みキー プロバイダ	ESXi ホストは、信頼できるホストであるか信頼機関のホストであるかに応じて、vSphere 信頼機関 サービスを実行します。信頼できる ESXi ホストは、信頼機関のホストによって公開されたキー プロバイダを使用して暗号化できるワークロード仮想マシンを実行します。信頼済みインフラストラクチャの概要を参照してください。
vSphere Native Key Provider	ESXi ホストは、vSphere Native Key Provider から直接キーを取得します。

このドキュメントでは、ESXi ホストによって生成されるキーのことを内部キーと呼びます。このキーは通常、データ暗号化キー (DEK) として使用されます。

暗号化プロセス フロー

キー プロバイダを設定すると、必要な権限を持ったユーザーが、暗号化した仮想マシンやディスクを作成できるようになります。これらのユーザーは、既存の仮想マシンの暗号化、暗号化された仮想マシンの復号化、仮想マシンへの仮想 Trusted Platform Module (vTPM) の追加を行うこともできます。

キー プロバイダのタイプに応じて、プロセス フローでキー サーバ、vCenter Server、ESXi ホストを使用します。

標準のキー プロバイダの暗号化プロセス フロー

暗号化プロセスでは、各種の vSphere コンポーネントが次のように作用し合います。

1 ユーザーが暗号化タスク（暗号化された仮想マシンの作成など）を実行すると、vCenter Server は、新しいキーをデフォルトのキー サーバに要求します。このキーが KEK として使用されます。

2 vCenter Server が、そのキー ID を保存し、ESXi ホストにキーを渡します。ESXi ホストがクラスタに属している場合、vCenter Server は、その KEK をクラスタ内の各ホストに送信します。

   キーそのものは vCenter Server システムに保存されません。把握されるのは、このキー ID だけです。

3 ESXi ホストが、仮想マシンとそのディスクに使用する内部キー (DEK) を生成します。さらに、生成した内部キーをメモリにのみ保持し、KEK を使用して内部キーを暗号化します。

   暗号化されていない内部キーがディスクに格納されることは決してありません。格納されるのは、暗号化されたデータだけです。KEK はキー サーバから取得されているため、ホストは同じ KEK を使用し続けます。

4 ESXi ホストが、暗号化された内部キーで仮想マシンを暗号化します。

   この KEK を保有し、かつ暗号化されたキー ファイルにアクセスできるすべてのホストは、暗号化された仮想マシンまたは暗号化されたディスクに対する操作を実行することができます。

信頼済みキー プロバイダの暗号化プロセス フロー

vSphere 信頼機関 暗号化プロセス フローには、vSphere 信頼機関 サービス、信頼済みキー プロバイダ、vCenter Server、および ESXi ホストが含まれます。

信頼済みキー プロバイダを使用した仮想マシンの暗号化は、仮想マシンの暗号化ユーザー エクスペリエンスとしては標準のキー プロバイダの使用を使用する場合と同様です。vSphere 信頼機関 を使用した仮想マシンの暗号化でも、仮想マシンの暗号化ストレージ ポリシーや vTPM デバイスの有無に基づいて、仮想マシンの暗号化のタイミングを決定します。vSphere Client から仮想マシンを暗号化するときは、引き続きデフォルトの設定済みキー プロバイダ（vSphere 6.5 および 6.7 では KMS クラスタと呼ばれていました）を使用します。また、同様の方法で API を使用して、キー プロバイダを手動で指定することもできます。vSphere 6.5 に追加された既存の暗号化権限は、vSphere 7.0 でも vSphere 信頼機関 に対して有効です。

信頼済みキー プロバイダの暗号化プロセスには、標準のキー プロバイダの場合とは異なるいくつかの重要な相違点があります。

- 信頼機関管理者は、vCenter Server インスタンスのキー サーバを設定するときに情報を直接指定することはなく、キー サーバの信頼を確立することもありません。代わりに、vSphere 信頼機関 は、信頼済みホストが使用できる信頼済みキー プロバイダを公開します。
- vCenter Server は ESXi ホストにキーをプッシュせず、代わりに各信頼済みキー プロバイダを 1 つのトップレベル キーとして扱うことができます。
- 信頼済みホストのみが、信頼機関ホストからの暗号化操作を要求できます。

vSphere Native Key Provider の暗号化プロセス フロー

vSphere 7.0 Update 2 リリース 以降では、vSphere Native Key Provider が提供されています。vSphere Native Key Provider を構成すると、vCenter Server はクラスタのすべての ESXi ホストにプライマリ キーをプッシュします。vSphere Native Key Provider を更新または削除した場合も、その変更がクラスタ内のホストにプッシュされます。暗号化プロセス フローは、信頼されているキー プロバイダの場合と同様です。違いは、vSphere Native Key Provider がキーを生成し、プライマリ キーでラップしてからキーを返して暗号化する点です。

キー サーバのカスタム属性

Key Management Interoperability Protocol (KMIP) は、ベンダー固有のニーズを満たすためにカスタム属性の追加をサポートしています。カスタム属性を使用すると、キー サーバに保存されているキーをより具体的に識別できます。vCenter Server では、仮想マシンのキーとホスト キーに次のカスタム属性が追加されます。

表 6-9. 仮想マシンの暗号化カスタム属性

カスタム属性	値
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server のバージョン
`x-Component`	仮想マシン
`x-Name`	仮想マシン名（ConfigInfo または ConfigSpec から収集）
`x-Identifier`	仮想マシンの instanceUuid（ConfigInfo または ConfigSpec から収集）

表 6-10. ホスト暗号化のカスタム属性

カスタム属性	値
`x-Vendor`	VMware, Inc.
`x-Product`	VMware vSphere
`x-Product_Version`	vCenter Server のバージョン
`x-Component`	ESXi Server

表 6-10. ホスト暗号化のカスタム属性 （続き）

カスタム属性	値
x-Name	ホスト名
x-Identifier	ホストのハードウェア UUID

vCenter Server は、キー サーバによるキーの作成時に x-Vendor、x-Product、および x-Product_Version 属性を追加します。キーを使用して仮想マシンまたはホストを暗号化する場合、vCenter Server は x-Component、x-Identifier、および x-Name 属性を設定します。これらのカスタム属性は、キー サーバのユーザー インターフェイスで表示できる場合があります。キー サーバのベンダーに確認してください。

ホスト キーと仮想マシン キーのどちらにも、6 つのカスタム属性があります。x-Vendor、x-Product、および x-Product_Version は、両方のキーで同じである場合があります。これらの属性は、キーの生成時に設定されます。キーが仮想マシン用かホスト用かに応じて、x-Component、x-Identifier、および x-Name 属性が付加されることがあります。

主なエラー

キー サーバから ESXi ホストへのキーの送信でエラーが発生すると、vCenter Server は次のイベントのイベント ログにメッセージを生成します。

- ホスト接続またはホストのサポートに問題があるため、ESXi ホストへのキーの追加に失敗しました。
- キー サーバにキーが見つからないため、キー サーバからキーを取得できませんでした。
- キー サーバの接続不良により、キー サーバからキーを取得できませんでした。

暗号化された仮想マシンの復号化

後で暗号化された仮想マシンを復号化する場合は、そのストレージ ポリシーを変更します。仮想マシンとすべてのディスクのストレージ ポリシーを変更することができます。コンポーネントを個別に復号化する必要がある場合は、まず選択したディスクを復号化したうえで、仮想マシン ホームのストレージ ポリシーを変更することによって仮想マシンを復号化します。個々のコンポーネントを復号化する場合、両方のキーが必要になります。暗号化された仮想マシンまたは仮想ディスクの復号化を参照してください。

仮想ディスクの暗号化

vSphere Client から暗号化された仮想マシンを作成する際に、暗号化から除外するディスクを指定できます。後からディスクを追加し、その暗号化ポリシーを設定することができます。暗号化されていない仮想マシンに暗号化された仮想ディスクを追加することや、仮想マシンが暗号化されていない状態でディスクを暗号化することはできません。

仮想マシンおよびそのディスクの暗号化は、ストレージ ポリシーによって制御します。仮想マシン ホームのストレージ ポリシーは仮想マシン自体に適用され、各仮想ディスクにはそれぞれに関連付けられたストレージ ポリシーがあります。

- 仮想マシン ホームのストレージ ポリシーを暗号化ポリシーに設定すると、仮想マシン自体のみが暗号化されます。

- 仮想マシン ホームおよびすべてのディスクのストレージ ポリシーを暗号化ポリシーに設定すると、すべてのコンポーネントが暗号化されます。

次の使用事例を考えます。

表 6-11. 仮想ディスクを暗号化する使用事例

使用事例	詳細
暗号化された仮想マシンを作成する。	暗号化された仮想マシンの作成時にディスクを追加すると、そのディスクはデフォルトで暗号化されます。ポリシーを変更して、1 つ以上のディスクが暗号化されないようにすることができます。 仮想マシンを作成した後で、各ディスクのストレージ ポリシーを明示的に変更できます。仮想ディスクの暗号化ポリシーの変更を参照してください。
仮想マシンを暗号化する。	既存の仮想マシンの暗号化するには、そのストレージ ポリシーを変更します。仮想マシンとすべての仮想ディスクに適用されるストレージ ポリシーを変更できます。仮想マシンのみを暗号化する場合は、仮想マシン ホームに対して暗号化ポリシーを指定し、各仮想ディスクに対して [データストアのデフォルト] などの別のストレージ ポリシーを選択します。暗号化された仮想マシンの作成を参照してください。
暗号化されていない既存のディスクを暗号化された仮想マシンに追加する（暗号化ストレージ ポリシー）。	エラーが発生して失敗します。デフォルトのストレージ ポリシーを指定してディスクを追加する必要があります。ただし、後からストレージ ポリシーを変更できます。仮想ディスクの暗号化ポリシーの変更を参照してください。
[データストアのデフォルト] などの暗号化を含まないストレージ ポリシーを指定して、暗号化されていない既存のディスクを暗号化された仮想マシンに追加する。	ディスクにはデフォルトのストレージ ポリシーが使用されます。ディスクを暗号化する場合は、ディスクを追加した後でストレージ ポリシーを明示的に変更できます。仮想ディスクの暗号化ポリシーの変更を参照してください。
暗号化された仮想マシンに暗号化された仮想ディスクを追加する。仮想マシン ホームのストレージ ポリシーは [暗号化] です。	ディスクを追加すると、その暗号化は維持されます。vSphere Client には、サイズや、暗号化ステータスなどの属性が表示されます。
暗号化された既存の仮想ディスクを暗号化されていない仮想マシンに追加する。	この使用事例はサポートされていません。
暗号化された仮想マシンを登録する。	暗号化された仮想マシンを vCenter Server から削除しても、ディスクから削除しない場合は、仮想マシンの仮想マシン構成ファイル (.vmx) を登録することで、vCenter Server インベントリに戻すことができます。暗号化された仮想マシンを登録するには、ユーザーが 暗号化操作.仮想マシンの登録権限を持っている必要があります。 標準のキー プロバイダを使用して仮想マシンが暗号化されている場合、暗号化された仮想マシンが登録されると、vCenter Server は必要なキーを ESXi ホストにプッシュします。仮想マシンを登録しているユーザーに 暗号化操作.仮想マシンの登録権限がない場合、vCenter Server は登録時に仮想マシンをロックします。仮想マシンはロックが解除されるまで使用できません。 信頼されているキー プロバイダまたは vSphere Native Key Provider を使用して仮想マシンが暗号化されている場合、暗号化された仮想マシンが登録されると、vCenter Server はキーを ESXi ホストにプッシュしなくなります。代わりに、仮想マシンの登録時に、キーがホストから取得されます。仮想マシンを登録しているユーザーに 暗号化操作.仮想マシンの登録権限がない場合、vCenter Server では操作が許可されません。

仮想マシンの暗号化のエラー

vCenter Server で仮想マシンの暗号化に関する重大なエラーが検出されると、イベントが作成されます。これらのイベントを表示して、暗号化のエラーのトラブルシューティングや解決に役立てることができます。

vCenter Server では、仮想マシンの暗号化に関する次のクリティカルなエラーに対してイベントが作成されます。

- KEK を生成できませんでした。
- 暗号化された仮想マシンを作成するための十分なディスク容量がデータストアにありません。
- 暗号化操作を開始するために必要なユーザー権限がありません。
- 指定されたキーがキー プロバイダにないため、ESXi ホスト キーが新しいキーで更新されます。
- 指定されたキーを持つキー プロバイダでエラーが発生したため、ESXi ホスト キーが新しいキーで更新されます。

暗号化タスクの前提条件と必要な権限

暗号化タスクは、vCenter Server を含んだ環境でのみ実行することができます。加えて、ESXi ホストでは、ほとんどの暗号化タスクについて、暗号化モードが有効になっている必要があります。このタスクを実行するユーザーには、適切な権限が与えられている必要があります。一連の暗号化操作権限によって、きめ細かな制御が可能となります。仮想マシンの暗号化タスクにホストの暗号化モードへの変更が伴う場合は、さらに別の権限が必要となります。

注： vSphere 信頼機関 には、前提条件および必要な権限が追加で必要です。vSphere 信頼機関の前提条件と必要な権限 を参照してください。

暗号化の権限とロール

デフォルトでは、vCenter Server の管理者ロールを持つユーザーにはすべての権限が与えられます。非暗号化管理者ロールには、暗号化操作に必要な次の権限がありません。

- 暗号化操作権限の追加
- グローバル.診断
- ホスト.インベントリ.クラスタへのホストの追加
- ホスト.インベントリ.スタンドアロン ホストの追加
- ホスト.ローカル操作.ユーザー グループの管理

暗号化操作権限を必要としない vCenter Server 管理者には、非暗号化管理者ロールを割り当てることができます。

ユーザーが実行できることに追加の制限を設定するには、非暗号化管理者ロールをクローン作成し、一部の暗号化操作権限のみを持つカスタム ロールを作成します。たとえば、ユーザーによる暗号化は許可するが、仮想マシンの復号化は許可しないロールを作成できます。ロールを使用した権限の割り当てを参照してください。

ホストの暗号化モード

ホスト暗号化モードでは、ESXi ホストが仮想マシンと仮想ディスクを暗号化するための暗号化マテリアルを受け入れる準備ができているかどうかを判断します。ホスト上で暗号化処理を実行できるようにするには、ホスト暗号化モードを有効にする必要があります。ホスト暗号化モードは、必要に応じて自動的に有効になる場合もありますが、明示的に有効にすることもできます。現在のホスト暗号化モードは、vSphere Client から、または vSphere API を使用して、確認および明示的な設定ができます。

ホスト暗号化モードを有効にすると、vCenter Server がホストにホスト キーをインストールし、ホストを暗号で「安全」な状態にすることができます。ホスト キーがインストールされると、vCenter Server によるキー プロバイダからのキーの取得や、ESXi ホストへのキーのプッシュなど、他の暗号化処理を続行できます。

「セーフ」モードでは、ユーザー ワールド（つまり hostd）と暗号化された仮想マシンのコア ダンプが暗号化されます。非暗号化仮想マシンでは、コア ダンプは暗号化されません。

暗号化されたコア ダンプと VMware テクニカル サポートでの使用方法については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/2147388) を参照してください。

手順については ホスト暗号化モードを明示的に有効にする を参照してください。

ホスト暗号化モードを有効にした後で無効にするのは簡単ではありません。API を使用したホスト暗号化モードの無効化 を参照してください。

ホスト暗号化モードを有効にしようと試みる暗号化操作が行われると、変更が自動的に行われます。たとえば、暗号化された仮想マシンをスタンドアローン ホストに追加し、ホスト暗号化モードが有効でないとします。ホストに対する必要な権限があれば、暗号化モードが自動的に有効になります。

クラスタに A、B、C の 3 台の ESXi ホストがあるとします。このとき、暗号化された仮想マシンをホスト A に作成する場合の結果は、いくつかの要因に左右されます。

- ホスト A、B、C で暗号化が既に有効な場合、暗号化操作.新規の暗号化の権限さえあれば、仮想マシンを作成できます。
- ホスト A とホスト B は暗号化が有効になっているものの、ホスト C は有効になっていない場合、次の規則が適用されます。
  - 暗号化操作.新規の暗号化と暗号化操作.ホストの登録の両方の権限が各ホストにあるとします。その場合、仮想マシンの作成プロセスにより、ホスト C の暗号化が有効になります。暗号化プロセスにより、ホスト C でホスト暗号化モードが有効になり、クラスタ内の各ホストにキーが送られます。

    このケースでは、ホスト C のホスト暗号化を明示的に有効にすることもできます。
  - 仮想マシンまたは仮想マシン フォルダに対し、暗号化操作.新規の暗号化権限だけがあるとします。その場合、仮想マシンの作成は成功し、キーがホスト A とホスト B で使用可能になります。ホスト C での暗号化は引き続き無効で、仮想マシン キーもありません。
- いずれのホストも暗号化が有効でなく、かつホスト A に対して暗号化操作.ホストの登録権限がある場合、仮想マシンの作成プロセスにより、そのホストでのホストの暗号化が有効になります。それ以外の場合は、エラーになります。

- vSphere API を使用して、クラスタの暗号化モードを「強制的に有効にする」ように設定することもできます。強制的に有効にすると、クラスタ内のすべてのホストが「安全」に暗号化されます。つまり、vCenter Server のホストにホスト キーがインストールされます。vSphere Web Services SDK プログラミング ガイド を参照してください。

ディスク容量要件

既存の仮想マシンを暗号化する場合、現在使用している仮想マシンの 2 倍以上の容量が必要になります。

暗号化された vSphere vMotion

暗号化された仮想マシンを vSphere vMotion で移行する場合、常に暗号化が使用されます。暗号化されていない仮想マシンについては、暗号化された vSphere vMotion のいずれかのオプションを選択できます。

暗号化された vSphere vMotion では、vSphere vMotion で転送されるデータの機密性、整合性、信頼性が確保されます。vSphere では、vCenter Server インスタンス間で、暗号化されていない仮想マシンおよび暗号化されている仮想マシンを暗号化された vMotion で移行できます。

暗号化されたコンポーネントへの対応

暗号化されたディスクの場合、データはいかなる場合でも暗号化された状態で転送されます。暗号化されていないディスクの場合は、次のようになります。

- ホスト内でディスク データを転送する場合、つまりホストを変更せずにデータストアのみを変更する場合、転送は暗号化されません。
- ホスト間でディスク データが転送され、暗号化された vMotion が使用される場合、転送は暗号化されます。暗号化された vMotion が使用されない場合、転送は暗号化されません。

暗号化された仮想マシンを vSphere vMotion で移行する場合は、常に暗号化された vSphere vMotion が使用されます。暗号化された仮想マシンの場合、暗号化された vSphere vMotion を無効にすることはできません。

暗号化された vSphere vMotion の状態

暗号化されていない仮想マシンの場合、暗号化された vSphere vMotion を次のいずれかの状態に設定することができます。デフォルトは [任意] です。

無効

暗号化された vSphere vMotion は使用されません。

任意

暗号化された vSphere vMotion は、ソースとターゲットの両方のホストでサポートされる場合に使用されます。ESXi バージョン 6.5 以降でのみ、暗号化された vSphere vMotion が使用されます。

必須

暗号化された vSphere vMotion のみ許可されます。暗号化された vSphere vMotion が、移行元と移行先の両方のホストでサポートされていなければ、vSphere vMotion による移行は許可されません。

仮想マシンを暗号化するときに、暗号化された vSphere vMotion の設定が仮想マシンに記録されます。後で仮想マシンの暗号化を無効にした場合、暗号化された vMotion の設定が [必須] のままになります。これは設定を明示的に変更するまで変わりません。この設定は [設定の編集] を使用して変更することができます。

暗号化されていない仮想マシンに対して、暗号化暗号化された vSphere vMotion を有効、無効化にする方法については、『vCenter Server およびホストの管理』のドキュメントを参照してください。

注： 現在、vCenter Server インスタンス間で暗号化された仮想マシンを移行するか、クローンを作成するには、vSphere API を使用する必要があります。『vSphere Web Services SDK プログラミング ガイド』および『vSphere Web Services API リファレンス』を参照してください。

vCenter Server インスタンス間での暗号化された仮想マシンの移行またはクローン作成

vSphere vMotion は、vCenter Server インスタンス間での暗号化された仮想マシンの移行とクローン作成をサポートします。

暗号化された仮想マシンを vCenter Server インスタンス間で移行またはクローン作成する場合、移行元と移行先の vCenter Server インスタンスが、仮想マシンの暗号化に使用されたキー プロバイダを共有するように設定されている必要があります。また、キー プロバイダ名が、移行元と移行先の両方の vCenter Server インスタンスで同じで、次の特性を持っている必要があります。

- 標準キー プロバイダ：同じキー サーバ（または複数のキー サーバ）がキー プロバイダに含まれている必要があります。
- 信頼済みキー プロバイダ：同じ vSphere 信頼機関 サービスをターゲット ホストで構成する必要があります。
- vSphere Native Key Provider: 同じ KDK が必要です。

移行先の vCenter Server では、移行先の ESXi ホストで暗号化モードを有効にしてあることを確認し、ホストが「セーフ」モードで暗号化されるようにします。

vSphere vMotion を使用して vCenter Server のインスタンス間で暗号化された仮想マシンを移行またはクローン作成する場合は、次の権限が必要です。

- 移行：仮想マシンでの暗号化操作.移行
- クローン作成：仮想マシンでの暗号化操作.クローン作成

また、移行先の vCenter Server での暗号化操作.EncryptNew 権限も必要です。移行先の ESXi ホストが「セーフ」モードでない場合は、移行先の vCenter Server で暗号化操作.RegisterHost 権限も必要です。

暗号化されていない、または暗号化されている仮想マシンを同じ vCenter Server で、または vCenter Server インスタンス間で移行する場合、特定のタスクが許可されません。

- 仮想マシン ストレージ ポリシーを変更することはできません。
- キーの変更は実行できません。

注： 仮想マシンのクローン作成中に仮想マシン ストレージ ポリシーを変更できます。

vCenter Server インスタンス間での暗号化された仮想マシンを移行またはクローン作成するための最小要件

標準キー プロバイダによって暗号化された仮想マシンを vSphere vMotion を使用して vCenter Server インスタンス間で移行またはクローン作成するための最小のバージョン要件は次のとおりです。

- 移行元と移行先の vCenter Server インスタンスの両方がバージョン 7.0 以降である必要があります。
- 移行元と移行先の ESXi ホストの両方がバージョン 6.7 以降である必要があります。

信頼済みキー プロバイダによって暗号化された仮想マシンを vSphere vMotion を使用して vCenter Server インスタンス間で移行またはクローン作成するための最小のバージョン要件は次のとおりです。

- vSphere 信頼機関 サービスが移行先ホスト用に設定されている必要があります。また、移行先ホストは証明を受けている必要があります。
- 移行時に暗号化を変更することはできません。たとえば、仮想マシンを新しいストレージに移行するときに、暗号化されていないディスクを暗号化することはできません。
- 標準の暗号化された仮想マシンを信頼済みホストに移行できます。キー プロバイダ名は、移行元と移行先の両方の vCenter Server インスタンスで同じである必要があります。
- vSphere 信頼機関 で暗号化された仮想マシンを、信頼されていないホストに移行することはできません。

信頼済みキー プロバイダの vMotion および vCenter Server 間 vMotion

信頼済みキー プロバイダは、ESXi ホスト間での vMotion を全面的にサポートします。

vCenter Server 間 vMotion はサポートされますが、次の制限があります。

1. 必要な信頼済みサービスが移行先ホスト用に設定されている必要があります。また、移行先ホストは証明を受けている必要があります。
2. 移行時に暗号化を変更することはできません。たとえば、仮想マシンを新しいストレージに移行するときに、ディスクを暗号化することはできません。

vCenter Server 間 vMotion を実行するとき、vCenter Server は、信頼済みキー プロバイダが移行先ホストで使用可能であること、およびホストからアクセスできるかどうかを確認します。

vSphere Native Key Provider の vMotion および vCenter Server 間 vMotion

vSphere Native Key Provider は、ESXi ホスト間での vMotion および暗号化された vMotion をサポートします。vCenter Server 間 vMotion は、vSphere Native Key Provider がターゲット ホスト上で構成されている場合にサポートされます。

暗号化のベスト プラクティス、注意事項、相互運用性

物理マシンの暗号化に該当するベスト プラクティスと注意事項はすべて仮想マシンの暗号化にも当てはまります。その他、仮想マシンの暗号化アーキテクチャに起因する推奨事項もいくつかあります。仮想マシンの暗号化方式を検討する際は、相互運用性に伴う制限を考慮してください。

注： vSphere 信頼機関 の相互運用性の詳細については、vSphere 信頼機関 のベスト プラクティス、注意事項、相互運用性を参照してください。

仮想マシンの暗号化のベスト プラクティス

後から問題が発生することを避けるために、たとえば `vm-support` バンドルを生成するときは、仮想マシンの暗号化のベスト プラクティスに従ってください。

一般的なベスト プラクティス

問題を回避するには、次の一般的なベスト プラクティスに従います。

- vCenter Server Appliance の仮想マシンは暗号化しないでください。
- ESXi ホストがクラッシュしたときは、できるだけ早くサポート バンドルを取得してください。パスワードを使用するサポート バンドルの生成や、コア ダンプの復号化のため、ホスト キーが必要になります。ホストが再起動されると、ホスト キーが変更される可能性があります。このような場合は、ホスト キーを使用して、パスワードを使用するサポート バンドルの生成や、サポート バンドルのコア ダンプの復号化ができなくなります。
- キー プロバイダの名前は慎重に管理します。すでに使用中のキー サーバのキー プロバイダ名が変更されると、そのキー サーバのキーで暗号化された仮想マシンは、パワーオンまたは登録のときにロック状態になります。この場合は、vCenter Server からキー サーバを削除し、最初に使用していたキー プロバイダ名で追加します。
- VMX ファイルと VMDK ディスクリプタ ファイルは編集しないでください。これらのファイルには暗号化バンドルが含まれています。変更を加えると、仮想マシンを復元できなくなり、この問題が修正できなくなる可能性があります。
- vSphere 仮想マシンの暗号化プロセスでは、データをストレージに書き込む前にホスト上のデータを暗号化します。この方法で仮想マシンを暗号化する場合、重複排除、圧縮、レプリケーションなどのバックエンド ストレージ機能の有効性が影響を受ける可能性があります。
- vSphere 仮想マシンの暗号化とゲスト内暗号化（BitLocker、dm-crypt など）のように、暗号化レイヤーを複数使用する場合、暗号化プロセスで追加の CPU およびメモリ リソースが使用されるため、仮想マシン全体のパフォーマンスが影響を受ける可能性があります。
- vSphere 仮想マシンの暗号化を使用して暗号化された仮想マシンのレプリケートされたコピーが、リカバリ サイトの暗号化キーにアクセスできることを確認します。標準のキー プロバイダの場合、これは vSphere の外部で、キー管理システムの設計の一部として処理されます。vSphere Native Key Provider の場合、Native Key Provider のキーのバックアップ コピーが存在し、消失から保護されていることを確認します。詳細については、『vSphere Native Key Provider のバックアップ』を参照してください。
- 暗号化は、CPU への負荷が高い処理です。AES-NI を使用すると、暗号化のパフォーマンスが大幅に向上します。BIOS で AES-NI を有効にします。

暗号化されたコア ダンプのベスト プラクティス

問題を診断するためにコア ダンプを調べる必要があるときは、問題を避けるために次のベスト プラクティスを実施してください。

- コア ダンプに関するポリシーを確立します。コア ダンプは、キーなどの機密情報を含む場合があるため、暗号化されています。コア ダンプを復号化する場合は、機密情報であることを考慮してください。ESXi のコア ダンプには、ESXi ホストのキーと、そこにホストされている仮想マシンのキーが含まれる場合があります。コア ダンプを復号化した後、ホスト キーを変更し、暗号化された仮想マシンを再暗号化することを検討してください。どちらのタスクも vSphere API を使用して実行できます。

  詳細については、vSphere 仮想マシンの暗号化とコア ダンプを参照してください。

- `vm-support` バンドルを収集するときは、必ずパスワードを使用します。vSphere Client からサポート バンドルを生成するとき、または `vm-support` コマンドを使用するときは、パスワードを指定できます。

  パスワードを指定すると、内部キーを使用しているコア ダンプはパスワードに基づくキーを使用するように再暗号化されます。暗号化されたコア ダンプがサポート バンドルに含まれている場合は、後でこのパスワードを使用して復号化できます。暗号化されていないコア ダンプとログは、パスワード オプションの使用に影響を受けません。

- `vm-support` バンドルの作成時に指定するパスワードは、vSphere コンポーネント内で維持されません。サポート バンドルのパスワードは、記録しておく必要があります。

- ホスト キーを変更する前に、パスワードを設定して `vm-support` バンドルを生成します。古いホスト キーで暗号化されたコア ダンプがある場合は、後でこのパスワードを使用してそれらにアクセスすることができます。

キーのライフサイクル管理のベスト プラクティス

キー サーバの可用性を確保し、キー サーバでキーを監視するためのベスト プラクティスを実践してください。

- キー サーバの可用性を保証するポリシーを設定する必要があります。

  キー サーバを使用できない場合は、仮想マシンの操作のうち vCenter Server がキー サーバにキーを要求する必要があるものは実行できません。稼動中の仮想マシンはそのまま稼動を続けますが、パワーオン、パワーオフ、仮想マシンの再設定は可能です。しかし、キー情報のないホストに仮想マシンを移動することはできません。

  ほとんどのキー サーバ ソリューションには、高可用性機能が含まれています。vSphere Client または API を使用して、キー プロバイダおよび関連するキー サーバを指定できます。

  注： vSphere 7.0 Update 2 以降では、キー サーバが一時的にオフラインまたは使用不可になった場合でも、暗号化された仮想マシンと仮想 TPM は引き続き機能します。ESXi ホストは、暗号化キーを保持して、暗号化および vTPM の操作を続行できます。キーの永続性の概要を参照してください。

- キーを記録し、既存の仮想マシンに対するキーがアクティブな状態でないときは修正する必要があります。

  KMIP 標準では、キーの状態が次のように定義されています。

  - Pre-Active（プレアクティブ）
  - Active（アクティブ）
  - Deactivated（非アクティブ）

- Compromised（侵害）
- Destroyed（破棄）
- Destroyed Compromised（破棄/侵害）

vSphere 仮想マシンの暗号化では、アクティブ状態のキーのみが暗号化に使用されます。プレアクティブ状態のキーは、vSphere 仮想マシンの暗号化によってアクティブにされます。キーの状態が非アクティブ、侵害、破棄、破棄/侵害のとき、そのキーで仮想マシンやディスクを暗号化することはできません。

キーが別の状態のとき、これらのキーを使用する仮想マシンは引き続き稼動します。クローン作成または移行の操作が成功するかどうかは、キーがすでにホスト上に存在するかどうかに依存します。

- ターゲット ホストにキーが存在する場合、キー サーバでキーがアクティブでなくても操作は成功します。
- 要求された仮想マシンと仮想ディスクのキーがターゲット ホスト上に存在しない場合、vCenter Server はキー サーバからキーを取得する必要があります。キーの状態が非アクティブ、侵害、破棄、破棄/侵害のとき、vCenter Server はエラーを表示し、操作は失敗します。

キーがすでにホスト上に存在する場合、クローン作成または移行の操作は成功します。vCenter Server がキー サーバからキーを取得する必要がある場合、操作は失敗します。

キーがアクティブでない場合は、API を使用して再キー化操作を実行します。『vSphere Web Services SDK Programming Guide』を参照してください。

- キー ローテーション ポリシーを作成して、特定の時間が経過するとキーが廃止されてロール オーバーされるようにします。
  - 信頼済みキー プロバイダ：信頼済みキー プロバイダのプライマリ キーを変更します。
  - vSphere Native Key Provider：vSphere Native Key Provider の `key_id` を変更します。

バックアップとリストアのベスト プラクティス

バックアップおよびリストア操作に関するポリシーを設定します。

- 一部のバックアップ アーキテクチャはサポートされません。仮想マシンの暗号化の相互運用性を参照してください。
- リストア操作に関するポリシーを設定します。バックアップは常にクリアテキストであるため、仮想マシンの暗号化はリストアが完了した直後に実行するように計画します。リストア操作の一部として仮想マシンが暗号化されるように指定することができます。機密情報が公開されることを避けるために、可能であればリストア プロセスの一部として仮想マシンを暗号化します。仮想マシンに関連付けられているディスクの暗号化ポリシーを変更するには、そのディスクのストレージ ポリシーを変更します。
- 仮想マシン ホーム ファイルが暗号化されているため、リストア時に暗号化キーが使用できることを確認します。

パフォーマンスのベスト プラクティス

- 暗号化のパフォーマンスは、CPU とストレージの速度に依存します。
- 既存の仮想マシンの暗号化には、新規に作成する仮想マシンの暗号化よりも長い時間がかかります。可能であれば、仮想マシンを作成する際に暗号化を行ってください。

ストレージ ポリシーのベスト プラクティス

バンドルされている仮想マシン暗号化のサンプル ストレージ ポリシーは、変更しないでください。代わりに、このポリシーのクローンを作成し、そのクローンを編集します。

注： 仮想マシン暗号化ポリシーを自動的に元の設定に戻す方法はありません。

ストレージ ポリシーのカスタマイズに関する詳細については、『vSphere のストレージ』を参照してください。

暗号化キーの削除のベスト プラクティス

暗号化キーをクラスタから確実に削除するには、暗号化された仮想マシンを削除、登録解除、または別の vCenter Server に移動した後、クラスタ内の ESXi ホストを再起動します。

仮想マシンの暗号化に関する注意

後から問題が発生しないように、仮想マシンの暗号化に関する注意事項を確認してください。

仮想マシンの暗号化で使用できないデバイスおよび機能については、仮想マシンの暗号化の相互運用性を参照してください。

制限

仮想マシンの暗号化戦略を立てるときは、次の注意点を考慮してください。

- 暗号化された仮想マシンのクローンを作成するとき、または Storage vMotion 操作を実行するときに、ディスク形式を変更することができます。しかし、ディスク形式の変換は成功しないことがあります。たとえば、仮想マシンのクローンを作成するときにディスク形式を lazy-zeroed シック フォーマットからシン フォーマットに変更しても、仮想マシンのディスクは lazy-zeroed シック フォーマットのままです。
- 仮想マシンからディスクを切り離すと、仮想ディスクのストレージ ポリシー情報は保持されません。
  - 仮想ディスクが暗号化されている場合は、ストレージ ポリシーを [仮想マシン暗号化ポリシー]、または暗号化を含むストレージ ポリシーに明示的に設定する必要があります。
  - 仮想ディスクが暗号化されていない場合は、そのディスクを仮想マシンに追加するときにストレージ ポリシーを変更できます。

  詳細については、仮想ディスクの暗号化を参照してください。
- コア ダンプは、仮想マシンを別のクラスタに移動する前に復号化してください。

  vCenter Server には KMS キーは保存されません。キー ID が記録されるだけです。そのため、vCenter Server に ESXi ホスト キーが永続的に保持されることはありません。

  一定の条件のとき、たとえば ESXi ホストを別のクラスタに移動してホストを再起動した場合は、そのホストには vCenter Server によって新しいホスト キーが割り当てられます。この新しいホスト キーで既存のコア ダンプを復号化することはできません。
- 暗号化された仮想マシンでは、OVF Export はサポートされません。
- VMware Host Client を使用して暗号化された仮想マシンを登録することはサポートされていません。

仮想マシンのロック状態

この仮想マシンのキー、または少なくとも 1 つの仮想ディスクのキーが失われると、仮想マシンはロック状態になります。ロック状態の間、仮想マシンの操作は実行できません。

- 仮想マシンとそのディスクの両方を vSphere Client から暗号化する場合は、両方に同じキーを使用する必要があります。
- API を使用して暗号化を実行する場合は、仮想マシンとディスクに異なる暗号化キーを使用できます。その場合、仮想マシンをパワーオンしようとしたときにディスク キーのいずれかがないと、パワーオン操作は失敗します。仮想ディスクを削除すると、仮想マシンをパワーオンできます。

トラブルシューティングのヒントについては、キー紛失に関する問題の解決を参照してください。

仮想マシンの暗号化の相互運用性

vSphere 仮想マシンの暗号化 には、相互運用が可能なデバイスと機能に関していくつかの制限があります。

次の制限事項と注釈は、vSphere 仮想マシンの暗号化を使用することを示しています。vSAN 暗号化の使用法に関する同様の情報については、『VMware vSAN の管理』ドキュメントを参照してください。

特定の暗号化タスクの制限

暗号化された仮想マシンで特定のタスクを実行する場合は、いくつかの制限が適用されます。

- パワーオン状態の仮想マシンでは、ほとんどの暗号化操作を実行できません。仮想マシンをパワーオフする必要があります。仮想マシンがパワーオンされていると、暗号化された仮想マシンのクローンを作成して、再暗号化（表層）を実行できます。
- スナップショットがある仮想マシンでは、再暗号化（深層）を実行することはできません。スナップショットがある仮想マシンでは、再暗号化（表層）を実行できます。

仮想 Trusted Platform Module デバイスと vSphere 仮想マシンの暗号化

仮想 Trusted Platform Module (vTPM) は、物理的な Trusted Platform Module 2.0 チップをソフトウェアにしたものです。vTPM は、新しい仮想マシンと既存の仮想マシンのどちらにも追加できます。仮想マシンに vTPM を追加するには、vSphere 環境でキー プロバイダを構成する必要があります。vTPM を構成すると、仮想マシンの「ホーム」ファイルが暗号化されます（メモリ スワップ ファイル、NVRAM ファイルなど）。ディスク ファイルまたは VMDK ファイルは自動的に暗号化されません。仮想マシンのディスクの暗号化は明示的に追加できます。

注意： 仮想マシンのクローンを作成すると、vTPM などの仮想デバイスを含む仮想マシン全体が複製されます。vTPM に保存されている情報（システムの ID を特定するためにソフトウェアが使用できる vTPM のプロパティなど）も複製されます。

vSphere 仮想マシンの暗号化とサスペンド状態およびスナップショット

暗号化された仮想マシンをサスペンド状態からレジュームすることや、暗号化されたマシンのメモリ スナップショットに戻すことができます。メモリ スナップショットがあり、サスペンド状態になっている暗号化された仮想マシンを、ESXi ホスト間で移行することができます。

vSphere 仮想マシンの暗号化 と IPv6

vSphere 仮想マシンの暗号化は、ピュア IPv6 モードまたは混在モードで使用できます。キー サーバは、IPv6 アドレスを使用して設定できます。IPv6 アドレスのみを使用して、vCenter Server とキー サーバの両方を構成することができます。

vSphere 仮想マシン暗号化でのクローン作成の制限

いくつかのクローン作成機能は、vSphere 仮想マシンの暗号化と同時に使用することはできません。

- 標準のキー プロバイダの場合、クローン作成は条件付きでサポートされます。
  - フル クローンはサポートされます。このクローンには、キーも含めて親の暗号化状態が継承されます。フル クローンを暗号化したり、再暗号化して新しいキーを使用したり、復号化したりできます。

    リンク クローンはサポートされており、このクローンはキーも含めて親の暗号化状態を継承します。リンク クローンを復号化することや、別のキーで再暗号化することはできません。

    注： 他のアプリケーションがリンク クローンをサポートしていることを確認します。たとえば、VMware Horizon® 7 はフル クローンとインスタント クローンの両方をサポートしていますが、リンク クローンはサポートしていません。
- 信頼済みのキー プロバイダ、または vSphere Native Key Provider の場合、クローン作成はサポートされますが、クローン時に暗号化キーを変更することはできません。これは、クローン作成時にキーを変更できる標準の暗号化とは対照的です。次の操作は、仮想マシンのクローン作成時に vSphere 信頼機関 または vSphere Native Key Provider によってサポートされません。
  - 暗号化されていない仮想マシンから暗号化された仮想マシンへのクローン作成
  - 暗号化された仮想マシンからのクローン作成と暗号化キーの変更
  - 暗号化された仮想マシンから暗号化されていない仮想マシンへのクローン作成
- インスタント クローンはすべてのキープロバイダータイプでサポートされていますが、、クローン上で暗号化キーを変更することはできません。

vSphere 仮想マシンの暗号化を使用したディスク構成はサポートされていません

仮想マシン ディスクの構成のうち、一部の種類は vSphere 仮想マシンの暗号化ではサポートされません。

- RDM（Raw デバイス マッピング）。ただし、vSphere Virtual Volumes (vVols) はサポートされます。
- マルチライターまたは共有ディスク（MSCS、WSFC、または Oracle RAC）。暗号化された仮想マシンの「ホーム」ファイルは、マルチライター ディスクでサポートされています。暗号化された仮想ディスクは、マルチライター ディスクではサポートされていません。暗号化された仮想ディスクを含む仮想マシンの [設定の編集] 画面でマルチライターを選択する際に、[OK] ボタンが無効になります。

vSphere 仮想マシンの暗号化に関するその他の制限事項

vSphere 仮想マシンの暗号化で動作しないその他の機能は、以下のとおりです。

- vSphere ESXi Dump Collector

- コンテンツ ライブラリ
  - コンテンツ ライブラリでは、OVF テンプレート タイプと仮想マシン テンプレート タイプの 2 種類のテンプレートがサポートされます。暗号化された仮想マシンを OVF テンプレート タイプにエクスポートすることはできません。OVF Tool は暗号化された仮想マシンをサポートしていません。仮想マシン テンプレート タイプを使用して、暗号化された仮想マシン テンプレートを作成できます。『vSphere 仮想マシン管理ガイド』 ドキュメントを参照してください。
- 暗号化された仮想ディスクをバックアップするソフトウェアは、VMware vSphere Storage API - Data Protection (VADP) を使用して、ホット アド モードまたは SSL が有効な NBD モードでディスクをバックアップする必要があります。ただし、仮想ディスクのバックアップに VADP を使用するすべてのバックアップ ソリューションがサポートされているわけではありません。詳細については、バックアップ ベンダーにお問い合わせください。
  - 暗号化された仮想ディスクのバックアップでは、VADP SAN 転送モード ソリューションはサポートされていません。
  - VADP ホット アド ソリューションは、暗号化された仮想ディスクでサポートされています。バックアップ ソフトウェアは、ホット アド バックアップ ワークフローの一部として使用されるプロキシ仮想マシンの暗号化をサポートしている必要があります。ベンダーのアプリケーションには、暗号化操作.直接アクセス権限権限が必要です。
  - 暗号化された仮想ディスクのバックアップでは、NBD-SSL 転送モードを使用するバックアップ ソリューションがサポートされています。ベンダーのアプリケーションには、Cryptographic Operations.Direct Access 権限が必要です。
- 暗号化された仮想マシンからの出力をシリアル ポートまたはパラレル ポートに送信することはできません。構成が成功したように見えても、出力はファイルに送信されます。
- vSphere 仮想マシンの暗号化は VMware Cloud on AWS ではサポートされていません。『VMware Cloud on AWS データセンターの管理』ドキュメントを参照してください。

キーの永続性の概要

vSphere 7.0 Update 2 以降では、キー サーバが一時的にオフラインまたは使用不可になった場合でも、暗号化された仮想マシンと仮想 TPM は必要に応じて機能し続けることができます。ESXi ホストは、暗号化キーを保持して、暗号化および vTPM の操作を続行できます。

vSphere 7.0 Update 2 より前のバージョンでは、暗号化された仮想マシンと vTPM が機能するように、キー サーバを常に使用できるようにする必要があります。vSphere 7.0 Update 2 以降では、キー サーバへの接続が切断された場合でも、暗号化されたデバイスは機能します。

vSphere 7.0 Update 3 以降では、キー プロバイダへの接続が切断された場合でも、暗号化された vSAN クラスタは機能します。

注： vSphere Native Key Provider を使用する場合、キーの永続性は必要ありません。vSphere Native Key Provider は、キー サーバにアクセスしなくても実行できるように、特別な設定が不要な設計になっています。「キーの永続性と vSphere Native Key Provider」のセクションを参照してください。

ESXi ホストでのキーの永続性

標準のキー プロバイダを使用する場合、ESXi ホストは vCenter Server を使用して暗号化キーを管理します。信頼済みキー プロバイダを使用する場合、ESXi ホストは信頼機関ホストのキーを直接使用します。vCenter Server は使用されません。

キー プロバイダのタイプに関係なく、ESXi ホストは最初にキーを取得し、キー キャッシュに保持します。ESXi ホストを再起動すると、そのキー キャッシュは失われます。その場合、ESXi ホストは、キー サーバ（標準のキー プロバイダ）または信頼機関ホスト（信頼済みキー プロバイダ）からのキーの取得を再度要求します。ESXi ホストがキーを取得する際に、キー サーバがオフラインまたはアクセス不可の場合、vTPM とワークロードの暗号化は機能しません。通常、キー サーバがサイトに展開されない Edge 形式の展開では、キー サーバへの接続が失われると、暗号化されたワークロードに不要なダウンタイムが発生する可能性があります。

vSphere 7.0 Update 2 以降では、キー サーバがオフラインまたはアクセス不可の場合でも、暗号化されたワークロードは引き続き機能します。ESXi ホストに TPM がある場合、暗号化キーは再起動後も TPM に保持されます。そのため、ESXi ホストは、再起動しても暗号化キーを要求する必要がありません。また、暗号化キーは TPM に保持されているため、キー サーバに接続できない場合でも、暗号化と復号の操作を続行できます。つまり、キー サーバや信頼機関ホストが使用できなくても、暗号化されたワークロードを「キー サーバなし」で続行できます。同様に、vTPM も、キー サーバに接続できなくても機能します。

キーの永続性と vSphere Native Key Provider

vSphere Native Key Provider を使用する場合、vSphere がキーを生成します。キー サーバは必要ありません。ESXi ホストは Key Derivation Key (KDK) を取得して、他のキーの抽出に使用します。KDK を受け取って他のキーを生成した後、ESXi ホストが vCenter Server にアクセスして暗号化操作を実行する必要はありません。つまり、vSphere Native Key Provider は常に「キー サーバなし」で実行されます。

ESXi ホストの再起動後も、このホストの再起動後に vCenter Server が使用できない場合も、KDK はデフォルトでこのホスト上に存続します。

vSphere Native Key Provider を使用してキーの永続性を有効にできますが、通常は不要です。ESXi ホストは vSphere Native Key Provider に完全にアクセスできるため、キーの永続性を強化する必要はありません。vSphere Native Key Provider でキーの永続性を有効にする使用事例の 1 つは、標準のキー プロバイダ（外部 KMIP サーバ）も構成されている場合です。

キーの永続性の設定方法

キーの永続性を有効または無効にするには、ESXi ホストでのキーの永続性の有効化および無効化を参照してください。

標準キー プロバイダの構成と管理 7

vSphere 環境で標準のキー プロバイダを使用するには、準備が必要です。環境を設定すると、暗号化された仮想マシンや仮想ディスクを作成したり、既存の仮想マシンやディスクを暗号化したりすることができます。

標準キー プロバイダ用に環境を設定すると、vSphere Client を使用して暗号化された仮想マシンや仮想ディスクを作成したり、既存の仮想マシンやディスクを暗号化したりすることができます。10 章 vSphere 環境における暗号化の使用を参照してください。

API と crypto-util CLI を使用することで、追加のタスクを実行できます。API に関するドキュメントについては『vSphere Web Services SDK プログラミング ガイド』を、`crypto-util` ツールについてはそのコマンド ライン ヘルプ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。

標準のキー プロバイダの概要

標準のキー プロバイダを使用して、仮想マシンの暗号化タスクを実行できます。

標準のキー プロバイダについて

vSphere では、標準のキー プロバイダーがキー サーバから直接暗号化キーを取得し、vCenter Server がデータセンター内の必要な ESXi ホストにキーを配布します。

ユーザーごとに個別の標準キー プロバイダを追加し、デフォルトの標準キー プロバイダを設定できます。

vSphere Standard キー プロバイダの要件

- vSphere 6.5 以降
- 外部キー サーバ (KMS)

キー管理サーバは、Key Management Interoperability Protocol (KMIP) 1.1 標準をサポートする必要があります。詳細については、『vSphere 互換性マトリックス』を参照してください。

VMware 認定の KMS ベンダーに関する情報は、VMware 互換性ガイドのプラットフォームとコンピューティングの下で入手できます。[Compatibility Guides] を選択すると、キー管理サーバ (KMS) の互換性ドキュメントを開くことができます。このドキュメントは頻繁に更新されます。

標準のキー プロバイダの権限

標準キー プロバイダは、Cryptographer.* 権限を使用します。暗号化操作権限を参照してください。

標準のキー プロバイダの設定

仮想マシンの暗号化タスクを開始するためには、標準のキー プロバイダを設定する必要があります。

標準のキー プロバイダの設定には、キー プロバイダの追加とキー サーバとの信頼の確立が含まれます。キー プロバイダを追加するときに、このプロバイダをデフォルトとして設定するように求められます。デフォルトのキー プロバイダは明示的に変更することができます。vCenter Server は、デフォルトのキー プロバイダからキーをプロビジョニングします。

注： 以前、vSphere 6.5 および 6.7 でキー管理サーバ クラスタと呼ばれていたものは、キー プロバイダに改称されました。

 (仮想マシンの暗号化、標準キー プロバイダの設定)

vSphere Client を使用した標準のキー プロバイダの追加

ご使用の vCenter Server システムに標準のキー プロバイダを追加するには、vSphere Client またはパブリック API を使用します。

vSphere Client を使用すると、vCenter Server システムに標準のキー プロバイダを追加し、キー サーバと vCenter Server 間の信頼を確立することができます。

- 同じベンダーの複数のキー サーバを追加できます。
- ご使用の環境がさまざまなベンダーのソリューションをサポートしている場合は、複数のキー プロバイダを追加することができます。
- ご使用の環境に複数のキー プロバイダが含まれていて、かつデフォルトのキー プロバイダを削除する場合は、別のデフォルトのキー プロバイダを明示的に設定する必要があります。
- キー サーバは、IPv6 アドレスを使用して設定できます。
  - IPv6 アドレスのみで、vCenter Server システムとキー サーバの両方を設定できます。

前提条件

- キー サーバ (KMS) が VMware Compatibility Guide for Key Management Servers (KMS) に記載されていて、KMIP 1.1 に準拠していることを確認し、さらに、Symmetric Key Foundry and Server として利用できることを確認します。
- 次の必要な権限があることを確認します。暗号化操作.キー サーバの管理

- キー サーバが高可用性になっていることを確認します。停電やディザスタ リカバリ イベントなどでキー サーバへの接続が切断されると、暗号化された仮想マシンがアクセス不能になります。

  注： vSphere 7.0 Update 2 以降、暗号化された仮想マシンと仮想 TPM は、キー サーバが一時的にオフラインまたは使用できない場合でも機能し続けることができます。キーの永続性の概要を参照してください。

- キー サーバに対するインフラストラクチャの依存関係を慎重に考慮してください。一部の KMS ソリューションは仮想アプライアンスとして提供されるため、KMS アプライアンスの配置が不適切な場合、依存関係のループやその他の可用性の問題が生じることがあります。

手順

1. vSphere Client で vCenter Server にログインします。
2. インベントリ リストを参照し、vCenter Server インスタンスを選択します。
3. [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。
4. [標準のキー プロバイダの追加] をクリックして、キー プロバイダ情報を入力します。

オプション	値
[名前]	キー プロバイダの名前。 各論理キー プロバイダには、そのタイプ（標準、信頼済み、ネイティブの各キー プロバイダ）に関係なく、すべての vCenter Server システムで一意の名前が付いている必要があります。 詳細については、『キー プロバイダの名前の指定』を参照してください。
[KMS]	キー サーバのエイリアス (KMS)。
[アドレス]	キー サーバの IP アドレスまたは FQDN。
[ポート]	vCenter Server からキー サーバに接続するときに使用するポート。
[プロキシ サーバ]	キー サーバに接続するためのオプションのプロキシ サーバ アドレス。
[プロキシ ポート]	キー サーバに接続するためのオプションのプロキシ ポート。
[ユーザー名]	一部のキー サーバ ベンダーでは、ユーザー名とパスワードを指定することによって、ユーザーまたはグループごとに暗号化キーを分離できるようになっています。機能がキー サーバでサポートされ、機能を使用する場合にのみ、ユーザー名を指定します。
[パスワード]	一部のキー サーバ ベンダーでは、ユーザー名とパスワードを指定することによって、ユーザーまたはグループごとに暗号化キーを分離できるようになっています。機能がキー サーバでサポートされ、機能を使用する場合にのみ、パスワードを指定します。

   [KMS の追加] をクリックすると、キー サーバを追加できます。

5. [キー プロバイダの追加] をクリックします。
6. [信頼] をクリックします。

   vCenter Server にキー プロバイダが追加され、ステータスは [接続済み] と表示されます。

次のステップ

証明書の交換による標準キー プロバイダの信頼された接続の確立を参照してください。

証明書の交換による標準キー プロバイダの信頼された接続の確立

vCenter Server システムに標準キー プロバイダを追加した後に、信頼された接続を確立することができます。実際のプロセスは、キー プロバイダが受け入れた証明書と企業ポリシーによって異なります。

前提条件

標準キー プロバイダを追加します。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 キー プロバイダを選択します。

キー プロバイダの KMS が表示されます。

4 KMS を選択します。

5 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。

6 ご使用のサーバに適したオプションを選択し、該当する手順を実行します。

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。
vCenter Server ルート CA 証明書	[ルート CA 証明書] オプションによる標準キー プロバイダの信頼済み接続の確立。
vCenter Server 証明書	[証明書] オプションによる標準キー プロバイダの信頼済み接続の確立。
証明書およびプライベート キーのアップロード	[証明書およびプライベート キーのアップロード] オプションによる標準キー プロバイダの信頼済み接続の確立。
新規証明書署名要求	[新規証明書署名要求] オプションによる標準キー プロバイダの信頼済み接続の確立。

[ルート CA 証明書] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、KMS にルート CA 証明書をアップロードすることが要求されます。ルート CA によって署名されたすべての証明書は、この KMS によって信頼されます。

vSphere 仮想マシンの暗号化で使用されるルート CA 証明書は、vCenter Server システムの VMware Endpoint Certificate Store (VECS) 内にある独立したストアに保存される自己署名証明書です。

注： ルート CA 証明書を生成するのは、既存の証明書を置き換える場合に限定してください。生成すると、そのルート CA によって署名された他の証明書は無効になります。新しいルート CA 証明書は、このワークフローの一部として生成できます。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 信頼された接続を確立するキー プロバイダを選択します。

キー プロバイダの KMS が表示されます。

4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。

5 [vCenter Server ルート CA 証明書] を選択し、[次へ] をクリックします。

vCenter Server が暗号化に使用するルート証明書に基づいて、[ルート CA 証明書のダウンロード] ダイアログ ボックスが入力されます。この証明書は、VMware Endpoint Certificate Store (VECS) に保存されます。

6 証明書をクリップボードにコピーするか、ファイルとしてダウンロードします。

7 KMS ベンダーからの指示に従って証明書をベンダーのシステムにアップロードします。

注： 一部の KMS ベンダーでは、アップロードしたルート証明書を取得する際に、KMS の再起動が要求されます。

次のステップ

証明書の交換を完了します。標準のキー プロバイダの信頼設定の完了を参照してください。

[証明書] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、KMS に vCenter Server 証明書をアップロードすることが要求されます。アップロード後、KMS はその証明書を使用しているシステムからのトラフィックを受け付けます。

vCenter Server は、KMS との接続を保護するための証明書を生成します。証明書は、vCenter Server システムの VMware Endpoint Certificate Store (VECS) 内にある独立したキー ストアに保存されます。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 信頼された接続を確立するキー プロバイダを選択します。

キー プロバイダの KMS が表示されます。

4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。

5 [vCenter Server 証明書] を選択し、[次へ] をクリックします。

vCenter Server が暗号化に使用するルート証明書に基づいて、[証明書のダウンロード] ダイアログ ボックスが入力されます。この証明書は、VMware Endpoint Certificate Store (VECS) に保存されます。

注： 既存の証明書を置き換える場合を除き、新しい証明書を生成しないでください。

6 証明書をクリップボードにコピーするか、ファイルとしてダウンロードします。

7 KMS ベンダーからの指示に従って証明書を KMS にアップロードします。

次のステップ

信頼関係を確立します。標準のキー プロバイダの信頼設定の完了を参照してください。

[証明書およびプライベート キーのアップロード] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、KMS サーバ証明書およびプライベート キーを vCenter Server システムにアップロードすることが要求されます。

一部の KMS ベンダーは、接続のための証明書およびプライベート キーを生成し、ユーザーが利用できるようにしています。ファイルをアップロードすると、KMS は vCenter Server インスタンスを信頼します。

前提条件

- 証明書およびプライベート キーを KMS ベンダーに要求します。ファイルは、PEM 形式の X509 ファイルです。

手順

1. vCenter Server に移動します。
2. [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。
3. 信頼された接続を確立するキー プロバイダを選択します。

   キー プロバイダの KMS が表示されます。
4. [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。
5. [KMS 証明書およびプライベート キー] を選択し、[次へ] をクリックします。
6. 一番上にあるテキスト ボックスに KMS ベンダーから受け取った証明書を貼り付けるか、[ファイルのアップロード] をクリックして証明書ファイルをアップロードします。
7. 一番下にあるテキスト ボックスにキー ファイルを貼り付けるか、[ファイルのアップロード] をクリックしてキー ファイルをアップロードします。
8. [信頼の確立] をクリックします。

次のステップ

信頼関係を確立します。標準のキー プロバイダの信頼設定の完了を参照してください。

[新規証明書署名要求] オプションによる標準キー プロバイダの信頼済み接続の確立

一部のキー管理サーバ (KMS) ベンダーでは、vCenter Server が証明書署名リクエスト (CSR) を生成して KMS に送信することが要求されます。KMS は CSR に署名し、署名済み証明書を返します。この署名済み証明書を vCenter Server にアップロードしてください。

[新規証明書署名要求] オプションの使用には、2 つのステップがあります。まず、CSR を生成して KMS に送信します。次に、KMS ベンダーから受け取った署名済み証明書を vCenter Server にアップロードします。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 信頼された接続を確立するキー プロバイダを選択します。

キー プロバイダの KMS が表示されます。

4 [信頼の確立] ドロップダウン メニューから [KMS が vCenter Server を信頼するようにします] を選択します。

5 [新規証明書署名要求 (CSR)] を選択し、[次へ] をクリックします。

6 ダイアログ ボックスで、テキスト ボックス内の証明書全体をクリップボードにコピーするか、ファイルとしてダウンロードします。

ダイアログ ボックスの [新規の証明書署名要求の生成] ボタンは、明示的に CSR を生成する場合にのみ使用します。このオプションを使用すると、以前の CSR に基づく署名済み証明書はすべて無効になります。

7 KMS ベンダーからの指示に従って CSR を送信します。

8 KMS ベンダーから署名付き証明書を受け取ったら、[キー プロバイダ] を再度クリックしてキー プロバイダを選択し、[信頼の確立] ドロップダウン メニューから、[署名済みの証明書署名要求の証明書のアップロード] を選択します。

9 一番下にあるテキスト ボックスに署名付き証明書を貼り付けるか、[ファイルのアップロード] をクリックしてファイルをアップロードし、[アップロード] をクリックします。

次のステップ

信頼関係を確立します。標準のキー プロバイダの信頼設定の完了を参照してください。

デフォルトのキー プロバイダの設定

1 つ目のキー プロバイダをデフォルトにしない場合や、ご利用の環境で複数のキー プロバイダを使用していてデフォルトのプロバイダを削除した場合、デフォルトのキー プロバイダを設定する必要があります。

前提条件

ベスト プラクティスとして、[キー プロバイダ] タブの [接続状態] に [正常] と表示され、緑色のチェック マークが表示されていることを確認します。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 キー プロバイダを選択します。

4 [デフォルトにする] をクリックします。

確認のダイアログ ボックスが表示されます。

5 [デフォルトにする] をクリックします。

キー プロバイダが現在のデフォルトとして表示されます。

標準のキー プロバイダの信頼設定の完了

[標準のキー プロバイダの追加] ダイアログ ボックスで KMS を信頼するように促すメッセージが表示されなかった場合は、証明書の交換が完了した後で信頼を明示的に確立する必要があります。

KMS を信頼するか、KMS 証明書をアップロードすることにより vCenter Server が KMS を信頼するように設定すると、信頼関係の設定が完了します。これには次の 2 つのオプションがあります。

- [KMS 証明書のアップロード] オプションを使用して明示的に証明書を信頼します。
- [vCenter Server が KMS を信頼するようにします] オプションを使用して KMS リーフ証明書または KMS CA 証明書を vCenter Server にアップロードします。

注： ルート CA 証明書または中間 CA 証明書をアップロードすると、その CA で署名されたすべての証明書が vCenter Server で信頼されるようになります。セキュリティを強化するために、KMS ベンダーで管理されているリーフ証明書または中間 CA 証明書をアップロードするようにしてください。

手順

1 vCenter Server に移動します。

2 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] を選択します。

3 信頼された接続を確立するキー プロバイダを選択します。

キー プロバイダの KMS が表示されます。

4 KMS を選択します。

5 [信頼の確立] ドロップダウン メニューから次のいずれかのオプションを選択します。

オプション	操作
vCenter Server が KMS を信頼するようにします	表示されたダイアログ ボックスで、[信頼] をクリックします。
KMS 証明書のアップロード	a 表示されたダイアログ ボックスで、証明書を貼り付けるか、[ファイルのアップロード] をクリックして証明書ファイルを参照します。 b [アップロード] をクリックします。

ユーザーごとの別々のキー プロバイダの設定

同じ KMS インスタンスのユーザーごとに、異なるキー プロバイダで環境を設定できます。複数のキー プロバイダを追加すると、たとえば、社内の部署ごとに異なる暗号化キー セットへのアクセス権を付与する場合などに便利です。

同じ KMS に複数のキー プロバイダを使用して、キーを分けることができます。別々のキー セットを持つことは、ビジネス部門や顧客ごとのユースケースを保持するために不可欠です。

注： すべての KMS ベンダーが複数のユーザーをサポートしているわけではありません。

前提条件

KMS との接続を設定します。

手順

1. KMS 上の対応するユーザー名とパスワード（C1 や C2 など）で 2 人のユーザーを作成します。
2. vCenter Server にログインし、最初のキー プロバイダを作成します。
3. ユーザー名とパスワードを求められたら、1 人目のユーザーの情報を指定します。
4. 2 つ目のキー プロバイダを作成します。同じ KMS を追加しますが、2 人目のユーザー名とパスワード (C2) を使用します。

結果

この 2 つのキー プロバイダには、KMS へのそれぞれ独立した接続があり、異なるキー セットを使用します。

vSphere Native Key Provider の構成と管理

8

vSphere 環境で VMware vSphere® Native Key Provider™ を使用するには、準備が必要です。vSphere Native Key Provider を構成した後、仮想マシン上に仮想 Trusted Platform Module (vTPM) を作成できます。

環境を vSphere Native Key Provider 用にセットアップしたら、vSphere Client と API を使用して vTPM を作成できます。VMware vSphere® Enterprise Plus エディション™を購入すると、仮想マシンと仮想ディスクの暗号化や既存の仮想マシンとディスクの暗号化も行うことができます。

 (vSphere Native Key Provider の構成)

この章には、次のトピックが含まれています。

- vSphere Native Key Provider の概要
- vSphere Native Key Provider のプロセス フロー
- vSphere Native Key Provider の構成
- vSphere Native Key Provider のバックアップ
- 拡張リンク モード構成での vSphere Native Key Provider のインポート
- vSphere Native Key Provider のリカバリ
- vSphere Native Key Provider の更新
- vSphere Native Key Provider の削除

vSphere Native Key Provider の概要

vSphere 7.0 Update 2 以降では、組み込みの vSphere Native Key Provider を使用して、仮想 TPM (vTPM) などの暗号化テクノロジーを有効にすることができます。

vSphere Native Key Provider はすべての vSphere エディションに含まれており、外部キー サーバ（業界内の別名はキー管理サーバ (KMS)）は不要です。vSphere 仮想マシンの暗号化に vSphere Native Key Provider を使用することもできますが、VMware vSphere® Enterprise Plus エディション™を購入する必要があります。

vSphere Native Key Provider について

標準キー プロバイダまたは信頼済みキー プロバイダでは、外部キー サーバを構成する必要があります。標準のキー プロバイダのセットアップでは、vCenter Server は外部キー サーバからキーを取得し、ESXi ホストに配布します。信頼済みキー プロバイダ (vSphere 信頼機関) のセットアップでは、信頼できる ESXi ホストがキーを直接取得します。

vSphere Native Key Provider で、外部キー サーバは不要になりました。vCenter Server は、Key Derivation Key (KDK) と呼ばれるプライマリ キーを生成し、クラスタ内のすべての ESXi ホストにプッシュします。次に、ESXi ホストはデータ暗号化キーを生成して（vCenter Server に接続されていない場合でも）、vTPM などのセキュリティ機能を有効にします。vTPM 機能は、すべての vSphere エディションに含まれています。vSphere 仮想マシンの暗号化に vSphere Native Key Provider を使用するには、vSphere Enterprise Plus エディションを購入する必要があります。vSphere Native Key Provider は、既存のキー サーバ インフラストラクチャと共存できます。

vSphere Native Key Provider：

- 外部キー サーバが不要な場合、または使用しない場合は、vTPM、vSphere 仮想マシンの暗号化、および vSAN の保存データの暗号化の使用を有効にします。
- VMware インフラストラクチャ製品でのみ機能します。
- 相互運用性またはコンプライアンスのために従来のサードパーティ製外部キー サーバが提供している外部の相互運用性、KMIP サポート、ハードウェア セキュリティ モジュール、またはその他の機能は提供しません。組織が VMware 以外の製品およびコンポーネントにこの機能を必要としている場合は、従来のサードパーティ製キー サーバをインストールします。
- 外部キー サーバを使用できない、または使用しない組織のニーズに対応できます。
- フラッシュや SSD などのサニタイズが困難なメディアで暗号化テクノロジーを早期に使用できるようにすることで、データのサニタイズとシステムの再利用の方法が改善されます。
- キー プロバイダ間の移行パスを提供します。vSphere Native Key Provider は、VMware 標準のキー プロバイダおよび vSphere Trust Authority の信頼されているキー プロバイダと互換性があります。
- 拡張リンク モード構成または vCenter Server High Availability 構成を使用して、複数の vCenter Server システムと連携します。
- vSphere のすべてのエディションで vTPM を有効にし、vSphere 仮想マシンの暗号化 を含む vSphere Enterprise Plus エディションを購入して仮想マシンを暗号化する場合に使用できます。vSphere 仮想マシンの暗号化は、VMware の標準キー プロバイダおよび信頼済みキー プロバイダと同様に、vSphere Native Key Provider と動作します。
- 適切な vSAN ライセンスを使用して vSAN の保存データの暗号化を有効にする場合に使用できます。
- Trusted Platform Module (TPM) 2.0 を使用して、ESXi ホストにインストールされている場合のセキュリティを強化できます。また、TPM 2.0 がインストールされているホストのみが使用できるように vSphere Native Key Provider を構成することもできます。

注： ESXi ホストは、vSphere Native Key Provider を使用するために TPM 2.0 を必要としません。ただし、TPM 2.0 を使用すれば、セキュリティが強化されます。

すべてのセキュリティ ソリューションと同様に、Native Key Provider を使用する場合のシステム設計、実装に関する考慮事項、トレードオフを考慮してください。たとえば、ESXi キーの永続性を使用することで、キー サーバへの依存関係が常に使用可能になることを回避できます。ただし、キーの永続性を有効にすると、Native Key Provider の暗号化情報がクラスタ化されたホストに保存されるため、悪意のあるユーザーが ESXi ホスト自体を盗んだ場合に引き続きリスクが生じます。環境が異なるため、組織の規制およびセキュリティに関するニーズ、運用要件、およびリスクの許容度に応じてセキュリティ制御を評価し、実装します。

vSphere Native Key Provider の概要情報については、https://core.vmware.com/native-key-provider を参照してください。

vSphere Native Key Provider の要件

vSphere Native Key Provider を使用するには、次の操作を行う必要があります。

- vCenter Server システムと ESXi ホストの両方で vSphere 7.0 Update 2 以降が実行されていることを確認します。
- クラスタ内で ESXi ホストを構成します。必須ではありませんが、ベスト プラクティスとして、TPM を含め、可能なかぎり同一の ESXi ホストを使用します。クラスタ ホストが同一の場合、クラスタの管理と機能の有効化が容易になります。
- vCenter Server ファイルベースのバックアップとリストアを構成し、Key Derivation Key が含まれているのでバックアップを安全に保存します。vCenter Server のインストールとセットアップに記載されている vCenter Server のバックアップとリストアに関するトピックを参照してください。

vSphere Native Key Provider を使用して vSphere 仮想マシンの暗号化または vSAN の暗号化を実行するには、適切なライセンスを含むこれらの製品のエディションを購入する必要があります。

vSphere Native Key Provider と拡張リンク モード

単一の vSphere Native Key Provider を構成し、拡張リンク モード構成の vCenter Server システム間で共有することができます。このシナリオの手順の概要は次のとおりです。

1 vCenter Server システムのいずれかで vSphere Native Key Provider を作成します

2 作成された vCenter Server で Native Key Provider をバックアップします

3 Native Key Provider をエクスポートします

4 拡張リンク モード構成の他の vCenter Server システムに Native Key Provider をインポートします

拡張リンク モード構成での vSphere Native Key Provider のインポートを参照してください。

vSphere Native Key Provider の権限

標準および信頼済みキー プロバイダと同様に、vSphere Native Key Provider は Cryptographer を使用します。* 権限を使用します。また、vSphere Native Key Provider は、vSphere Native Key Provider に固有の Cryptographer.ReadKeyServersInfo 権限を使用して、vSphere Native Key Provider を一覧表示します。暗号化操作権限を参照してください。

vSphere Native Key Provider のアラーム

vSphere Native Key Provider をバックアップする必要があります。vSphere Native Key Provider がバックアップされていない場合、vCenter Server はアラームを生成します。アラームが生成された vSphere Native Key Provider をバックアップすると、vCenter Server はアラームをリセットします。デフォルトでは、vCenter Server はバックアップされた vSphere Native Key Provider を 1 日に 1 回チェックします。チェックする間隔は、`vpxd.KMS.backupCheckInterval` オプションで変更できます。

vSphere Native Key Provider の定期的な修正チェック

vCenter Server は、vCenter Server と ESXi ホストの vSphere Native Key Provider 構成が一致していることを定期的にチェックします。たとえば、ホストの状態が変化すると、クラスタにホストを追加すると、クラスタのキー プロバイダ構成がホストの構成から削除されます。ホストで構成 (keyID) が異なる場合、vCenter Server はホストの構成を自動的に更新します。手動での介入は必要ありません。

デフォルトでは、vCenter Server は 5 分ごとに構成をチェックします。`vpxd.KMS.remediationInterval` オプションを使用して間隔を変更できます。

ディザスタ リカバリ サイトでの vSphere Native Key Provider の使用

vSphere Native Key Provider はバックアップ ディザスタ リカバリ サイトで使用できます。vSphere Native Key Provider バックアップをプライマリ サイトからバックアップ DR サイトの vCenter Server にインポートすると、そのクラスタでは暗号化された仮想マシンを復号化して実行できます。

DR ソリューションは必ずテストしてください。リカバリすることなくソリューションが機能すると思い込まないでください。vSphere Native Key Provider バックアップのコピーは、DR サイトでも使用できることを確認してください。

vSphere Native Key Provider のプロセス フロー

vSphere Native Key Provider のプロセス フローを理解することは、vSphere Native Key Provider を構成および管理する方法を学ぶために不可欠です。

組み込みの vSphere Native Key Provider を使用して、暗号化ベースの仮想 TPM (vTPM) を強化できます。vSphere Native Key Provider は、すべての vSphere エディションに含まれており、外部キー サーバは必要としません。vSphere 仮想マシンの暗号化に vSphere Native Key Provider を使用するには、vSphere Enterprise+ エディションを購入する必要があります。

vSphere Native Key Provider の構成

vSphere Native Key Provider の構成には、次の基本操作が含まれます。

1 適切な管理者権限を持つユーザーが vSphere Client を使用して、vSphere Native Key Provider を vCenter Server に作成します。

2 次に vCenter Server が ESXi ホストのすべてのクラスタに vSphere Native Key Provider を構成 します。

この手順では、vCenter Server はクラスタ内のすべての ESXi ホストにプライマリ キーを をプッシュします。vSphere Native Key Provider を更新または削除した場合も、その変更がクラスタ内のホストにプッシュされます。

3 適切な暗号化権限を持つユーザーは、vTPMs と暗号化された仮想マシンを作成します (vSphere Enterprise+ エディションを購入している場合)。

『11 章 仮想 Trusted Platform Module を使用する仮想マシンの保護』と『10 章 vSphere 環境における暗号化の使用』を参照してください。

vSphere Native Key Provider の暗号化プロセス フロー

さまざまなコンポーネントが相互作用して vSphere Native Key Provider を使用して暗号化タスクを実行する方法を理解するには、暗号化プロセス フローを参照してください。

vSphere Native Key Provider の構成

暗号化タスクを開始する前に、vCenter Server で vSphere Native Key Provider を構成する必要があります。

vSphere 7.0 Update 2 以降には、vSphere Native Key Provider と呼ばれるキー プロバイダが含まれています。vSphere Native Key Provider は、外部キー サーバ (KMS) を必要とせずに暗号化関連の機能を有効にします。最初は、vCenter Server には vSphere Native Key Provider が構成されていません。vSphere Native Key Provider を手動で構成する必要があります。

ESXi ホストは、vSphere Native Key Provider を使用するために TPM 2.0 を必要としません。ただし、TPM 2.0 を使用すれば、セキュリティが強化されます。

注： vSphere Native Key Provider を構成すると、キー プロバイダを構成した vCenter Server のすべてのクラスタでキー プロバイダを使用できます。その結果、vCenter Server に接続されているすべてのホストは、構成したすべての vSphere Native Key Provider にアクセスできます。

前提条件

必要な権限：暗号化操作.キー サーバの管理

手順

1 vSphere Client で vCenter Server にログインします。

2 インベントリ リストを参照し、vCenter Server インスタンスを選択します。

3 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。

4 [追加] をクリックしてから、[ネイティブ キー プロバイダの追加] をクリックします。

5 vSphere Native Key Provider の名前を入力します。

各論理キー プロバイダには、そのタイプ（標準、信頼済み、ネイティブの各キー プロバイダ）に関係なく、すべての vCenter Server システムで一意の名前が付いている必要があります。

詳細については、『キー プロバイダの名前の指定』を参照してください。

6 この vSphere Native Key Provider を TPM 2.0 を備えたホストのみで使用する場合は、[TPM で保護された ESXi ホストでのみキー プロバイダを使用する] チェック ボックスをオンにします。

有効にすると、vSphere Native Key Provider は、TPM 2.0 を備えたホストでのみ使用できるようになります。

7 [キー プロバイダの追加] をクリックします。

注： データセンター内のすべてのクラスタ化された ESXi ホストがキー プロバイダを取得し、vCenter Server がそのキャッシュを更新するのに、約 5 分かかります。情報の伝達方法によっては、一部のホストでのキー操作にキー プロバイダを使用するには、数分待つ必要がある場合があります。

結果

vSphere Native Key Provider が追加され、[キー プロバイダ] ペインに表示されます。この時点では、vSphere Native Key Provider はバックアップされていません。vSphere Native Key Provider を使用するには、バックアップする必要があります。

次のステップ

vSphere Native Key Provider のバックアップを参照してください。

vSphere Native Key Provider のバックアップ

キー プロバイダの構成をリストアする必要がある場合は、ディザスタ リカバリ シナリオの一部として、vSphere Native Key Provider のバックアップが必要です。vSphere Client、PowerCLI、または API を使用して、vSphere Native Key Provider をバックアップできます。

vSphere Native Key Provider は、vCenter Server ファイルベースのバックアップの一部としてバックアップされます。ただし、vSphere Native Key Provider を使用するには、少なくとも 1 回バックアップする必要があります。vSphere Native Key Provider を作成するときに、バックアップは作成されません。

構成をリストアする場合に備えて、バックアップが必要です。vSphere Native Key Provider をリストアするには、vSphere Client を使用した vSphere Native Key Provider のリストアを参照してください。

バックアップ ファイルは安全な場所に保管します。バックアップを作成するときに、パスワードで保護することができます。バックアップ ファイルは PKCS# 12 形式です。

vCenter Server は、vSphere Native Key Provider がバックアップされていない場合にアラームを作成します。アラームを確認することはできますが、vSphere Native Key Provider をバックアップするまで、24 時間ごとに再表示されます。

前提条件

必要な権限：暗号化操作.キー サーバの管理

注： 拡張リンクモード構成では、キー プロバイダが属する vCenter Server でバックアップを実行する必要があります。

手順

1 vSphere Client で vCenter Server にログインします。

2 インベントリ リストを参照し、vCenter Server インスタンスを選択します。

3 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。

4 バックアップする vSphere Native Key Provider を選択します。

バックアップしていないキー プロバイダについては、「バックアップされていません」というステータスが表示されます。

5 [バックアップ] をクリックします。

6 バックアップをパスワードで保護するには、[ネイティブ キー プロバイダ データをパスワードで保護] チェックボックスをオンにします。

a パスワードを入力し、安全な場所に保存します。

b [パスワードを安全な場所に保存しました] ボックスをオンにして、パスワードを安全な場所に保存したことを示します。

7 [キー プロバイダのバックアップ] をクリックします。

バックアップ ファイルは PKCS# 12 形式です。

8 バックアップ ファイルを安全な場所に保存します。

結果

vSphere Native Key Provider のステータスが、[バックアップされていません] から、[警告]、[アクティブ] に変わります。[警告] は、vCenter Server がまだデータセンター内のすべての ESXi ホストに情報をプッシュしている途中であることを示しています。[アクティブ] は、情報がすべてのホストにプッシュされたことを意味します。

次のステップ

ESXi ホストに vTPM を追加するには、11 章 仮想 Trusted Platform Module を使用する仮想マシンの保護を参照してください。仮想マシンを暗号化するには、10 章 vSphere 環境における暗号化の使用を参照してください。

拡張リンク モード構成での vSphere Native Key Provider のインポート

拡張リンク モード構成の 1 つの vCenter Server で Native Key Provider を作成した後、vSphere Client を使用して構成内の別の vCenter Server にインポートすることができます。

単一の vSphere Native Key Provider を構成し、拡張リンク モード構成の vCenter Server システム間で共有することができます。拡張リンク モード構成内のいずれかの vCenter Server システムで vSphere Native Key Provider を作成し、[リストア] 機能を使用して、暗号化キー ファイルを ELM で接続された他の vCenter Server システムにインポートします。

前提条件

- 必要な権限：暗号化操作.キー サーバの管理

- 拡張リンク モード構成内のいずれかの vCenter Server システムで vSphere Native Key Provider を作成します。vSphere Native Key Provider の構成を参照してください。
- vSphere Native Key Provider をバックアップし、バックアップ暗号化キー ファイルをダウンロードします。vSphere Native Key Provider のバックアップを参照してください。バックアップ暗号化キー ファイルを、インポート時にアクセスできる安全な場所に配置します。

手順

1. vSphere Client で、vSphere Native Key Provider をインポートする拡張リンク モード構成内の vCenter Server にログインします。
2. インベントリ リストを参照し、vCenter Server インスタンスを選択します。
3. [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。
4. [リストア] をクリックします。
5. vSphere Native Key Provider のバックアップ暗号化キー ファイルを保存したファイルの場所を参照します。

   ファイルは PKCS#12 形式で保存されました。
6. ファイルを選択します。
7. （オプション） ファイルがパスワードで保護されている場合は、パスワードを入力します。
8. [次へ] をクリックします。
9. （オプション）このキー プロバイダを ESXi TPM で保護された ホストでのみ使用する場合は、チェック ボックスを選択します。
10. [終了] をクリックします。

結果

vSphere Native Key Provider が vCenter Server にインポートされます。vSphere Native Key Provider を暗号化タスクに使用するには、まず [キー プロバイダ] ペインで選択してから、[デフォルトとして設定] をクリックします。

次のステップ

vSphere Native Key Provider を追加する拡張リンク モード構成内の他の vCenter Server システムに、これらの手順を繰り返します。

vSphere Native Key Provider のリカバリ

vSphere Native Key Provider は、vSphere Client または vCenter Server Appliance のバックアップからリカバリできます。

必要に応じて、次の方法で vSphere Native Key Provider をリカバリできます。

1 vCenter Server Appliance を再構築する必要がない場合は、キー プロバイダをリストアするために vSphere Client を使用します。vSphere Client を使用した vSphere Native Key Provider のリストアを参照してください。

2 vCenter Server Appliance を再構築する必要がある場合は、vCenter Server Appliance のバックアップからキー プロバイダをリストアする必要があります。vCenter Server Appliance のバックアップを実行すると、Native Key Provider が保存されます。バックアップから vCenter Server Appliance をリストアする詳細については、https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html を参照してください。

vSphere Client を使用した vSphere Native Key Provider のリストア

vSphere Client 使用して、vSphere Native Key Provider をリストアできます。

誤って削除された場合、またはディザスタ リカバリを実行する必要がある場合に備え、ネイティブ キー プロバイダをリストアできます。

vSphere Native Key Provide でリストアする場合、キー プロバイダを再度バックアップする必要はありません。最初のバックアップで十分です。バックアップ ファイルを安全な場所に引き続き保管してください。

前提条件

- 必要な権限：暗号化操作.キー サーバの管理
- キー プロバイダのバックアップ ファイル。
- キー プロバイダ ファイルのパスワード（キー プロバイダをバックアップするときに入力した場合）。

手順

1 vSphere Client で vCenter Server にログインします。

2 インベントリ リストを参照し、vCenter Server インスタンスを選択します。

3 [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。

4 vSphere Native Key Provide を選択し、[リストアする] をクリックします。

5 ファイルの場所を参照し、バックアップ暗号化キー ファイルを選択します。

ファイルは PKCS#12 形式で保存されました。

6 （オプション） ファイルがパスワードで保護されている場合は、パスワードを入力します。

7 [次へ] をクリックします。

8 （オプション）このキー プロバイダを ESXi TPM で保護された ホストでのみ使用する場合は、チェック ボックスを選択します。

9 [終了] をクリックします。

結果

The vSphere Native Key Provider is restored.

vSphere Native Key Provider の更新

通常のキー ローテーション プランの一環として、PowerCLI を使用して、vSphere Native Key Provider を更新することができます。

キー ローテーションのポリシーがある場合は、vSphere Native Key Provider を更新し、そのキー プロバイダで暗号化した仮想マシンを再キー化することができます。vSphere Native Key Provider を更新するには、PowerCLI を使用する必要があります。キー プロバイダを更新せずに、暗号化された仮想マシンを再キー化することもできます。この場合、仮想マシンのキーのみが変更されます。仮想マシンを再キー化するには、vSphere Client を使用した暗号化された仮想マシンの再キー化を参照してください。

前提条件

- 必要な権限：暗号化操作.キー サーバの管理
- PowerCLI 12.3.0

手順

1 PowerCLI セッションで `Connect-VIServer` コマンドレットを実行して、アップデートする vSphere Native Key Provider を構成した vCenter Server に管理者ユーザーとして接続します。

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

2 vSphere Native Key Provider 名を取得するには、オプションの `Type` パラメータを指定して `Get-KeyProvider` コマンドレットを実行します。

```
Get-KeyProvider -Type NativeKeyProvider
```

3 キー プロバイダを更新するには、キー プロバイダ名と GUID を指定して `Set-KeyProvider` コマンドレットを実行します。

`New-Guid` コマンドレットを実行して、使用する GUID を生成できます。

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

構成のバックアップに関する警告が表示されます。

4 キー プロバイダをバックアップするには、`Export-KeyProvider` コマンドレットを実行します。

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

vSphere Client を使用してキー プロバイダをバックアップすることもできます。vSphere Native Key Provider のバックアップを参照してください。

結果

キー プロバイダが更新されると、ステータスは [バックアップされていません] に変わります。キー プロバイダをバックアップすると、ステータスは [有効] に変わります。

vSphere Native Key Provider の削除

vCenter Server から vSphere Native Key Provider を削除できます。

vSphere Native Key Provider を削除した後も、vTPM を備えた仮想マシンまたは暗号化された仮想マシンは引き続き実行されます。ESXi ホストを再起動すると、暗号化された仮想マシンはロック状態になります。これらの仮想マシンの登録を解除した後、再登録しようとすると、ロック状態になります。仮想マシンのロックを解除する唯一の方法は、以前の vSphere Native KeyProvider をリストアすることです。

前提条件

必要な権限：暗号化操作.キー サーバの管理

vSphere Native Key Provider を削除する前に、暗号化された仮想マシンと、そのキー プロバイダを使用して暗号化されたデータストアを別のキー プロバイダに再キー化します。vSphere Client を使用した暗号化された仮想マシンの再キー化を参照してください。

また、キー プロバイダを削除した後に暗号化された仮想マシンのキーを再キー化する必要がある場合に備えて、vSphere Native Key Provider のバックアップを維持します。

手順

1. vSphere Client で vCenter Server にログインします。
2. インベントリ リストを参照し、vCenter Server インスタンスを選択します。
3. [構成] をクリックし、[セキュリティ] の [キー プロバイダ] をクリックします。
4. 削除するキー プロバイダを選択します。
5. [削除] をクリックします。
6. 警告メッセージを読み、スライダを右端までスライドします。
7. [削除] をクリックします。

結果

vSphere Native Key Provider が vCenter Server から削除されます。

vSphere 信頼機関

9

vSphere 7.0 以降では、VMware® vSphere Trust Authority™ の利点を活用することができます。vSphere 信頼機関 は、ワークロード セキュリティを強化する基盤となるテクノロジーです。vSphere 信頼機関 は、ESXi ホストのハードウェアによる証明のルートをワークロード自体に関連付けることにより、組織内でより高いレベルの信頼を確立します。

この章には、次のトピックが含まれています。

vSphere 信頼機関 の概念と機能

vSphere 信頼機関 は、信頼済みコンピューティング ベースの信頼領域を組織のコンピューティング インフラストラクチャ全体に拡張することで、悪意のある攻撃から SDDC を保護します。vSphere 信頼機関 では、高度な暗号化機能に対するリモート証明および制限付きアクセスが使用されます。

vSphere 信頼機関 は、高度なセキュリティ要件を満たす一連のサービスです。vSphere 信頼機関 を使用すると、安全なインフラストラクチャを設定および維持できます。起動したソフトウェアが認証済みであると確認された ESXi ホストでのみ、機密性の高いワークロードを実行できるようにすることができます。

vSphere 信頼機関で環境を保護する方法

ESXi ホストを証明するように vSphere 信頼機関 サービスを設定すると、そのホストは信頼された暗号化操作を実行できるようになります。

vSphere 信頼機関 は ESXi ホストのリモート証明を使用して、起動されたソフトウェアの信頼性を証明します。証明では、ESXi ホストで実行されているソフトウェアが VMware の認証済みソフトウェア、または VMware によって署名されているパートナー ソフトウェアであることが検証されます。証明には、ESXi ホストに取り付けられた Trusted Platform Module (TPM) 2.0 チップに基づく測定値が使用されます。vSphere 信頼機関 では、ESXi は証明されるまで、暗号化キーにアクセスしたり暗号化操作を実行したりできません。

vSphere 信頼機関 用語集

vSphere 信頼機関 では独自の用語と定義が使用されており、これらを理解することが重要です。

表 9-1. vSphere 信頼機関 用語集

用語	定義
VMware vSphere® 信頼機関™	信頼済みインフラストラクチャを有効にする一連のサービスを指定します。ESXi ホストで実行されているソフトウェアが信頼済みであることを確認し、信頼された ESXi ホストに対してのみ暗号化キーをリリースすることに責任を負います。
vSphere 信頼機関のコンポーネント	vSphere 信頼機関のコンポーネントは次のとおりです。 ■ 証明サービス ■ キー プロバイダ サービス
証明サービス	リモート ESXi ホストの状態を証明します。TPM 2.0 を使用して信頼のハードウェア ルートを確立し、管理者が承認した ESXi バージョンのリストにソフトウェア測定値を照合して検証します。
キー プロバイダ サービス	1 台以上のキー サーバをカプセル化し、仮想マシンを暗号化するときに指定できる信頼済みキー プロバイダを公開します。現在、キー サーバは KMIP プロトコルに限定されています。
信頼済みインフラストラクチャ	信頼済みインフラストラクチャは、以下の要素から構成されています。 ■ 信頼機関 vCenter Server ■ ワークロード vCenter Server ■ 少なくとも 1 つの vSphere 信頼機関クラスタ（信頼機関 vCenter Server の一部として構成） ■ 少なくとも 1 つの信頼済みクラスタ（ワークロード vCenter Server の一部として構成） ■ 信頼済みクラスタで実行されている暗号化されたワークロード仮想マシン ■ 少なくとも 1 台の KMIP 準拠キー管理サーバ **注：** 信頼機関クラスタと信頼済みクラスタには、別の vCenter Server システムを使用する必要があります。
信頼機関クラスタ	vSphere 信頼機関コンポーネント（証明サービスおよびキー プロバイダ サービス）を実行する ESXi ホストの vCenter Server クラスタで構成されます。
信頼機関ホスト	vSphere 信頼機関コンポーネント（証明サービスおよびキー プロバイダ サービス）を実行する ESXi ホスト。
信頼できるクラスタ	信頼機関クラスタによってリモートから証明された信頼済み ESXi ホストの vCenter Server クラスタで構成されています。厳格に要求されているわけではありませんが、キー プロバイダ サービスを構成すると、信頼済みクラスタによって得られる価値が大幅に向上します。
信頼済みホスト	信頼機関クラスタの証明サービスによってソフトウェアが検証された ESXi ホスト。このホストでは、信頼機関クラスタのキー プロバイダ サービスによって公開されたキー プロバイダを使用して暗号化できるワークロード仮想マシンが実行されます。
仮想マシンの vSphere 暗号化	vSphere 仮想マシンの暗号化を使用すると、暗号化された仮想マシンを作成したり、既存の仮想マシンを暗号化したりできます。 ■ vSphere 6.5 以降では、vCenter Server は外部 キー サーバからのキーの取得を要求します。キー サーバはキーを生成して保存し、配布のために vCenter Server に渡します。 ■ vSphere 7.0 以降では、vSphere Trust Authority とキー サーバの間に信頼できる接続を設定できます。この設定により、vCenter Server およびワークロード ESXi ホストがキー サーバ認証情報を直接要求する必要がなくなり、多層防御セキュリティが実現されます。
信頼済みキー プロバイダ	キー サーバ上の単一の暗号化キーをカプセル化するキー プロバイダ。暗号化キーへのアクセスには、ESXi ソフトウェアが信頼済みホストで検証されていることを証明サービスが確認することが必要です。
標準のキー プロバイダ	キー サーバから直接暗号化キーを取得し、データセンター内の必要なホストにキーを配布するキー プロバイダ。以前の vSphere では KMS クラスタと呼ばれていました。
キー サーバ	キー プロバイダに関連付けられている KMIP キー管理サーバ (KMS)。
ワークロード vCenter Server	1 つ以上の信頼済みクラスタを管理し、設定するために使用される vCenter Server。

vSphere 信頼機関 の基本

vSphere 信頼機関 を使用すると、次のことを実行できます。

- ESXi ホストに信頼のハードウェア ルートとリモート証明機能を提供する
- 証明された ESXi ホストにのみキーをリリースすることにより、暗号化キーの管理を制限する
- 信頼を管理するための安全性の高い管理環境を作成する
- 複数のキー サーバの管理を一元化する
- 仮想マシンで引き続き実行する暗号化操作で、暗号化キー管理のレベルを強化する

vSphere 6.5 および 6.7 での仮想マシンの暗号化では、vCenter Server を使用してキー サーバから暗号化キーを取得し、必要に応じて ESXi ホストにプッシュします。vCenter Server は、VMware Endpoint Certificate Store (VECS) に保存されているクライアントとサーバの証明書を使用して、キー サーバで認証します。キー サーバから送信される暗号化キーは、vCenter Server のメモリを介して必要な ESXi ホストに渡されます（送信時のデータ暗号化には TLS が使用されます）。さらに、vSphere は vCenter Server での権限の検証によりユーザー権限を検証し、キー サーバのアクセスを制限します。このアーキテクチャはセキュリティで保護されていますが、vCenter Server の侵害、悪意のある vCenter Server 管理者、管理または設定のエラーによるシークレットの漏洩や盗難の可能性については対処しません。

vSphere 7.0 では、vSphere 信頼機関 によってこれらの問題に対処しています。安全で管理可能な ESXi ホストのセットで構成された、信頼できるコンピューティング ベースを作成できます。vSphere 信頼機関 は、信頼する ESXi ホスト用のリモート証明サービスを実装します。さらに、vSphere 信頼機関 では TPM 2.0 証明のサポート（6.7 リリースから vSphere に追加）が進歩し、暗号化キーに対するアクセス制限が実装されたため、仮想マシンのワークロード シークレットの保護が強化されました。また、vSphere 信頼機関 では、認証された信頼機関管理者のみが vSphere 信頼機関 サービスを設定し、信頼機関ホストを設定することができます。信頼機関管理者には、vSphere 管理者ユーザーと同じユーザー、または別のユーザーを指定できます。

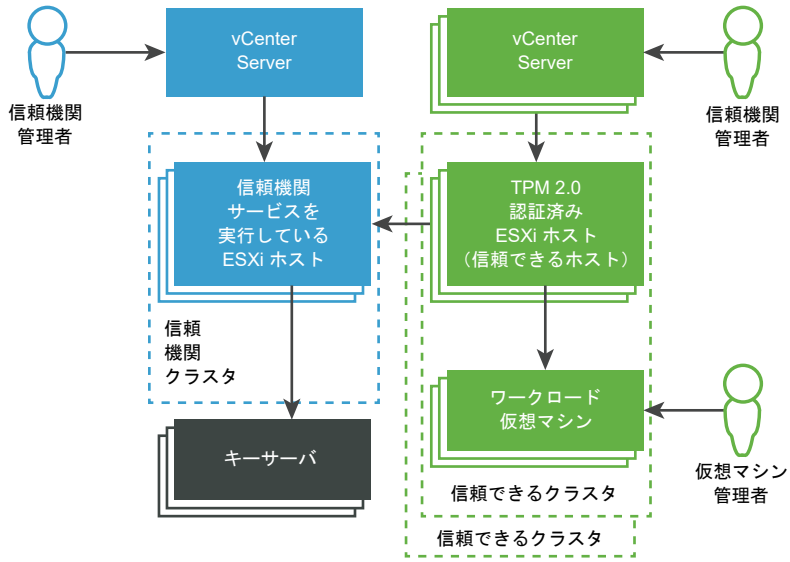
したがって、vSphere 信頼機関 では、次のような機能により、安全性が高いセキュアな環境でワークロードを実行できます。

- 改ざんの検出
- 権限のない変更の禁止
- マルウェアおよび変更の阻止
- 機密性の高いワークロードは、検証済みの安全なハードウェアおよびソフトウェア スタックでのみ実行されるように制限

vSphere 信頼機関 アーキテクチャ

次の図に、vSphere 信頼機関 アーキテクチャを簡略化して示します。

図 9-1. vSphere 信頼機関 アーキテクチャ



図の中の要素

1 vCenter Server システム

それぞれ別の vCenter Server システムが信頼機関クラスタと信頼済みクラスタを管理します。

2 信頼機関クラスタ

vSphere 信頼機関 コンポーネントが実行される ESXi ホストから構成されます。

3 キー サーバ

暗号化操作の実行時にキー プロバイダ サービスによって使用される暗号化キーを格納します。キー サーバは、vSphere 信頼機関 の外部にあります。

4 信頼済みクラスタ

TPM を使用してリモートで証明され、暗号化されたワークロードを実行する ESXi 信頼済みホストで構成されます。

5 信頼機関管理者

vCenter Server TrustedAdmins グループのメンバーである管理者。信頼済みインフラストラクチャを設定します。

vSphere 信頼機関 では、信頼機関管理者の指定方法に柔軟性が得られます。この図の信頼機関管理者は、それぞれ別のユーザーにすることができます。また、vCenter Server システム全体にリンクされた認証情報を使用して、信頼機関管理者を同じユーザーにすることも可能です。その場合は、同じユーザー、同じ TrustedAdmins グループになります。

6 仮想マシン管理者

信頼済みホスト上の暗号化されたワークロード仮想マシンを管理する権限が付与された管理者。

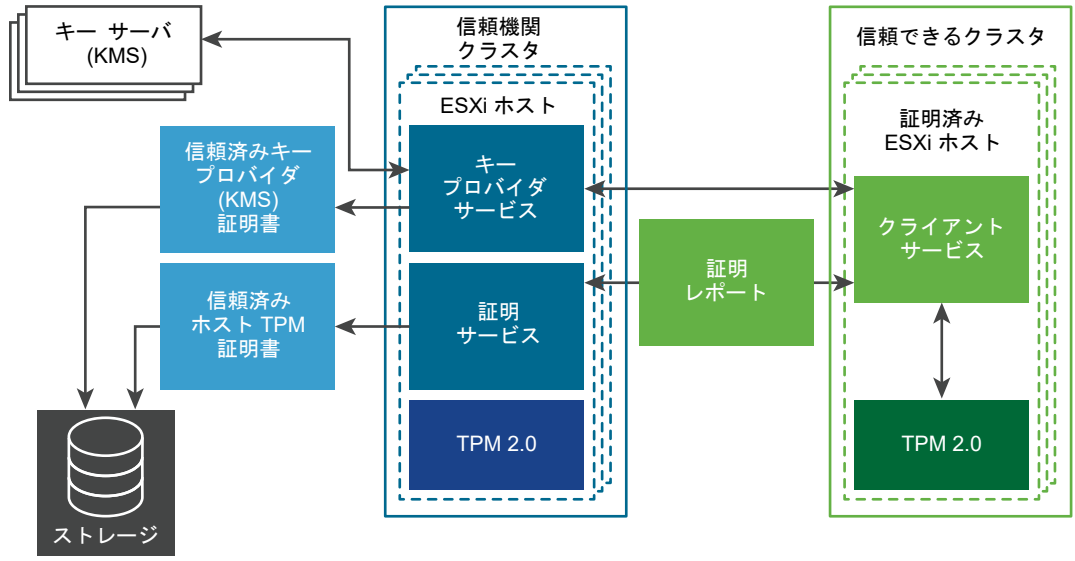
信頼済みインフラストラクチャの概要

vSphere 信頼機関 サービス、少なくとも 1 台の外部 KMIP 準拠のキー サーバ、vCenter Server システム、および ESXi ホストが信頼済みインフラストラクチャの機能を提供します。

信頼済みインフラストラクチャについて

信頼済みインフラストラクチャは、少なくとも 1 つの vSphere Trust Authority クラスタ、1 つ以上の信頼済みクラスタ、および少なくとも 1 台の外部 KMIP 準拠のキー サーバで構成されます。各クラスタには、次の図に示すように、特定の vSphere 信頼機関 サービスを実行する ESXi ホストが含まれています。

図 9-2. vSphere 信頼機関 サービス



Trust Authority クラスタを構成すると、次の 2 つのサービスが有効になります。

- 証明サービス
- キー プロバイダ サービス

vSphere 信頼機関 を構成すると、信頼済みクラスタ内の ESXi ホストは、証明サービスと通信します。キー プロバイダ サービスは、信頼済みホストと 1 つ以上の信頼済みキー プロバイダの間に介入します。

注： 現在、Trust Authority クラスタ内の ESXi ホストでは、TPM は必要ありません。ただし、ベスト プラクティスとして、TPM を使用して新しい ESXi ホストをインストールすることを検討してください。

vSphere 信頼機関 証明サービスについて

証明サービスは、信頼済みクラスタ内のリモート ESXi ホストのバイナリおよび構成状態を記述するアサーションを含む署名付きドキュメントを生成します。証明サービスは、Trusted Platform Module (TPM) 2.0 チップを使用して ESXi ホストの状態を証明し、ソフトウェアの測定およびレポート作成の基盤として使用します。リモート ESXi ホストでの TPM では、ソフトウェア スタックを測定し、構成データを証明サービスに送信します。証明サー

ビスは、ソフトウェア測定の署名を、以前に構成された認証済みの TPM 保証キー (EK) に関連付けられることを確認します。証明サービスによって、ソフトウェア測定が以前に付与された ESXi イメージのいずれかに一致することも確認されます。証明サービスでは、ESXi ホストに発行する JSON Web Token (JWT) に署名し、ESXi ホストの ID、有効性、および構成に関するアサーションを提供します。

vSphere 信頼機関 キー プロバイダ サービスについて

キー プロバイダ サービスによって、vCenter Server および ESXi ホストが直接キー サーバの認証情報を要求する必要がなくなります。vSphere 信頼機関 では、ESXi ホストが暗号化キーにアクセスできるように、キー プロバイダ サービスで認証する必要があります。

キー プロバイダ サービスをキー サーバに接続するには、Trust Authority 管理者が信頼設定を行う必要があります。ほとんどの KMIP 準拠サーバでは、信頼の構成には、クライアントおよびサーバ証明書の構成が含まれます。

キー プロバイダ サービスは、キーが ESXi 信頼済みホストのみにリリースされるようにキー サーバのゲートキーパーとして機能します。キー プロバイダ サービスでは、信頼済みキー プロバイダの概念を基に、他のデータセンターのソフトウェア スタックにはキー サーバの詳細を表示しません。信頼済みキー プロバイダはそれぞれが 1 つの設定済みプライマリ暗号化キーを持ち、1 台以上のキー サーバを参照します。キー プロバイダ サービスでは、いくつかの信頼済みキー プロバイダを設定できます。たとえば、組織内の部門ごとに個別の信頼済みキー プロバイダを割り当てることができます。信頼済みキー プロバイダはそれぞれ異なるプライマリ キーを使用しますが、同じバッキング キー サーバを参照できます。

信頼済みキー プロバイダを作成すると、キー プロバイダ サービスが ESXi 信頼済みホストからの要求を受け入れ、その信頼済みキー プロバイダに対して暗号化操作を実行できます。

ESXi 信頼済みホストが信頼済みキー プロバイダに対して操作を要求すると、キー プロバイダ サービスは、暗号化キーを取得する ESXi ホストが証明されていることを確認します。すべてのチェックが正常に終了すると、ESXi 信頼済みホストは、キー プロバイダ サービスから暗号化キーを受け取ります。

vSphere 信頼機関 で使用されるポート

vSphere 信頼機関 サービスは、ESXi ホストのリバース プロキシの背後にある接続を待機します。すべての通信は、ポート 443 で HTTPS を介して行われます。

vSphere 信頼機関 の信頼済みホストについて

ESXi 信頼済みホストは、信頼済みキー プロバイダを使用して暗号化操作を実行するように構成されます。ESXi 信頼済みホストは、キー プロバイダ サービスおよび証明サービスと通信することでキー操作を実行します。認証と認可では、ESXi 信頼済みホストは証明サービスから取得したトークンを使用します。有効なトークンを取得するには、信頼済み ESXi ホストが証明サービスを正常に証明する必要があります。このトークンには、ESXi 信頼済みホストが信頼済みキー プロバイダへのアクセスを許可されているかどうかを判断するために使用される特定の要求が含まれます。

vSphere 信頼機関 およびキー サーバ

vSphere 信頼機関 では、少なくとも 1 台のキー サーバを使用する必要があります。以前の vSphere リリースでは、キー サーバはキー管理サーバまたは KMS と呼ばれていました。現在、vSphere 仮想マシンの暗号化ソリューションは KMIP 1.1 準拠のキー サーバをサポートしています。

vSphere 信頼機関 の構成および状態情報の保存方法

vCenter Server は、主に vSphere 信頼機関 の構成および状態情報のためのパススルー サービスです。ほとんどの vSphere 信頼機関 の構成および状態の情報は、ConfigStore データベース内の ESXi ホストに保存されます。一部の状態情報は vCenter Server データベースにも格納されます。

注： ほとんどの vSphere 信頼機関 構成情報は ESXi ホストに格納されているため、vCenter Server のファイルベースのバックアップ メカニズムでは、この情報のバックアップが行われません。vSphere 信頼機関 デプロイの構成情報が保存されていることを確認するには、vSphere 信頼機関構成のバックアップを参照してください。

vSphere 信頼機関 と vCenter Server の統合方法

Trust Authority クラスタおよび信頼済みクラスタを管理するために、個別の vCenter Server インスタンスを構成します。vSphere 信頼機関 の設定を参照してください。

信頼済みクラスタでは、vCenter Server は Trust Authority API 呼び出しを管理し、それらを ESXi ホストに渡します。vCenter Server は、信頼済みクラスタ内のすべての ESXi ホストに API 呼び出しを複製します。

vSphere 信頼機関 を最初に構成した後、Trust Authority クラスタまたは信頼済みクラスタで ESXi ホストを追加または削除できます。vSphere 信頼機関 ホストの追加と削除を参照してください。

vSphere 信頼機関のプロセス フロー

vSphere 信頼機関 プロセス フローを理解することは、信頼済みインフラストラクチャを構成および管理する方法を学習するために不可欠です。

vSphere 信頼機関 の構成方法

デフォルトでは、vSphere 信頼機関 は有効になっていません。環境内の vSphere 信頼機関 を手動で設定する必要があります。vSphere 信頼機関 の設定を参照してください。

vSphere 信頼機関 を構成するときには、証明サービスが受け入れる ESXi ソフトウェアのバージョン、および信頼できる Trusted Platform Module (TPM) を指定する必要があります。

TPM と証明

このガイドでは、TPM と証明についての説明に次の定義を使用します。

表 9-2. TPM と証明の用語集

用語	定義
承認キー (EK)	TPM は、承認キー (EK) と呼ばれる RSA パブリック/プライベート キー ペアがハードウェアに組み込まれた状態で製造されています。EK は個々の TPM ごとに固有です。
EK パブリック キー	EK キー ペアのパブリック部分。
EK プライベート キー	EK キー ペアのプライベート部分。

表 9-2. TPM と証明の用語集 （続き）

用語	定義
EK 証明書	EK パブリック キーが署名付きでラップされています。EK 証明書は、認証局のプライベート キーを使用して EK パブリック キーに署名する TPM メーカーによって作成されます。すべての TPM に EK 証明書が含まれているわけではありません。その場合、EK パブリック キーは署名されていません。
TPM 証明	リモート ホストで実行されているソフトウェアを検証する証明サービスの機能。TPM 証明は、リモート ホストの起動時に TPM によって行われる暗号化測定を通じて行われ、要求に応じて証明サービスに渡されます。証明サービスは、EK パブリック キーまたは EK 証明書のいずれかを介して TPM 内の信頼を確立します。

信頼済みホストでの TPM 信頼の設定

ESXi 信頼済みホストには、TPM が含まれている必要があります。TPM は、承認キー (EK) と呼ばれるパブリック/プライベート キー ペアがハードウェアに組み込まれた状態で製造されています。TPM 2.0 では多くのキー/証明書ペアが許可されますが、最も一般的なものは RSA-2048 キー ペアです。TPM EK パブリック キーが CA によって署名されている場合、EK 証明書が得られます。通常、TPM の製造元は少なくとも 1 つの EK を事前に生成し、認証局を使用してパブリック キーに署名して、署名付きの証明書を TPM の不揮発性メモリに埋め込みます。

証明サービスは、次のように TPM を信頼するように設定できます。

- 製造元が TPM への署名に使用したすべての認証局証明書を信頼します（EK パブリック キー）。証明サービスのデフォルト設定では、認証局証明書を信頼します。この方法では、1 つの認証局証明書で多くの ESXi ホストに対応できるため、管理オーバーヘッドが軽減されます。
- ESXi ホストの TPM 認証局証明書と EK パブリック キーを信頼します。後者は、EK 証明書または EK パブリック キーのいずれかです。この方法ではセキュリティが強化されますが、各信頼済みホストに関する情報を設定する必要があります。
- 一部の TPM には EK 証明書が含まれていません。その場合は、EK パブリック キーを信頼します。

すべての TPM 認証局証明書を信頼するよう決定すると、運用面で利便性が向上します。新しい証明書は、新しいクラスのハードウェアをデータセンターに追加する場合にのみ設定します。個々の EK 証明書を信頼するようにすると、特定の ESXi ホストへのアクセスを制限できます。

TPM 認証局証明書を信頼しないよう決定することもできます。あまり発生しない状況ではありますが、この設定は EK が認証局によって署名されていない場合に使用できます。現在、この機能は全面的には実装されていません。

注： 一部の TPM には EK 証明書が含まれていません。ESXi ホストを個別に信頼するには、TPM に EK 証明書が含まれている必要があります。

TPM の証明

証明プロセスを開始するために、信頼済みクラスタ内の ESXi 信頼済みホストが事前設定済みの EK パブリック キーと EK 証明書を Trust Authority クラスタの証明サービスに送信します。証明サービスは、要求を受信すると設定内で EK を検索します。EK は、設定に応じて EK パブリック キーか EK 証明書、またはその両方です。有効なものが見つからない場合、証明サービスは証明の要求を拒否します。

EK は署名には直接使用されないため、認証キー（AK または AIK）がネゴシエートされます。ネゴシエーション プロトコルにより、新しく作成された AK が検証済みの EK にバインドされ、中間者攻撃やなりすましが確実に回避されます。ネゴシエートされた AK は将来の認証要求で再利用され、毎回 AK が生成されることはありません。

ESXi 信頼済みホストは、TPM から Quote と PCR の値を読み取ります。Quote は AK によって署名されています。ESXi 信頼済みホストは TCG イベント ログも読み取ります。これには、現在の PCR 状態をもたらしたすべてのイベントが含まれます。この TPM 情報は、検証のために証明サービスに送信されます。証明サービスはイベント ログを使用して PCR の値を確認します。

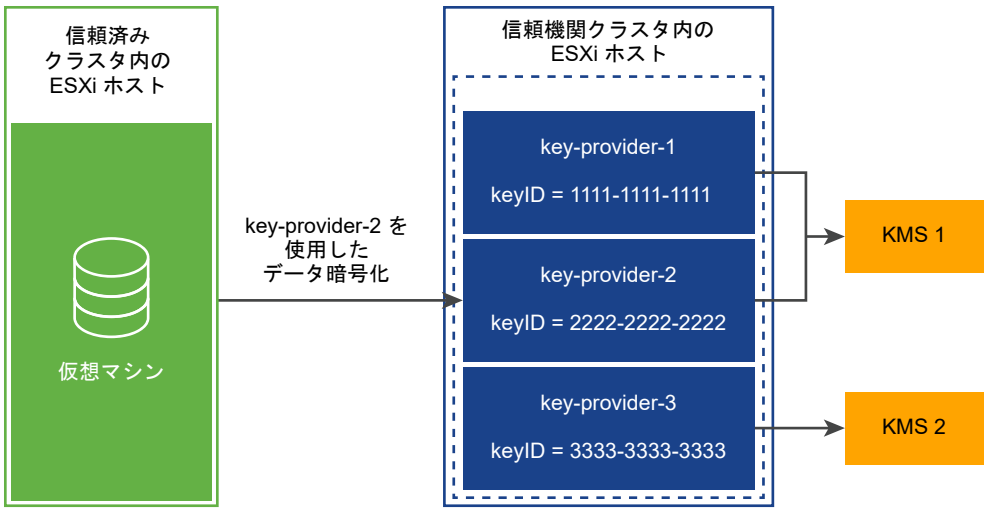
キー プロバイダとキー サーバの連携方法

キー プロバイダ サービスは、信頼済みキー プロバイダの考え方を使用して、データセンターの他のソフトウェアからキー サーバの詳細を隠蔽します。信頼済みキー プロバイダはそれぞれが 1 つの設定済みプライマリ暗号化キーを持ち、1 台以上のキー サーバを参照します。プライマリ暗号化キーは、キー サーバに置かれます。vSphere 信頼機関 の構成の一部として、プライマリ キーを別個のアクティビティとしてプロビジョニングし、有効にする必要があります。キー プロバイダ サービスでは、いくつかの信頼済みキー プロバイダを設定できます。信頼済みキー プロバイダはそれぞれ異なるプライマリ キーを使用しますが、同じバッキング キー サーバを参照できます。

新しい信頼済みキー プロバイダが追加された場合、信頼機関管理者は、キー サーバと、そのキー サーバ上の既存のキー識別子を指定する必要があります。

次の図に、キー プロバイダ サービスとキー サーバの関係を示します。

図 9-3. キー プロバイダとキー サーバ



信頼済みクラスタに対して信頼済みキー プロバイダを設定すると、キー プロバイダ サービスは、その信頼済みキー プロバイダに対して暗号化操作を実行する要求を受け入れることができます。たとえば、この図では、3 つの信頼済みキー プロバイダ（KMS-1 用として 2 つ、KMS-2 用として 1 つ）が設定されています。信頼済みホストは、キー プロバイダ 2 に対して暗号化操作を要求します。信頼済みホストは、暗号化キーが生成されて返されることを要求し、この暗号化キーを使用して暗号化操作を実行します。

キー プロバイダ サービスは、キー プロバイダ 2 が参照するプライマリ キーを使用して、指定されたプレーンテキスト データを暗号化し、対応する暗号テキストを返します。その後、信頼済みホストは、復号化操作に対して同じ暗号テキストを提供して、元のプレーンテキストを取得できます。

vSphere 信頼機関 の認証と認可

vSphere 信頼機関 管理操作には、TrustedAdmins グループのメンバーであるユーザーが必要です。信頼機関管理者の権限だけでは、ESXi ホストが関係するすべての管理操作を実行することはできません。詳細については、『vSphere 信頼機関の前提条件と必要な権限』を参照してください。

信頼済みクラスタへの信頼済みホストの追加

信頼済みクラスタに ESXi ホストを初めて追加するときの手順については、vSphere 信頼機関 の設定を参照してください。

その後、信頼済みクラスタに ESXi ホストを追加するときは、ワークフローが異なります。vSphere 信頼機関 ホストの追加と削除を参照してください。

信頼済みクラスタに ESXi ホストを初めて追加するときは、次の情報を収集する必要があります。

- クラスタ内の各ハードウェア タイプの TPM 証明書
- クラスタ内にある ESXi の各バージョンの ESXi イメージ
- vCenter Server のプリンシパル情報

信頼済みクラスタに後から ESXi ホストを追加するとき、いくつかの追加的な情報の収集が必要になることがあります。具体的には、新しい ESXi ホストのハードウェアまたは ESXi のバージョンが元のホストと異なる場合、新しい ESXi ホストの情報を収集して、それを信頼機関クラスタにインポートする必要があります。vCenter Server のプリンシパル情報は、vCenter Server システムごとに 1 回のみ収集する必要があります。

vSphere 信頼機関 のトポロジ

vSphere 信頼機関 では、信頼機関クラスタと信頼済みクラスタに別の vCenter Server システムが必要です。

信頼機関クラスタは、独立し、隔離されている vCenter Server で設定および管理されます。信頼機関クラスタの vCenter Server は、信頼済みクラスタの vCenter Server を兼ねることはできません。信頼済みクラスタには、切り離された独自の vCenter Server が必要です。1 つの vCenter Server で複数の信頼済みクラスタを管理できます。信頼済みクラスタの複数の vCenter Server システムが拡張リンク モードに参加することができます。信頼機関クラスタの vCenter Server は、他の信頼機関クラスタ vCenter Server システムまたは信頼済みクラスタ vCenter Server システムとともに拡張リンク モードに参加することはできません。

信頼機関管理者は、セキュリティ上の適切な隔離の手法として、信頼機関クラスタおよび関連する vCenter Server を他の vCenter Server インスタンスとは分離して管理します。

信頼機関管理者は、信頼済みクラスタ管理者がクラスタを構成するために使用するホスト名と SSL 証明書を文書化または公開します。また、信頼機関管理者は、組織とその部門、または個々の管理者のために信頼済みキー プロバイダをプロビジョニングします。

ワークロード管理者には ESXi ホストへの強力なアクセス権があるため、ワークロード vCenter Server によって管理されている信頼済みクラスタに vSphere 信頼機関 サービスを直接デプロイすることはできません。このタイプのデプロイでは、vSphere 信頼機関 のセキュリティ目標を満たすために必要なロールの分離が達成されません。

vSphere 信頼機関の前提条件と必要な権限

vSphere 信頼機関 を構成するときは、ハードウェアおよびソフトウェアの要件を考慮する必要があります。暗号化を使用するには、暗号化の権限とロールを設定する必要があります。vSphere 信頼機関 タスクを実行するユーザーには、適切な権限が与えられている必要があります。

vSphere 信頼機関 の要件

vSphere 信頼機関 を使用するには、vSphere 環境が以下の要件を満たす必要があります。

- ESXi 信頼済みホストのハードウェア要件
  - TPM 2.0
  - セキュア ブートを有効にしてあること
  - EFI ファームウェア
- コンポーネントの要件：
  - vCenter Server 7.0 以降
  - vSphere Trust Authority クラスタと ESXi ホスト専用の vCenter Server システム
  - 信頼済みクラスタと ESXi 信頼済みホストの個別の vCenter Server システム
  - キー サーバ（以前の vSphere リリースではキー管理サーバまたは KMS と呼ばれていました）
- 仮想マシンの要件：
  - EFI ファームウェア
  - セキュア ブートが有効になっていること

注： vSphere 信頼機関 の構成を開始する前に、Trust Authority クラスタと信頼済みクラスタ用に vCenter Server システムを設定し、各クラスタに ESXi ホストを追加していることを確認します。

暗号化の権限

vSphere 信頼機関 では、新しい暗号化権限は導入されません。暗号化の権限とロールに記載されているものと同じ暗号化権限が vSphere 信頼機関 に適用されます。

ホストの暗号化モード

vSphere 信頼機関 では、ESXi 信頼済みホストでホスト暗号化モードを有効にするための新しい要件は導入されません。ホスト暗号化モードの詳細については、暗号化タスクの前提条件と必要な権限を参照してください。

vSphere 信頼機関 ロールおよび TrustedAdmins グループについて

vSphere 信頼機関 操作には、TrustedAdmins グループのメンバーであるユーザーが必要です。このユーザーは、信頼機関管理者と呼ばれます。vSphere 管理者は、信頼済みインフラストラクチャ管理者ロールを取得するために、自分自身または他のユーザーを TrustedAdmins グループに追加する必要があります。vCenter Server 認証には、信頼済みインフラストラクチャ管理者ロールが必要です。信頼済みインフラストラクチャの一部である ESXi ホストでの認証には、TrustedAdmins グループが必要です。ESXi ホストで、Cryptographic

Operations.Register host 権限を持つユーザーは、信頼されたクラスターを管理できます。vCenter Server 権限は、信頼できるホストには伝達されず、信頼できるホストにのみ伝達されます。信頼できるホストでの権限が付与されるのは、TrustedAdmins グループのメンバーだけです。グループ メンバーシップは、ESXi ホスト本体で検証されます。

注： vSphere 管理者と管理者グループのメンバーには、信頼済みインフラストラクチャ管理者ロールが割り当てられますが、このロールだけではユーザーが vSphere 信頼機関 操作を実行することは許可されません。TrustedAdmins グループのメンバーシップも必要です。

vSphere 信頼機関 が有効になると、信頼機関管理者は信頼済みキー プロバイダを信頼済みホストに割り当てることができます。それにより、この信頼済みホストは信頼済みキー プロバイダを使用して暗号化タスクを実行できます。

vSphere 信頼機関 では、信頼済みインフラストラクチャ管理者ロールに加えて、vSphere 信頼機関 API を呼び出すための権限を除く vCenter Server 内のすべての権限を備えた、信頼なしインフラストラクチャ管理者ロールが提供されます。

vSphere 信頼機関 のグループ、ロール、およびユーザーは、次のように機能します。

- 最初の起動時に、vSphere から TrustedAdmins グループに対して、グローバル権限を持つ信頼済みインフラストラクチャ管理者ロールが付与されます。
- 信頼済みインフラストラクチャ管理者ロールは、vSphere 信頼機関 API (`TrustedAdmin.*`) を呼び出すために必要な権限と、インベントリ オブジェクトを表示するための System.Read、System.View、System.Anonymous の各システム権限を備えたシステム ロールです。
- 信頼なしインフラストラクチャ管理者ロールは、vSphere 信頼機関 API を呼び出すための権限を除く vCenter Server 内のすべての権限を備えたシステム ロールです。新しい権限を vCenter Server に追加すると、その権限は信頼なしインフラストラクチャ管理者ロールにも追加されます（信頼なしインフラストラクチャ管理者ロールは、非暗号化管理者ロールに似ています）。
- vSphere 信頼機関 権限 (`TrustedAdmin.*` API) は非暗号化管理者ロールに含まれていないため、このロールを持つユーザーは信頼済みインフラストラクチャを設定したり暗号化操作を実行したりすることができません。

次の表に、これらのユーザー、グループ、およびロールの使用事例を示します。

表 9-3. vSphere 信頼機関のユーザー、グループ、およびロール

ユーザー、グループ、またはロール	vSphere 信頼機関 vCenter Server API を呼び出し可能（vSphere 信頼機関 ESXi API の呼び出しを含む）	vSphere 信頼機関 vCenter Server API を呼び出し可能（vSphere 信頼機関 ESXi API の呼び出しを含まない）	vSphere 信頼機関 に関連しないクラスタでホスト操作を実行可能	コメント
Administrators@*system.domain* グループと TrustedAdmins@*system.domain* グループの両方に属するユーザー	はい	はい	はい	なし
TrustedAdmins@*system.domain* グループのみに属するユーザー	はい	はい	なし	このようなユーザーは、通常のクラスタ管理操作を実行できません。

表 9-3. vSphere 信頼機関のユーザー、グループ、およびロール （続き）

ユーザー、グループ、またはロール	vSphere 信頼機関 vCenter Server API を呼び出し可能（vSphere 信頼機関 ESXi API の呼び出しを含む）	vSphere 信頼機関 vCenter Server API を呼び出し可能（vSphere 信頼機関 ESXi API の呼び出しを含まない）	vSphere 信頼機関 に関連しないクラスタでホスト操作を実行可能	コメント
Administrators@*system.domain* グループのみに属するユーザー	はい	なし	はい	なし
信頼済みインフラストラクチャ管理者ロールを持ち、TrustedAdmins@*system.domain* グループには属さないユーザー	はい	なし	なし	ESXi ホストは、権限を付与するユーザーのグループ メンバーシップを確認します。
信頼なしインフラストラクチャ管理者ロールのみを持つユーザー	なし	なし	はい	このようなユーザーは、vSphere 信頼機関 の操作を実行できない管理者とほぼ同等です。

vSphere 信頼機関 のベスト プラクティス、注意事項、相互運用性

vSphere 信頼機関 のアーキテクチャからは、いくつかの追加的な推奨事項が発生します。vSphere 信頼機関 の利用を検討する際には、相互運用性の制約を考慮してください。

信頼済みインフラストラクチャの相互運用性

ESXi のバージョンについては、証明サービスは下位および上位互換性があります。たとえば、ESXi 7.0 を実行している ESXi ホストのクラスタを vSphere 信頼機関クラスタ内に保持しながら、信頼済みクラスタ内の ESXi ホストにアップグレードまたはパッチを適用して新しい ESXi バージョンにすることができます。同様に、信頼済みクラスタ内の ESXi ホストは現在のバージョンに維持したまま、信頼機関クラスタ内の ESXi ホストにアップグレードまたはパッチを適用できます。

1 つのクラスタが信頼機関クラスタと信頼済みクラスタの両方として機能することはできません。そのような設定はサポートされていません。

信頼済みクラスタ設定の制限

ワークロード vCenter Server ごとに信頼済みクラスタを 1 つのみ構成できます。信頼済みクラスタが複数の信頼機関クラスタを参照するように構成することはできません。

サポートされている機能

vSphere 信頼機関 は、以下をサポートします。

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS

- DPM
- SRM。以下のことに注意が必要です。
  - リカバリ側で同じ vSphere 信頼機関 サービス構成が使用可能な場合は、アレイ ベースのレプリケーションを伴う SRM がサポートされます。
  - SPPG
- VADP
  - サポートは、標準の暗号化の場合と同じです。ホットアド モードと NFC モードはサポートされますが、SAN モードはサポートされません。バックアップは復号化されます。VADP パートナーには、元の仮想マシンと同じ暗号化キーを使用して、バックアップした仮想マシンをリカバリするオプションがあります。
- vSAN
  - 仮想マシンの暗号化は、vSAN 上で全面的にサポートされます。
- OVF
  - 暗号化された仮想マシンを OVF にエクスポートすることはできません。ただし、OVF からインポートするときに仮想マシンを暗号化することはできます。
- vVol

サポートされていない機能

現在、vSphere 信頼機関 は以下をサポートしていません。

- vSAN 暗号化
- 最初のクラス ディスク (FCD) 暗号化
- vSphere Replication
- vSphere ホスト プロファイル

vSphere Trust Authority のライフサイクル

vSphere 信頼機関 サービスは、基本 ESXi イメージの一部としてパッケージ化され、インストールされます。

サービスの開始と停止

vSphere Client で、ESXi ホスト上で実行されている vSphere 信頼機関 サービスを開始、停止、および再起動できます。構成の変更時や、機能またはパフォーマンス上の問題が疑われる場合に、サービスを再起動できます。ESXi 信頼済みホストでサービスを再起動するには、ホスト自体にログインしてサービスを再起動する必要があります。vSphere 信頼機関 サービスの開始、停止、および再起動を参照してください。

アップグレードとパッチ適用

ESXi 信頼済みホストのアップグレードまたはパッチ適用を行う際は、新しい ESXi バージョン情報を使用して vSphere 信頼機関 クラスタを更新する必要があります。そのための 1 つの方法は、テスト用の ESXi ホストのアップグレードまたはパッチ適用を行い、ESXi 基本イメージ情報をエクスポートして Trust Authority クラスタにイメージ ファイルをインポートしてから、ESXi 信頼済みホストのアップグレードまたはパッチ適用を行うというものです。

アップグレードのベスト プラクティス

vSphere 信頼機関 インフラストラクチャをアップグレードするときのベスト プラクティスは、最初に信頼機関 vCenter Server と信頼機関ホストをアップグレードすることです。これにより、vSphere 信頼機関 の最新の機能を最大限に活用できるようになります。ただし、ビジネスの要件に合わせて、vCenter Server と ESXi ホストを個別にスタンドアローンでアップグレードすることもできます。

vSphere 信頼機関 インフラストラクチャをアップグレードする場合は、原則として次の順序に従います。

1 信頼機関クラスタの vCenter Server をアップグレードします。

2 信頼機関ホストをアップグレードします。

3 信頼済みクラスタの vCenter Server をアップグレードします。

4 信頼済みホストをアップグレードします。

プロセスをスムーズに進行するには、信頼機関ホストと信頼済みホストを 1 台ずつ段階的にアップグレードします。

アップグレードの問題についてのトラブルシューティング

信頼機関ホストのアップグレードに失敗した場合は、次の手順を実行します。

1 信頼済みクラスタから信頼機関ホストを削除します。

2 ESXi を以前のバージョンに戻します。

3 https://kb.vmware.com/s/article/77234 にある VMware ナレッジベースの記事で説明されているとおりに、信頼機関ホストをクラスタに再追加します。

4 信頼機関ホストの構成と、信頼機関クラスタ内の他の信頼機関ホストとの間に整合性があることを確認します。信頼済みクラスタの健全性の確認を参照してください。

信頼済みホストの ESXi を新しいバージョンにアップグレードすると、新しい ESXi 基本イメージ情報で信頼機関クラスタを更新するまでの間、証明は失敗します。これは想定どおりの動作です。この問題を修正するまで、仮想マシンを暗号化することや、アップグレード前に暗号化した既存の仮想マシンを使用することはできません。証明のエラー メッセージが vSphere Client の [最近のタスク] ペイン、および `attestd.log`、`kmxa.log`、`vpxd.log` の各ファイルに出力されます。

この問題を修正するには、次の手順に従います。

1 `Export-VMHostImageDb` コマンドレットを実行して、ESXi 基本イメージを再エクスポートします。信頼する ESXi ホストおよび vCenter Server に関する情報の収集の手順 5 を参照してください。

2 `New-TrustAuthorityVMHostBaseImage` コマンドレットを実行して、新しい基本イメージを信頼機関クラスタの vCenter Server に再インポートします。信頼機関クラスタへの信頼済みホストの情報のインポートの手順 8 を参照してください。

3 以前のバージョンの ESXi を証明する必要がなくなった（すべての信頼済みホストがアップグレードされた）場合は、Remove-TrustAuthorityVMHostBaseImage コマンドレットを実行してそのバージョンを削除します。例：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

vSphere 信頼機関 構成のバックアップ

ほとんどの vSphere 信頼機関 構成情報は ESXi ホストに格納されているため、vCenter Server バックアップではこの vSphere 信頼機関 情報のバックアップは行われません。vSphere 信頼機関構成のバックアップを参照してください。

vSphere 信頼機関 の設定

デフォルトでは、vSphere 信頼機関 は有効になっていません。vSphere 信頼機関 の使用を開始する前に、環境を構成する必要があります。

vSphere 信頼機関 クラスタと呼ばれる専用の vCenter Server クラスタで vSphere 信頼機関 サービスを有効にします。信頼機関クラスタは、一元化されたセキュアな管理プラットフォームとして機能します。次に、信頼済みクラスタとして vCenter Server ワークロード クラスタを有効にします。信頼済みクラスタには、ESXi 信頼済みホストなどがあります。

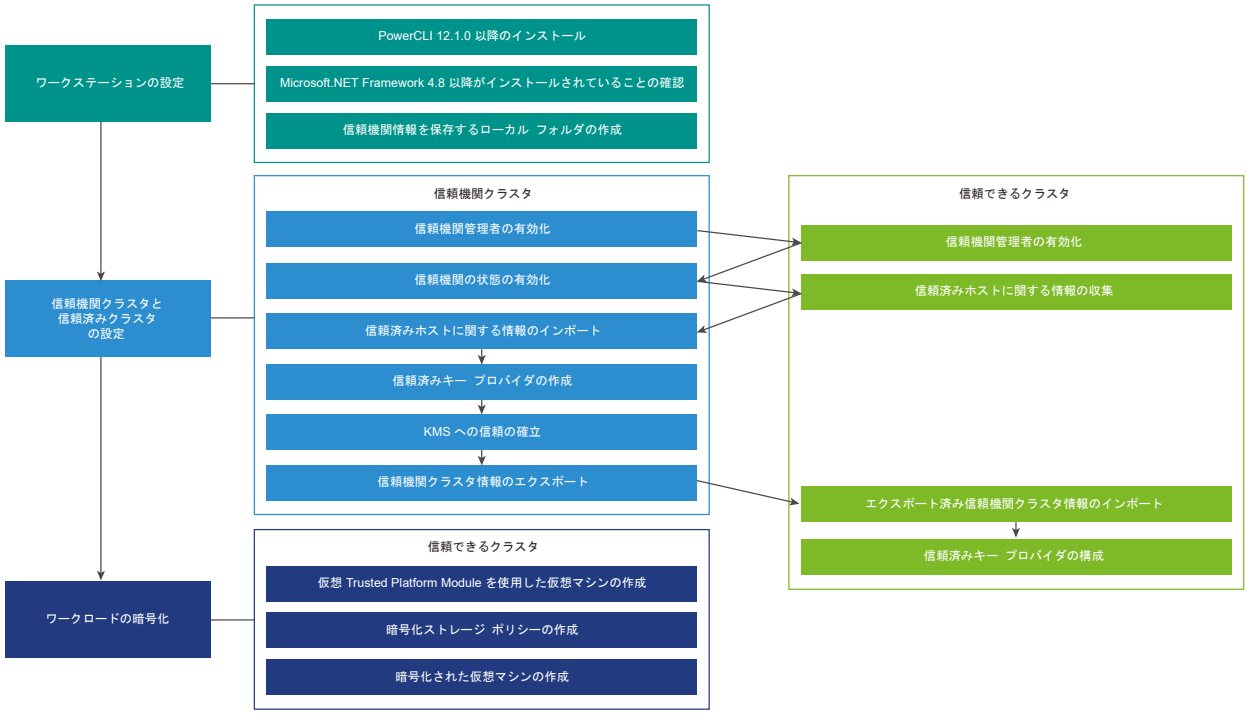
信頼機関クラスタは、信頼済みクラスタ内の ESXi ホストをリモートで証明します。信頼機関クラスタは、信頼済みクラスタ内の証明された ESXi ホストにのみ暗号化キーをリリースし、信頼済みキー プロバイダを使用して仮想マシンと仮想ディスクを暗号化します。

vSphere 信頼機関 の設定を開始する前に、vCenter Server システムと ESXi ホストに必要なセットアップの詳細について vSphere 信頼機関の前提条件と必要な権限を参照してください。

vSphere 信頼機関 のさまざまな側面は、次の方法で管理します。

- PowerCLI コマンドレットまたは vSphere API を使用して、vSphere 信頼機関 サービスおよび信頼できる接続を設定します。『VMware PowerCLI コマンドレット リファレンス』および『vSphere Automation SDK プログラミング ガイド』を参照してください。
- PowerCLI コマンドレットまたは vSphere Client を使用して、信頼済みキー プロバイダの設定を管理します。
- vSphere Client と API を使用して、以前の vSphere リリースと同様に暗号化ワークフローを実行します。

図 9-4. vSphere Trust Authority のワークフロー



vSphere 信頼機関 を構成および管理するには、VMware PowerCLI を使用しますが、一部の機能は vSphere Client で使用可能です。

vSphere 信頼機関 を設定する場合は、信頼機関クラスタと信頼済みクラスタの両方でセットアップ タスクを完了する必要があります。これらのタスクの一部は、順序が決まっています。このガイドで説明されているタスクの順序を使用します。

注： 最初の vSphere 信頼機関 セットアップの完了後に信頼済みクラスタに ESXi ホストを追加するときに、信頼済みホストの情報を再度エクスポートしてインポートしなければならない場合があります。つまり、新しい ESXi ホストが元のホストと異なる場合は、新しい ESXi ホストの情報を収集して、それを信頼機関クラスタにインポートする必要があります。vSphere 信頼機関 ホストの追加と削除を参照してください。

手順

1 ワークステーションの設定

vSphere 信頼機関 のデプロイを構成するには、まず必要なソフトウェアとセットアップを備えたワークステーションを準備する必要があります。

2 信頼機関管理者の有効化

vSphere 信頼機関 を有効にするには、ユーザーを vSphere TrustedAdmins グループに追加する必要があります。このユーザーは、信頼機関管理者になります。ほとんどの vSphere 信頼機関 設定タスクでは、信頼機関の管理者を使用します。

3 信頼機関の状態の有効化

vCenter Server クラスタを vSphere 信頼機関 クラスタにする（信頼機関の状態を有効にする）と、必要な信頼機関サービスがクラスタ内の ESXi ホストで開始されます。

4 信頼する ESXi ホストおよび vCenter Server に関する情報の収集

信頼を確立するには、vSphere 信頼機関クラスタは信頼済みクラスタの ESXi ホストおよび vCenter Server に関する情報を必要とします。この情報をファイルとしてエクスポートし、信頼機関クラスタにインポートします。これらのファイルは、その機密を確実に保持し、安全な状態で転送してください。

5 信頼機関クラスタへの信頼済みホストの情報のインポート

信頼機関クラスタが証明できるホストを把握できるように、エクスポートされた ESXi ホストおよび vCenter Server の情報を vSphere 信頼機関 クラスタにインポートします。

6 信頼機関クラスタでのキー プロバイダの作成

キー プロバイダ サービスをキー プロバイダに接続するには、信頼済みキー プロバイダを作成してから、vSphere 信頼機関 クラスタとキー サーバ (KMS) の間に信頼関係を設定する必要があります。KMIP 準拠のほとんどのキー サーバでは、この設定にはクライアント証明書とサーバ証明書の設定が含まれます。

7 信頼機関クラスタ情報のエクスポート

信頼済みクラスタを vSphere 信頼機関 クラスタに接続するには、信頼機関クラスタのサービス情報をファイル形式でエクスポートしてから、そのファイルを信頼済みクラスタにインポートする必要があります。このファイルは、機密を確実に保持し、安全な状態で転送してください。

8 信頼済みホストへの信頼機関クラスタ情報のインポート

vSphere 信頼機関 クラスタの情報を信頼済みクラスタにインポートすると、信頼済みホストは信頼機関クラスタを使用して証明プロセスを開始します。

9 vSphere Client を使用した信頼済みホストの信頼済みキー プロバイダの構成

vSphere Client を使用して、信頼済みキー プロバイダを構成できます。

10 コマンドラインを使用した信頼済みホストの信頼済みキー プロバイダの構成

コマンドラインを使用して、信頼済みキー プロバイダを構成できます。vCenter Server、または vCenter Server オブジェクト階層のクラスタまたはフォルダ レベルで、デフォルトの信頼済みキー プロバイダを構成できます。

ワークステーションの設定

vSphere 信頼機関 のデプロイを構成するには、まず必要なソフトウェアとセットアップを備えたワークステーションを準備する必要があります。

vSphere 信頼機関 環境へのアクセスがあるワークステーションで、以下の手順を実行します。

手順

1 PowerCLI 12.1.0 以降をインストールします。『PowerCLI User's Guide』を参照してください。

2 Microsoft .NET Framework 4.8 以降がインストールされていることを確認します。

3 ファイルとしてエクスポートする信頼機関の情報が保存されるローカル フォルダを作成します。

次のステップ

この後は信頼機関管理者の有効化に続きます。

信頼機関管理者の有効化

vSphere 信頼機関 を有効にするには、ユーザーを vSphere TrustedAdmins グループに追加する必要があります。このユーザーは、信頼機関管理者になります。ほとんどの vSphere 信頼機関 設定タスクでは、信頼機関の管理者を使用します。

信頼機関管理者には、vCenter Server 管理者とは別のユーザーを使用してください。それぞれに別のユーザーを使用することで、環境のセキュリティを強化できます。信頼機関の管理者は、信頼機関クラスタと信頼できるクラスタの両方に対して有効する必要があります。

前提条件

信頼機関の管理者となるユーザーを作成するか、この管理者となる既存ユーザーを識別します。

手順

1 vSphere Client を使用して、信頼機関クラスタの vCenter Server に接続します。

2 管理者としてログインします。

3 [ホーム] メニューから [管理] を選択します。

4 [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

5 [グループ] をクリックし、[TrustedAdmins] グループをクリックします。

   TrustedAdmins グループが最初に表示されない場合は、[フィルタ] アイコンを使用してフィルタするか、ペインの下部にある右矢印をクリックしてグループ内を移動します。

6 [グループ メンバー] 領域で、[メンバーの追加] をクリックします。

   ローカルな ID ソース（デフォルトは vsphere.local、ただしインストール中に別のドメインを選択した可能性がある）が選択されていることを確認し、信頼機関の管理者としてグループに追加するメンバー（ユーザー）を検索します。

7 メンバーを選択します。

8 [保存] をクリックします。

9 信頼済みクラスタの vCenter Server について、手順 1 から 8 を繰り返します。

次のステップ

この後は信頼機関の状態の有効化に続きます。

信頼機関の状態の有効化

vCenter Server クラスタを vSphere 信頼機関 クラスタにする（信頼機関の状態を有効にする）と、必要な信頼機関サービスがクラスタ内の ESXi ホストで開始されます。

前提条件

- 信頼機関管理者の有効化。

手順

1 PowerCLI セッションで `Connect-VIServer` コマンドレットを実行し、信頼機関の管理者ユーザーとして信頼機関クラスタの vCenter Server に接続します。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'パスワード'
```

2 クラスタの現在の状態を確認するには、`Get-TrustAuthorityCluster` コマンドレットを実行します。

たとえば、次のコマンドは、クラスタ `vTA Cluster` を表示し、このクラスタが無効になっていることを示します。

```
Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
```

出力では、検出された各クラスタの [状態] 列に [無効] または [有効] が表示されます。[無効] は、信頼機関サービスが実行されていないことを意味します。

3 信頼機関クラスタを有効にするには、`Set-TrustAuthorityCluster` コマンドレットを実行します。

たとえば、次のコマンドは、クラスタ `vTA Cluster` を有効にします。

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

システムは確認プロンプトによって応答します。

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

4 確認プロンプトに対して Enter キーを押します（デフォルトは **`Y`** です）。

出力にはクラスタの状態が表示されます。たとえば、次の例は、クラスタ `vTA Cluster` が有効になっていることを示しています。

```
Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

結果

信頼機関クラスタ内の ESXi ホストで、2 つのサービス（証明サービスおよびキー プロバイダ サービス）が開始されます。

例： 信頼機関クラスタで信頼済み状態を有効にする

この例では、PowerCLI を使用して信頼機関クラスタでサービスを有効にする方法を示します。次の表に、使用されるコンポーネントと値の例を示します。

表 9-4. vSphere 信頼機関セットアップの例

コンポーネント	値
信頼機関クラスタの vCenter Server	192.168.210.22
信頼機関クラスタ名	vTA クラスタ
信頼機関管理者	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

次のステップ

この後は信頼する ESXi ホストおよび vCenter Server に関する情報の収集に続きます。

信頼する ESXi ホストおよび vCenter Server に関する情報の収集

信頼を確立するには、vSphere 信頼機関クラスタは信頼済みクラスタの ESXi ホストおよび vCenter Server に関する情報を必要とします。この情報をファイルとしてエクスポートし、信頼機関クラスタにインポートします。これらのファイルは、その機密を確実に保持し、安全な状態で転送してください。

信頼するソフトウェアとハードウェアを把握するために vSphere 信頼機関 PowerCLI コマンドレットを使用して、信頼機関クラスタの信頼済みクラスタの ESXi ホストから次の情報をファイルとしてエクスポートします。

- ESXi のバージョン
- TPM のメーカー（CA 証明書）

- （オプション）個々の TPM（EK 証明書）

注： エクスポートされたこれらのファイルは、vSphere 信頼機関構成をリストアする必要が発生した場合に備えて安全な場所に保管します。

タイプとベンダーが同一で、かつ同じ時間枠と場所で製造された複数のホストについては、1 つの TPM の CA 証明書を取得するだけですべての TPM を信頼できることがあります。TPM を個別に信頼するには、その TPM の EK 証明書を取得します。

また、信頼済みクラスタの vCenter Server からプリンシパル情報を取得する必要があります。プリンシパル情報には、vpxd ソリューション ユーザーとその証明書チェーンが含まれています。プリンシパル情報を使用すると、信頼済みクラスタの vCenter Server は、信頼機関クラスタで設定されている利用可能な信頼済みキー プロバイダを検出できるようになります。

vSphere 信頼機関を最初に設定するときは、ESXi のバージョンと TPM 情報を収集する必要があります。また、パッチをアップグレードまたは適用する場合を含め、ESXi の新しいバージョンを展開するたびに ESXi のバージョンを収集する必要があります。

vCenter Server のプリンシパル情報は、vCenter Server システムごとに 1 回のみ収集されます。

前提条件

- 信頼済みクラスタ内にある ESXi のバージョンおよび TPM ハードウェアのタイプを特定し、すべての TPM ハードウェア タイプ、特定のホストのみ、個々のホストのいずれを信頼するかを指定します。
- PowerCLI cmdlet を実行するマシンで、ファイルとしてエクスポートした情報を保存するローカル フォルダを作成します。
- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。

手順

1 PowerCLI セッションで以下のコマンドを実行して、現在の接続を切断し、信頼済みクラスタ内の ESXi ホストの 1 台に root ユーザーとして接続します。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

2 `Get-VMHost` コマンドレットを実行して、ESXi ホストを確認します。

```
Get-VMHost
```

ホスト情報が表示されます。

3 `Get-VMHost` を変数に割り当てます。

例：

```
$vmhost = Get-VMHost
```

4 `Export-Tpm2CACertificate` コマンドレットを実行して、特定の TPM メーカーの CA 証明書をエクスポートします。

a `Get-Tpm2EndorsementKey -VMHost $vmhost` を変数に割り当てます。

たとえば、このコマンドは、`Get-Tpm2EndorsementKey -VMHost $vmhost` を変数 `$tpm2` に割り当てます。

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

b `Export-Tpm2CACertificate` コマンドレットを実行します。

たとえば、このコマンドは、TPM 証明書を `cacert.zip` ファイルにエクスポートします。このコマンドを実行する前に、宛先ディレクトリが存在することを確認します。

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

ファイルが作成されます。

c 信頼するクラスタ内の各 TPM ハードウェア タイプに対して繰り返します。TMP ハードウェアタイプごとに異なるファイル名を使用して、以前にエクスポートしたファイルを上書きしないようにします。

5 `Export-VMHostImageDb` コマンドレットを実行して、ESXi ホストのソフトウェアの説明（ESXi イメージ）をエクスポートします。

たとえば、このコマンドは、情報を `image.tgz` ファイルにエクスポートします。このコマンドを実行する前に、宛先ディレクトリが存在することを確認します。

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

注： `Export-VMHostImageDb` コマンドレットは、信頼済みクラスタの vCenter Server にログインする場合にも機能します。

ファイルが作成されます。

信頼するクラスタ内の各 ESXi バージョンに対して繰り返します。バージョンごとに異なるファイル名を使用して、以前にエクスポートしたファイルを上書きしないようにします。

6 信頼済みクラスタの vCenter Server プリンシパル情報をエクスポートします。

a ESXi ホストとの接続を切断します。

```
Disconnect-VIServer -server * -Confirm:$false
```

b 信頼機関の管理者ユーザーを使用して、信頼済みクラスタの vCenter Server に接続します。(または、管理者権限を持つユーザーを使用することもできます。)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c 信頼済みクラスタの vCenter Server プリンシパル情報をエクスポートするには、`Export-TrustedPrincipal` コマンドレットを実行します。

たとえば、このコマンドは、`principal.json` ファイルに情報をエクスポートします。このコマンドを実行する前に、宛先ディレクトリが存在することを確認します。

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

ファイルが作成されます。

7 (オプション) ホストを個別に信頼するには、TPM EK パブリック キー証明書をエクスポートする必要があります。

TPM 承認キー証明書のエクスポートとインポートを参照してください。

結果

次のファイルが作成されます。

- TPM CA 証明書ファイル (.zip ファイル拡張子)
- ESXi イメージ ファイル (.tgz ファイル拡張子)
- vCenter Server プリンシパル ファイル (.json ファイル拡張子)

例: 信頼する ESXi ホストおよび vCenter Server に関する情報の収集

この例では、PowerCLI を使用して信頼済みクラスタから ESXi ホスト情報および vCenter Server プリンシパルをエクスポートする方法を示します。次の表に、使用されるコンポーネントと値の例を示します。

表 9-5. vSphere 信頼機関セットアップの例

コンポーネント	値
信頼済みクラスタ内の ESXi ホスト	192.168.110.51
信頼済みクラスタの vCenter Server	192.168.110.22
変数 `$vmhost`	`Get-VMHost`
変数 `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`

表 9-5. vSphere 信頼機関セットアップの例 （続き）

コンポーネント	値
信頼機関管理者	trustedadmin@vsphere.local
出力ファイルを格納するローカル ディレクトリ	C:\vta

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576
1.614         7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

次のステップ

この後は信頼機関クラスタへの信頼済みホストの情報のインポートに続きます。

TPM 承認キー証明書のエクスポートとインポート

ESXi ホストから TPM 承認キー (EK) 証明書をエクスポートして、vSphere 信頼機関 クラスタにインポートできます。この操作は、信頼済みクラスタ内の個々の ESXi ホストを信頼する必要がある場合に行います。

TPM EK 証明書を信頼機関クラスタにインポートするには、信頼機関クラスタのデフォルトの証明タイプを、EK 証明書を受け入れるように変更する必要があります。デフォルトの証明タイプは、TPM 認証局 (CA) 証明書を受け入れます。一部の TPM には EK 証明書が含まれていません。ESXi ホストを個別に信頼するには、TPM に EK 証明書が含まれている必要があります。

注： エクスポートされた EK 証明書ファイルは、vSphere 信頼機関 構成をリストアする必要が発生した場合に備えて安全な場所に保管します。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。

手順

1 信頼機関クラスタの vCenter Server に信頼機関の管理者として接続していることを確認します。

たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション） 必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'パスワード'
```

3 信頼機関クラスタの証明タイプを変更するには、次の操作を行います。

a この vCenter Server によって管理されているクラスタを表示するは、`Get-TrustAuthorityCluster` コマンドレットを実行します。

```
Get-TrustAuthorityCluster
```

クラスタが表示されます。

b `Get-TrustAuthorityCluster` 情報を変数に割り当てます。

たとえば、次のコマンドは、`vTA Cluster` という名前のクラスタを変数 `$vTA` に割り当てます。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

c `Get-TrustAuthorityTpm2AttestationSettings` 情報を変数に割り当てます。

たとえば、次のコマンドは情報を変数 `$tpm2Settings` を割り当てます。

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d `Set-TrustAuthorityTpm2AttestationSettings` コマンドレットを実行して、`RequireEndorsementKey`、`RequireCertificateValidation`、または両方を指定します。

たとえば、次のコマンドは `RequireEndorsementKey` を指定します。

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

システムは、次のような確認メッセージで応答します。

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e 確認プロンプトに対して Enter キーを押します（デフォルトは **Y** です）。

出力には、指定された設定のステータスが True と表示されます。たとえば、このステータスは、True for Require Endorsement Key の場合は True、Require Certificate Validation の場合は False と表示されます。

```
Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 TPM EK 証明書をエクスポートするには、次の操作を行います。

a 信頼機関クラスタの vCenter Server から切断します。

```
Disconnect-VIServer -server * -Confirm:$false
```

b `Connect-VIServer` コマンドレットを実行して、信頼済みクラスタ内の ESXi ホストの 1 台に root ユーザーとして接続します。

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c `Get-VMHost` コマンドレットを実行して、ESXi ホストを確認します。

```
Get-VMHost
```

ホスト情報が表示されます。

d Get-VMHost を変数に割り当てます。

例：

```
$vmhost = Get-VMHost
```

e Export-Tpm2EndorsementKey コマンドレットを実行して、ESXi ホストの EK 証明書をエクスポートします。

たとえば、次のコマンドは、EK 証明書を tpm2ek.json ファイルにエクスポートします。

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

ファイルが作成されます。

5 TPM EK をインポートするには、次の操作を実行します。

a 信頼済みクラスタ内の ESXi ホストから切断します。

```
Disconnect-VIServer -server * -Confirm:$false
```

b 信頼機関の管理者ユーザーを使用して、信頼機関クラスタの vCenter Server に接続します。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'パスワード'
```

c Get-TrustAuthorityCluster コマンドレットを実行します。

```
Get-TrustAuthorityCluster
```

信頼機関クラスタ内のクラスタが表示されます。

d 変数に Get-TrustAuthorityCluster '*cluster*' を割り当てます。

たとえば、次のコマンドは変数 $vTA にクラスタ vTA Cluster の情報を割り当てます。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

e New-TrustAuthorityTpm2EndorsementKey コマンドレットを実行します。

たとえば、次のコマンドは、手順 4 で以前にエクスポートした tpm2ek.json ファイルを使用します。

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json
```

インポートされた承認キーの情報が表示されます。

結果

信頼機関クラスタの証明タイプが、EK 証明書を受け入れるように変更されます。EK 証明書が信頼済みクラスタからエクスポートされ、信頼機関クラスタにインポートされます。

例： TPM EK 証明書のエクスポートとインポート

この例では、PowerCLI を使用して信頼機関クラスタのデフォルトの証明タイプを変更し、EK 証明書を受け入れ、信頼済みクラスタの ESXi ホストから TPM EK 証明書をエクスポートして、信頼機関クラスタにインポートする方法を示します。次の表に、使用されるコンポーネントと値の例を示します。

表 9-6. vSphere 信頼機関 セットアップの例

コンポーネント	値
信頼機関クラスタの vCenter Server	192.168.210.22
変数 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
変数 `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
変数 `$vmhost`	`Get-VMHost`
信頼済みクラスタ内の ESXi ホスト	192.168.110.51
信頼機関管理者	trustedadmin@vsphere.local
出力ファイルを格納するローカル ディレクトリ	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
```

```
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB   MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------
-------------   ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster ‘vTA Cluster’
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json

TrustAuthorityClusterId                 Name                                    Health
-----------------------                 ----                                    ------
TrustAuthorityCluster-domain-c8         1a520e42-4db8-1cbb-6dd7-f493fd921ccb    Ok
```

次のステップ

この後は信頼機関クラスタへの信頼済みホストの情報のインポートに続きます。

信頼機関クラスタへの信頼済みホストの情報のインポート

信頼機関クラスタが証明できるホストを把握できるように、エクスポートされた ESXi ホストおよび vCenter Server の情報を vSphere 信頼機関 クラスタにインポートします。

これらのタスクを順番どおりに実行している場合、信頼機関クラスタの vCenter Server に接続されたままです。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。

手順

1 信頼機関クラスタの vCenter Server に信頼機関の管理者として接続していることを確認します。

たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション） 必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'パスワード'
```

3 この vCenter Server で管理されているクラスタを表示するには、`Get-TrustAuthorityCluster` コマンドレットを実行します。

```
Get-TrustAuthorityCluster
```

クラスタが表示されます。

4 変数に `Get-TrustAuthorityCluster` '*cluster*' を割り当てます。

たとえば、次のコマンドは変数 `$vTA` にクラスタ `vTA Cluster` の情報を割り当てます。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 信頼済みクラスタの vCenter Server プリンシパル情報を信頼機関クラスタにインポートするには、`New-TrustAuthorityPrincipal` コマンドレットを実行します。

たとえば、次のコマンドは、信頼する ESXi ホストおよび vCenter Server に関する情報の収集で以前にエクスポートされた `principal.json` ファイルをインポートします。

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

TrustAuthorityPrincipal information が表示されます。

6 インポートを確認するには、`Get-TrustAuthorityPrincipal` コマンドレットを実行します。

例：

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

インポートされた TrustAuthorityPrincipal が表示されます。

7 Trusted Platform Module (TPM) CA 証明書情報をインポートするには、`New-TrustAuthorityTpm2CACertificate` コマンドレットを実行します。

たとえば、次のコマンドは、信頼する ESXi ホストおよび vCenter Server に関する情報の収集で以前にエクスポートされた `cacert.zip` ファイルから TPM CA 証明書の情報をインポートします。

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
```

インポートされた証明書情報が表示されます。

8 ESXi ホストの基本イメージの情報をインポートするには、`New-TrustAuthorityVMHostBaseImage` コマンドレットを実行します。

たとえば、次のコマンドは、信頼する ESXi ホストおよび vCenter Server に関する情報の収集で以前にエクスポートされた `image.tgz` ファイルからイメージ情報をインポートします。

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

インポートされたイメージ情報が表示されます。

結果

信頼機関クラスタでは、どの ESXi ホストがリモートから証明できるか、すなわち、どのホストが信頼できるかが把握されています。

例： 信頼機関クラスタへの信頼済みホストの情報のインポート

この例では、PowerCLI を使用して、信頼済みクラスタの情報ファイルおよび信頼済みホストの情報ファイルの vCenter Server プリンシパル情報を信頼機関クラスタにインポートする方法を示しています。ここでは、信頼機関の管理者として信頼機関クラスタの vCenter Server に接続していることを前提としています。次の表に、使用されるコンポーネントと値の例を示します。

表 9-7. vSphere 信頼機関 セットアップの例

コンポーネント	値
変数 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
信頼機関クラスタの vCenter Server	192.168.210.22
信頼機関クラスタ名	vTA Cluster1（有効） vTA Cluster2（無効）
プリンシパル情報ファイル	`C:\vta\principal.json`
TPM 証明書ファイル	`C:\vta\cacert.cer`

表 9-7. vSphere 信頼機関 セットアップの例 （続き）

コンポーネント	値
ESXi ホストの基本イメージ ファイル	C:\vta\image.tgz
信頼機関管理者	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster1         Enabled             TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled            TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                        Domain          Type
TrustAuthorityClusterId
----                                        ------          ----
------------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                        Domain          Type
TrustAuthorityClusterId
----                                        ------          ----
------------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                 Name                                    Health
------------------------                ----                                    ------
TrustAuthorityCluster-domain-c8         52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                 VMHostVersion                           Health
```

```
------------------------                  -------------                          ------
TrustAuthorityCluster-domain-c8           ESXi 7.0.0-0.0.14828939                Ok
```

次のステップ

この後は信頼機関クラスタでのキー プロバイダの作成に続きます。

信頼機関クラスタでのキー プロバイダの作成

キー プロバイダ サービスをキー プロバイダに接続するには、信頼済みキー プロバイダを作成してから、vSphere 信頼機関 クラスタとキー サーバ (KMS) の間に信頼関係を設定する必要があります。KMIP 準拠のほとんどのキー サーバでは、この設定にはクライアント証明書とサーバ証明書の設定が含まれます。

vSphere 6.7 で KMS クラスタと呼ばれていたものは、vSphere 7.0 ではキー プロバイダと呼ばれることになりました。キー プロバイダの詳細については、vSphere 信頼機関 キー プロバイダ サービスについてを参照してください。

本番環境では、複数のキー プロバイダを作成できます。複数のキー プロバイダを作成することで、会社の組織、さまざまなビジネス ユニット、顧客などに基づいて展開の管理方法を決定できます。

これらのタスクを順番どおりに実行している場合、vSphere 信頼機関 クラスタの vCenter Server に接続されたままです。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- キー サーバでキーを作成し、有効にして、信頼済みキー プロバイダのプライマリ キーとして使用します。このキーは、この信頼済みキー プロバイダによって使用される他のキーとシークレットをラップします。キーの作成に関する詳細については、キー サーバ ベンダーのドキュメントを参照してください。

手順

1. 信頼機関クラスタの vCenter Server に接続していることを確認します。たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。
2. （オプション） 必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 信頼済みキー プロバイダを作成するには、New-TrustAuthorityKeyProvider コマンドレットを実行します。

たとえば、このコマンドは、PrimaryKeyID に 1 を使用し、名前に clkp を使用します。これらのタスクを順番どおりに実行している場合、Get-TrustAuthorityCluster 情報を変数（$vTA = Get-TrustAuthorityCluster 'vTA Cluster' など）に割り当て済みです。

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
-KmipServerAddress ip_address
```

通常、PrimaryKeyID は、キー サーバから取得された、UUID の形式のキー ID です。PrimaryKeyID にはキー名を使用しないでください。PrimaryKeyID の値は、ベンダーによって異なります。キー サーバのドキュメントを参照してください。New-TrustAuthorityKeyProvider コマンドレットで、KmipServerPort、ProxyAddress、ProxyPort などの他のオプションを使用できます。詳細については、New-TrustAuthorityKeyProvider のヘルプ システムを参照してください。

各論理キー プロバイダには、そのタイプ（標準、信頼済み、ネイティブの各キー プロバイダ）に関係なく、すべての vCenter Server システムで一意の名前が付いている必要があります。

詳細については、『キー プロバイダの名前の指定』を参照してください。

注： 複数のキー サーバをキー プロバイダに追加するには、Add-TrustAuthorityKeyProviderServer コマンドレットを使用します。

キー プロバイダの情報が表示されます。

4 キー サーバが信頼済みキープロバイダを信頼するように、信頼された接続を確立します。実際のプロセスは、キー サーバが受け入れた証明書と企業ポリシーによって異なります。ご使用のサーバに適したオプションを選択し、該当する手順を終了します。

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。
クライアント証明書のアップロード	クライアント証明書をアップロードして、信頼済みキー プロバイダの信頼済み接続を確立する。
KMS 証明書およびプライベート キーのアップロード	証明書およびプライベート キーをアップロードして、信頼済みキー プロバイダの信頼済み接続を確立する。
新規証明書署名要求	証明書署名リクエストを作成して、信頼済みキー プロバイダの信頼済み接続を確立する。

5 キー サーバ証明書をアップロードし、信頼済みキー プロバイダがキー サーバを信頼するように設定して、信頼関係の設定を終了します。

a `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 情報を変数に割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

この変数は、指定された信頼機関クラスタ内の信頼済みキー プロバイダ（この場合は `$vTA`）を取得します。

注： 信頼済みキー プロバイダが複数ある場合は、次のようなコマンドを使用して、必要なものを選択します。

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1` を使用すると、リスト内の最後の信頼済みキー プロバイダが選択されます。

b キー サーバ証明書を取得するには、`Get-TrustAuthorityKeyProviderServerCertificate` コマンドを実行します。

例：

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

サーバ証明書の情報が表示されます。初期状態では、証明書は信頼されていないため [信頼済み] 状態は False です。複数のキー サーバが設定されている場合は、証明書のリストが返されます。次の手順を使用して、各証明書を確認して追加します。

c 証明書を信頼する前に、`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` の情報を変数に割り当て（たとえば、`cert`）、`$cert.Certificate.ToString()` コマンドを実行して出力を確認します。

例：

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

件名、発行者などの情報を含む、証明書の情報が表示されます。

d KMIP サーバ証明書を信頼済みキー プロバイダに追加するには、`Add-TrustAuthorityKeyProviderServerCertificate` を実行します。

例：

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

証明書情報が表示され、[信頼済み] 状態が True になっています。

6 キー プロバイダのステータスを確認します。

a キー プロバイダのステータスを更新するには、`$kp` 変数を再度割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

注： 信頼済みキー プロバイダが複数ある場合は、次のようなコマンドを使用して、必要なものを選択します。

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1` を使用すると、リスト内の最後の信頼済みキー プロバイダが選択されます。

b `$kp.Status` コマンドを実行して、キー プロバイダのステータスを取得します。

例：

```
$kp.Status
```

注： ステータスが更新されるまでに数分間かかることがあります。ステータスを表示するには、`$kp` 変数を再度割り当てて、`$kp.Status` コマンドを再実行します。

健全性ステータスが [OK] の場合、キー プロバイダが正しく実行されていることを示しています。

結果

信頼済みキー プロバイダが作成され、キー サーバとの信頼が確立されました。

例： 信頼機関クラスタでのキー プロバイダの作成

この例では、PowerCLI を使用して信頼済みキー プロバイダを信頼機関クラスタに作成する方法を示します。ここでは、信頼機関の管理者として信頼機関クラスタの vCenter Server に接続していることを前提としています。また、CSR をベンダーに送信した後、キー サーバ ベンダーによって署名された証明書も使用します。

次の表に、使用されるコンポーネントと値の例を示します。

表 9-8. vSphere 信頼機関 セットアップの例

コンポーネント	値
変数 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
変数 `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
変数 `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
信頼機関クラスタの vCenter Server	192.168.210.22
KMIP 準拠のキー サーバ	192.168.110.91
KMIP 準拠のキー サーバ ユーザー	vcqekmip
信頼機関クラスタ名	vTA クラスタ
信頼機関管理者	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
```

```
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

次のステップ

この後は信頼機関クラスタ情報のエクスポートに続きます。

クライアント証明書をアップロードして、信頼済みキー プロバイダの信頼済み接続を確立する

一部のキー サーバ (KMS) ベンダーは、信頼できるキー プロバイダのクライアント証明書をキー サーバにアップロードすることを要求します。アップロード後、キー サーバは信頼できるキー プロバイダからのトラフィックを受け入れます。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。

- 信頼機関クラスタでのキー プロバイダの作成。

手順

1 信頼機関クラスタの vCenter Server に接続していることを確認します。たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション）必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 情報を変数に割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

これらのタスクを順番どおりに実行している場合、`Get-TrustAuthorityCluster` 情報を変数（`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'` など）に割り当て済みです。

この変数は、指定された信頼機関クラスタ内の信頼済みキー プロバイダ（この場合は `$vTA`）を取得します。

注： 信頼済みキー プロバイダが複数ある場合は、次のようなコマンドを使用して、必要なものを選択します。

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1` を使用すると、リスト内の最後の信頼済みキー プロバイダが選択されます。

---

4 信頼済みキー プロバイダのクライアント証明書を作成するには、`New-TrustAuthorityKeyProviderClientCertificate` コマンドレットを実行します。

例：

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

サムプリントが表示されます。

5 キー プロバイダのクライアント証明書をエクスポートするには、`Export-TrustAuthorityKeyProviderClientCertificate` コマンドレットを実行します。

例：

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

証明書がファイルにエクスポートされます。

6 証明書ファイルをキー サーバにアップロードします。

詳細については、キー サーバのドキュメントを参照してください。

結果

信頼済みキー プロバイダがキー サーバとの信頼関係を確立しました。

証明書およびプライベート キーをアップロードして、信頼済みキー プロバイダの信頼済み接続を確立する

一部のキー サーバ (KMS) ベンダーは、キー サーバによって提供されるクライアント証明書とプライベート キーを使用して信頼できるキー プロバイダを構成する必要があります。信頼されたキー プロバイダを構成した後、キー サーバは信頼されたキー プロバイダからのトラフィックを受け入れます。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。
- キー サーバ ベンダーに PEM 形式の証明書とプライベート キーを要求します。証明書が PEM 以外の形式で返された場合は、PEM に変換します。プライベート キーがパスワードで保護されている場合は、パスワードが削除された PEM ファイルを作成します。両方の操作に `openssl` コマンドを使用できます。例：
  - 証明書を CRT 形式から PEM 形式に変換するには：

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - 証明書を DER 形式から PEM 形式に変換するには：

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

  - プライベート キーからパスワードを削除するには：

    ```
    openssl rsa -in key.pem -out keynopassword.pem
    Enter pass phrase for key.pem:
    writing RSA key
    ```

手順

1 信頼機関クラスタの vCenter Server に接続していることを確認します。たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション） 必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 情報を変数に割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

これらのタスクを順番どおりに実行している場合、`Get-TrustAuthorityCluster` 情報を変数（`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'` など）に割り当て済みです。

`$kp` 変数は、指定された信頼機関クラスタ内の信頼済みキー プロバイダ（この場合は `$vTA`）を取得します。

注： 信頼済みキー プロバイダが複数ある場合は、次のようなコマンドを使用して、必要なものを選択します。

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1` を使用すると、リスト内の最後の信頼済みキー プロバイダが選択されます。

4 `Set-TrustAuthorityKeyProviderClientCertificate` コマンドを使用して、証明書とプライベート キーをアップロードします。

例：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

結果

信頼済みキー プロバイダがキー サーバとの信頼関係を確立しました。

証明書署名リクエストを作成して、信頼済みキー プロバイダの信頼済み接続を確立する

一部のキー サーバ (KMS) ベンダーでは、証明書署名リクエスト (CSR) を生成してキー サーバ ベンダーに送信することが要求されます。キー サーバ ベンダーは CSR に署名し、署名済み証明書を返します。この署名済み証明書を信頼済みキー プロバイダのクライアント証明書として設定すると、キー サーバは信頼済みキー プロバイダからのトラフィックを受け入れます。

このタスクは 2 段階のプロセスで行います。まず、CSR を生成してキー サーバ ベンダーに送信します。次に、キー サーバ ベンダーから受け取った署名済み証明書をアップロードします。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。

手順

1 信頼機関クラスタの vCenter Server に接続していることを確認します。たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション）必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 情報を変数に割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

これらのタスクを順番どおりに実行している場合、`Get-TrustAuthorityCluster` 情報を変数（`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'` など）に割り当て済みです。

この変数は、指定された信頼機関クラスタ内の信頼済みキー プロバイダ（この場合は `$vTA`）を取得します。

注： 信頼済みキー プロバイダが複数ある場合は、次のようなコマンドを使用して、必要なものを選択します。

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1` を使用すると、リスト内の最後の信頼済みキー プロバイダが選択されます。

4 CSR を生成するには、`New-TrustAuthorityKeyProviderClientCertificateCSR` コマンドレットを使用します。

例：

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

CSR が表示されます。また、`Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp` コマンドレットを使用して CSR を取得することもできます。

5 署名済み証明書を取得するには、キー サーバ ベンダーに CSR を送信します。

証明書は PEM 形式である必要があります。証明書が PEM 以外の形式で返された場合は、`openssl` コマンドを使用して PEM に変換します。例：

- 証明書を CRT 形式から PEM 形式に変換するには：

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- 証明書を DER 形式から PEM 形式に変換するには：

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

6 キー サーバ ベンダーから署名済み証明書を受信したら、`Set-TrustAuthorityKeyProviderClientCertificate` コマンドレットを使用して証明書をキー サーバにアップロードします。

例：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

結果

信頼済みキー プロバイダがキー サーバとの信頼関係を確立しました。

信頼機関クラスタ情報のエクスポート

信頼済みクラスタを vSphere 信頼機関 クラスタに接続するには、信頼機関クラスタのサービス情報をファイル形式でエクスポートしてから、そのファイルを信頼済みクラスタにインポートする必要があります。このファイルは、機密を確実に保持し、安全な状態で転送してください。

これらのタスクを順番どおりに実行している場合、信頼機関クラスタの vCenter Server に接続されたままです。

注： エクスポートされたサービス情報ファイルは、vSphere 信頼機関 構成をリストアする必要が発生した場合に備えて安全な場所に保管します。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。

手順

1 信頼機関クラスタの vCenter Server に接続していることを確認します。たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション） 必要に応じて次のコマンドを実行して、信頼機関クラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'パスワード'
```

3 信頼機関クラスタの証明サービスおよびキー プロバイダ サービス情報をエクスポートするには、`Export-TrustAuthorityServicesInfo` コマンドレットを実行します。

たとえば、このコマンドは、サービス情報を `clsettings.json` ファイルにエクスポートします。これらのタスクを順番どおりに実行している場合、変数に `Get-TrustAuthorityCluster` の情報を割り当て済みです（`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'` など）。

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

ファイルが作成されます。

結果

信頼機関クラスタの情報を含むファイルが作成されます。

例： 信頼機関クラスタ情報のエクスポート

この例は、PowerCLI を使用して信頼機関クラスタのサービス情報をエクスポートする方法を示しています。次の表に、使用されるコンポーネントと値の例を示します。

表 9-9. vSphere 信頼機関 セットアップの例

コンポーネント	値
変数 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
信頼機関クラスタの vCenter Server	192.168.210.22
信頼機関管理者	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       10/16/2019   9:59 PM           8177 clsettings.json
```

次のステップ

この後は信頼済みホストへの信頼機関クラスタ情報のインポートに続きます。

信頼済みホストへの信頼機関クラスタ情報のインポート

vSphere 信頼機関 クラスタの情報を信頼済みクラスタにインポートすると、信頼済みホストは信頼機関クラスタを使用して証明プロセスを開始します。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。
- 信頼機関クラスタ情報のエクスポート。

手順

1 信頼済みクラスタの vCenter Server に信頼機関の管理者として接続していることを確認します。

たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション） 必要に応じて次のコマンドを実行して、信頼済みクラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

注： または、別の PowerCLI セッションを開始して信頼済みクラスタの vCenter Server に接続することもできます。

3 信頼済みクラスタの状態が無効になっていることを確認します。

```
Get-TrustedCluster
```

[状態] は [無効] と表示されます。

4 `Get-TrustedCluster` 情報を変数に割り当てます。

たとえば、次のコマンドは、変数 `$TC` にクラスタ `Trusted Cluster` の情報を割り当てます。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

5 変数の値を表示して確認します。

例：

```
$TC
```

`Get-TrustedCluster` 情報が表示されます。

6 信頼機関クラスタ情報を vCenter Server にインポートするには、`Import-TrustAuthorityServicesInfo` コマンドレットを実行します。

たとえば、次のコマンドは、信頼機関クラスタ情報のエクスポートで以前にエクスポートされた `clsettings.json` ファイルからサービス情報をインポートします。

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

システムは確認プロンプトによって応答します。

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 確認プロンプトに対して Enter キーを押します（デフォルトは **Y** です）。

信頼機関クラスタ内のホストのサービス情報が表示されます。

8 信頼済みクラスタを有効にするには、`Set-TrustedCluster` コマンドレットを実行します。

例：

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

システムは確認プロンプトによって応答します。

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

信頼済みクラスタが健全な状態でない場合は、次の警告メッセージが表示されてから、確認メッセージが表示されます。

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 確認プロンプトに対して Enter キーを押します（デフォルトは **Y** です）。

信頼済みクラスタが有効になります。

注： 証明サービスとキー プロバイダ サービスを個別に有効にすることで、信頼済みクラスタを有効にすることもできます。`Add-TrustedClusterAttestationServiceInfo` および `Add-TrustedClusterKeyProviderServiceInfo` コマンドを使用します。たとえば、次のコマンドを実行すると、2 つのキー プロバイダ サービスと 2 つの証明サービスが設定されているクラスタ `Trusted Cluster` でサービスを 1 つずつ有効にすることができます。

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

---

10 信頼済みクラスタに証明サービスとキー プロバイダ サービスが設定されていることを確認します。

a `Get-TrustedCluster` 情報を変数に割り当てます。

たとえば、次のコマンドは、変数 `$TC` にクラスタ `Trusted Cluster` の情報を割り当てます。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b 証明サービスが設定されていることを確認します。

```
$tc.AttestationServiceInfo
```

証明サービスの情報が表示されます。

c キー プロバイダ サービスが設定されていることを確認します。

```
$tc.KeyProviderServiceInfo
```

キー プロバイダ サービスの情報が表示されます。

結果

信頼済みクラスタ内の ESXi 信頼済みホストは、信頼機関クラスタを使用して証明プロセスを開始します。

例： 信頼済みホストへの信頼機関クラスタ情報のインポート

この例では、信頼機関クラスタ サービスの情報を信頼済みクラスタにインポートする方法を示します。次の表に、使用されるコンポーネントと値の例を示します。

表 9-10. vSphere 信頼機関 セットアップの例

コンポーネント	値
信頼済みクラスタの vCenter Server	192.168.110.22
信頼機関管理者	trustedadmin@vsphere.local
信頼済みクラスタの名前	信頼できるクラスタ
信頼機関クラスタ内の ESXi ホスト	192.168.210.51 および 192.168.210.52
変数 `$TC`	`Get-TrustedCluster -Name 'Trusted Cluster'`

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name                   State             Id
----                   -----             --
```

```
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                  State             Id
----                  -----             --
Trusted Cluster       Disabled          TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

Name                  State             Id
----                  -----             --
Trusted Cluster       Enabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                ServicePort          ServiceGroup
--------------                -----------          ------------
192.168.210.51                443                  host-13:dc825986-73d2-463c-...
192.168.210.52                443                  host-16:dc825986-73d2-463c-...
```

次のステップ

vSphere Client を使用した信頼済みホストの信頼済みキー プロバイダの構成またはコマンドラインを使用した信頼済みホストの信頼済みキー プロバイダの構成に進みます。

vSphere Client を使用した信頼済みホストの信頼済みキー プロバイダの構成

vSphere Client を使用して、信頼済みキー プロバイダを構成できます。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。
- 信頼機関クラスタ情報のエクスポート。
- 信頼済みホストへの信頼機関クラスタ情報のインポート。

手順

1. vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。
2. vCenter Server 管理者、または暗号化操作.キー サーバの管理権限を持つ管理者としてログインします。
3. vCenter Server を選択してから、[構成] を選択します。
4. [セキュリティ] で [キー プロバイダ] を選択します。
5. [信頼されているキー プロバイダの追加] を選択します。

   使用可能な信頼済みキー プロバイダが、接続済みステータスで表示されます。
6. 信頼済みキー プロバイダを選択し、[キー プロバイダの追加] をクリックします。

   信頼済みキー プロバイダが信頼済みおよび接続済みとして表示されます。これが最初に追加する信頼済みキー プロバイダである場合は、デフォルトとしてマークされます。

   注： すべてのホストがキー プロバイダを取得できるようになり、vCenter Server がそのキャッシュを更新するまで、しばらく時間がかかります。情報の伝達方法によっては、一部のホストでのキー操作にキー プロバイダを使用するには、数分待つ必要がある場合があります。

結果

これで ESXi 信頼済みホストは、暗号化された仮想マシンの作成など、暗号化操作を実行できるようになりました。

次のステップ

信頼済みキー プロバイダを使用した仮想マシンの暗号化は、ユーザー エクスペリエンスとしては vSphere 6.5 で最初に提供された仮想マシンの暗号化と同様です。10 章 vSphere 環境における暗号化の使用を参照してください。

コマンドラインを使用した信頼済みホストの信頼済みキー プロバイダの構成

コマンドラインを使用して、信頼済みキー プロバイダを構成できます。vCenter Server、または vCenter Server オブジェクト階層のクラスタまたはフォルダ レベルで、デフォルトの信頼済みキー プロバイダを構成できます。

前提条件

- 信頼機関管理者の有効化。
- 信頼機関の状態の有効化。
- 信頼する ESXi ホストおよび vCenter Server に関する情報の収集。
- 信頼機関クラスタへの信頼済みホストの情報のインポート。
- 信頼機関クラスタでのキー プロバイダの作成。
- 信頼機関クラスタ情報のエクスポート。
- 信頼済みホストへの信頼機関クラスタ情報のインポート。

信頼できるクラスタ上で、暗号化操作.KMS の管理権限を含むロールが必要です。

手順

1 信頼できるクラスタの vCenter Server に管理者として接続していることを確認します。

たとえば、接続先のサーバをすべて表示するには `$global:defaultviservers` と入力します。

2 （オプション）必要に応じて次のコマンドを実行して、信頼済みクラスタの vCenter Server に接続していることを確認できます。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
```

3 信頼済みキー プロバイダを取得します。

```
Get-KeyProvider
```

`-Name` *keyprovider* オプションを使用して、信頼された単一のキープロバイダを指定できます。

4 `Get-KeyProvider` 信頼済みキー プロバイダ情報を変数に割り当てます。

たとえば、次のコマンドは情報を変数 `$workload_kp` を割り当てます。

```
$workload_kp = Get-KeyProvider
```

複数の信頼済みキー プロバイダがある場合は、`Select-Object` を使用して 1 つを選択できます。

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

5 信頼済みキー プロバイダを登録します。

```
Register-KeyProvider -KeyProvider $workload_kp
```

追加の信頼済みキー プロバイダを登録するには、手順 4 と手順 5 を繰り返します。

注： すべてのホストがキー プロバイダを取得できるようになり、vCenter Server がそのキャッシュを更新するまで、しばらく時間がかかります。情報の伝達方法によっては、一部のホストでのキー操作にキー プロバイダを使用するには、数分待つ必要がある場合があります。

6 使用するデフォルトの信頼済みキー プロバイダを設定します。

a vCenter Server レベルでデフォルトのキー プロバイダを設定するには、次のコマンドを実行します。

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

b クラスタ レベルでキー プロバイダを設定するには、次のコマンドを実行します。

たとえば、このコマンドにより、クラスタ `Trusted Cluster` のキー プロバイダが設定されます。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

c フォルダ レベルでキー プロバイダを設定するには、次のコマンドを実行します。

たとえば、このコマンドで `workLoad` データセンターで作成されたフォルダ `TC Folder` のキー プロバイダが設定されます。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

次のステップ

信頼済みキー プロバイダを使用した仮想マシンの暗号化は、ユーザー エクスペリエンスとしては vSphere 6.5 で最初に提供された仮想マシンの暗号化と同様です。10 章 vSphere 環境における暗号化の使用を参照してください。

vSphere 環境での vSphere 信頼機関 の管理

vSphere 信頼機関 を構成したら、サービスの停止および開始、クラスタへのホストの追加、Trust Authority クラスタのステータスの表示など、追加の操作を実行できます。

vSphere Client、API、および PowerCLI コマンドレットを使用してタスクを実行できます。『vSphere Web Services SDK プログラミング ガイド』、『VMware PowerCLI』ドキュメント、および『VMware PowerCLI コマンドレットのリファレンス』ドキュメントを参照してください。

vSphere 信頼機関 サービスの開始、停止、および再起動

vSphere Client を使用して vSphere 信頼機関 サービスを開始、停止、および再起動できます。

vSphere 信頼機関 を構成するサービスは、証明サービス (attestd) およびキー プロバイダ サービス (kmxd) です。

手順

1 vSphere Client を使用して、vSphere Trust Authority クラスタの vCenter Server に接続します。

2 管理者としてログインします。

3 Trust Authority クラスタ内の ESXi ホストを参照します。

4 [構成] を選択し、[システム] の [サービス] を選択します。

5 attestd サービスと kmxd サービスを見つけます。

6 必要に応じて [再起動]、[開始]、または [停止] 操作を選択します。

Trust Authority ホストの表示

vSphere Client を使用して、信頼済みクラスタ用に構成された vSphere 信頼機関 ホストを表示できます。

手順

1 vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。

2 管理者としてログインします。

3 vCenter Server インスタンスを選択します。

4 [構成] タブをクリックし、[セキュリティ] の下の [Trust Authority] を選択します。

信頼済みクラスタ用に構成された Trust Authority クラスタ内の ESXi ホストが表示されます。

vSphere 信頼機関 クラスタの状態の表示

vSphere Client を使用して vSphere 信頼機関 クラスタの状態を表示できます。状態は有効または無効のいずれかです。

Trust Authority クラスタの状態が有効な場合は、信頼できるクラスタの信頼できるホストは、認証サービスおよびキー プロバイダ サービスと通信できます。

手順

1 vSphere Client を使用して、信頼機関クラスタの vCenter Server に接続します。

2 管理者としてログインします。

3 オブジェクト階層内の Trust Authority クラスタを選択します。

4 [構成] タブをクリックし、[信頼機関] の下の [信頼機関クラスタ] を選択します。

ステータスは、有効または無効と表示されます。

信頼済みホスト サービスの再起動

信頼済みホストで実行されているサービスを再起動できます。

kmxa サービスは、ESXi 信頼済みホストで実行されます。

前提条件

ESXi Shell へのアクセスが有効になっている必要があります。ESXi Shell へのアクセスの有効化を参照してください。

手順

1 SSH などのリモート コンソール接続を使用して、ESXi 信頼済みホストでセッションを開始します。

2 root としてログインします。

3 次のコマンドを実行します。

```
/etc/init.d/kmxa restart
```

vSphere 信頼機関 ホストの追加と削除

VMware 提供のスクリプトを使用して、ESXi ホストを vSphere 信頼機関 クラスタに追加および削除します。

vSphere 7.0 では、VMware 提供のスクリプトを使用して、ESXi ホストを既存の vSphere 信頼機関 クラスタまたは信頼できるクラスタに追加および削除します。vSphere 7.0 Update 1 以降では、修正機能を使用して、既存の信頼できるクラスタに ESXi ホストを追加します。『vSphere Client を使用した信頼できるクラスタへのホストの追加』と『CLI を使用した信頼できるクラスタへのホストの追加』を参照してください。vSphere 7.0 Update 1 では、スクリプトを使用して、既存の信頼機関クラスタに ESXi ホストを追加する必要もあります。VMware ナレッジベースの記事 https://kb.vmware.com/s/article/77234 および https://kb.vmware.com/s/article/77146 を参照してください。

vSphere Client を使用した信頼できるクラスタへのホストの追加

vSphere Client を使用して、ESXi ホストを既存の信頼できるクラスタに追加できます。

信頼できるクラスタの最初の構成が完了した後に ESXi ホストの追加が必要になる場合があります。ただし、信頼できるクラスタにホストを追加する場合は、修正手順を追加で実行する必要があります。信頼できるクラスタを修正する際は、必要な構成状態が適用構成と適合することを確認します。

vSphere 7.0 でリリースされた vSphere 信頼機関 の最初のバージョンでスクリプトを実行し、既存の信頼できるクラスタにホストを追加します。vSphere 7.0 Update 1 以降では、修正機能を使用して、信頼できるクラスタにホストを追加します。vSphere 7.0 Update 1 では、スクリプトを使用して既存の信頼機関クラスタにホストを追加する必要もあります。vSphere 信頼機関 ホストの追加と削除を参照してください。

前提条件

信頼できるクラスタの vCenter Server で vSphere 7.0 Update 1 以降が実行されている必要があります。

信頼できるクラスタに最初に構成したものとは異なる ESXi バージョンまたは異なる TPM ハードウェア タイプを持つ ESXi ホストを追加する場合は、追加の手順が必要になります。この情報をエクスポートして、vSphere 信頼機関 クラスタにインポートする必要があります。『信頼する ESXi ホストおよび vCenter Server に関する情報の収集』と『信頼機関クラスタへの信頼済みホストの情報のインポート』を参照してください。

必要な権限については、一般的なタスクに必要な権限で「ホストの追加」タスクを参照してください。

手順

1. vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。
2. 信頼機関管理者としてログインします。
3. 信頼できるクラスタに移動します。
4. [設定] タブで、[設定] - [クイックスタート] を選択します。
5. [ホストの追加] セクションで [追加] をクリックします。
6. プロンプトに従います。
7. [信頼機関] タブで [修正] をクリックします。
8. 信頼できるクラスタが健全であることを確認するには、[健全性の確認] をクリックします。

CLI を使用した信頼できるクラスタへのホストの追加

コマンド ラインを使用して、既存の信頼できるクラスタに ESXi ホストを追加できます。

信頼できるクラスタの最初の構成が完了した後に ESXi ホストの追加が必要になる場合があります。ただし、信頼できるクラスタにホストを追加する場合は、修正手順を追加で実行する必要があります。信頼できるクラスタを修正する際は、必要な構成状態が適用構成と適合することを確認します。

vSphere 7.0 でリリースされた vSphere 信頼機関 の最初のバージョンでスクリプトを実行し、既存の信頼できるクラスタにホストを追加します。vSphere 7.0 Update 1 以降では、修正機能を使用して、信頼済みホストを追加します。vSphere 7.0 Update 1 では、スクリプトを使用して既存の信頼機関クラスタにホストを追加する必要もあります。vSphere 信頼機関 ホストの追加と削除を参照してください。

前提条件

- 信頼できるクラスタの vCenter Server で vSphere 7.0 Update 1 以降が実行されている必要があります。
- PowerCLI 12.1.0 以降が必要です。
- 必要な権限については、一般的なタスクに必要な権限で「ホストの追加」タスクを参照してください。

手順

1. ESXi ホストを信頼できるクラスタに追加する場合に通常行う手順をすべて実行します。
2. PowerCLI セッションで `Connect-VIServer` コマンドレットを実行し、信頼機関の管理者として信頼できるクラスタの vCenter Server に接続します。

   ```
   Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
   'password'
   ```

3. 信頼できるクラスタのステータスを確認するには、`Get-TrustedClusterAppliedStatus` PowerCLI コマンドレットを実行します。

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
   ```

4. 信頼できるクラスタが健全でない場合は、`-Remediate` パラメータを指定して `Set-TrustedCluster` コマンドレットを実行します。

   ```
   Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
   ```

5. 信頼できるクラスタが健全であることを確認するには、`Get-TrustedClusterAppliedStatus` コマンドレットを再実行します。

   ```
   Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
   ```

信頼済みクラスタ内の信頼済みホストの廃止

信頼済みクラスタから信頼済みホストを削除（廃止）することができます。シナリオに応じて、信頼済みクラスタ内の 1 つまたはすべての信頼済みホストを廃止できます。

信頼済みホストを廃止すると、修正機能によって、信頼済みホストに必要な状態が、移動先の信頼されていないクラスタの状態に設定されます。廃止された信頼済みホストは、通常のホストになります。信頼済みホストの移動元の信頼済みクラスタは、必要な状態構成を維持したまま、信頼済みクラスタとして引き続き機能します。

信頼済みクラスタからすべての信頼済みホストを削除すると、信頼済みクラスタは廃止されます。信頼済みホストと信頼済みクラスタから必要な状態構成と適用構成を両方削除してから、すべての信頼済みホストを信頼されていないクラスタに移動します。

環境内で、廃止された信頼済みホストを再利用することができます。たとえば、信頼されていないインフラストラクチャのキャパシティ内でホストを再利用したり、vSphere 信頼機関 ホストとして再利用したりできます。廃止されたホストは、同じ vCenter Server または別の vCenter Server で使用できます。

信頼済みクラスタの構成と健全性の詳細については、信頼済みクラスタの健全性と修正の概要を参照してください。

前提条件

- 信頼できるクラスタの vCenter Server で vSphere 7.0 Update 1 以降が実行されている必要があります。
- PowerCLI を使用する場合は、バージョン 12.1.0 以降が必要です。

手順

1. vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。
2. 信頼機関管理者としてログインします。
3. 信頼できるクラスタに移動します。
4. 信頼済みクラスタ内の信頼済みホストを廃止する方法を決定します。

タスク	手順
信頼済みクラスタと残りの信頼済みホストに必要な構成状態を維持する	a ホストをメンテナンス モードにして、新しい空のクラスタ（ホストが含まれていないクラスタ）にホストを移動します。 b ホストのメンテナンス モードを終了します。 c 新しい空のクラスタ（信頼されていないクラスタ）の [信頼機関] タブで、[修正] をクリックします。 修正を行うと、移動されたホストから信頼済みの構成が削除されます。信頼済みクラスタに必要な状態構成は維持されます。

すべての信頼済みホストから必要な構成状態および適用構成状態を削除する	a PowerCLI セッションで `Connect-VIServer` コマンドレットを実行し、信頼機関の管理者として信頼できるクラスタの vCenter Server に接続します。
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b 次の例のように `Set-TrustedCluster` コマンドレットを実行します。
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled`
	すべての信頼済みホストから信頼済みインフラストラクチャの構成が削除され、信頼済みクラスタに必要な状態構成が削除されます。
	c すべてのホストをメンテナンス モードに切り替えて、別のクラスタに移動します。
	d ホストのメンテナンス モードを終了します。

5 信頼済みクラスタが健全であることを確認するには、信頼済みクラスタの [信頼機関] タブで [健全性の確認] をクリックします。

次のステップ

廃止された ESXi ホストから特定のバージョンの ESXi または TPM ハードウェアを認証する予定がなくなった場合は、信頼機関クラスタの構成を更新して、セキュリティを最適化します。VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/77146) を参照してください。

vSphere 信頼機関構成のバックアップ

vSphere 信頼機関を信頼機関のバックアップとして構成する際は、エクスポートしたファイルを使用します。これらのファイルを使用して、Trust Authority デプロイをリストアできます。これらの構成ファイルの機密を保持し、安全に転送します。

ほとんどの vSphere 信頼機関の構成および状態の情報は、ConfigStore データベース内の ESXi ホストに保存されます。vCenter Server インスタンスのバックアップに使用する vCenter Server 管理インターフェイスでは、vSphere 信頼機関 の構成情報のバックアップは行われません。vSphere 信頼機関環境を設定する際に、エクスポートした構成ファイルを安全に保存すれば、vSphere 信頼機関 構成のリストアに必要な情報が確保されます。この情報を生成する必要がある場合は、信頼する ESXi ホストおよび vCenter Server に関する情報の収集を参照してください。

キー プロバイダのプライマリ キーの変更

使用されているプライマリ キーをローテーションする場合などにキー プロバイダのプライマリ キーを変更することができます。

キーのライフ サイクルのガイダンスについては、仮想マシンの暗号化のベスト プラクティスを参照してください。

前提条件

キー サーバ (KMS) で、信頼済みキー プロバイダの新しいプライマリ キーとして使用するキーを作成し、有効にします。このキーは、この信頼済みキー プロバイダによって使用される他のキーとシークレットをラップします。キーの作成に関する詳細については、KMS ベンダーのドキュメントを参照してください。

手順

1 `Set-TrustAuthorityKeyProvider` コマンドを実行します。

例：

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 キー プロバイダのステータスを確認します。

a `Get-TrustAuthorityCluster` 情報を変数に割り当てます。

例：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 情報を変数に割り当てます。

例：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c `$kp.Status` を実行して、キー プロバイダのステータスを確認します。

例：

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

健全性ステータスが [OK] の場合、キー プロバイダが正しく実行されていることを示しています。

結果

すべての新しい暗号化操作に、新しいプライマリ キーが使用されます。古いプライマリ キーを使用して暗号化されたデータは、引き続き古いキーを使用して復号化されます。

信頼済みホストの証明レポートの概要

vSphere 信頼機関 では、vCenter Server が信頼済みホストの証明ステータスを検証して報告します。vSphere Client を使用して、信頼済みホストの証明ステータスを表示できます。

vSphere 信頼機関 は、信頼済みホストのリモート証明を使用して、起動されているソフトウェアの信頼性を証明します。証明では、信頼済みホストで実行されているソフトウェアが VMware の認証済みソフトウェア、または VMware によって署名されているパートナー ソフトウェアであることが検証されます。信頼済みクラスタの vCenter Server は、信頼済みホストと通信して内部の証明レポートを取得します。証明レポートは、信頼機関クラスタで実行されている証明サービスによって信頼済みホストが証明されているかどうかを示します。信頼済みホストが証明されていない場合、証明レポートはエラー メッセージも表示します。vSphere Client には、信頼済みホストについて次の証明ステータスが表示されます。

パス

信頼済みホストは vSphere 信頼機関 証明サービスによって証明されており、vCenter Server で内部証明レポートを使用可能です。

Failed

信頼済みホストは、vSphere 信頼機関 証明サービスによって証明することができませんでした。vCenter Server 内部証明レポートには、信頼済みホストが証明を試行した証明サービスから報告されたエラーが含まれています。

vSphere Client は、ホストが vSphere 信頼機関 と vCenter Server のどちらによって証明されたかも表示します。

信頼済みホストが証明されていない場合でも、信頼済みホストで実行されている仮想マシンは、暗号化された仮想マシンも含めて引き続きアクセス可能です。証明されていない信頼済みホスト上の仮想マシンをパワーオンすることはできません。ただし、暗号化されていない仮想マシンを追加することはできます。信頼済みホストが証明されていない場合は、証明の問題を解決するための手順を実行します。証明の概念の詳細については、vSphere 信頼機関のプロセス フローを参照してください。

複数の信頼機関ホストを構成している場合、各ホストから利用可能な証明レポートは複数になる可能性があります。ステータスのレポートでは、vSphere Client は最初に検出した「証明済み」レポートのステータスを表示します。「証明済み」レポートがない場合、vSphere Client は、最初に検出した「証明されていない」レポートのエラーを表示します。

複数の信頼機関ホストを構成済みの場合でも、vSphere Client は 1 つの証明レポートのみに基づいてステータスやエラー メッセージを表示します。

信頼済みクラスタの証明ステータスの表示

vSphere Client を使用して信頼済みホストの証明ステータスを表示できます。

前提条件

- 信頼済みホストと vSphere 信頼機関 ホストの両方で、ESXi 7.0 Update 1 以降が実行されている必要があります。
- 各クラスタの vCenter Server ホストで vSphere 7.0 Update 1 以降が実行されている必要があります。

手順

1. vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。
2. 管理者としてログインします。

   信頼機関管理者または vSphere 管理者としてログインできます。
3. データセンターに移動し、[監視] タブをクリックします。
4. [セキュリティ] をクリックします。
5. [証明] 列で信頼済みホストのステータスを確認し、[メッセージ] 列で付随するメッセージを参照します。

次のステップ

エラーがある場合は、信頼済みホスト証明の問題のトラブルシューティングを参照してください。

信頼済みホスト証明の問題のトラブルシューティング

vSphere 信頼機関 の証明レポートは、信頼済みホスト証明のエラーに対するトラブルシューティングの開始点です。

手順

1 信頼済みクラスタの証明ステータスの表示。

2 次の表を使用してトラブルシューティングを行い、エラーを解決してください。

Error	原因と解決策
認証サービスが設定されていません。	証明サービスが構成されていません。修正アクションを使用して、信頼済みホストが証明サービスを使用するように構成します。信頼済みクラスタの修正を参照してください。
使用可能な TPM2 デバイスがありません。	信頼済みホストをインストールし、Trusted Platform Module (TPM) を使用するように構成します。ベンダーのドキュメントを参照してください。
TPM2 保証パブリック キーまたは証明書を取得できませんでした。	TPM がサポートされていること、および TPM の有効な承認キーがあることを確認します。場合によっては、VMware サポートへの問い合わせが必要です。
証明レポートを使用できません。	信頼済みホストの証明が完了していない可能性があります。数分待ってから、証明ステータスを再確認します。
証明サービスのバージョンと要求の間に互換性がありません。	証明サービスを実行している証明機関ホストを vSphere 7.0 Update 1 以降に更新します。
セキュア ブートが有効でないため、認証に失敗しました。	信頼済みホストがセキュア ブートを使用するように構成されていることを確認します。ESXi ホストの UEFI セキュア ブートを参照してください。
認証で、リモート ソフトウェアのバージョンの識別に失敗しました。	信頼済みホストの基本イメージ情報を証明サービスにインポートします。信頼機関クラスタへの信頼済みホストの情報のインポートを参照してください。
TPM 証明書が必要なため、認証に失敗しました。	TPM がサポートされていることを確認します。または、次の PowerCLI コマンドレットを実行して、`requireCertificateValidation` を `false` に設定するように com.vmware.esx.attestation.tpm2.settings を変更します。 `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`
TPM が不明なため、認証に失敗しました。	TPM 承認キーを証明サービスにインポートします。信頼機関クラスタへの信頼済みホストの情報のインポートを参照してください。
エラー：vapi.send が失敗しました。	信頼済みホストで kmxa サービスが実行されていないか、kmxa サービスが証明サービスに接続できない可能性があります。kmxa サービスが開始されていることを確認します。また、証明サービスが実行されていることを確認します。信頼済みホスト サービスの再起動を参照してください。

信頼済みクラスタの健全性の確認と修正

信頼済みクラスタの健全性を確認して検証することができます。信頼済みクラスタの健全性に関する問題が発生した場合は、信頼済みクラスタの構成を修正できます。

信頼済みクラスタの健全性と修正の概要

信頼済みクラスタの構成に健全性の問題がある場合は、構成の不整合を解決する必要があります。これを行うには、信頼済みクラスタを修正します。信頼済みクラスタを修正するときは、信頼済みクラスタ内のすべての信頼済みホストについて信頼構成が同じであることを確認します。

信頼済みクラスタは、信頼機関クラスタによってリモートから証明された信頼済み ESXi ホストの vCenter Server クラスタで構成されています。最初に vSphere 信頼機関 を構成するときは、信頼機関クラスタから信頼済みクラスタに信頼機関サービス情報をインポートする必要があります。信頼済みクラスタは、コンポーネントのこの構成を使用して、信頼機関クラスタで実行されているキー プロバイダ サービスおよび証明サービスに接続します。信頼済みクラスタを構成する方法の詳細については、信頼済みホストへの信頼機関クラスタ情報のインポートを参照してください。信頼済みクラスタを構成したら、その健全性を確認して修正できます。

信頼済みクラスタの健全性の概要

信頼済みクラスタの健全性を確認する方法は、次の条件によって異なります。

目的の状態構成

目的の状態構成は、信頼済みクラスタにインポートする信頼機関サービス情報に基づきます。目的の状態構成は、信頼済みクラスタの「信頼できる情報源」です。目的の状態構成は、信頼済みクラスタを設定するときに最初に作成されるものと考えることができます。

適用構成

適用構成とは、信頼済みクラスタを構成した特定の証明サービスおよびキー プロバイダ サービスの登録です。適用構成は、信頼済みクラスタが現在実行しているものです。適用構成は、「ランタイム」構成と考えることができます。目的の状態構成は、適用される構成と一致する必要があります。適用構成が目的の状態構成と一致しない場合、信頼済みクラスタは「健全ではない」と見なされます。健全ではない信頼済みクラスタは、パフォーマンスが低下するか、まったく機能しません。

この健全性チェックは、信頼済みクラスタまたは vSphere 信頼機関 インフラストラクチャの全体的な健全性を示すものではありません。健全性チェックでは、信頼済みクラスタの目的の状態構成と適用構成が比較されます。

信頼済みクラスタの修正の概要

修正とは、vSphere 信頼機関 が信頼済みクラスタの構成の不整合を解決するためのプロセスです。信頼済みクラスタの構成は、時間の経過と共に、または操作上のエラーによって不整合になる可能性があります。

修正は次のように使用します。

- 信頼済みクラスタの健全性を確認します。
- 信頼済みクラスタが健全でない場合は、修正します。

vSphere Client または CLI のいずれかを使用して、信頼済みクラスタの健全性を確認できます。信頼済みクラスタの健全性の確認を参照してください。また、vSphere Client または CLI のいずれかを使用して、信頼済みクラスタを修正することもできます。信頼済みクラスタの修正を参照してください。

注： 修正は、既存の信頼済みクラスタにホストを追加するときの適切なプロセスとしても使用されます。『vSphere Client を使用した信頼できるクラスタへのホストの追加』と『CLI を使用した信頼できるクラスタへのホストの追加』を参照してください。

信頼済みクラスタの健全性の確認

vSphere Client またはコマンド ラインを使用して、信頼済みクラスタの健全性ステータスを確認できます。

詳細については、『信頼済みクラスタの健全性と修正の概要』を参照してください。

前提条件

- 信頼できるクラスタの vCenter Server で vSphere 7.0 Update 1 以降が実行されている必要があります。
- PowerCLI を使用する場合は、バージョン 12.1.0 以降が必要です。

手順

1 信頼済みクラスタの健全性を確認します。

ツール	手順
vSphere Client	a vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。 b 信頼機関管理者としてログインします。 c 信頼済みクラスタに移動し、[構成] を選択してから [信頼機関] を選択します。 d [健全性の確認] をクリックします。

CLI	a PowerCLI セッションで `Connect-VIServer` コマンドレットを実行し、信頼機関の管理者として信頼できるクラスタの vCenter Server に接続します。
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b 次の例のように `Get-TrustedClusterAppliedStatus` コマンドレットを実行します。
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2 エラーがある場合は、信頼済みクラスタの修正を参照してください。

信頼済みクラスタの修正

信頼済みクラスタの構成は、vSphere Client またはコマンドラインのいずれかを使用して修正できます。

前提条件

信頼できるクラスタの vCenter Server で vSphere 7.0 Update 1 以降が実行されている必要があります。

手順

1 信頼済みクラスタの vCenter Server に接続します。

ツール	手順
vSphere Client	a vSphere Client を使用して、信頼済みクラスタの vCenter Server に接続します。 b 信頼機関管理者としてログインします。
CLI	PowerCLI セッションで `Connect-VIServer` コマンドレットを実行し、信頼機関の管理者として信頼できるクラスタの vCenter Server に接続します。 `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2 信頼済みクラスタを修正してから、信頼済みクラスタの健全性を再確認します。

ツール	手順
vSphere Client	a 信頼できるクラスタに移動します。 b [構成] を選択し、[信頼機関] を選択します。 c [修正] をクリックします。 d [健全性の確認] をクリックします。

CLI	a 次のように、-Remediate パラメータを指定して Set-TrustedCluster コマンドレットを実行します。
	`Set-TrustedCluster -TrustedCluster '*TrustedCluster*' -Remediate`
	b 次の例のように Get-TrustedClusterAppliedStatus コマンドレットを実行します。
	`Get-TrustedClusterAppliedStatus -TrustedCluster '*TrustedCluster*'`

vSphere 環境における暗号化の使用 10

標準のキー プロバイダ、信頼されたキー プロバイダ、または vSphere Native Key Provider のいずれを使用する場合でも、vSphere 環境で暗号化を使用するには準備が必要になります。

環境を設定すると、vSphere Client を使用して暗号化された仮想マシンや仮想ディスクを作成したり、既存の仮想マシンやディスクを暗号化したりすることができます。

API と `crypto-util` CLI を使用することで、追加のタスクを実行できます。API に関するドキュメントについては『vSphere Web Services SDK プログラミング ガイド』を、`crypto-util` ツールについてはそのコマンドライン ヘルプを参照してください。

暗号化ストレージ ポリシーの作成

暗号化された仮想マシンを作成するには、暗号化ストレージ ポリシーを作成する必要があります。仮想マシンや仮想ディスクを暗号化する際には、作成したストレージ ポリシーをその都度適用します。

その他の I/O フィルタで仮想マシンの暗号化を使用する場合、または vSphere Client で [仮想マシン ストレージ ポリシーの作成] ウィザードを使用する場合は、vSphere のストレージ ドキュメントで詳細を確認してください。

前提条件

- キー プロバイダへの接続をセットアップします。

  キー プロバイダへの接続が設定されていなくても仮想マシン暗号化ストレージ ポリシーを作成することは可能ですが、キー プロバイダとの間で信頼できる接続が確立されるまで暗号化タスクを実行できません。

- 必要な権限：暗号化操作.暗号化ポリシーの管理。

手順

1. vSphere Client を使用して、vCenter Server にログインします。
2. [ホーム] を選択し、[ポリシーおよびプロファイル] をクリックし、[仮想マシン ストレージ ポリシー] をクリックします。
3. [作成] をクリックします。
4. vCenter Server を選択し、ポリシー名を入力して、必要に応じて説明を入力してから、[次へ] をクリックします。
5. [ポリシー構造] 画面で、[ホスト ベースのロールを有効化] を選択し、[次へ] をクリックします。

6 [ホスト ベースのサービス] 画面で、[ストレージ ポリシー コンポーネントの使用] を選択し、ドロップダウン メニューから [デフォルトの暗号化プロパティ] を選択し、[次へ] をクリックします。

7 [ストレージ互換性] 画面で、[互換性あり] が選択されていることを確認し、データストアを選択して、[次へ] をクリックします。

8 情報を確認し、[終了] をクリックします。

結果

仮想マシン暗号化ストレージ ポリシーがリストに追加され、仮想マシンの暗号化の際に使用できるようになります。

ホスト暗号化モードを明示的に有効にする

暗号化された仮想マシンの作成など、暗号化タスクを ESXi ホストで実行する必要がある場合は、ホスト暗号化モードを有効にする必要があります。ホスト暗号化モードは、ほとんどの場合、暗号化タスクを実行した時点で自動的に有効になります。

暗号化モードを明示的に有効にしなければならない場合があります。暗号化タスクの前提条件と必要な権限を参照してください。

前提条件

必要な権限：暗号化 operations.Register ホスト

手順

1 vSphere Client を使用して、vCenter Server にログインします。

2 ESXi ホストに移動して参照し、[構成] 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 [ホスト暗号化モード] パネルで [編集] をクリックします。

5 [有効] を選択し、[OK] をクリックします。

API を使用したホスト暗号化モードの無効化

暗号化モードを有効にする権限を持つユーザーの場合、暗号化タスクを実行すると、ホスト暗号化モードが自動的に有効になります。ホスト暗号化モードが有効になると、すべてのコア ダンプが暗号化され、サポート担当者に機密情報がみることができません。ESXi ホストで仮想マシンの暗号化を行う必要がない場合は、暗号化モードを無効にできます。

ESXi ホストの暗号化モードを有効にした後で、無効化が必要になる場合があります。たとえば、ESXi サポート バンドルを（`vm-support` コマンドを使用して）生成するために、暗号化モードを無効にする必要がある場合が考えられます。ホストに鍵マテリアルがある場合は、ホストの暗号化モードの無効化の切り替え（[ホスト] - [構成] - [セキュリティ プロファイル] - [ホストの暗号化モードの編集]）を使用しても機能しません。

API を使用してホストの暗号化モードを無効にする場合は、`CryptoManagerHostDisable` API メソッドを呼び出します。

ESXi ホストに定義されている暗号化モード（暗号化の状態）は次のとおりです。

- pendingIncapable：ホストの暗号化は無効です。したがって、ホストで vSphere 仮想マシンの暗号化操作を実行できません。
- incapable：ホストは、機密情報を安全に受信できる状態ではありません。
- prepared：ホストは機密情報を受信する準備ができていますが、ホスト キーがまだ設定されていません。
- safe：ホストは暗号化が safe（有効）であり、ホスト キーが設定されています。したがって、vSphere 仮想マシンの暗号化操作が可能です。

ホストで `CryptoManagerHostDisable` を呼び出すと、ホストの暗号化状態は次のように変わります。

- ホストの元の暗号化状態が incapable か prepared の場合、ホストの暗号化状態は incapable に変わります。
- ホストの元の暗号化状態が safe の場合、ホストの暗号化状態は pendingIncapable に変わります。
- ホストの元の暗号化状態が pendingIncapable の場合、ホストの暗号化状態は引き続き pendingIncapable です。

このタスクでは、vCenter Server 管理対象オブジェクト ブラウザ (MOB) を使用してホストの暗号化モードを無効にする方法を示します。API の使用の詳細については、『vSphere Web Services API』ドキュメント (https://developer.vmware.com/apis/968/vsphere) を参照してください。

手順

1 管理者として vCenter Server にログインします。

2 暗号化モードを無効にする ESXi ホストから、暗号化されたすべての仮想マシンを登録解除します。

3 vCenter Server 上の MOB にアクセスします。

```
https://vcenter_server/mob
```

4 ホストで `CryptoManagerHostDisable` メソッドを呼び出します。

   a [コンテンツ名] で、[コンテンツ] をクリックします。

   b [rootFolder] で、[group-D1 (Datacenters)] をクリックします。

   c [childEntity] で、適切なデータセンターをクリックします。

   d [hostFolder] で、適切なホストをクリックします。

   e [childEntity] で、適切なクラスタをクリックします。

   f [ホスト] で、適切なホストをクリックします。

   g [configManager] で、[configManager] をクリックします。

   h [cryptoManager] で、[CryptoManagerHost-]*number* をクリックします。

   i [CryptoManagerHostDisable] をクリックします。

   ホストの暗号化状態が、元の暗号化状態に応じて pendingIncapable または incapable に変わります。

5 暗号化モードを無効にする他のホストについて、手順 4 を繰り返します。

6 ホストを再起動します。

結果

ホストの暗号化モードを無効にすると、再度有効にするまで、暗号化した仮想マシンの追加などの暗号化操作を実行できなくなります。

注： 元の暗号化状態が pendingIncapable だった ESXi ホストで暗号化モードを無効にし、再起動すると、ホストの暗号化状態は引き続き pendingIncapable になります。ホストの暗号化モードを再度有効にするには、vCenter Server の MOB に再度アクセスし、`ConfigureCryptoKey` API メソッドを呼び出します。ホストの暗号化状態が pendingIncapable の場合、ホストの暗号化モードを再度有効にするときには元のホスト キー ID を使用します。

暗号化された仮想マシンの作成

KMS の設定後に、暗号化された仮想マシンを作成できます。

このタスクでは、vSphere Client を使用して暗号化された仮想マシンを作成する方法について説明します。vSphere Client では、仮想マシンの暗号化ストレージ ポリシーによるフィルタリングにより、暗号化された仮想マシンの作成が容易になっています。

注： 既存の仮想マシンを暗号化するよりも、暗号化された仮想マシンを作成した方が早く、使用ストレージ リソースも少なくて済みます。可能な場合には、作成中に仮想マシンを暗号化します。

前提条件

- KMS との信頼された接続を確立して、デフォルトの KMS を選択します。
- 暗号化ストレージ ポリシーを作成するか、バンドルされているサンプルの仮想マシン暗号化ポリシーを使用します。
- 仮想マシンがパワーオフ状態であることを確認します。
- 次の必要な権限があることを確認します。
  - 暗号化操作.新規暗号化
  - ホストの暗号化モードが有効でない場合は、暗号化操作.ホストの登録も必要です。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 オブジェクトを右クリックし、[新規仮想マシン] を選択します。

4 画面の指示どおりに暗号化された仮想マシンを作成します。

オプション	操作
作成タイプの選択	新しい仮想マシンを作成します。
名前とフォルダの選択	仮想マシンの一意の名前と作成先を指定します。
コンピューティング リソースの選択	暗号化された仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。暗号化タスクの前提条件と必要な権限を参照してください。
ストレージの選択	[この仮想マシンを暗号化] チェック ボックスをオンにします。暗号化を含む仮想マシン ストレージ ポリシーが表示されます。仮想マシン ストレージ ポリシーを選択し（バンドルされているサンプルは仮想マシン暗号化ポリシーです）、互換性のあるデータストアを選択します。
互換性の選択	互換性を選択します。暗号化された仮想マシンは、互換性が ESXi 6.5 以降であるホストにのみ移行できます。
ゲスト OS を選択	後で仮想マシンにインストールすることを検討しているゲスト OS を選択します。
ハードウェアのカスタマイズ	ディスク サイズや CPU を変更するなどしてハードウェアをカスタマイズします。 （オプション）[仮想マシン オプション] タブをクリックし、[暗号化] を展開します。暗号化から除外するディスクを選択します。ディスクを選択解除すると、仮想マシン ホームとその他の選択されたディスクのみが暗号化されます。 追加した新規ハード ディスクはすべて暗号化されます。ハード ディスクのストレージ ポリシーは後から個別に変更することができます。
設定の確認	情報を確認し、[終了] をクリックします。

暗号化された仮想マシンのクローン

暗号化された仮想マシンのクローンを作成すると、そのクローンは同じキーで暗号化されます。クローンのキーを変更するには、API を使用してクローンの再暗号化を実行します。vSphere Web Services SDK プログラミング ガイド を参照してください。

クローン作成時には次の操作を実行できます。

- 暗号化されていない仮想マシンまたはテンプレート仮想マシンから、暗号化された仮想マシンを作成する。
- 暗号化された仮想マシンまたはテンプレート仮想マシンから、復号化された仮想マシンを作成する。
- ソース仮想マシンのキーとは異なるキーを使用して、ターゲット仮想マシンを再暗号化する。

暗号化された仮想マシンからインスタント クローン仮想マシンを作成する。この場合、インスタント クローンはソース仮想マシンと同じキーを共有することに注意します。ソース仮想マシンでもインスタント クローン仮想マシンでも、キーを再暗号化することはできません。vSphere Web Services SDK プログラミング ガイド を参照してください。

前提条件

- KMS との信頼された接続を確立して、デフォルトの KMS を選択します。
- 暗号化ストレージ ポリシーを作成するか、バンドルされているサンプルの仮想マシン暗号化ポリシーを使用します。

- 必要な権限：
  - 暗号化操作.クローン作成
  - 暗号化操作.暗号化
  - 暗号化操作.復号化
  - 暗号化操作.再暗号化
  - ホストの暗号化モードが有効でない場合は、暗号化操作.ホストの登録権限も必要です。

手順

1 vSphere Client インベントリで、仮想マシンに移動して参照します。

2 暗号化されたマシンのクローンを作成するには、仮想マシンを右クリックし、[クローン] - [仮想マシンにクローン作成] を選択してから、プロンプトの指示に従います。

オプション	操作
名前とフォルダの選択	クローンの名前と作成先を指定します。
コンピューティング リソースの選択	暗号化された仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。暗号化タスクの前提条件と必要な権限を参照してください。
ストレージの選択	[仮想ディスク フォーマットの選択]メニューで必要な選択を行い、データストアを選択します。クローン操作の過程でストレージ ポリシーを変更できます。たとえば、暗号化ポリシーを使用している状態から非暗号化ポリシーに変更すると、ディスクが復号化されます。
クローン オプションの選択	『vSphere の仮想マシン管理』ドキュメントの説明に従ってクローン オプションを選択します。
設定の確認	情報を確認し、[終了] をクリックします。

3 （オプション） クローンが作成された仮想マシンのキーを変更します。

デフォルトでは、親と同じキーでクローンが作成された仮想マシンが作成されます。ベスト プラクティスは、複数の仮想マシンが同一のキーを持つことがないよう、クローン作成された仮想マシンのキーを変更することです。

a 表層と深層のどちらの再暗号化を行うかを決定します。

異なる DEK と KEK を使用するには、クローンが作成された仮想マシンの再暗号化（深層）を実行します。異なる KEK を使用するには、クローンが作成された仮想マシンの再暗号化（表層）を実行します。再暗号化（深層）を行うには、仮想マシンをパワーオフする必要があります。再暗号化（表層）は、仮想マシンのスナップショットが作成済みであれば仮想マシンがパワーオン状態でも実行できます。スナップショットが作成済みの暗号化された仮想マシンの再暗号化（表層）は、単一のスナップショット分岐（ディスク チェーン）に対してのみ許可されます。複数のスナップショット分岐はサポートされていません。チェーン内のすべてのリンクを新しい KEK で更新する前に再暗号化（表層）が失敗した場合でも、古い KEK と新しい KEK があれば暗号化された仮想マシンにアクセスできます。

b API を使用して、クローンの再暗号化を実行します。vSphere Web Services SDK プログラミング ガイド を参照してください。

既存の仮想マシンまたは仮想ディスクの暗号化

既存の仮想マシンまたは仮想ディスクは、そのストレージ ポリシーを変更することによって暗号化することができます。暗号化できるのは、暗号化された仮想マシンの仮想ディスクだけです。

このタスクでは、vSphere Client を使用して既存の仮想マシンや仮想ディスクを暗号化する方法について説明します。

 (vSphere Client での仮想マシンの暗号化)

前提条件

- KMS との信頼された接続を確立して、デフォルトの KMS を選択します。
- 暗号化ストレージ ポリシーを作成するか、バンドルされているサンプルの仮想マシン暗号化ポリシーを使用します。
- 仮想マシンがパワーオフ状態であることを確認します。
- 次の必要な権限があることを確認します。
  - 暗号化操作.新規暗号化
  - ホストの暗号化モードが有効でない場合は、暗号化操作.ホストの登録も必要です。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 変更対象の仮想マシンを右クリックし、[仮想マシン ポリシー] - [仮想マシン ストレージ ポリシーの編集] を選択します。

仮想マシン ファイル（仮想マシン ホーム）のストレージ ポリシーと仮想ディスクのストレージ ポリシーを設定することができます。

3 ストレージ ポリシーを選択します。

- 仮想マシンとそのハード ディスクを暗号化するには、暗号化ストレージ ポリシーを選択し、[OK] をクリックします。
- 仮想ディスクは暗号化せずに仮想マシンだけを暗号化するには、[ディスクごとに設定] で切り替えることにより、仮想マシン ホームについては暗号化ストレージ ポリシーを選択し、仮想ディスクについては他のストレージ ポリシーを選択して、[OK] をクリックします。

暗号化されていない仮想マシンの仮想ディスクを暗号化することはできません。

4 必要に応じて、vSphere Client の [設定の編集] メニューから、仮想マシンまたは仮想マシンとディスクの両方を暗号化できます。

a 仮想マシンを右クリックし、[設定の編集] を選択します。

b [仮想マシン オプション] タブをクリックし、[暗号化] を開きます。暗号化ポリシーを選択します。すべてのディスクを選択解除した場合、仮想マシン ホームのみが暗号化されます。

c [OK] をクリックします。

暗号化された仮想マシンまたは仮想ディスクの復号化

ストレージ ポリシーを変更することで、仮想マシン、そのディスク、またはその両方を復号できます。

このタスクでは、vSphere Client を使用して暗号化された仮想マシンを復号化する方法について説明します。

暗号化されたすべての仮想マシンには、暗号化された vMotion が必要となります。仮想マシンの復号化中は、暗号化された vMotion の設定が維持されます。暗号化された vMotion が今後使用されないようにこの設定を変更するには、明示的に設定を変更してください。

このタスクでは、ストレージ ポリシーを使用して復号化を実行する方法について説明します。仮想ディスクの復号化には、[設定の編集] メニューを使用することもできます。

前提条件

- 仮想マシンが暗号化されていること。
- 仮想マシンがパワーオフ状態またはメンテナンス モードであること。
- 必要な権限：暗号化操作.暗号化解除

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 変更対象の仮想マシンを右クリックし、[仮想マシン ポリシー] - [仮想マシン ストレージ ポリシーの編集] を選択します。

仮想マシン ファイル（仮想マシン ホーム）のストレージ ポリシーと仮想ディスクのストレージ ポリシーを設定することができます。

3 ストレージ ポリシーを選択します。

- 仮想マシンとそのハード ディスクを復号するには、[ディスクごとに設定] をオフにして、ドロップダウン メニューからストレージ ポリシーを選択し、[OK] をクリックします。
- 仮想ディスクを復号し、仮想マシンは復号しない場合は、[ディスクごとに設定] をオンにして、仮想マシン ホームについては暗号化ストレージ ポリシーを選択し、仮想ディスクについては他のストレージ ポリシーを選択して、[OK] をクリックします。

仮想マシンのみを復号化し、ディスクだけを暗号化した状態にすることはできません。

4 必要に応じて、vSphere Client を使用して、[設定の編集] メニューから仮想マシンとディスクを復号することができます。

a 仮想マシンを右クリックし、[設定の編集] を選択します。

b [仮想マシン オプション] タブをクリックし、[暗号化] を展開します。

c 仮想マシンとそのハード ディスクを復号するには、[仮想マシンの暗号化] ドロップダウン メニューから [なし] を選択します。

d 仮想ディスクを復号し、仮想マシンは復号しない場合は、ディスクを選択解除します。

e [OK] をクリックします。

5 （オプション）[暗号化された vMotion] の設定を変更することができます。

a 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。

b [仮想マシン オプション] をクリックし、[暗号化] を開きます。

c [暗号化された vMotion] の値を設定します。

仮想ディスクの暗号化ポリシーの変更

暗号化された仮想マシンを vSphere Client から作成するとき、仮想マシンの作成中に追加する仮想ディスクのうちどれを暗号化するかを選択できます。暗号化された仮想ディスクは、[仮想マシン ストレージ ポリシーの編集]オプションを使用して復号化できます。

注： 暗号化された仮想マシンに暗号化されていない仮想ディスクを割り当てることはできます。一方、暗号化されていない仮想マシンに暗号化された仮想ディスクを割り当てることはできません。

仮想ディスクの暗号化を参照してください。

このタスクでは、ストレージ ポリシーを使用して暗号化ポリシーを変更する方法について説明します。この変更は、[設定の編集]メニューを使用して行うこともできます。

前提条件

- 暗号化操作.暗号化ポリシーの管理 権限が必要となります。
- 仮想マシンがパワーオフ状態であることを確認します。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 仮想マシンを右クリックし、[仮想マシン ポリシー] - [仮想マシン ストレージ ポリシーの編集] の順に選択します。

3 ストレージ ポリシーを変更します。

- 仮想マシンとそのハード ディスクのストレージ ポリシーを変更するには、暗号化ストレージ ポリシーを選択し、[OK] をクリックします。
- 仮想ディスクは暗号化せずに仮想マシンだけを暗号化するには、[ディスクごとに設定] で切り替えることにより、仮想マシン ホームについては暗号化ストレージ ポリシーを選択し、仮想ディスクについては他のストレージ ポリシーを選択して、[OK] をクリックします。

暗号化されていない仮想マシンの仮想ディスクを暗号化することはできません。

4 目的に応じて、[設定の編集] メニューからストレージ ポリシーを変更できます。

a 仮想マシンを右クリックし、[設定の編集] を選択します。

b [仮想ハードウェア] タブを選択してハード ディスクを展開し、ドロップダウン メニューから暗号化ポリシーを選択します。

c [OK] をクリックします。

キー紛失に関する問題の解決

ESXi ホストが vCenter Server から暗号化された仮想マシンまたは暗号化された仮想ディスクのキー (KEK) を取得できない場合、暗号化された仮想マシンはロックされます。キーを KMS で使用できるようにすると、ロックされている暗号化された仮想マシンをロック解除できます。

特定の状況下では、標準キー プロバイダの使用時に、ESXi ホストは vCenter Server から暗号化された仮想マシンまたは暗号化された仮想ディスクのキー暗号化キー (KEK) を取得できません。その場合でも、仮想マシンを登録解除または再ロードできます。ただし、他の仮想マシン操作（仮想マシンのパワーオンなど）を実行することはできません。必要なキーを KMS で使用できるようにするために必要な手順を実行した後、vSphere Client を使用して、ロックされている暗号化された仮想マシンをロック解除できます。

仮想マシン キーを使用できない場合は、vCenter Server アラームで通知され、仮想マシンの状態が無効と表示されます。仮想マシンはパワーオンできません。仮想マシン キーは利用できるものの、暗号化されたディスクのキーが利用できない場合、仮想マシンの状態が無効として表示されることはありません。ただし、仮想マシンをパワーオンすることはできず、次のエラーが発生します。

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

注： 以下の手順では、仮想マシンがロック状態になる状況、対応するアラームと記録されるイベント ログ、およびそれぞれのケースでの対処方法について説明します。

手順

1 vCenter Server システムと KMS との間の接続に問題がある場合は、vCenter Server で仮想マシン アラームが生成されます。また、エラー メッセージがイベント ログに表示されます。

KMS への接続をリストアします。KMS とキーが使用可能になったら、ロック状態の仮想マシンのロックを解除します。ロックされた仮想マシンのロック解除を参照してください。ホストを再起動し、接続を復旧した後に仮想マシンを再登録してロックを解除することもできます。

KMS への接続を失っても仮想マシンは自動的にロックされません。仮想マシンがロック状態になるのは、次の条件が満たされた場合だけです。

- キーが ESXi ホストで使用できない。
- vCenter Server が KMS からキーを取得できない。

ESXi ホストは、再起動のたびに、vCenter Server にアクセスできる必要があります。vCenter Server は、対応する ID を持つキーを KMS に要求し、ESXi で利用できるようにします。

注： vSphere 7.0 Update 2 以降では、ESXi を再起動すると暗号化キーを保持できます。キーの永続性の概要を参照してください。

キー プロバイダへの接続を復旧した後も仮想マシンがロック状態の場合は、ロックされた仮想マシンのロック解除 を参照してください。

2 接続が復旧したら、仮想マシンを登録します。エラーが発生した場合、または操作が正常に実行されても仮想マシンがロック状態である場合、vCenter Server システムに対し 暗号化操作.RegisterVM 権限があることを確認します。

キーが利用可能である場合に、暗号化された仮想マシンをパワーオンするだけなら、この権限は必要ありません。キーを取得する必要がある場合に、仮想マシンを登録するためには、この権限が必要です。

3 キーが KMS で使用できなくなった場合、vCenter Server で仮想マシン アラームが生成されます。また、エラー メッセージがイベント ログに表示されます。

キーの復元を KMS 管理者に依頼します。キーが無効になる可能性があるのは、既にインベントリから削除されて長い間登録されていない仮想マシンをパワーオンする場合です。また、ESXi ホストを再起動したときに KMS が利用できない場合にも、この状況が発生します。

a 管理対象オブジェクト ブラウザ (MOB) または vSphere API を使用してキー ID を取得します。

`VirtualMachine.config.keyId.keyId` から `keyId` を取得します。

b キー ID に関連付けられているキーを再度有効にするよう KMS 管理者に依頼します。

c キーを復元したら、ロックされた仮想マシンのロック解除を参照してください。

KMS でキーを復元できる場合、vCenter Server は、そのキーを取得し、次回必要になったときに、ESXi ホストにプッシュします。

4 KMS が利用可能で、かつ ESXi ホストがパワーオン状態であるにもかかわらず、vCenter Server システムが利用できない場合は、次の手順に従って仮想マシンのロックを解除します。

a vCenter Server システムをリストアするか、または別の vCenter Server システムを設定した後、KMS との信頼を確立します。

使用しているキー プロバイダ名は同じにする必要がありますが、KMS の IP アドレスは異なっていてもかまいません。

b ロックされているすべての仮想マシンを再登録します。

新しい vCenter Server インスタンスが KMS からキーを取得し、仮想マシンのロックが解除されます。

5 キーが ESXi ホスト上でのみ見つからない場合は、vCenter Server で仮想マシン アラームが生成され、イベント ログに次のメッセージが記録されます。

ホストにキーが見つからないため、仮想マシンはロックされています。

vCenter Server システムは、見つからないキーをキー プロバイダから取得できます。手動によるキーのリカバリは必要ありません。ロックされた仮想マシンのロック解除を参照してください。

ロックされた仮想マシンのロック解除

vCenter Server アラームは、暗号化された仮想マシンがロック状態であることを通知します。暗号化された仮想マシンがロックされているとき、ロックを解除するには、必要なキーを使用できるようにするために必要な手順を KMS で実行してから、vSphere Client（HTML5 ベースのクライアント）を使用します。

前提条件

- 必要な権限（暗号化操作.RegisterVM）があることを確認します。

- ホストの暗号化を有効にするなど、オプションのタスクに必要なその他の権限が必要になる可能性があります。
- ロックされている仮想マシンのロックを解除する前に、ロックの原因をトラブルシューティングし、手動で問題を解決するように試みてください。キー紛失に関する問題の解決を参照してください。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 仮想マシンの [サマリ] タブに移動します。

仮想マシンがロックされると、仮想マシンがロックされているというアラームが表示されます。

3 アラームを確認するか、今はアラームを緑にリセットするだけで仮想マシンのロックを解除しないかを決定します。

[確認] または [緑にリセット] をクリックすると、アラームは停止しますが、仮想マシンはロックを解除するまでロックされたままです。

4 仮想マシンの [監視] タブに移動し、[イベント] をクリックして、仮想マシンがロックされている理由に関する詳細を取得します。

5 仮想マシンのロックを解除する前に、推奨されるトラブルシューティングを実行します。

6 仮想マシンの [サマリ] タブに移動し、仮想マシン コンソールの下にある [仮想マシンのロック解除] をクリックします。

暗号化キー データがホストに転送されることを警告するメッセージが表示されます。

7 [はい] をクリックします。

ESXi ホストの暗号化モードの問題の解決

特定の状況において、ESXi ホストの暗号化モードが無効になることがあります。

ESXi ホストでは、暗号化された仮想マシンが含まれている場合にホスト暗号化モードを有効にする必要があります。ホスト キーがないことをホストが検出した場合、またはキー プロバイダを使用できない場合、ホストが暗号化モードを有効にできないことがあります。ホスト暗号化モードを有効にできないとき、vCenter Server はアラームを生成します。

手順

1 vCenter Server システムとキー プロバイダ間の接続に問題がある場合は、アラームが生成され、イベント ログにエラー メッセージが記録されます。

問題となっている暗号化キーを含むキー プロバイダへの接続をリストアする必要があります。

2 キーが見つからない場合は、アラームが生成され、イベント ログにエラー メッセージが記録されます。

キーがキー プロバイダ内にあることを確認する必要があります。バックアップからの リストアの詳細については、キー管理ベンダーのドキュメントを参照してください。

次のステップ

キー プロバイダへの接続を復旧した後またはキー プロバイダにキーを手動で復元した後もホスト暗号化モードが無効な場合は、ホスト暗号化モードを再度有効にします。ESXi ホストの暗号化モードの再有効化を参照してください。

ESXi ホストの暗号化モードの再有効化

vSphere 6.7 以降では、ESXi ホストの暗号化モードが無効になると vCenter Server のアラームで通知されます。ホスト暗号化モードが無効な場合は、再度有効にできます。

前提条件

- 次の必要な権限があることを確認します。暗号化操作.ホストの登録
- 暗号化モードを再度有効にする前に、原因のトラブルシューティングを行い、手動で問題を解決してください。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. ESXi ホストの [概要] タブに移動します。

   暗号化モードが無効になると、[ホストの暗号化モードを有効にする必要があります] アラームが表示されます。
3. アラームを確認するか、アラームを緑色にリセットする一方で現状ではホスト暗号化モードを再び有効にしないか、どちらかを選択します。

   [確認] または [緑にリセット] をクリックするとアラームは消えますが、ホストの暗号化モードは再度有効にするまで無効のままになります。
4. ESXi ホストの [監視] タブに移動し、[イベント] をクリックして、暗号化モードが無効な理由の詳細情報を表示します。

   暗号化モードを再度有効にする前に、推奨されるトラブルシューティングを実行します。
5. [概要] タブで [ホストの暗号化モードを有効にする] をクリックして、ホストの暗号化を再度有効にします。

   暗号化キー データがホストに転送されることを警告するメッセージが表示されます。
6. [はい] をクリックします。

キー管理サーバ証明書の有効期限しきい値の設定

デフォルトでは、キー管理サーバ (KMS) 証明書の期限が切れる 30 日前に vCenter Server から通知されます。このデフォルト値は変更できます。

KMS 証明書には有効期限があります。有効期限のしきい値に達すると、アラームで通知されます。

vCenter Server とキー プロバイダは、サーバおよびクライアントの 2 つのタイプの証明書を交換します。vCenter Server システムの VMware Endpoint Certificate Store (VECS) は、サーバ証明書と、キー プロバイダごとに 1 つのクライアント証明書を保存します。証明書には 2 つのタイプがあるため、証明書タイプごとに 2 つのアラーム（クライアント用とサーバ用）があります。

手順

1 vSphere Client を使用して、vCenter Server システムにログインします。

2 オブジェクト階層で、vCenter Server システムを選択します。

3 [構成] をクリックします。

4 [設定] で、[詳細設定] をクリックし、[設定の編集] をクリックします。

5 [フィルタ] アイコンをクリックして「`vpxd.kmscert.threshold`」と入力するか、構成パラメータ自体が表示されるまでスクロールします。

6 日数の値を入力し、[保存] をクリックします。

vSphere 仮想マシンの暗号化とコア ダンプ

vSphere 仮想マシンの暗号化を使用している環境で ESXi ホストのエラーが発生すると、その結果として出力されるコア ダンプは、ユーザーのデータを保護するために暗号化されます。vm-support パッケージに含まれるコア ダンプも暗号化されます。

注： コア ダンプには機密情報が含まれることがあります。コア ダンプを使用する際は、組織のデータ セキュリティおよびプライバシーに関するポリシーに従ってください。

ESXi ホスト上のコア ダンプ

ESXi ホスト、ユーザー ワールド、または仮想マシンで障害が発生すると、コア ダンプが生成され、ホストは再起動します。ESXi ホストの暗号化モードが有効になっている場合、このコア ダンプは ESXi キー キャッシュ内にあるキーを使用して暗号化されます。このキーは、KMS から取得されます。背景情報については、vSphere 仮想マシンの暗号化で環境を保護する方法を参照してください。

ESXi ホストが暗号的な意味で「安全」なときにコア ダンプが生成されると、イベントが作成されます。このイベントにより、コア ダンプが発生したこと、および次の情報が示されます。ワールド名、発生時刻、コア ダンプの暗号化に使用されたキーの keyID、コア ダンプ ファイル名。イベントは、vCenter Server の [タスクとイベント] のイベント ビューアで確認できます。

次の表に、各 vSphere リリースで使用される暗号化キーをコア ダンプの種類ごとに示します。

表 10-1. コア ダンプの暗号化キー

コア ダンプの種類	暗号化キー (ESXi 6.5)	暗号化キー（ESXi 6.7 以降）
ESXi カーネル	ホスト キー	ホスト キー
ユーザー ワールド (hostd)	ホスト キー	ホスト キー
暗号化された仮想マシン (VM)	ホスト キー	仮想マシン キー

ESXi ホストの再起動後に実行できることは、いくつかの要素によって決まります。

- ほとんどの場合、vCenter Server はホストのキーを KMS から取得し、そのキーを再起動後の ESXi ホストにプッシュしようと試みます。この操作が成功すると、vm-support パッケージを生成でき、コア ダンプを復号化または再暗号化できます。暗号化されたコア ダンプの復号または再暗号化を参照してください。

- vCenter Server から ESXi ホストに接続できない場合、KMS からキーを取得できる可能性があります。キー紛失に関する問題の解決を参照してください。
- ホストでカスタム キーを使用していた場合、そのキーが vCenter Server からホストにプッシュされたキーと異なると、コア ダンプを操作できません。カスタム キーの使用は避けてください。

コア ダンプと vm-support パッケージ

深刻なエラーが発生し、VMware テクニカル サポートに連絡すると、サポート担当者は通常、vm-support パッケージを生成するように要請します。このパッケージには、ログ ファイルのほか、コア ダンプなどの情報が含まれます。サポート担当者がログ ファイルやその他の情報を調べても問題を解決できない場合、コア ダンプを復号化して、必要な情報を参照できるようにすることを要請する可能性があります。キーなどの機密情報を保護するために、組織のセキュリティおよびプライバシー ポリシーを守ってください。暗号化を使用する ESXi ホストにある vm-support パッケージの収集を参照してください。

vCenter Server システム上のコア ダンプ

vCenter Server システム上のコア ダンプは、暗号化されていません。vCenter Server にはすでに、機密である可能性のある情報が存在します。少なくとも、vCenter Server が保護されていることを確認します。4 章 vCenter Server システムのセキュリティを参照してください。また、vCenter Server システムのコア ダンプを無効にすることも考えられます。ログ ファイル内のその他の情報によって問題を解決できる可能性があります。

暗号化を使用する ESXi ホストにある vm-support パッケージの収集

ESXi ホストでホスト暗号化モードが有効になっている場合、`vm-support` パッケージのコア ダンプはすべて暗号化されます。vSphere Client からパッケージを収集し、後でコア ダンプを復号する必要がある場合は、パスワードを指定できます。

`vm-support` パッケージにはログ ファイルやコア ダンプ ファイルなどが含まれています。

前提条件

ESXi ホストでホスト暗号化モードが有効になっていることをサポート担当者に伝えてください。サポート担当者から、コア ダンプを復号して必要な情報を抽出するように依頼される場合がありますが、

注: コア ダンプには機密情報が含まれている可能性があります。組織のセキュリティ ポリシーおよびプライバシー ポリシーに従ってホスト キーなどの機密情報を保護してください。

手順

1. vSphere Client を使用して、vCenter Server システムにログインします。
2. [ホストおよびクラスタ] をクリックし、ESXi ホストを右クリックします。
3. [システム ログのエクスポート] を選択します。
4. ダイアログ ボックスで [暗号化されたコア ダンプ用のパスワード] を選択し、パスワードを入力して、確認のために再度パスワードを入力します。
5. その他のオプションはデフォルトのままにしておきます。VMware テクニカル サポートから依頼された場合は、変更を加えて、[ログのエクスポート] をクリックします。

6 ファイルの場所を指定します。

7 vm-support パッケージ内のコア ダンプを復号するようにサポート担当者から依頼された場合は、いずれかの ESXi ホストにログインして次の手順に従います。

a ESXi にログインし、vm-support パッケージが配置されているディレクトリに接続します。

ファイル名は esx.<日時>.tgz という形式になっています。

b ディレクトリにパッケージを解凍できるだけの空き容量があることを確認し、パッケージを解凍し、パッケージを再圧縮するか移動します。

c パッケージをローカル ディレクトリに抽出します。

```
vm-support -x *.tgz .
```

抽出されたファイル階層には、ESXi ホストのコア ダンプ ファイル（通常は /var/core にあります）と、仮想マシンの複数のコア ダンプ ファイルが含まれている場合があります。

d 暗号化されたコア ダンプ ファイルを個別に復号します。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

vm-support-incident-key-file の部分では、ディレクトリの最上位レベルにあるインシデント キー ファイルを指定します。

encryptedZdump の部分では、暗号化されたコア ダンプ ファイルの名前を指定します。

decryptedZdump の部分では、コマンド実行後に生成されるファイルの名前を指定します。*encryptedZdump* で指定するファイル名に似た名前を使用してください。

e vm-support パッケージの作成時に使用したパスワードを入力します。

f 暗号化されたコア ダンプを削除し、パッケージを再び圧縮します。

```
vm-support --reconstruct
```

8 機密情報を含むファイルがある場合は、それらのファイルも削除します。

暗号化されたコア ダンプの復号または再暗号化

ESXi ホスト上で暗号化されているコア ダンプは crypto-util CLI を使用して復号化または再暗号化できます。

vm-support パッケージに含まれるコア ダンプは手動で復号化できます。コア ダンプには機密情報が含まれることがあります。組織のセキュリティ ポリシーとプライバシー ポリシーに基づき、キーなどの機密情報を保護してください。

コア ダンプの再暗号化と crypto-util のその他の機能の詳細については、コマンドライン ヘルプを参照してください。

注： crypto-util は上級ユーザー向けのコマンドです。

前提条件

コア ダンプの暗号化に使用されたキーが、コア ダンプを生成した ESXi ホストで使用可能であることが必要です。

手順

1 コア ダンプが存在する ESXi ホストに直接ログインします。

ESXi ホストがロックダウン モードになっている場合や、SSH アクセスが無効になっている場合は、最初にアクセスを有効にしなければならない場合があります。

2 コア ダンプが暗号化されているかどうかを確認します。

オプション	説明
コア ダンプの監視	`crypto-util envelope describe vmmcores.ve`
zdump ファイル	`crypto-util envelope describe --offset 4096 zdumpFile`

3 種類に応じてコア ダンプを復号化します。

オプション	説明
コア ダンプの監視	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump ファイル	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

ESXi ホストでのキーの永続性の有効化および無効化

ESXi ホストでキーの永続性を有効にする必要があります。デフォルトでは、有効になっていません。

キーの永続性に関する概念情報については、キーの永続性の概要を参照してください。

前提条件

キーの永続性を有効にするための要件：

- ESXi 7.0 Update 2 以降
- ESXi ホストが TPM 2.0 を使用してインストールされている
- ESXCLI コマンド セットにアクセス可能であること。ESXCLI コマンドはリモートで実行することも、ESXi Shell で実行することもできます。

注： vSphere Native Key Provider を使用する場合、キーの永続性は必要ありません。vSphere Native Key Provider は、キー サーバにアクセスしなくても実行できるように、特別な設定が不要な設計になっています。

セキュリティを強化するため、TPM はシーリング ポリシーを使用して ESXi ホストの起動中の改ざんを防ぐこともできます。TPM シーリング ポリシーの概要を参照してください。

手順

1 SSH などのリモート コンソール接続を使用して、ESXi ホストでセッションを開始します。

2 root としてログインします。

3 キーの永続性を有効または無効にします。

a キーの永続性を有効にするには、次の手順を実行します。

```
esxcli system security keypersistence enable
```

b 永続性を無効にするには、次の手順を実行します。

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

vSphere Client を使用した暗号化された仮想マシンの再キー化

vSphere Client を使用して、暗号化された仮想マシンの再キー化（表層）を実行できます。ビジネスまたはコンプライアンス上の理由で、暗号化された仮想マシンの再キー化を実行する場合があります。

再キー化（表層）または再キー化（別名、再暗号化（表層））を使用すると、暗号化された仮想マシンで新しい（異なる）キー暗号化キー (KEK) を使用できます。再キー化操作は仮想マシンがパワーオン状態のときに実行できます。仮想マシンにスナップショットがある場合も、再キー化を実行できます。スナップショットが作成済みの暗号化された仮想マシンの再キー化は、単一のスナップショット分岐（ディスク チェーン）に対してのみ許可されます。複数のスナップショット分岐はサポートされていません。チェーン内のすべてのリンクを新しい KEK で更新する前に再キー化が失敗した場合でも、古い KEK と新しい KEK があれば暗号化された仮想マシンにアクセスできます。

前提条件

必要な権限：暗号化操作.キー サーバの管理

手順

1 vSphere Client で vCenter Server にログインします。

2 インベントリ リストを参照して、暗号化された仮想マシンを選択します。

3 暗号化された仮想マシンを右クリックし、[仮想マシン ポリシー] を選択します。

4 [再暗号化] を選択します。

5 [はい] をクリックします。

暗号化された仮想マシンが新しい KEK で再キー化されます。

注： 再キー化に失敗すると、イベント サブシステムから次のイベントがポストされます。

```
com.vmware.vc.vm.crypto.RekeyFail
```

仮想 Trusted Platform Module を使用する仮想マシンの保護

11

仮想 Trusted Platform Module (vTPM) 機能を使用して、仮想マシンに TPM 2.0 仮想暗号化プロセッサを追加できます。

vTPM は、物理的な Trusted Platform Module 2.0 チップをソフトウェアにしたものです。vTPM は、他のすべての仮想デバイスと同様に動作します。仮想マシンへの vTPM の追加は、仮想 CPU、メモリ、ディスク コントローラ、ネットワーク コントローラを追加する場合と同じように実行できます。vTPM には、ハードウェアとしての Trusted Platform Module チップは不要です。

この章には、次のトピックが含まれています。

仮想 Trusted Platform Module の概要

仮想 Trusted Platform Module (vTPM) は、物理的な Trusted Platform Module 2.0 チップをソフトウェアにしたものです。vTPM は、他のすべての仮想デバイスと同様に動作します。

vTPM ついて

vTPM は、ランダムな番号の生成、証明、キーの生成など、ハードウェア ベースのセキュリティ関連の機能を提供します。vTPM を仮想マシンに追加すると、ゲスト OS はプライベート キーを作成して、保管できるようになります。これらのキーは、ゲスト OS 自体には公開されません。そのため、仮想マシン攻撃の対象領域が狭められます。通常、ゲスト OS の侵害が起きると機密情報が侵害されますが、ゲスト OS で vTPM を有効にしておくと、このリスクを大幅に低減できます。これらのキーは、ゲスト OS が暗号化または署名の目的にのみ使用できます。アタッチされた vTPM を使用することで、クライアントは仮想マシンの ID をリモートで認証し、実行中のソフトウェアを確認できます。

vTPM は、新しい仮想マシンと既存の仮想マシンのどちらにも追加できます。vTPM は、TPM の重要なデータを保護するために仮想マシン暗号化に依存します。vTPM を構成すると、仮想マシン ファイルは暗号化されますが、ディスクは暗号化されません。仮想マシンとそのディスクの暗号化は、明示的に追加できます。

vTPM を有効にした仮想マシンをバックアップする場合、バックアップには `*.nvram` ファイルを含むすべての仮想マシン データが含まれる必要があります。バックアップに `*.nvram` ファイルが含まれていない場合、vTPM で仮想マシンをリストアすることはできません。また、vTPM が有効になっている仮想マシンの仮想マシン ホーム ファイルは暗号化されるため、リストア時に暗号化キーが使用できることを確認します。

vTPM を利用する場合、ESXi ホストに物理的な Trusted Platform Module (TPM) 2.0 チップは不要です。ただし、ホスト証明を実行する場合は、TPM 2.0 物理チップなどの外部のエンティティが必要です。Trusted Platform Module による ESXi ホストの保護を参照してください。

注： デフォルトでは、vTPM が有効になっている仮想マシンにストレージ ポリシーは関連付けられていません。仮想マシン ファイル（仮想マシン ホーム）のみが暗号化されます。仮想マシンとそのディスクの暗号化を明示的に追加することもできますが、仮想マシン ファイルはすでに暗号化されています。

vTPM での vSphere の要件

vTPM を使用するには、vSphere 環境が以下の要件を満たす必要があります。

- 仮想マシンの要件：
  - EFI ファームウェア
  - ハードウェア バージョン 14 以降
- コンポーネントの要件：
  - vCenter Server 6.7 以降 (Windows 仮想マシンの場合)、vCenter Server 7.0 Update 2 以降 (Linux 仮想マシンの場合)。
  - 仮想マシン暗号化（仮想マシン ホーム ファイルを暗号化するため）。
  - vCenter Server に構成されたキー プロバイダ。vSphere キー プロバイダの比較を参照してください。
- ゲスト OS のサポート：
  - Linux
  - Windows Server 2008 以降
  - Windows 7 以降

ハードウェア TPM と仮想 TPM の違い

ハードウェアの Trusted Platform Module (TPM) は、認証情報やキーのセキュアなストレージを提供するために使用されます。vTPM では TPM と同じ機能が実行されますが、実行される内容はソフトウェアによる暗号化コプロセッサ機能です。vTPM では、仮想マシン暗号化を使用して暗号化された `.nvram` ファイルがセキュアなストレージとして使用されます。

ハードウェア TPM には、承認キー (EK) と呼ばれる事前ロードされたキーが含まれます。EK には、プライベート キーとパブリック キーが含まれます。EK は、TPM に一意の ID を提供します。vTPM の場合、このキーは VMware 認証局 (VMCA) またはサードパーティの認証局 (CA) によって提供されます。vTPM がキーを使用した後、通常は変更されません。これは、変更すると vTPM に保存されている機密情報が無効になるためです。vTPM からサードパーティの CA にアクセスすることはありません。

仮想 Trusted Platform Module を使用した仮想マシンの作成

仮想マシンを作成するときに仮想 Trusted Platform Module (vTPM) を追加することで、ゲスト OS のセキュリティを強化することができます。vTPM を追加する前にキー プロバイダを作成する必要があります。

VMware の仮想 TPM は TPM 2.0 と互換性があり、仮想マシンおよびホストされているゲスト OS で使用される、TPM が有効な仮想チップを作成します。

前提条件

- vSphere 環境がキー プロバイダを使用して構成されていることを確認します。詳細については、次のセクションを参照してください。
  - vSphere 信頼機関 の設定
  - 7 章 標準キー プロバイダの構成と管理
  - 8 章 vSphere Native Key Provider の構成と管理
- 使用できるゲスト OS は、Windows Server 2008 以降、Windows 7 以降、または Linux です。
- 環境内で実行されている ESXi ホストは、ESXi 6.7 以降（Windows ゲスト OS の場合）または 7.0 Update 2（Linux ゲスト OS の場合）である必要があります。
- 仮想マシンで EFI ファームウェアを使用する必要があります。
- 次の必要な権限があることを確認します。
  - 暗号化操作.クローン作成
  - 暗号化操作.暗号化
  - 暗号化操作.新規暗号化
  - 暗号化操作.移行
  - 暗号化操作.仮想マシンの登録

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 オブジェクトを右クリックして [新規仮想マシン] を選択し、表示される画面に沿って仮想マシンを作成します。

オプション	操作
作成タイプの選択	新しい仮想マシンを作成します。
名前とフォルダの選択	名前とターゲットの場所を指定します。
コンピューティング リソースの選択	仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。暗号化タスクの前提条件と必要な権限を参照してください。
ストレージの選択	互換データストアを選択します。
互換性の選択	Windows ゲスト OS の場合は [ESXi 6.7 以降]、Linux ゲスト OS の場合は [ESXi 7.0 U2] 以降を選択する必要があります。
ゲスト OS を選択	使用するゲスト OS には、Windows または Linux を選択します。
ハードウェアのカスタマイズ	[新規デバイスを追加] をクリックして、[Trusted Platform Module] を選択します。 ディスク サイズや CPU を変更するなどしてハードウェアをさらにカスタマイズできます。
設定の確認	情報を確認し、[終了] をクリックします。

結果

vTPM が有効な仮想マシンが、指定のとおりインベントリに表示されます。

仮想 Trusted Platform Module の既存の仮想マシンでの有効化

既存の仮想マシンに仮想 Trusted Platform Module (vTPM) を追加して、ゲスト OS のセキュリティを強化を提供することができます。vTPM を追加する前にキー プロバイダを作成する必要があります。

VMware の仮想 TPM は TPM 2.0 と互換性があり、仮想マシンおよびホストされているゲスト OS で使用される、TPM が有効な仮想チップを作成します。

前提条件

- vSphere 環境がキー プロバイダを使用して構成されていることを確認します。詳細については、次のセクションを参照してください。
  - vSphere 信頼機関 の設定
  - 7 章 標準キー プロバイダの構成と管理
  - 8 章 vSphere Native Key Provider の構成と管理
- 使用できるゲスト OS は、Windows Server 2008 以降、Windows 7 以降、または Linux です。
- 仮想マシンがオフであることを確認します。
- 環境内で実行されている ESXi ホストは、ESXi 6.7 以降（Windows ゲスト OS の場合）または 7.0 Update 2（Linux ゲスト OS の場合）である必要があります。
- 仮想マシンで EFI ファームウェアを使用する必要があります。
- 次の必要な権限があることを確認します。
  - 暗号化操作.クローン作成

- 暗号化操作.暗号化
- 暗号化操作.新規暗号化
- 暗号化操作.移行
- 暗号化操作.仮想マシンの登録

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。

3 [設定の編集] ダイアログ ボックスで、[新規デバイスを追加] をクリックし、[Trusted Platform Module] を選択します。

4 [OK] をクリックします。

これで、仮想マシンの [サマリ] タブを表示すると、[仮想マシンのハードウェア] ペインに仮想 Trusted Platform Module が含まれるようになります。

仮想マシンからの仮想 Trusted Platform Module の削除

仮想マシンから仮想 Trusted Platform Module (vTPM) セキュリティを削除することができます。

vTPM デバイスを削除すると、仮想マシン上の暗号化された情報がすべてリカバリ不能になります。仮想マシンから vTPM を削除する前に、BitLocker など、vTPM デバイスを使用するゲスト OS 内のアプリケーションをすべて無効にします。この操作に失敗すると、仮想マシンが起動しない可能性があります。また、スナップショットが含まれている仮想マシンから vTPM を削除することはできません。

前提条件

- 仮想マシンがパワーオフ状態であることを確認します。
- 次の必要な権限があることを確認します。暗号化操作.復号化

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリで、変更する仮想マシンを右クリックして、[設定の編集] を選択します。

3 [設定の編集] ダイアログ ボックスの [仮想ハードウェア] タブで、Trusted Platform Module のエントリを見つけます。

4 デバイス上にポインタを移動し、[削除] アイコンをクリックします。

このアイコンは、安全に削除できる仮想ハードウェアに対してのみ表示されます。

5 [削除] をクリックして、デバイスを削除することを確認します。

vTPM デバイスが削除対象としてマークされます。

6 [OK] をクリックします。

仮想 Trusted Platform Module エントリが、[仮想マシンのハードウェア] ペインにある仮想マシンの [サマリ] タブに表示されなくなったことを確認します。

Virtual Trusted Platform Module 対応の仮想マシンの特定

Virtual Trusted Platform Module (vTPM) を使用できる仮想マシンを特定することができます。

インベントリ内のすべての仮想マシンのリストを生成して、仮想マシン名、オペレーティング システム、vTPM ステータスを表示できます。コンプライアンス監査で使用するため、このリストを CSV ファイルにエクスポートすることもできます。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 vCenter Server インスタンス、ホスト、クラスタのいずれかを選択します。

3 [仮想マシン] タブ > [仮想マシン] の順にクリックします。

4 TPM が有効になっているすべての仮想マシンを表示するには、左下隅にある 3 バーの [列セレクタ] をクリックし、[TPM] を選択します。

TPM が有効になっている仮想マシンは、TPM 列に「あり」と表示されます。TPM が有効でない仮想マシンは、「なし」と表示されます。

5 インベントリのリスト ビューの内容を CSV ファイルにエクスポートできます。

a リスト ビューの右下隅にある [エクスポート] をクリックします。

[リスト内容のエクスポート] ダイアログ ボックスが開き、CSV ファイルに含めることが可能なオプションが一覧表示されます。

b CSV ファイルに、すべての行または現在選択している行のどちらを含めるか選択します。

c オプションの中から、CSV ファイルにリストする列を選択します。

d [エクスポート] をクリックします。

CSV ファイルが生成され、ダウンロードできるようになります。

仮想 Trusted Platform Module デバイス証明書の表示

Virtual Trusted Platform Module (vTPM) デバイスにはデフォルトの証明書が事前設定されており、確認することができます。

前提条件

vTPM に対応した仮想マシンが環境内に必要です。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 [仮想マシン] > [仮想マシン] の順にクリックします。

4 証明書情報を表示する、vTPM が有効な仮想マシンを選択します。

必要に応じて、左下隅にある 3 バーの [列セレクタ] をクリックし、[TPM] を選択して、TPM が「あり」の仮想マシンを表示します。

5 [設定] タブをクリックします。

6 [TPM] の下で [証明書] を選択します。

7 証明書を選択し、その情報を表示します。

8 （オプション）証明書情報をエクスポートするには、[エクスポート] をクリックします。

証明書がディスクに保存されます。

次のステップ

デフォルトの証明書を、サード パーティの認証局 (CA) によって発行された証明書で置き換えることができます。仮想 Trusted Platform Module デバイス証明書のエクスポートと置き換えを参照してください。

仮想 Trusted Platform Module デバイス証明書のエクスポートと置き換え

仮想 Trusted Platform Module (vTPM) デバイスに付属するデフォルトの証明書を置き換えることができます。

前提条件

vTPM に対応した仮想マシンが環境内に必要です。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 証明書情報を置き換えるインベントリで、TPM に対応した仮想マシンを選択します。

4 [設定] タブをクリックします。

5 [TPM] の下で [署名要求] を選択します。

6 証明書を選択します。

7 証明書情報をエクスポートするには、[エクスポート] をクリックします。

証明書がディスクに保存されます。

8 エクスポートした証明書署名リクエスト (CSR) に対し、サードパーティの認証局 (CA) によって発行された証明書を取得します。

使用中の IT 環境に保存されている任意のテスト CA を使用できます。

9 新しい証明書がある場合は、既存の証明書を置き換えます。

a インベントリで、証明書を置き換える仮想マシンを右クリックして、[設定の編集] を選択します。

b [設定の編集] ダイアログ ボックスで、[セキュリティ デバイス] を展開し、次に [Trusted Platform Module] を展開します。

証明書が表示されます。

c 置き換える証明書の [置き換え] をクリックします。

[ファイルのアップロード] ダイアログ ボックスが表示されます。

d ローカル マシンで新しい証明書を見つけ、これをアップロードします。

新しい証明書によって、vTPM デバイスに付属するデフォルトの証明書が置き換えられます。

e 仮想マシンの [サマリ] タブで、[仮想 Trusted Platform Module] リストに記載された証明書の名前が更新されます。

仮想化ベース セキュリティによる Windows ゲスト OS の保護

12

vSphere 6.7 以降、Microsoft の仮想化ベース セキュリティ (VBS) がサポートされている Windows ゲスト OS では、これを有効にすることができます。

Microsoft VBS は、Windows 10 および Windows Server 2016 オペレーティング システムの機能の 1 つで、ハードウェアおよびソフトウェア仮想化を使用することにより、隔離され、ハイパーバイザーで制限された特別なサブシステムを作成して、システム セキュリティを強化します。

VBS では、以下の Windows セキュリティ機能を使用して、システムを強化し、システムの重要部分およびユーザーの秘密情報が侵害されないように隔離します。

- Credential Guard：システムの重要部分およびユーザーの秘密情報を隔離し、侵害されないように保護することを目的とします。
- Device Guard：マルウェアが Windows システム上で実行されることを予防および阻止するために、連携して動作するように設計された一連の機能を提供します。
- 構成可能なコードの整合性：ブートローダーから信頼済みコードのみが実行できるようにします。

詳細については、Microsoft のドキュメントで仮想化ベース セキュリティのトピックを参照してください。

vCenter Server から仮想マシンで VBS を有効にしたあと、Windows ゲスト OS 内で VBS を有効にします。

この章には、次のトピックが含まれています。

仮想化ベース セキュリティのベスト プラクティス

Windows ゲスト OS 環境のセキュリティと管理性を最大にするには、仮想化ベースのセキュリティ (VBS) のベスト プラクティスを遵守してください。

これらのベスト プラクティスを遵守することで、次の問題を回避できます。

仮想化ベースのセキュリティ ハードウェア

仮想化ベースのセキュリティには次のハードウェアを使用します。

- Intel 社
  - Haswell CPU 以降。最適なパフォーマンスを実現するには、Skylake-EP CPU 以降を使用します。
  - Ivy Bridge CPU が許容されます。
  - Sandy Bridge CPU では、パフォーマンスが低下する可能性があります。
- AMD 社
  - Zen 2 シリーズ CPU (Rome) 以降。
  - 古い CPU を使用すると、パフォーマンスが低下することがあります。

VBS が使用中の場合に、ページ サイズ変更に伴う Intel CPU の脆弱性に対するマシン チェックの例外を緩和すると、ゲスト OS のパフォーマンスが低下する可能性があります。詳細については、VMware ナレッジベースの記事 (https://kb.vmware.com/kb/76050) を参照してください。

Windows ゲスト OS の互換性

Intel の場合、VBS は Windows 10 および Windows Server 2016 以降の仮想マシンでサポートされていますが、Windows Server 2016 バージョンの 1607 および 1703 にはパッチが必要です。ESXi ホストのハードウェア互換性については、Microsoft 社のドキュメントを確認してください。VBS に Intel CPU を使用するには、vSphere 6.7 以降およびハードウェア バージョン 14 が必要です。

AMD の場合、VBS は Windows 10 バージョン 1809、および Windows 2019 以降の仮想マシンでサポートされています。VBS に AMD CPU を使用するには、vSphere 7.0 Update 2 以降およびハードウェア バージョン 19 が必要です。

当初、Windows 10 では、VBS の使用には Hyper-V の有効化が必要でした。現在、Hyper-V の有効化は Windows 10 で不要になりました。これは、Windows Server 2016 以降にも該当します。詳細については、現在の Microsoft のドキュメントおよび「VMware vSphere リリース ノート」を参照してください。

VBS でサポートされていない VMware の機能

VBS を有効にすると、仮想マシンで次の機能はサポートされません。

- フォールト トレランス
- PCI パススルー
- CPU またはメモリのホット アド

仮想化ベースのセキュリティに関するインストールとアップグレードの注意事項

仮想化ベースのセキュリティを設定する前に、インストールとアップグレードに関する次の注意事項をよくお読みください。

- 仮想ハードウェア バージョン 14 未満で Windows 10 および Windows Server 2016 以降用に構成された新規仮想マシンは、デフォルトでレガシー BIOS を使用して作成されます。ゲスト OS を再インストールする前に、仮想マシンのファームウェア タイプをレガシーの BIOS から UEFI に変更する必要があります。
- 以前の vSphere リリースから vSphere 6.7 以降に仮想マシンを移行し、その仮想マシンで仮想化ベースのセキュリティを有効にする場合は、UEFI を使用することで、オペレーティング システムの再インストールを回避できます。

仮想マシンでの仮想化ベースのセキュリティの有効化

仮想マシンを作成するときに、サポート対象の Windows ゲスト OS で Microsoft の仮想化ベースのセキュリティ (VBS) を有効にできます。

VBS を有効にするプロセスでは、まず仮想マシンで VBS を有効にしてから、Windows ゲスト OS で VBS を有効にします。

前提条件

許容可能な CPU については、仮想化ベース 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。

VBS に Intel CPU を使用するには、vSphere 6.7 以降が必要です。ハードウェア バージョン 14 以降および次のサポート対象ゲスト OS のいずれかを使用する仮想マシンを作成します。

- Windows 10（64 ビット）以降のリリース
- Windows Server 2016（64 ビット）以降のリリース

VBS に AMD CPU を使用するには、vSphere 7.0 Update 2 以降が必要です。ハードウェア バージョン 19 以降および次のサポート対象ゲスト OS のいずれかを使用する仮想マシンを作成します。

- Windows 10（64 ビット）、バージョン 1809 以降のリリース
- Windows Server 2019（64 ビット）以降のリリース

VBS を有効にする前に、Windows 10 バージョン 1809、および Windows Server 2019 の最新のパッチをインストールしてください。

手順

1. vCenter Server に vSphere Client を使用して接続します。
2. インベントリ内のオブジェクトから、仮想マシンの有効な親オブジェクト、例えば ESXi ホストまたはクラスタを選択します。

3 オブジェクトを右クリックして [新規仮想マシン] を選択し、表示される画面に沿って仮想マシンを作成します。

オプション	操作
作成タイプの選択	仮想マシンを作成します。
名前とフォルダの選択	名前とターゲットの場所を指定します。
コンピューティング リソースの選択	仮想マシンを自分の権限で作成することのできるオブジェクトを指定します。
ストレージの選択	仮想マシン ストレージ ポリシーでストレージ ポリシーを選択します。互換データストアを選択します。
互換性の選択	Intel CPU：[ESXi 6.7 以降] が選択されていることを確認します。 AMD CPU：[ESXi 7.0 U2 以降] が選択されていることを確認します。
ゲスト OS を選択	オペレーティング システムのリリースに最も適した Windows ゲスト OS オプションを選択します。 [Windows 仮想化ベースのセキュリティの有効化] チェック ボックスを選択します。
ハードウェアのカスタマイズ	ディスク サイズや CPU を変更するなどしてハードウェアをカスタマイズします。
設定の確認	情報を確認し、[終了] をクリックします。

結果

仮想マシンが作成されたら、その [サマリ] タブで、ゲスト OS の説明に「VBS true」と表示されることを確認します。

次のステップ

ゲスト OS での仮想化ベース セキュリティの有効化を参照してください。

既存の仮想マシンでの仮想化ベース セキュリティの有効化

サポート対象 Windows ゲスト OS で、既存の仮想マシンに対する Microsoft の仮想化ベースのセキュリティ (VBS) を有効にできます。

VBS を有効にするプロセスでは、まず仮想マシンで VBS を有効にしてから、ゲスト OS で VBS を有効にします。

注： ハードウェア バージョン 14 未満で Windows 10、Windows Server 2016 および Windows Server 2019 用に構成された新規仮想マシンは、デフォルトでレガシー BIOS を使用して作成されます。仮想マシンのファームウェア タイプをレガシー BIOS から UEFI に変更する場合は、ゲスト OS を再インストールする必要があります。

前提条件

許容可能な CPU については、仮想化ベース 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。

VBS に Intel CPU を使用するには、vSphere 6.7 以降が必要です。仮想マシンは、ハードウェア バージョン 14 以降、および次のサポート対象ゲスト OS のいずれかを使用して作成されている必要があります。

- Windows 10（64 ビット）以降のリリース
- Windows Server 2016（64 ビット）以降のリリース

VBS に AMD CPU を使用するには、vSphere 7.0 Update 2 以降が必要です。仮想マシンは、ハードウェア バージョン 19 以降、および次のサポート対象ゲスト OS のいずれかを使用して作成されている必要があります。

- Windows 10（64 ビット）、バージョン 1809 以降のリリース
- Windows Server 2019（64 ビット）以降のリリース

VBS を有効にする前に、Windows 10 バージョン 1809、および Windows Server 2019 の最新のパッチをインストールしてください。

手順

1 vSphere Client で、仮想マシンを参照します。

2 仮想マシンを右クリックし、[設定の編集] を選択します。

3 [仮想マシン オプション] タブをクリックします。

4 仮想化ベースのセキュリティの [有効化] チェック ボックスをオンにします。

5 [OK] をクリックします。

結果

仮想マシンの [サマリ] タブで、ゲスト OS の説明に「VBS true」と表示されることを確認します。

次のステップ

ゲスト OS での仮想化ベース セキュリティの有効化を参照してください。

ゲスト OS での仮想化ベース セキュリティの有効化

サポート対象 Windows ゲスト OS で Microsoft の仮想化ベースのセキュリティ (VBS) を有効にできます。

Windows ゲスト OS から VBS を有効にします。Windows は、グループ ポリシー オブジェクト (GPO) により VBS を構成し、実施します。GPO により、VBS が提供するセキュア ブート、デバイス ガード、および資格情報ガードなどのさまざまなサービスのオンとオフを切り替えることができます。特定の Windows バージョンでは、Hyper-V プラットフォームを有効にするための追加の手順も実行する必要があります。

詳細については、仮想化ベースのセキュリティを有効にするためのデバイス ガードの導入に関する Microsoft のドキュメントを参照してください。

前提条件

- 仮想マシンで仮想化ベースのセキュリティが有効になっていることを確認します。

手順

1 Microsoft Windows で、グループ ポリシーを編集して VBS をオンにし、その他の VBS 関連のセキュリティ オプションを選択します。

2 （オプション） Redstone 4 未満の Microsoft Windows バージョンの場合は、[Windows の機能] コントロール パネルで Hyper-V プラットフォームを有効にします。

3 ゲスト OS を再起動します。

仮想化ベース セキュリティの無効化

仮想マシンで仮想化ベースのセキュリティ (VBS) を使用しなくなった場合は、VBS を無効にできます。仮想マシンの VBS を無効にした場合、Windows の VBS オプションは変更されませんが、パフォーマンスの問題が発生する可能性があります。仮想マシンで VBS を無効にする前に、Windows で VBS オプションを無効にしてください。

前提条件

仮想マシンがパワーオフ状態であることを確認します。

手順

1 vSphere Client で、VBS が有効になっている仮想マシンを参照します。

VBS が有効になっている仮想マシンの特定に関するヘルプについては、VBS 対応仮想マシンの特定を参照してください。

2 仮想マシンを右クリックし、[設定の編集] を選択します。

3 [仮想マシン オプション] をクリックします。

4 仮想化ベースのセキュリティの [有効化] チェック ボックスを選択解除します。

ゲスト OS で VBS を無効にするように通知するメッセージが表示されます。

5 [OK] をクリックします。

6 仮想マシンの [サマリ] タブで、ゲスト OS の説明に「VBS true」と表示されなくなったことを確認します。

VBS 対応仮想マシンの特定

レポート作成やコンプライアンスに必要なときに、VBS 対応仮想マシンを判別することができます。

手順

1 vCenter Server に vSphere Client を使用して接続します。

2 インベントリで vCenter Server インスタンス、データセンター、またはホストを選択します。

3 [仮想マシン] タブ > [仮想マシン] の順にクリックします。

4 [VBS] 列を表示するには、左下隅にある 3 バーの [列セレクタ] をクリックし、[VBS] チェック ボックスを選択します。

5 [VBS] 列で「あり」を調べます。

vSphere ネットワークのセキュリティ強化

13

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 の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

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により、パフォーマンスが低下する場合があります。仮想ネットワーク内の他の場所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調整してください。

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。セグメント化は、アドレス解決プロトコル (ARP) のスプーフィングなど、さまざまな脅威を防ぎます。ARP スプーフィングにより、攻撃者は MAC アドレスと IP アドレスを再マップして ARP テーブルを操作し、ネットワーク トラフィックからホスト、またはホストからネットワーク トラフィックへのアクセスを実行します。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。

セグメント化を慎重に計画すると、仮想マシン ゾーン間でのパケット転送の可能性が下がります。その結果、被害者へのネットワーク トラフィック送信を伴うスニフィング攻撃を阻止できます。さらに、攻撃者は特定の仮想マシン ゾーンにある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。

- 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、最初にセグメントを作成した後では、おそらく最も安全です。これは、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した場合のセキュリティ上の利点をほぼすべて備えており、ハードウェアのオーバーヘッドもありません。VLAN を使用すると、追加のデバイスやケーブル接続を導入、保守するためのコストを節約できます。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。

不正アクセスの防止

仮想マシンを保護するための要件は、多くの場合、物理マシンを保護する際の要件と同じです。

- 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。
- 物理ネットワークに仮想マシンを接続しない場合でも、仮想マシンが他の仮想マシンから攻撃されることはあり得ます。

仮想マシンはそれぞれ隔離されています。ある仮想マシンから別の仮想マシンに対し、メモリの読み取りや書き込み、データへのアクセス、アプリケーションの使用を行うことはできません。ただし、ネットワーク内で、仮想マシンまたは仮想マシン グループが、他の仮想マシンから不正にアクセスされることはあります。このような不正アクセスから、仮想マシンを保護してください。

仮想マシンを保護する方法の詳細については、次の URL にある「仮想マシン (VM) を保護するためのセキュアな仮想ネットワーク構成」という NIST ドキュメントを参照してください。

https://csrc.nist.gov/publications/detail/sp/800-125b/final

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ることがないように、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。

vSphere、vSAN を含む VMware 製品でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。VMware 製品別のポート検索、ポートのカスタマイズ リストの作成、およびポート リストの出力または保存を行うことができます。

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。

ファイアウォールは、すべてのエントリ ポイントで必要です。クライアントと vCenter Server の間にファイアウォールを配置するか、vCenter Server とクライアントの両方をファイアウォールの背後に配置することができます。

vSphere、vSAN を含む VMware 製品でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。VMware 製品別のポート検索、ポートのカスタマイズ リストの作成、およびポート リストの出力または保存を行うことができます。

vCenter Server を使用して構成したネットワークは、vSphere Client、他のユーザー インターフェイス クライアント、または vSphere API を使用する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。

ネットワークの使用量や、クライアントで必要とされるセキュリティ レベルに応じて、ネットワーク内の他のアクセス ポイントにもファイアウォールを含める場合があります。ファイアウォールの配置場所は、ネットワーク構成のセキュリティ リスクに基づいて選択します。一般的に使用されるファイアウォールの場所を次に示します。

- vSphere 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 Client を介して仮想マシンにアクセスする場合は、vSphere Client と ESXi ホストの間。この接続は、vSphere 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、仮想マシンを移行する場合は、ターゲット ホストとソース ホストの間にあるすべてのファイアウォールのポートを開きます。
- 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合わせ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 が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。

デフォルトで、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。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。

ファイアウォールを介した ESXi ホストの接続

ESXi ホストと vCenter Server の間にファイアウォールがある場合は、管理対象ホストがデータを受け取れることを確認します。

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 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。ポートのリストについては、https://ports.vmware.com の VMware Ports and Protocols Tool™ 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

お使いの環境に vCenter Server が含まれていない場合は、クライアントは ESXi ネットワークに直接接続できます。

いくつかの方法でのスタンドアロン ESXi ホストに接続できます。

- VMware Host Client
- ESXCLI インターフェイス
- vSphere Web Services SDK または vSphere Automation SDK
- サードパーティ製のクライアント

スタンドアロン ホストのファイアウォール要件は、vCenter Server がある場合の要件と似ています。

- ファイアウォールを使用して ESXi 層を保護するか、構成によっては、クライアントと ESXi 層を保護します。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。
- 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 ESXi に属するため、ファイアウォールを備えた個別の License Server は必要ありません。

ESXCLI または VMware Host Client を使用してファイアウォール ポートを構成できます。vSphere の単一ホスト管理：VMware Host Client を参照してください。

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と、vSphere Client を使用して vCenter Server を介して接続するか VMware Host Client から直接 ESXi ホストに接続するかによって異なります。

ポート、目的、および分類（受信、送信、双方向）の詳細については、https://ports.vmware.com の VMware Ports and Protocols Tool™を参照してください。

vSphere 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 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 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 443 での vSphere Client の vCenter Server へのアクセスを許可する必要がある。
- 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る。

vSphere Client を介した VMware Remote Console との接続

vSphere Client を使用し、VMware Remote Console (VMRC) に接続している場合は、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 443 での vSphere Client の vCenter Server へのアクセスを許可する必要がある。

- ファイアウォールは VMRC に、vCenter Server へのアクセスをポート 443 で許可する必要があります。また、ESXi ホストへのアクセスについては、11.0 よりも前のバージョンの VMRC にはポート 902 で許可し、11.0 以降のバージョンの VMRC にはポート 443 で許可する必要があります。VMRC バージョン 11.0 と ESXi ポートの要件の詳細については、https://kb.vmware.com/s/article/76672 にある VMware のナレッジベースの記事を参照してください。

ESXi ホストの VMware Host Client との直接接続

ESXi ホストに直接接続する場合は、VMware Host Client 仮想マシン コンソールを使用できます。

注： VMware Host 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 VMware Host 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。

VMware Host 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

VMkernel ポート グループまたは標準スイッチの仮想マシン ポート グループには、構成可能なセキュリティ ポリシーがあります。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。

物理ネットワークのアダプタと同じように、仮想マシン ネットワーク アダプタも別の仮想マシンを偽装できます。なりすましは、セキュリティ リスクの 1 つです。

- 仮想マシンは、別のマシンからであることを装ってフレームを送信し、そのマシン宛てのネットワーク フレームを受信できます。
- 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。

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場合、ESXi はグループ内のポート用にセキュリティ ポリシーを設定します。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。なりすましをする可能性があるゲスト OS は、なりすましが阻止されたことを検知しません。

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、『vSphere のネットワーク』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。このセクションは、次について説明しています。

- 仮想マシン ネットワーク アダプタが送信を制御する仕組み
- このレベルでどのように攻撃が行われるか

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、仮想マシン ネットワーク アダプタの MAC アドレス モードの一部を制限することで、レイヤー 2 攻撃から保護できます。

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。そのため、オペレーティング システムは、受信側ネットワークが許可するネットワーク アダプタになりすまし、ネットワーク内のデバイスに対して悪意のある攻撃を実行できます。

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 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。

- MAC アドレス変更 （MAC アドレス変更 を参照）
- プロミスキャス モード （無差別モード操作 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 Client から選択することにより、表示および変更できます。vSphere のネットワーク 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。このオプションにより、MAC アドレスが VMX で構成されているものとは異なるフレームを仮想マシンで受信できるようになります。

[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 は仮想マシンの有効な 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 は仮想マシンの有効な 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 モードで使用される場合、アダプタは MAC アドレスを共有しません。

注： vSphere 7.0 以降、[偽装転送] および [MAC アドレス変更] のデフォルトが [承諾] ではなく [拒否] に変更されました。検証する場合は、ストレージ ベンダーにお問い合わせください。

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。

注： vSphere 7.0 以降、[偽装転送] および [MAC アドレス変更] のデフォルトが [承諾] ではなく [拒否] に変更されました。

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。

仮想マシンのアダプタを無差別モードに構成する方法については、『vSphere のネットワーク』ドキュメントの vSphere 標準スイッチまたは標準ポート グループのセキュリティ ポリシーの構成に関するトピックを参照してください。

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 スニファーを実行している場合などです。

標準スイッチの保護および VLAN

VMware の標準スイッチは、VLAN の特定のセキュリティ脅威に対する保護を提供します。標準スイッチの設計により、主に VLAN ホッピングに関係するさまざまな攻撃から VLAN を保護します。

ただし、この保護により、仮想スイッチ構成がその他のタイプの攻撃に対して強化されるわけではありません。たとえば、標準スイッチは、これらの攻撃から物理ネットワークを保護しません。 仮想ネットワークのみを保護します。

標準スイッチおよび VLAN は、次のタイプの攻撃から保護できます。

MAC フラッディング

送信元が異なるとタグ付けされた MAC アドレスを含むパケットで、スイッチをフラッディングします。多くのスイッチは、CAM (Content-Addressable Memory) テーブルを使用して、各パケットの送信元アドレスを

学習および保存します。テーブルがいっぱいになると、スイッチは完全に開いた状態になり、すべての着信パケットがすべてのポートにブロードキャストされることがあります。この場合、攻撃者はすべてのスイッチのトラフィックを参照できます。この状態では、VLAN でパケットがリークする可能性があります。

VMware 標準スイッチは MAC アドレス テーブルを保存しますが、観測可能なトラフィックから MAC アドレスを取得しないので、このタイプの攻撃に対する耐性がありません。

802.1q および ISL タギング攻撃

スイッチをトランクとして機能するように不正に操作し、トラフィックをほかの VLAN にブロードキャストすることで、ある VLAN から別の VLAN へフレームがリダイレクトされるようにスイッチを強制します。

VMware 標準スイッチは、このタイプの攻撃で必要な動的トランキングを実行しないので、このタイプの攻撃に対する耐性があります。

ダブル カプセル化攻撃

内部タグの VLAN ID が外部タグの VLAN ID と異なるダブル カプセル化パケットを攻撃者が作成したときに発生します。後方互換性のため、ネイティブ VLAN は、転送されたパケットから外側のタグを取り外します (無効に設定されていない場合)。ネイティブ VLAN スイッチが外側のタグを取り外すと、内側のタグだけが残ります。 この内側のタグは、取り外された外側のタグで識別される VLAN とは異なる VLAN にパケットを送ります。

VMware 標準スイッチは、特定の VLAN に構成されているポートに仮想マシンが送信しようとする任意のダブル カプセル化フレームを削除します。したがって、このタイプの攻撃に対する耐性があります。

マルチキャスト総当り攻撃

存在が分かっている VLAN にほぼ同時に大量のマルチキャストのフレームを送信してスイッチに負荷をかけ、一部のフレームを別の VLAN へ誤ってブロードキャストさせます。

VMware 標準スイッチでは、フレームはその正しいブロードキャスト ドメイン (VLAN) の外へ出ることはできないので、このタイプの攻撃に対する耐性があります。

スパニング ツリー攻撃

LAN の各部分のブリッジを制御するときに使用される STP （Spanning-Tree Protocol） を標的にします。攻撃者は、ネットワーク トポロジを変更しようとする BPDU （Bridge Protocol Data Unit） パケットを送信し、攻撃者自体をルート ブリッジとして確立します。ルート ブリッジとなった攻撃者は、転送されるフレームの内容を傍受できます。

VMware 標準スイッチは、STP をサポートしていないので、このタイプの攻撃に対する耐性があります。

ランダム フレーム攻撃

ソースとターゲットのアドレスは同じでも、フィールドの長さ、タイプ、または内容がランダムに変わるパケットを大量に送信します。この攻撃の目的は、別の VLAN にパケットが誤って送信されるようにすることです。

VMware 標準スイッチは、このタイプの攻撃に対する耐性があります。

新しいセキュリティ脅威は常に開発されるので、これは攻撃の完全なリストではありません。セキュリティ、最新のセキュリティ警告、VMware セキュリティ戦術については、Web 上で VMware のセキュリティ関連資料を定期的に確認してください。

vSphere Distributed Switch および分散ポート グループのセキュリティ強化

管理者は、vSphere 環境で vSphere Distributed Switch を保護するオプションを利用できます。

vSphere Distributed Switch の VLAN には、標準スイッチと同様のルールが適用されます。詳細については、標準スイッチの保護および VLAN を参照してください。

手順

1 静的バインドを使用する分散ポート グループの場合は、自動展開機能を無効にします。

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 タグ付けを使用する場合、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 が正しく追跡されていない場合、ID が誤って再利用され、意図しないトラフィックが許可されることがあります。同様に、VLAN ID が誤っているか欠落していると、物理マシンと仮想マシン間をトラフィックが失われることがあります。

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、スイッチ名のテキスト ボックスが必要です。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、スイッチに内部というラベルを付けて、それが、仮想マシンのプライベート仮想スイッチ上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。このトラフィックは物理ネットワーク アダプタをしません。

6 vSphere Distributed Switch のネットワーク健全性チェックを頻繁に利用しない場合、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です。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無効にします。

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 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。

- MAC アドレス変更 （MAC アドレス変更 を参照）
- プロミスキャス モード （無差別モード操作 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 のネットワーク』を参照してください。

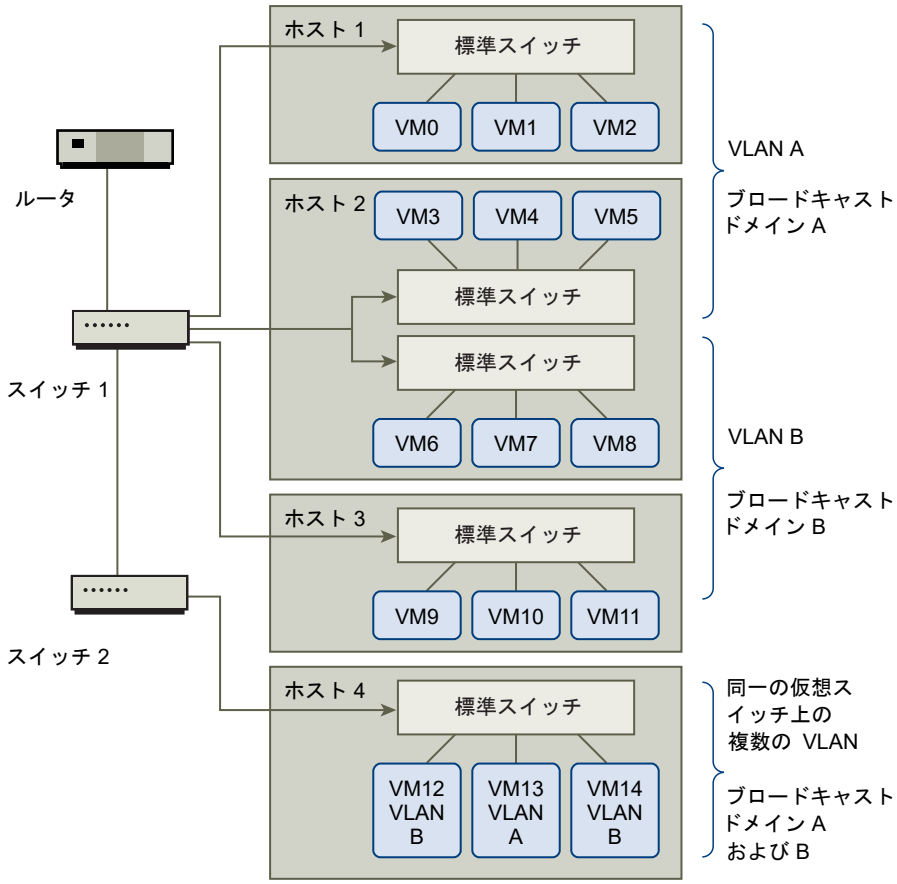
VLAN を使用した仮想マシンのセキュリティ強化

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 13-1. 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 4094 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。

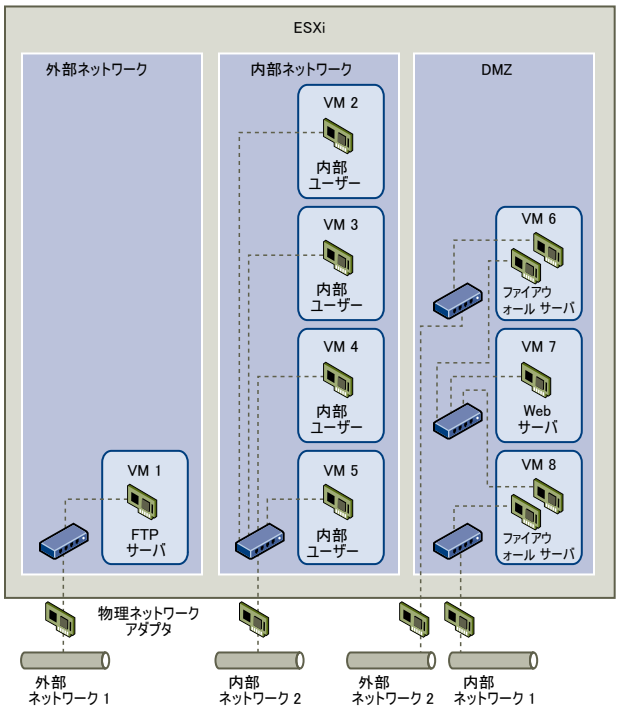
標準スイッチでは、VLAN ネットワーク モードをスイッチ レベルまたはポート グループ レベルで構成できます。Distributed Switch では、VLAN ネットワーク モードを分散ポート グループ レベルまたはポート レベルで構成できます。

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 13-2. 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 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、マーケティング部門および財務部門が企業の Web サイトをホストするために使用する Web サーバ、および外部ユーザーをホストしているその他の Web 機能をサポートしています。内部ネットワーク 1 は、マーケティング部門による企業 Web サイトへのコンテンツ公開、ダウンロードの掲載、およびユーザー フォーラムなどのサービスの保守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て、各仮想マシン グループの仮想スイッチや物理ネットワーク アダプタをほかの仮想マシングループ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ので、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 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、`esxcli` コマンド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、`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
`--sa-source=` ***source address***	必須。ソース アドレスを指定します。
`--sa-destination=` ***destination address***	必須。ターゲット アドレスを指定します。
`--sa-mode=` ***mode***	必須。`transport` か `tunnel` の、どちらかのモードを指定します。

オプション	説明
--sa-spi= ***security parameter index***	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。
--encryption-algorithm= ***encryption algorithm***	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。 ■ `3des-cbc` ■ `aes128-cbc` ■ `null`（暗号化なし）
--encryption-key= ***encryption key***	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。
--integrity-algorithm= ***authentication algorithm***	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。
--integrity-key= ***authentication key***	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。
--sa-name=*name*	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 0x697076367265616479 6c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

IPsec セキュリティ アソシエーションの削除

セキュリティ アソシエーションは、ESXCLI コマンドを使用して削除できます。

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 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、**esxcli network ip ipsec sp list** コマンドを入力します。

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。セキュリティ ポリシーは、ESXCLI コマンドを使用して追加できます。

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
--sp-source= *source address*	必須。ソース IP アドレスとプリフィックスの長さを指定します。
--sp-destination= *destination address*	必須。ターゲット IP アドレスとプリフィックスの長さを指定します。
--source-port= *port*	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。
--destination-port= *port*	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。
--upper-layer-protocol= *protocol*	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。 ■ `tcp` ■ `udp` ■ `icmp6` ■ `any`
--flow-direction= *direction*	`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。
--action= *action*	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。 ■ `none`： 何も処理を行いません。 ■ `discard`： データの送受信を許可しません。 ■ `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。
--sp-mode= *mode*	`tunnel` か `transport` の、どちらかのモードを指定します。

オプション	説明
--sa-name=*security association name*	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。
--sp-name=*name*	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=sa1
--sp-name=sp1
```

IPsec セキュリティ ポリシーの削除

ESXCLI 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。

ESXi には SNMP エージェントが含まれており、通知（トラップおよびインフォーム）の送信と、`GET`、`GETBULK`、`GETNEXT` の各要求の受信ができます。SNMP はデフォルトでは有効になっていません。SNMP は、ESXi ホストごとに構成する必要があります。構成には ESXCLI、PowerCLI、または vSphere Web Services SDK を使用できます。

SNMP v3 を含む SNMP の構成の詳細については、『vSphere の監視とパフォーマンス』ドキュメントを参照してください。SNMP v3 には、キー認証や暗号化など、SNMP v1 または SNMP v2c より強化されたセキュリティが備わっています。`esxcli system snmp` コマンド オプションの詳細については、ESXCLI のリファレンス を参照してください。

手順

1 SNMP が使用されているかどうかを確認するには、次のコマンドを実行します。

```
esxcli system snmp get
```

2 SNMP を有効にするには、次のコマンドを実行します。

```
esxcli system snmp set --enable true
```

3 SNMP を無効にするには、次のコマンドを実行します。

```
esxcli system snmp set --enable false
```

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。

- STP (Spanning Tree Protocol) は、ネットワーク トポロジ内でのループの形成を検出および防止します。VMware 仮想スイッチの場合、ループは他の方法で防止されており、STP は直接サポートされません。ネットワーク トポロジが変更されたときは、ネットワークがトポロジを再学習するのにある程度の時間が必要になります（30 ～ 50 秒）。この間、トラフィックの通過は許可されません。これらの問題を回避するため、ネットワーク ベンダーは、スイッチ ポートが引き続きトラフィックを転送できるようにする機能を作成しています。詳細については、https://kb.vmware.com/kb/1003804 にある VMware のナレッジベースの記事を参照してください。適切なネットワーク構成とネットワーク ハードウェア構成については、ネットワーク ベンダーのドキュメントを参照してください。
- 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ます。この情報により、転送中の機密情報が攻撃者によって閲覧および取得される可能性が増加します。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、仮想マシン管理者には、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付与します。ネットワーク管理者には、すべての仮想ネットワーク コンポーネントに対するアクセス権を付与し、仮想マシンへのアクセス権は与えないようにします。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。多くの場合、物理スイッチはネイティブ VLAN を使用するように構成され、このネイティブ VLAN は、デフォルトで VLAN 1 になります。ESXi には、ネイティブ VLAN はありません。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ため、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。オーバーライドが有効になっている場合は、ポートグループ レベルでの設定とは異なるセキュリティ設定を仮想マシンに使用することができます。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。

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 ヘッダを持つフレームが、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。

ネットワーク隔離プラクティスの採用

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 グループを一般的な標準スイッチ上の専用 VLAN に配置します。本番環境（仮想マシン）のトラフィックは、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ていない場合、標準スイッチを共有できます。

ネットワーク セグメントが、その他の管理関連エンティティが見つかったネットワーク以外のネットワークにルーティングされていないことを確認します。ネットワーク セグメントのルーティングは、vSphere Replication に適している場合があります。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。

次の方法のいずれかを使用して、管理機能へのアクセスを厳密に制御します。

- 機密性の高い環境で管理ネットワークにアクセスするには、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、管理者が VPN 経由で管理ネットワークに接続する必要がある場合です。信頼できる管理者に対してのみ、管理ネットワークへのアクセスを許可します。
- 管理クライアントを実行する Bastion ホストを構成します。

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 アドレス 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 アドレス 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 アドレス ベースのストレージは暗号化されていないことがよくあります。このネットワークへのアクセス権限があれば、誰でも IP アドレス ベースのストレージ トラフィックを表示できます。承認されていないユーザーが IP アドレス 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 アドレス 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 ルーター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 グループの一般的な標準スイッチ上の専用 VLAN を使用します。本番環境（仮想マシン）のトラフィックは、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ていない場合、同じ標準スイッチを使用できます。

vSAN トラフィックの隔離

vSAN ネットワークを構成するときは、vSAN トラフィックを専用のレイヤー 2 ネットワーク セグメントに隔離します。この隔離は、専用のスイッチまたはポートを使用するか、VLAN を使用して実行できます。

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る場合を除き、仮想マシンにネットワーク情報を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。『vSphere 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. vSphere Client インベントリで、ホストに移動して参照します。
2. [構成] 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] をクリックします。
4. `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] テキスト ボックスに **`DVFilter`** と入力して、関連するパラメータすべてを表示します。
5. 設定を確認します。
   - 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。
   - DvFilter 設定を使用している場合は、パラメータの値が正しいことを確認します。値は、DvFilter を使用している製品で使用されている値と一致する必要があります。

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

14

環境内の PTP または 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、3 章 ESXi ホストのセキュリティ強化および 5 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刻の同期
- 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であることを確認する
- ESXi Shell および vSphere Client のタイムアウトの設定

vSphere ネットワーク上の時刻の同期

vSphere ネットワーク上のすべてのコンポーネントの時刻が同期されていることを確認します。vSphere ネットワークの物理マシンの時刻が同期されていなければ、時刻に依存する SSL 証明書と SAML トークンは、 ネットワーク上のマシン間の通信で有効と認識されないことがあります。

時刻が同期されていないと認証に問題が発生し、インストールに失敗したり、vCenter Server の `vmware-vpxd` サービスが起動しないことがあります。

vSphere での時間の不整合によって、初期起動がさまざまなサービスで失敗する場合があります。どのサービスが失敗するかは、環境内のどこで時刻が正確でないかと、いつ時刻が同期されるかによって決まります。問題がよく発生するのは、対象 vCenter Server のターゲット ESXi ホストが NTP または PTP と同期されていない場合です。同様に、ターゲット vCenter Server を、別の時刻に設定されている ESXi ホストに移行する場合にも、完全に自動化された DRS のために問題が発生することがあります。

時刻同期の問題を回避するには、vCenter Server のインストール、移行、またはアップグレードの前に、次のことが正しくできていることを確認します。

- 対象 vCenter Server がデプロイされるターゲット ESXi ホストは、NTP または PTP と同期されます。
- ソース vCenter Server を実行している ESXi ホストが NTP または PTP と同期されます。
- vSphere 6.5 または 6.7 から vSphere 7.0 へのアップグレードまたは移行で、vCenter ServerAppliance が外部の Platform Services Controller に接続されている場合は、外部の Platform Services Controller を実行している ESXi ホストが NTP または PTP と同期されていることを確認します。

- vSphere 6.5 または 6.7 から vSphere 7.0 へのアップグレードまたは移行では、移行元の vCenter Server または vCenter Server アプライアンスと外部 Platform Services Controller の時刻が正しいことを確認する。
- 外部 Platform Services Controller を使用する vCenter Server 6.5 または 6.7 インスタンスを vSphere 7.0 にアップグレードする場合は、アップグレード プロセスにより組み込みの Platform Services Controller を使用する vCenter Server インスタンスに変換される。

vCenter Server が実行されるすべての Windows ホスト マシンが、ネットワーク タイム サーバ （NTP サーバ）によって同期されていることを確認します。詳細については、VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/1318) を参照してください。

ESXi の時刻を NTP サーバまたは PTP サーバと同期するため、VMware Host Client を使用できます。ESXi ホストの時刻設定の編集については、『vSphere 単一ホスト管理：VMware Host Client』を参照してください。

vCenter Server の時刻同期設定を変更する方法については、『 vCenter Server の構成』の「システムのタイム ゾーンおよび時刻同期の設定の構成」を参照してください。

vSphere Client を使用してホストの時刻設定を編集する方法については、『vCenter Server およびホスト管理』の「ホストの時刻設定の編集」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 の時刻の同期

  vCenter Server のインストールの前に、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 の時刻同期設定

  デプロイ後、vCenter Server 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 の時刻の同期

vCenter Server のインストールの前に、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、VMware Host Client から NTP をセットアップする方法を説明します。

手順

1. VMware Host Client を起動し、ESXi ホストに接続します。
2. [管理] をクリックします。
3. [システム] の [時間と日付] をクリックし、[設定の編集] をクリックします。
4. [Network Time Protocol を使用（NTP クライアントを有効にする)] を選択します。
5. [NTP サーバ] テキスト ボックスで、同期する 1 台以上の 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。
6. [NTP サービス起動ポリシー] ドロップダウン メニューから、[ホストと連動して起動および停止] を選択します。
7. [保存] をクリックします。

   ホストが NTP サーバと同期します。

vCenter Server の時刻同期設定

デプロイ後、vCenter Server の時刻同期設定を変更できます。

vCenter Server をデプロイするとき、時刻同期の方法として NTP サーバと VMware Tools のどちらを使用するか選択できます。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 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 で使用できる定期的な時刻同期の形態は 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 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 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 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 を設定するには、NTP サーバを vCenter Server 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 次の `ntp.set` コマンドを実行して、NTP サーバを vCenter Server 構成に追加します。

```
ntp.set --servers IP-addresses-or-host-names
```

このコマンドの *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。

このコマンドを実行すると、現在の NTP サーバ（存在する場合）が削除され、新しい 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。それ以外の場合は、このコマンドによって NTP 構成内の現在の NTP サーバが指定した新しい NTP サーバに置き換えられます。

3 （オプション） 新しい NTP 構成設定が正常に適用されたことを確認するには、次のコマンドを実行します。

```
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。

4 （オプション） NTP サーバにアクセスできるかどうかを確認するには、次のコマンドを実行します。

```
ntp.test --servers IP-addresses-or-host-names
```

このコマンドにより、NTP サーバのステータスが返されます。

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 の時間同期設定を構成できます。vCenter Server と NTP サーバとの時刻同期を参照してください。

vCenter Server 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 の時刻同期設定を構成できます。

前提条件

vCenter Server 構成内に 1 つ以上の Network Time Protocol (NTP) サーバを設定します。vCenter Server 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 vSAN 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、対策を講じてセキュリティ リスクを最小にできます。

iSCSI 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を交換します。iSCSI トランザクションは、iSCSI レコード内の raw SCSI データのブロックをカプセル化し、要求側デバイスまたはユーザーにデータを送信します。

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して、動的に共有できるストレージ リソースへのアクセスをホストに提供します。iSCSI SAN は、多数のユーザーを対象とした一般的なストレージ プールを基盤とする環境向けの経済的なストレージ ソリューションです。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、ホストと関連付けられたハードウェア 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

iSCSI デバイスを保護するには、ホストがターゲット LUN のデータにアクセスするときに、ESXi ホストまたはイニシエータが iSCSI デバイスまたはターゲットに対して必ず認証を行うようにします。

認証により、イニシエータにターゲットへのアクセス権限があることを確実にすることができます。この権限は、iSCSI デバイスで認証を設定するときに付与します。

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 のストレージ』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。ホストごとに異なる相互認証シークレットを設定します。可能であれば、ESXi ホストの各クライアントに異なるシークレットを設定します。一意のシークレットにより、1 台のホストがセキュリティ侵害を受けても、攻撃者が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不可能になります。共有シークレットの場合、1 台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てしまいます。

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も 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、攻撃者がスペア 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 スイッチ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 のストレージ のドキュメントを参照してください。

NFS 4.1 用 Kerberos 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。

RPCSEC_GSS Kerberos メカニズムは認証サービスです。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 セキュリティでは、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。

ESXi の NFS 4.1 用の Kerberos 実装には、krb5 と krb5i の 2 つのセキュリティ モデルがあり、それぞれが異なるセキュリティ レベルを提供します。

- 認証のみの Kerberos (krb5) では　ID 検証がサポートされます。
- 認証とデータ整合性用の Kerberos (krb5i) では、ID 検証に加えて、データの整合性サービスも提供されます。これらのサービスを使用すると、データ パケットが改変されている可能性がないかがチェックされ、NFS トラフィックの改ざん保護に役立ちます。

Kerberos は暗号化アルゴリズムをサポートし、認証されていないユーザーによる NFS トラフィックへのアクセスを防止します。ESXi の NFS 4.1 クライアントは、NAS サーバ上の共有へのアクセスに、AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 アルゴリズムの使用を試みます。NFS 4.1 データストアを使用する前に、NAS サーバで AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 が有効であることを確認します。

次の表は、ESXi がサポートする Kerberos セキュリティ レベルの比較です。

表 14-1. Kerberos セキュリティのタイプ

		ESXi 6.0	ESXi 6.5 以降
認証のみの Kerberos (krb5)	RPC ヘッダーの整合性チェックサム	あり (DES)	あり (AES)
	RPC データの整合性チェックサム	いいえ	いいえ
認証とデータ整合性用 Kerberos (krb5i)	RPC ヘッダーの整合性チェックサム	なし (krb5i)	あり (AES)
	RPC データの整合性チェックサム		あり (AES)

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 ドメインで Kerberos 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 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。割り当てプロセスを自動化するには、ホスト プロファイル内にユーザーを設定し、そのプロファイルをすべての ESXi ホストに適用します。
- 複数のホストで共有される 1 つの NFS 4.1 データストアには、2 つのセキュリティ メカニズム（AUTH_SYS と Kerberos）を使用できません。

詳細な手順については、『vSphere のストレージ』ドキュメントを参照してください。

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であることを確認する

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。

デフォルトでは、仮想マシンにホストのパフォーマンス データを送信する機能はが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。仮想マシンのセキュリティ侵害が発生した場合、設定により攻撃者はホストのデータを使用できません。

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、ESXCLI または VMware PowerCLI コマンドの使用を検討してください。

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/`*`datastore`* 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 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 Client のタイムアウトを設定します。

ESXi Shell のタイムアウト

ESXi Shell の場合は、vSphere 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、セッションがアイドル状態になってから、ユーザーが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、ユーザーが次回 ESXi Shell にログインする際に適用されます。既存のセッションは影響を受けません。

vSphere Client のタイムアウト

vSphere Client のセッションは、デフォルトで 120 分後に終了します。デフォルトを変更するには、次の手順を実行します。

1 vSphere Client で、vCenter Server インスタンスに移動します。

2 [構成] タブを選択し、[設定] で [全般] を選択します。

3 [編集] をクリックします。

4 [タイムアウト設定] を選択します。

5 選択を入力し、[保存] をクリックします。

TLS Configurator Utility を使用した TLS プロトコル構成の管理

15

vSphere では、デフォルトで TLS のみが有効です。TLS 1.0 と TLS 1.1 は、デフォルトで無効になっています。フレッシュ インストール、アップグレード、または移行のいずれを実行するのかに関係なく、vSphere では TLS 1.0 および TLS 1.1 が無効になります。TLS Configurator ユーティリティを使用すると、vSphere システム上で旧バージョンのプロトコルを一時的に有効にすることができます。すべての接続で TLS 1.2 を使用した後、安全性の低い旧バージョンを無効にすることができます。

再構成を実行する前に、お使いの環境を確認してください。使用環境の要件およびソフトウェア バージョンによっては、相互運用性を維持するために、TLS 1.2 だけでなく TLS 1.0 および TLS 1.1 も再び有効にしなければならないことがあります。TLS 1.2 をサポートする VMware 製品のリストについては、https://kb.vmware.com/s/article/2145796 にある VMware ナレッジベースの記事を参照してください。サードパーティの統合については、ベンダーのドキュメントを参照してください。TLS Configurator ユーティリティは、vSphere 7.0 およびそれ以前のリリース（6.7、6.5、および 6.0 を含む）で動作します。

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 環境で TLS Configurator ユーティリティを実行すると、vCenter Server 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。

vSphere 7.0 以降の vCenter Server では、次の 2 つのリバース プロキシ サービスが実行されます。

- VMware リバース プロキシ サービスである `rhttpproxy`
- Envoy

Envoy はオープン ソースのエッジおよびサービス プロキシです。Envoy はポート 443 を占有し、すべての受信 vCenter Server 要求は Envoy を経由してルーティングされます。vSphere 7.0 では、`rhttpproxy` は Envoy の構成管理サーバとして機能します。その結果、TLS 構成が `rhttpproxy` に適用され、そこから構成が Envoy に送信されます。

vCenter Server および ESXi では、TLS プロトコルに対して有効または無効にできるポートが使用されます。TLS 構成ユーティリティの `scan` オプションを使用すると、各サービスで有効な TLS のバージョンが表示されます。vCenter Server での有効な TLS プロトコルのスキャンを参照してください。

vSphere、vSAN を含む VMware 製品でサポートされているすべてのポートとプロトコルのリストについては、https://ports.vmware.com/の VMware Ports and Protocols Tool™ を参照してください。VMware 製品別のポート検索、ポートのカスタマイズ リストの作成、およびポート リストの出力または保存を行うことができます。

メモと注意事項

- vSphere 6.7 リリースが vCenter Server for Windows の最後のリリースでした。vCenter Server for Windows で Update Manager ポート用に TLS を再構成する方法の詳細については、バージョン 6.7 の製品の『vSphere のセキュリティ』ドキュメントを参照してください。
- TLS 1.2 を使用して vCenter Server と外部の Microsoft SQL Server の間の接続を暗号化することができます。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。VMware のナレッジベースの記事 (https://kb.vmware.com/kb/2149745) を参照してください。
- vSphere 6.7 およびそれ以前のリリースでは、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。
- TLS プロトコルを変更する場合は、ESXi ホストを再起動して変更を適用する必要があります。ホスト プロファイルを使用したクラスタ構成を通じて変更を適用する場合でも、ホストを再起動する必要があります。ホストをすぐに再起動するか、または都合の良い時間まで再起動を延期するかを選択できます。

vSphere での TLS バージョンの有効化または無効化

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、環境はそのままで実行されるようにします。

vSphere Lifecycle Manager は常に vCenter Server システムに含まれており、対応するポートがスクリプトによって更新されます。

1 vCenter Server で TLS Configurator ユーティリティを実行します。

2 vCenter Server によって管理されている各 ESXi ホスト上で、TLS Configurator 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。

前提条件

環境内での TLS の使用には、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。

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 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。

ESXi 構成のバックアップはサポートされていません。

vCenter Server の場合、デフォルトのディレクトリは `/tmp/yearmonthdayTtime` です。

手順

1 ディレクトリを `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator` に変更します。

2 特定のディレクトリにバックアップを作成するには、次のコマンドを実行します。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

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。表示されるサービスの順序は、`reconfigureVc backup` コマンドの実行方法により、コマンドを実行するたびに異なることがあります。

```
vCenter Transport Layer Security reconfigurator, version=7.0.0, build=15518531
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20200206T183550
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmcam
Backing up: vmware-stsd
Backing up: vmdird
Backing up: vmware-sps
Backing up: vmware-rhttpproxy
Backing up: vami-lighttp
Backing up: vmware-updatemgr
Backing up: rsyslog
```

4 （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します。

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

vCenter Server システムでの TLS バージョンの有効化または無効化

TLS 構成ユーティリティを使用して vCenter Server システムの TLS バージョンを有効または無効にできます。プロセスの実行時に TLS 1.0 を無効にし、TLS 1.1 および TLS 1.2 を有効にすることができます。また、TLS 1.0 および TLS 1.1 を無効にして、TLS 1.2 のみを有効にすることができます。

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 administrator@vsphere.local のユーザー名とパスワードを使用して、またはスクリプトを実行できる vCenter Single Sign-On 管理者グループの別のメンバーとして、vCenter Server システムにログインします。

2 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。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 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。

```
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。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
```

4 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。

5 各 ESXi ホストで設定を繰り返します。

ESXi ホストでの TLS バージョンの有効化または無効化

TLS 構成ユーティリティを使用して ESXi ホストの TLS バージョンを有効または無効にできます。プロセスの実行時に TLS 1.0 を無効にし、TLS 1.1 および TLS 1.2 を有効にすることができます。また、TLS 1.0 および TLS 1.1 を無効にして、TLS 1.2 のみを有効にすることができます。

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ユーティリティを使用します。ユーティリティはリリースに対して固有であり、以前のリリースでは使用できません。

スクリプトを記述することで、複数のホストに対する設定が可能です。

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。

vCenter Server Appliance では、Bash シェルを有効にする必要があります。

手順

1 SSH を使用すると、スクリプトを実行できる vCenter Single Sign-On ユーザーのユーザー名とパスワードを使用して、vCenter Server Appliance システムに接続します。

2 Bash シェルを有効にするには、コマンド ラインで **shell** と入力します。

3 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。

```
cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator
```

4 クラスタの一部になっている ESXi ホストでは、次のコマンドのいずれかを実行します。

- 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。

  ```
  ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1
  TLSv1.2
  ```

- 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。

  ```
  ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
  ```

5 クラスタに含まれていないホストごとに、次のコマンドのいずれかを実行します。

- TLS 1.0 を無効にして、個々のホストで 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。

  ```
  ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1
  TLSv1.2
  ```

- 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。

  ```
  ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.2
  ```

  注： スタンドアローン ESXi ホストを再構成するには、vCenter Server システムにログインし、`ESXiHost -h` *HOST* `-u` *ESXi_ USER* オプションを指定して `reconfigureEsx` コマンドを実行します。*HOST* オプションには、単一 ESXi ホストの IP アドレスまたは FQDN か、ホスト IP アドレスまたは FQDN のリストを指定できます。たとえば、vCenter Server にログインして次のコマンドを実行すると、2 台の ESXi ホストで TLS 1.1 と TLS 1.2 の両方が有効になります。

  ```
  ./reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
  ```

  また、スタンドアローン ESXi ホストを再構成するためにホストにログインし、`UserVars.ESXiVPsDisabledProtocols` の詳細設定を変更することもできます。詳細については、vSphere の単一ホスト管理：VMware Host Client ドキュメントの「高度な TLS/SSL キー オプションの構成」というトピックを参照してください。

6 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。

vCenter Server での有効な TLS プロトコルのスキャン

vCenter Server で TLS バージョンを有効または無効にした後に、TLS 構成ユーティリティを使用して変更を確認することができます。

TLS 構成ユーティリティの `scan` オプションを使用すると、各サービスで有効な TLS のバージョンが表示されます。

手順

1 vCenter Server システムにログインします。

   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。

   b 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。

```
shell.set --enabled true
shell
```

2 `VcTlsReconfigurator` ディレクトリに移動します。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 TLS が有効なサービス、および使用されているポートを表示するには、次のコマンドを実行します。

```
reconfigureVc scan
```

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。

前提条件

変更を元に戻す前に、vCenter Server 管理インターフェイスを使用して vCenter Server のバックアップを実行します。

手順

1 スクリプトを実行する権限を持つユーザーとして変更を元に戻す vCenter Server に接続します。

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。

```
shell.set --enabled true
shell
```

3 `VcTlsReconfigurator` ディレクトリに移動します。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

4 以前のバックアップを確認します。

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
```

出力は次の例のようになります。

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

5 以下のコマンドを実行してリストアを実行します。

```
reconfigureVc restore -d Directory_path_from_previous_step
```

出力は次の例のようになります。

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

6 その他の vCenter Server インスタンスで手順を繰り返します。

事前定義された権限

16

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。

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。

- グローバル権限
- 健全性更新プロバイダ権限
- 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
- vSphere with Tanzu 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
- VcTrusts/VcIdentity の権限
- 信頼済みインフラストラクチャ管理者権限
- vApp 権限
- VcIdentityProviders の権限
- VMware vSphere Lifecycle Manager の構成権限
- VMware vSphere Lifecycle ManagerESXi 健全性パースペクティブの権限
- VMware vSphere Lifecycle Manager の一般的な権限
- VMware vSphere Lifecycle Manager のハードウェア互換性の権限
- VMware vSphere Lifecycle Manager イメージの権限
- VMware vSphere Lifecycle Manager イメージの修正権限
- VMware vSphere Lifecycle Manager 設定の権限
- VMware vSphere Lifecycle Manager のベースラインの管理権限
- VMware vSphere Lifecycle Manager のパッチおよびアップグレードの管理権限

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 16-1. 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 アクションを無効にする	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.エンティティのアラームを無効または有効にします	特定のターゲット タイプで特定のアラームを有効または無効にできます。	アラームをトリガできるオブジェクト
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

表 16-1. アラーム権限 （続き）

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、ホストを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。vCenter Server 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 16-2. 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.有効にする	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 証明書の管理については、『vSphere の認証』ドキュメントの「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 16-3. 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

認証局の権限

認証局の権限は、VMware Certificate Authority (VMCA) 証明書の特性を制御します。

表 16-4. 認証局の権限

権限名	説明	必要とするオブジェクト
認証局.作成/削除（管理者権限）。	vCenter Server 証明書を管理するための完全な管理者レベル アクセスを許可します。	vCenter Server
認証局.作成/削除（管理者権限より下）。	vSphere Client の [証明書の管理] ページで VMCA ルート証明書の表示を許可します。	vCenter Server

証明書管理の権限

証明書管理の権限により、vCenter Server の証明書を管理できるユーザーを制御します。

表 16-5. 証明書管理の権限

権限名	説明	必要とするオブジェクト
証明書の管理.作成/削除（管理者権限）。	vCenter Server 証明書関連の操作を行うために、さまざまな内部 API および機能に対する完全な管理レベル アクセスを許可します。	vCenter Server
証明書管理.作成/削除（管理者権限より下）。	さまざまな内部 API および機能への制限された管理者アクセスを許可します。この権限は、証明書関連の操作を制限し、ユーザーが管理者以外の権限を昇格できないようにします。許可されている操作は、次のとおりです。 ■ 証明書署名要求の生成 ■ 信頼できるルート チェーンの作成と取得 ■ 権限 証明書管理.作成/削除（管理者権限より下）。 を持つユーザーによって作成された信頼できるルート チェーンの削除 ■ マシン SSL 証明書の取得 ■ vCenter Server によって発行されたトークンを検証するための署名証明書チェーンの取得	vCenter Server

Cns 権限

クラウド ネイティブ ストア (Cns) 権限は、クラウド ネイティブ ストレージのユーザー インターフェイスにアクセスできるユーザーを制御します。

表 16-6. Cns 権限

権限名	説明	必要とするオブジェクト
Cns.検索	ストレージ管理者がクラウド ネイティブ ストレージのユーザー インターフェイスを表示できるようにします。	ルート 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。

注： コンテンツ ライブラリの権限の継承は、単一の vCenter Server インスタンスのコンテキストで機能します。ただし、インベントリの観点からは、コンテンツ ライブラリは vCenter Server システムの直系の子ではありません。コンテンツ ライブラリの直系の親はグローバル ルートです。これは、権限を vCenter Server レベルで設定して子オブジェクトに伝達すると、その権限はデータセンター、フォルダ、クラスタ、ホスト、仮想マシンなどには適用されますが、vCenter Server インスタンスに表示され、操作するコンテンツ ライブラリには適用されないことを意味します。コンテンツ ライブラリに権限を割り当てるには、管理者が権限をグローバル権限としてユーザーに付与する必要があります。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。

表 16-7. 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.ルート証明書のトラスト ストアへの追加	信頼されているルート証明書ストアにルート証明書を追加できるようにします。	vCenter Server
コンテンツ ライブラリ.テンプレートをチェックイン	テンプレートをチェックインできるようにします。	ライブラリ
コンテンツ ライブラリ.テンプレートをチェックアウト	テンプレートをチェックアウ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.公開ライブラリのサブスクリプションを作成	ライブラリ サブスクリプションを作成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.Harbor レジストリの作成または削除	VMware Tanzu Harbor レジストリ サービスを作成または削除できるようにします。	作成する場合は vCenter Server。削除する場合はレジストリ。
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

表 16-7. 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.Harbor レジストリ プロジェクトの作成、削除、またはパージ	VMware Tanzu Harbor レジストリ プロジェクトを作成、削除、またはパージできるようにします。	レジストリ
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.トラスト ストアからのルート証明書の削除	信頼されているルート証明書ストアからルート証明書を削除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.公開ライブラリのサブスクリプションを削除	ライブラリのサブスクリプション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
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です。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ない場合に限り、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.指定されたコンピューティング リソースでの、Harbor レジストリ リソースの管理	VMware Tanzu Harbor レジストリ リソースを管理できるようにします。	コンピューティング クラスタ
コンテンツ ライブラリ.サブスクリプション情報の検知	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 ライブラリのサブスクリプション情報をプローブできるようになります。表示される構造は、サブスクリプション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

表 16-7. 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.そのサブスクライバにライブラリ アイテムを公開	サブスクライバにライブラリ アイテムを公開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.そのサブスクライバにライブラリを公開	サブスクライバにライブラリを公開できるようにします。	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、Content Library Service 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.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 Client 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.公開ライブラリのサブスクリプションを更新	サブスクリプション パラメータを更新できるようにします。ユーザーは、購読済みライブラリの vCenter Server インスタンスの仕様やその仮想マシン テンプレート項目の配置などのパラメータを更新できます。	ライブラリ
コンテンツ ライブラリ.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 Client 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

暗号化操作権限

暗号化操作権限は、どのユーザーがどのタイプの暗号化操作をどのタイプのオブジェクトに対して実行できるかを制御します。

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 16-8. 暗号化操作権限

権限名	説明	必要とするオブジェクト
暗号化操作.直接アクセス	暗号化されたリソースへのアクセスをユーザーに許可します。ユーザーは、仮想マシンのエクスポート、NFC から仮想マシンへのアクセス許可、暗号化された仮想マシンとのコンソール セッションの開始が可能になります。	仮想マシン、ホスト、またはデータストア
暗号化操作.ディスクの追加	暗号化された仮想マシンへのディスクの追加をユーザーに許可します。	仮想マシン
暗号化操作.クローン作成	暗号化された仮想マシンのクローン作成をユーザーに許可します。	仮想マシン
暗号化操作.復号化	仮想マシンまたはディスクの復号化をユーザーに許可します。	仮想マシン
暗号化操作.暗号化	仮想マシンまたは仮想マシン ディスクの暗号化をユーザーに許可します。	仮想マシン
暗号化操作.新規暗号化	仮想マシン作成中の仮想マシンの暗号化、またはディスク作成中のディスクの暗号化をユーザーに許可します。	仮想マシンのフォルダ
暗号化操作.暗号化ポリシーの管理	暗号化 IO フィルタで仮想マシン ストレージ ポリシーを管理することをユーザーに許可します。デフォルトでは、暗号化ストレージ ポリシーを使用する仮想マシンは、他のストレージ ポリシーを使用しません。	vCenter Server ルート フォルダ
暗号化操作.KMS の管理	vCenter Server システムのキー管理サーバの管理をユーザーに許可します。管理タスクには、KMS インスタンスの追加および削除、KMS との信頼関係の確立などが含まれます。	vCenter Server システム
暗号化操作.キーの管理	キー管理操作の実行をユーザーに許可します。これらの操作を vSphere Client から実行することはサポートされていませんが、`crypto-util` または API を使用して実行できます。	vCenter Server ルート フォルダ
暗号化操作.移行	暗号化された仮想マシンを別の ESXi ホストに移行することをユーザーに許可します。vMotion を使用した移行、または使用しない移行と、Storage vMotion をサポートします。別の vCenter Server インスタンスへの移行をサポートします。	仮想マシン

表 16-8. 暗号化操作権限 （続き）

権限名	説明	必要とするオブジェクト
暗号化操作.再暗号化	異なるキーを持つ仮想マシンまたはディスクの再暗号化をユーザーに許可します。この権限は、深い再暗号化と浅い再暗号化の両方の操作に必要です。	仮想マシン
暗号化操作.仮想マシンの登録	暗号化された仮想マシンを ESXi ホストに登録することをユーザーに許可します。	仮想マシンのフォルダ
暗号化操作.ホストの登録	ホストの暗号化を有効にすることをユーザーに許可します。暗号化をホストで明示的に有効にするか、仮想マシンの作成プロセスで有効にできます。	スタンドアロン ホストのホスト フォルダ、クラスタ内のホストのクラスタ
暗号化操作.KMS 情報の読み取り	ユーザーが vCenter Server およびホストで vSphere Native Key Provider を一覧表示できるようにします。また、ユーザーは vSphere Native Key Provider 情報を取得できます。	vCenter Server またはホスト

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 16-9. 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

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 16-10. vSphere Distributed Switch の権限

権限名	説明	必要とするオブジェクト
Distributed Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.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 Siwtch.VSPAN の操作	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

データセンター権限

データセンター権限は、vSphere 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 16-11. 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設定	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 アドレス 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設定	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 アドレスの割り当て解除	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に対してこの権限が割り当てられている必要があります。	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 16-12. 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.容量の割り当て	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.データストアの設定	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
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

表 16-12. 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.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 クラスタの権限

データストア クラスタによって、ストレージ DRS のデータストア クラスタ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 16-13. データストア クラスタの権限

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.データストア クラスタの設定	ストレージ DRS のデータストア クラスタ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

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 16-14. ESX Agent Manager

権限名	説明	必要とするオブジェクト
ESX Agent Manager.設定	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 16-15. 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.拡張機能のアップデート	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

外部統計プロバイダ権限

外部統計プロバイダ権限は、vCenter Server にプロアクティブな Distributed Resource Scheduler (DRS) 統計情報を通知する機能を制御します。

これらの権限は、VMware 内部でのみ使用される API に適用されます。

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 16-16. 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 16-17. 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 ヘッダ、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.メソッドを無効にする	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.メソッドを有効にする	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	アラームとともにスクリプト アクションをスケジューリング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	ESXCLI で `resxtop` 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

健全性更新プロバイダ権限

健全性更新プロバイダ権限は、ハードウェア ベンダーが vCenter Server に対して、プロアクティブに HA イベントを通知する機能を制御します。

これらの権限は、VMware の内部でのみ使用される API に適用されます。

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 16-18. 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 16-19. 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 パススルー設定の変更	ホストの PCI パ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.ハイパースレッディング	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。	

表 16-19. 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.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
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設定	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 16-20. 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

表 16-20. 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.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
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、VMware Host Client がホストに直接接続されているときのアクションを制御します。

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 16-21. 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 Server へのホストの追加	vpxa や aam などの vCenter Server エージェントのホストへのインストールや、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.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.仮想マシンの再設定	仮想マシンの再構成を許可します。	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 16-22. 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 16-23. 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

vSphere with Tanzu の権限

名前空間の権限は、VMware vSphere® with VMware Tanzu™ 名前空間を作成および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 16-24. 名前空間の権限

権限名	説明	必要とするオブジェクト
名前空間.ディスクの廃止操作を許可	データ ストアの運用を終了できるようにします。	データストア
名前空間.ワークロード コンポーネント ファイルのバックアップ	etcd クラスタのコンテンツをバックアップできるようにします（VMware Cloud on AWS でのみ使用）。	クラスタ
名前空間.クラスタ全体の構成の変更	クラスタ全体の構成の変更、およびクラスタの名前空間の有効化または無効化を行うことができます。	クラスタ
名前空間.クラスタ全体での名前空間のセルフサービス構成の変更	名前空間のセルフサービス構成を変更できるようにします。	クラスタ （アクティブ化および非アクティブ化用） テンプレート （構成の変更用） vCenter Server （テンプレートの作成用）
名前空間.名前空間構成の変更	リソース割り当て、ユーザー権限など、名前空間構成オプションを変更できます。	クラスタ
名前空間.クラスタ機能の切り替え	クラスタ機能の状態を操作できるようにします（VMware Cloud on AWS でのみ内部で使用）。	クラスタ
名前空間.クラスタを新しいバージョンにアップグレード	クラスタのアップグレードを開始できるようにします。	クラスタ

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 16-25. 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
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 16-26. 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 16-27. 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 Client 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 16-28. 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
Profile-Driven Storage.Profile-Driven Storage の更新	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
Profile-Driven Storage.Profile-Driven Storage の表示	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 16-29. 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
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 16-30. 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 16-31. 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用されます。	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
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 人以上のログイン 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 16-32. 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 16-33. 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 Client 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 Client 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。

VcTrusts/VcIdentity の権限

VcTrusts/VcIdentity の権限は、vCenter Server システム間の信頼に関連するさまざまな内部 API および機能へのアクセスを制御します。

表 16-34. VcTrusts/VcIdentity の権限

権限名	説明	必要とするオブジェクト
VcTrusts/VcIdentity.作成/更新/削除（Admin 権限）	vCenter Server システム間の信頼に関連するさまざまな内部 API および機能への完全な管理者レベルのアクセスを許可します。	該当なし
VcTrusts/VcIdentity.作成/更新/削除（Admin 権限より低い）	vCenter Server システム間の信頼に関連するさまざまな内部 API および機能への制限された管理者アクセスを許可します。この権限は、VcTrusts/VcIdentity の作成/更新/削除を制限し、ユーザーが管理者以外の権限を昇格できないようにします。	該当なし

信頼済みインフラストラクチャ管理者権限

信頼済みインフラストラクチャ管理者権限は、vSphere 信頼機関 環境を構成および管理します。

これらの権限により、vSphere 信頼機関 環境に対して構成タスクおよび管理タスクを実行できるユーザーが決定されます。信頼機関のロールと TrustedAdmins グループの詳細については、vSphere 信頼機関の前提条件と必要な権限を参照してください。

表 16-35. 信頼済みインフラストラクチャ管理者権限

権限名	説明	必要とするオブジェクト
信頼できるインフラストラクチャ管理者.キー サーバの信頼の設定	キー プロバイダ サービスのキー プロバイダの管理を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.信頼機関ホストの TPM 証明書の設定	証明サービス設定の作成および変更を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.信頼機関ホストのメタデータの設定	どの基本イメージが証明サービスによって証明されるかの編集を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.認証 SSO の設定	どのホストを信頼機関ホストによって信頼できるようにするかについて編集を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.トークン変換ポリシーの設定	トークン変換ポリシーの構成を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.信頼できるインフラストラクチャ ホストの一覧表示	信頼済みホストおよび信頼機関ホストに関する情報の読み取りを許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.STS に関する情報を一覧表示	信頼済みホストの詳細をエクスポートして信頼機関クラスタにインポートできるようにすることを許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.信頼できるインフラストラクチャ ホストの管理	信頼済みホストおよび信頼機関ホストに関する情報の編集を許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.キー サーバの信頼の読み取り	キー プロバイダ サービスのキー プロバイダの読み取りを許可します。	ルート vCenter Server

表 16-35. 信頼済みインフラストラクチャ管理者権限 （続き）

権限名	説明	必要とするオブジェクト
信頼できるインフラストラクチャ管理者.認証 SSO の読み取り	どのホストを信頼機関ホストによって信頼できるようにするかについて読み取りを許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.TPM 信頼機関ホスト証明書の取得	証明サービスの設定の読み取りを許可します。	ルート vCenter Server
信頼できるインフラストラクチャ管理者.信頼機関ホストのメタデータの取得	どの基本イメージが証明サービスによって証明されるかの読み取りを許可します。	ルート vCenter Server

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 16-36. 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
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

表 16-36. vApp 権限 （続き）

権限名	説明	必要とするオブジェクト
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設定	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 インスタンスの設定	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 の設定	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 Client ユーザー インターフェイス要素はありません。	vApp
vApp.vApp リソースの設定	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

VcIdentityProviders の権限

VcIdentityProviders の権限は、VcIdentityProviders API へのアクセスを制御します。

表 16-37. VcIdentityProviders の権限

権限名	説明	必要とするオブジェクト
VcIdentityProviders.作成	VcIdentityProviders API（vCenter ServerID プロバイダ）への作成のみのアクセスを許可します。	該当なし
VcIdentityProviders.管理	VcIdentityProviders API（vCenter ServerID プロバイダ）への管理レベルの書き込みアクセス（作成、読み取り、更新、削除）を許可します。	該当なし
VcIdentityProviders.読み取り	VcIdentityProviders API（vCenter ServerID プロバイダ）への読み取りアクセスを許可します。	該当なし

VMware vSphere Lifecycle Manager の構成権限

VMware vSphere Lifecycle Manager の構成権限は、vSphere Lifecycle Manager サービ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。

注： URL を受け入れる VMware vSphere Lifecycle Manager API を呼び出すことをユーザーに許可する権限を管理者または信頼できるユーザーにのみ割り当てます。

表 16-38. VMware vSphere Lifecycle Manager の構成権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.構成.サービスの構成	vSphere Lifecycle Manager サービスとスケジュール設定されたパッチのダウンロード タスクの構成を許可します。	ルート vCenter Server

VMware vSphere Lifecycle ManagerESXi 健全性パースペクティブの権限

VMware vSphere Lifecycle ManagerESXi 健全性パースペクティブの権限は、ESXi ホストとクラスタの健全性のチェック機能を制御します。

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 16-39. VMware vSphere Lifecycle ManagerESXi 健全性パースペクティブの権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.ESXi 健全性パースペクティブ.読み取り	ESXi ホストおよびクラスタの健全性のクエリを許可します。	ホスト クラスタ
VMware vSphere Lifecycle Manager.ESXi 健全性パースペクティブ.書き込み	該当なし	該当なし

VMware vSphere Lifecycle Manager の一般的な権限

VMware vSphere Lifecycle Manager の一般的な権限は、Lifecyle Manager リソースの読み取りおよび書き込み機能を制御します。

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 16-40. VMware vSphere Lifecycle Manager の一般的な権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.Lifecycle Manager: 一般的な権限.読み取り	vSphere Lifecycle Manager リソースの読み取りを許可します。この権限は、タスク情報を取得する際に必要です。	ルート vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: 一般的な権限.書き込み	vSphere Lifecycle Manager リソースの書き込みを許可します。この権限は、vSphere Lifecycle Manager タスクをキャンセルする際に必要です。	ルート vCenter Server

VMware vSphere Lifecycle Manager のハードウェア互換性の権限

VMware vSphere Lifecycle Manager のハードウェア互換性の権限は、潜在的なハードウェア互換性の問題を検出して解決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 16-41. VMware vSphere Lifecycle Manager のハードウェア互換性の権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.Lifecycle Manager: ハードウェア互換性の権限.アクセス ハードウェアの互換性	ハードウェア互換性データへのアクセスと潜在的なハードウェア互換性の問題の解決を許可します。	ホスト

VMware vSphere Lifecycle Manager イメージの権限

VMware vSphere Lifecycle Manager イメージの権限は、イメージを管理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。

注： URL を受け入れる VMware vSphere Lifecycle Manager API を呼び出すことをユーザーに許可する権限を管理者または信頼できるユーザーにのみ割り当てます。

表 16-42. VMware vSphere Lifecycle Manager イメージの権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.Lifecycle Manager: イメージ権限.読み取り	vSphere Lifecycle Manager イメージの読み取りを許可します。この権限は次の操作に必要です。 ■ クラスタのすべてのドラフトを一覧表示 ■ ドラフトの詳細情報の確認 ■ ドラフトでのスキャンの実行 ■ ドラフトの検証 ■ ドラフトのコンテンツの取得 ■ 有効なコンポーネント リストの計算 ■ 現在の目的の状態ドキュメントのコンテンツを取得 ■ クラスタでのスキャンの開始 ■ コンプライアンスの結果の取得 ■ 推奨の取得 ■ 現在の目的の状態を、デポ、JSON ファイル、または ISO としてエクスポート	ルート vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: イメージ権限.書き込み	vSphere Lifecycle Manager イメージの管理を許可します。この権限は次の操作に必要です。 ■ ドラフトの作成、削除、またはコミット ■ 目的の状態をインポート ■ 推奨の生成 ■ ドラフトのさまざまな部分の設定または削除	ルート vCenter Server

VMware vSphere Lifecycle Manager イメージの修正権限

VMware vSphere Lifecycle Manager イメージの修正権限は、イメージを修正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 16-43. VMware vSphere Lifecycle Manager イメージの修正権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.Lifecycle Manager: イメージ修復権限.読み取り	修正の事前チェックの実行を許可します。	クラスタ
VMware vSphere Lifecycle Manager.Lifecycle Manager: イメージ修復権限.書き込み	修正を実行を許可します。	クラスタ

VMware vSphere Lifecycle Manager 設定の権限

VMware vSphere Lifecycle Manager 設定の権限は、デポおよび修正ポリシーを管理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。

注： URL を受け入れる VMware vSphere Lifecycle Manager API を呼び出すことをユーザーに許可する権限を管理者または信頼できるユーザーにのみ割り当てます。

表 16-44. VMware vSphere Lifecycle Manager 設定の権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.Lifecycle Manager: 設定権限.読み取り	vSphere Lifecycle Manager デポおよび修正ポリシーの読み取りを許可します。	ルート vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: 設定権限.書き込み	vSphere Lifecycle Manager デポおよび修正ポリシーへの書き込みを許可します。	ルート vCenter Server

VMware vSphere Lifecycle Manager のベースラインの管理権限

VMware vSphere Lifecycle Manager のベースラインの管理権限は、ベースラインおよびベースライン グループを管理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 16-45. VMware vSphere Lifecycle Manager のベースラインの管理権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.ベースラインの管理.ベースラインの添付	vSphere インベントリのオブジェクトへのベースラインおよびベースライン グループの添付を許可します。	ルート vCenter Server
VMware vSphere Lifecycle Manager.ベースラインの管理.ベースラインの管理	ベースラインおよびベースライン グループの作成、編集、削除を許可します。	ルート vCenter Server

VMware vSphere Lifecycle Manager のパッチおよびアップグレードの管理権限

VMware vSphere Lifecycle Manager のパッチおよびアップグレードの管理権限は、適用可能なパッチ、拡張機能、アップグレードを表示、スキャン、修正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 16-46. VMware vSphere Lifecycle Manager のパッチおよびアップグレードの管理権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.パッチおよびアップグレードの管理.修正してパッチ、拡張機能、アップグレードを適用	ベースラインを使用している場合に、パッチ、拡張機能、またはアップグレードの適用による仮想マシンおよびホストの修正を許可します。また、コンプライアンス状態の表示を許可します。	ルート vCenter Server
VMware vSphere Lifecycle Manager.パッチおよびアップグレードの管理.適用可能なパッチ、拡張機能、アップグレードのスキャン	ベースラインを使用している場合に、仮想マシンおよびホストをスキャンして適用可能なパッチ、拡張機能、またはアップグレードを検索することを許可します。	ルート vCenter Server
VMware vSphere Lifecycle Manager.パッチおよびアップグレードの管理.パッチおよび拡張機能のステージング	ベースラインを使用している場合に、ESXi ホストへのパッチまたは拡張機能のステージングを許可します。また、この権限で ESXi ホストのコンプライアンス状態の表示も許可します。	ルート vCenter Server
VMware vSphere Lifecycle Manager.パッチおよびアップグレードの管理.コンプライアンス状態の表示	vSphere インベントリにあるオブジェクトのベースライン コンプライアンス情報の表示を許可します。	ルート vCenter Server

VMware vSphere Lifecycle Manager のファイルのアップロード権限

VMware vSphere Lifecycle Manager のファイルのアップロード権限は、アップデートを vSphere Lifecycle Manager デポにインポート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。

注： URL を受け入れる VMware vSphere Lifecycle Manager API を呼び出すことをユーザーに許可する権限を管理者または信頼できるユーザーにのみ割り当てます。

表 16-47. VMware vSphere Lifecycle Manager のファイルのアップロード権限

権限名	説明	必要とするオブジェクト
VMware vSphere Lifecycle Manager.ファイルのアップロード.ファイルのアップロード	アップグレード ISO およびオフライン パッチ バンドルのアップロードを許可します。	ルート vCenter Server

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 16-48. 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.設定.ディスク リースの取得	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.設定.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.設定.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.設定.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.設定.詳細設定	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.設定.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.設定.メモリの変更	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.設定.設定の変更	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.設定.スワップ ファイルの配置の変更	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.設定.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.設定.ホスト USB デバイスの設定	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

表 16-48. 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.設定.Raw デバイスの設定	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.設定.managedBy の設定	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.設定.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
仮想マシン.設定.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.設定.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.設定.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
仮想マシン.設定.所有していないファイルの照会	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.設定.パスからの再ロード	仮想マシンの ID を維持しながら、仮想マシンの構成パ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.設定.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.設定.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.設定.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.設定.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.設定.ディスク変更の追跡の切り替え	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

表 16-48. 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.設定.フォークの親の切り替え	vmfork の親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.設定.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 内部のファイルやアプリケーションと 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、『vSphere Web Services 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 16-49. 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
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 Client 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	仮想マシンでのアプリケーション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 Client 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 Client 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 16-50. 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
仮想マシン.相互作用.CD メディアの設定	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 メディアの設定	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
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.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
仮想マシン.相互作用.VIX API によるゲスト オペレーティング システム管理	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
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

表 16-50. 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.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
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.仮想マシン上でのセッション再生	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 を再開	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
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 Tolerance 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
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 を無効にする	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
仮想マシン.相互作用.Fault Tolerance を有効にする	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 インストーラ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 16-51. 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
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 16-52. 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.ファイル アクセスの許可	仮想マシンに関連するファイル（vmx、ディスク、ログ、nvram など）への操作を可能にします。	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

表 16-52. 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.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.ゲストのカスタマイズ	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
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。

表 16-53. 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。

表 16-53. 仮想マシンのサービス構成権限 （続き）

権限名	説明
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 16-54. 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 16-55. 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設定	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

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 16-56. 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.依存関係の再設定	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

vSphere タギングの権限

vSphere タギングの権限は、タグおよびタグ カテゴリの作成および削除、vCenter Server 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 16-57. vSphere タギングの権限

権限名	説明	必要とするオブジェクト
vSphere 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
vSphere タグ付け.オブジェクトの vSphere タグを割り当てまたは割り当て解除	オブジェクトにタグの割り当てまたは割り当て解除をできるようにします。この権限を使用して、ユーザーがタグを割り当てまたは割り当て解除できるオブジェクトを制限します。	任意のオブジェクト
vSphere 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
vSphere 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
vSphere タグ付け.vSphere タグの削除	タグを削除できるようにします。	任意のオブジェクト
vSphere タグ付け.vSphere タグ カテゴリの削除	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
vSphere 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
vSphere 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
vSphere 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
vSphere 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

vSphere Client の権限

vSphere Client の権限では、vCenter Server へのオフライン アクセスを管理します。

これらの権限は、VMware Cloud にのみ適用されます。

vSphere のセキュリティ強化とコンプライアンスについて

17

組織は、データの盗難、サイバー攻撃、不正アクセスのリスクを軽減して、データの安全性を保つ必要があります。また、多くの場合、米国国立標準技術研究所 (NIST)、米国国防情報システム局のセキュリティ技術実装ガイド (DISA STIG) などの政府標準から私企業の標準まで、1 つ以上の規制を遵守する必要があります。vSphere 環境がこのような標準に準拠していることを確認するには、ユーザー、プロセス、テクノロジーなど、広範な検討事項を把握する必要があります。

注意を要するセキュリティとコンプライアンスの要点について、大まかな概要を把握しておくと、コンプライアンス戦略の計画に役立ちます。VMware Web サイトで閲覧できる他のコンプライアンス関連資料も有用です。

この章には、次のトピックが含まれています。

vSphere 環境でのセキュリティとコンプライアンス

多くの場合、セキュリティとコンプライアンスという用語は同義です。ただし、これらの用語の概念は固有であり、異なります。

多くの場合、情報セキュリティと考えられるセキュリティは、通常、機密性、整合性、可用性を実現する一連の技術制御、物理制御、および管理制御と定義されます。たとえば、ログインできるアカウントのロックダウンや、通信方式（SSH、ダイレクト コンソールなど）によって、ホストを安全に保護します。一方、コンプライアンスは、特定のタイプのテクノロジー、ベンダー、構成に関する手順を制限するさまざまな規制の枠組みによって確立された、最小限の制御に対応するために必要な一連の要件です。たとえば、クレジット カード業界 (PCI) では、セキュリティ ガイドラインを確立して、組織が顧客のアカウント データを積極的に保護できるようにしています。

セキュリティは、データの盗難、サイバー攻撃、不正アクセスのリスクを軽減します。一方、コンプライアンスは、通常定義された期間においてセキュリティ制御を実施することを証明します。セキュリティは、主に設計に関する決定事項の概要であり、テクノロジー構成で最も重視されます。コンプライアンスは、セキュリティ制御と特定の要件との相関関係を明確にすることに重点を置いています。コンプライアンスを明確にすると、必要な多くのセキュリティ制御を一目でわかるように列挙できます。セキュリティ制御それぞれのコンプライアンスの例証を取り入れると、これらのセキュリティ制御をさらに詳細に策定できます。このコンプライアンスの例証は、NIST、PCI、FedRAMP、HIPAA などの定義によって決まります。

有効なサイバーセキュリティ プログラムとコンプライアンス プログラムは、ユーザー、処理、テクノロジーの 3 つ柱から成ります。一般的には、テクノロジーのみでサイバーセキュリティに必要なすべての対策をとることができると誤解されています。テクノロジーは、情報セキュリティ プログラムの開発と実行において多くの重要な役割を果たしますが、処理と手順、認知とトレーニングを伴わないテクノロジーは、組織を脆弱にします。

セキュリティとコンプライアンスの戦略を定義する際は、次の点に注意してください。

- ユーザーは一般的な認知とトレーニングが必要であり、IT 担当者は特別なトレーニングが必要です。
- 処理には、リスクを軽減するために組織のアクティビティ、ロール、およびドキュメントをどのように用いるかを定義します。処理は、ユーザーが正しく行ってこそ効果があります。
- テクノロジーを使用すると、サイバーセキュリティのリスクが組織に与える影響を避けたり軽減できます。使用するテクノロジーは、組織が許容できるリスク レベルによって異なります。

VMware には、監査ガイドと製品適用ガイドの両方を含むコンプライアンス キットが用意されています。コンプライアンス要件と規制要件と実装ガイドのギャップを埋めるのに役立つものがあります。詳細については、『https://core.vmware.com/compliance』を参照してください。

コンプライアンスの用語集

コンプライアンスでは、独自の用語と定義が使用されており、これらを理解することが重要となります。

表 17-1. コンプライアンス用語

用語	定義
CJIS	Criminal Justice Information Services の略称で、刑事司法情報サービスを意味します。コンプライアンスにおいて、CJIS は指紋や犯罪歴などの機密情報を保護するために、地域、州、連邦の刑事司法機関や法執行機関が講じる必要があるセキュリティ対策を策定するセキュリティ ポリシーを提供する機関です。
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide の略称で、国防情報システム局のセキュリティ技術導入ガイドを意味します。国防情報システム局 (DISA) は、米国国防総省 (DoD) で使用される IT インフラストラクチャのセキュリティ状態の保守を担当するエンティティです。DISA は、セキュリティ技術導入ガイド (STIG) を開発および使用することで、このタスクを遂行します。
FedRAMP	Federal Risk and Authorization Management Program の略称で、連邦のリスクおよび認証管理プログラムを意味します。FedRAMP は、クラウド製品やサービスのセキュリティ評価、承認、および継続的監視の方法を標準化した政府規模のプログラムです。

表 17-1. コンプライアンス用語 （続き）

用語	定義
HIPAA	Health Insurance Portability and Accountability Act の略称で、医療保険の相互運用性と説明責任に関する法律を意味します。 1996 年に議会で承認された HIPAA の詳細は、以下のとおりです。 ■ 米国の何百万もの労働者やその家族が転職または失業しても、医療保険を移転して継続できるようにする ■ 医療詐欺や悪用を減らす ■ 電子請求およびその他の処理において、医療保険情報を業界全体で標準化することを義務付ける ■ 保護対象の医療情報には、保護および機密扱いを要する 後半の項目は、『vSphere セキュリティ』で最も重視されています。
NCCoE	National Cybersecurity Center of Excellence の略称で、国立のサイバーセキュリティ拠点を意味します。NCCoE は、米国の政府機関です。米国の企業が遭遇したサイバーセキュリティの問題に対する解決策を見いだし、公表して共有します。この機関では、それぞれの問題に対処するため、サイバーセキュリティ テクノロジー企業やその他の連邦政府機関、および学術界の人材を迎えてチームを組んでいます。
NIST	National Institute of Standards and Technology の略称で、米国国立標準技術研究所を意味します。1901 年に設立された NIST は、米国商務省内の連邦政府非監督機関です。NIST の使命は、計測学、標準化、およびテクノロジーを進展させて経済の安定性を高め、生活水準を向上させることで、米国の技術革新や産業の競争力を後押しすることです。
PAG	Product Applicability Guide の略称で、製品適用ガイドを意味します。コンプライアンス要件を満たす方法を模索している組織に、一般的なガイダンスを示す文書です。
PCI DSS	Payment Card Industry Data Security Standard の略称で、クレジット カード業界の情報セキュリティ標準を意味します。クレジット カード情報の受け取り、処理、保存、転送を行うすべての企業が、安全な環境を維持できるように設計された一連のセキュリティ標準です。
VVD/VCF コンプライアンス ソリューション	VMware Validated Design/VMware Cloud Foundation のコンプライアンスソリューションです。VMware Validated Design は、Software-Defined Data Center を構築し、運用するために、包括的かつ広範囲にテストされたブルー プリントを提供します。 VVD/VCF コンプライアンス ソリューションにより、複数の政府機関および業界の規制におけるコンプライアンス要件を満たすことができます。

vSphere セキュリティ設定ガイドについて

VMware は、安全な方法で VMware 製品を展開および操作するための規範的なガイダンスを示すセキュリティ強化ガイドを用意しています。vSphere では、このガイドは「vSphere セキュリティ設定ガイド」（旧称「セキュリティ強化ガイド」）と呼ばれています。

vSphere セキュリティ設定ガイドには、セキュリティのベスト プラクティスが含まれています。vSphere セキュリティ設定ガイドは、規制ガイドラインやフレームワークに直接対応していないため、コンプライアンス ガイドではありません。また、vSphere セキュリティ設定ガイドチェックリストとして使用するためのものではありません。セキュリティには常に妥協があります。セキュリティ制御を実装すると、操作性、パフォーマンス、その他の運用タスクに悪影響を及ぼす可能性があります。セキュリティの変更を行う前に、VMware からのアドバイスであっても、他の業界からのアドバイスであっても、ワークロード、使用パターン、組織構造などを慎重に検討してください。組織が規制順守のニーズの対象である場合は、vSphere 環境でのセキュリティとコンプライアンス を参照するか、https://core.vmware.com/compliance にアクセスしてください。このサイトにはコンプライアンス キットと製品監査ガイドが含まれています。管理者および規制監査者は、NIST 800-53v4、NIST 800-171、PCI DSS、HIPAA、CJIS、ISO 27001 などの規制フレームワークの仮想インフラストラクチャを保護および証明します。

「vSphere セキュリティ設定ガイド」では、次のアイテムのセキュリティについては説明されていません。

- ゲスト OS やアプリケーションなど、仮想マシン内で実行されているソフトウェア
- 仮想マシン ネットワーク経由で送受信されているトラフィック
- アドオン製品のセキュリティ

「vSphere セキュリティ設定ガイド」を「コンプライアンス」遵守の手段として使用することは意図されていません。「vSphere セキュリティ設定ガイド」は、コンプライアンス導入の初歩的ガイドとして参照するものであり、このガイドの手順を実行してもデプロイ環境がコンプライアンスを遵守しているとは限りません。コンプライアンスの詳細については、vSphere 環境でのセキュリティとコンプライアンスを参照してください。

vSphere セキュリティ設定ガイドについて

「vSphere セキュリティ設定ガイド」では、スプレッドシート形式でセキュリティ関連のガイドラインを示しています。このガイドは、vSphere セキュリティ設定を変更する際に役立ちます。これらのガイドラインは、影響を受けるコンポーネントに基づいてタブにグループ化され、次の列の一部またはすべてが含まれます。

表 17-2. 「vSphere セキュリティ設定ガイド」のスプレッドシートの列

列見出し	説明
ガイドライン ID	セキュリティ設定またはセキュリティ強化の推奨事項を参照するための一意の ID。2 つの部分から成ります。前半の部分はコンポーネントを示し、次のように定義されます。 ■ ESXi: ESXi ホスト ■ VM: 仮想マシン ■ vNetwork: 仮想スイッチ
説明	特定の推奨事項の簡単な説明。
議論	特定の推奨事項における脆弱性の説明。
構成パラメータ	該当する構成パラメータまたはファイル名（該当する場合）を入力します。

表 17-2. 「vSphere セキュリティ設定ガイド」のスプレッドシートの列 （続き）

列見出し	説明
設定値	最適な状態または推奨値。値には、次の種類があります。 ■ 該当なし ■ サイト固有 ■ False ■ True ■ 有効にする ■ 無効 ■ なし。または False
デフォルト値	vSphere で設定されているデフォルト値。
望ましい値はデフォルト値か	セキュリティ設定がデフォルトの製品設定かどうかを示します。
必要なアクション	特定の推奨事項を実行するアクションのタイプ。アクション タイプは次のとおりです。 ■ 更新 ■ 監査のみ ■ 変更 ■ 追加 ■ 削除
vSphere Client で場所を設定する	vSphere Client を使用して値を確認する手順。
デフォルトからの変更における機能への悪影響？	セキュリティ推奨事項を使用することによる潜在的な悪影響の説明（該当する場合）。
PowerCLI コマンドの評価	PowerCLI を使用して値を確認する手順。
PowerCLI コマンドの修正例	PowerCLI を使用して値を設定（修正）する手順。
vCLI コマンドの修正	vCLI コマンドを使用して値を設定（修正）する手順。
PowerCLI コマンドの評価	PowerCLI コマンドを使用して値を確認する手順。
PowerCLI コマンドの修正	PowerCLI コマンドを使用して値を設定（修正）する手順。
ホスト プロファイルを使用した設定の有効化	ホスト プロファイルを使用して設定を行うかどうかを指定します (ESXi ガイドラインにのみ適用)。
堅牢化	TRUE の場合、ガイドラインには、準拠する実装は 1 つしかありません。FALSE の場合、複数の設定によってガイドラインの実装を満たすことができます。多くの場合、実際の設定はサイト固有です。
サイト固有の設定	TRUE の場合、ガイドラインに準拠する設定は、展開されている vSphere に固有のルールや標準によって異なります。
監査の設定	TRUE の場合、サイト固有のルールを満たすため、リストの設定値の変更が必要なこともあります。

注： 上記の列は、時間の経過とともに必要に応じて変わることがあります。たとえば、「DISA STIG ID」、「堅牢化」、「サイト固有の設定」の列は、最近追加されました。「vSphere セキュリティ設定ガイド」の更新に関する告知については、https://blogs.vmware.com を確認してください。

ご使用の環境に、「vSphere セキュリティ設定ガイド」のガイドラインを盲目的に適用しないでください。十分に時間をかけて各設定を評価し、その設定を適用するかどうかについては十分な情報に基づいて決定してください。少なくとも、評価に関する列の手順を実行して、展開するセキュリティを確認してください。

「vSphere セキュリティ設定ガイド」は、展開している環境にコンプライアンスを導入する際に役立つガイドです。国防情報システム局 (DISA) およびその他のコンプライアンス ガイドラインとともに「vSphere セキュリティ設定ガイド」を使用すると、vSphere セキュリティ制御を各ガイドラインごとの特徴的なコンプライアンスにマッピングできます。

米国国立標準技術研究所について

米国国立標準技術研究所 (NIST) は、テクノロジー、メトリック、標準、およびガイドラインを開発する、非監督政府機関です。NIST の標準およびガイドラインへの準拠は、今日、多くの業界で最優先事項となっています。

米国国立標準技術研究所 (NIST) は、1901 年に設立され、現在は、米国商務省に所属しています。NIST は、米国で最も古い物理科学研究所の 1 つです。現在、NIST で対応する標準は、人類が作り出すテクノロジーのうち、ナノ単位のデバイスといった最小のものから、耐震の超高層ビルやグローバル通信ネットワークなどの極めて複雑で巨大なものに至るまで多岐に渡ります。

連邦情報セキュリティ管理法 (FISMA) は、2002 年に成立した米国連邦法で、情報セキュリティと保護プログラムを開発、文書化、および実装する連邦機関で必須となっています。NIST は、キーのセキュリティ標準およびガイドライン（FIPS 199、FIPS 200、SP 800 シリーズなど）を作成して、FISMA の実装で重要な役割を果たしています。

政府機関も民間組織も、情報システムの保護に NIST 800-53 を使用しています。多様な脅威から組織の業務（主要業務、機能、イメージ、風評を含む）、組織の資産、および個人を保護するために不可欠なのがサイバーセキュリティとプライバシー管理です。脅威には、悪意のあるサイバー攻撃、自然災害、構造的な障害、人的ミスなども含まれます。VMware は、サードパーティの監査パートナーの協力を得て、NIST 800-53 の管理策に対する VMware 製品およびソリューションの準拠度を評価しています。詳細については、https://www.nist.gov/cyberframework の NIST に関する Web ページを参照してください。

DISA STIG について

国防情報システム局 (DISA) は、セキュリティ技術導入ガイド (STIG) を開発し、公開しています。DISA STIG は、システムの強化と脅威の軽減のための技術的なガイダンスです。

国防情報システム局 (DISA) は、米国国防総省 (DoD) の戦闘支援機関で、DOD 情報ネットワーク (DODIN) のセキュリティ状態の保守を担当します。DISA がこのタスクを遂行する方法の 1 つは、セキュリティ技術導入ガイド (STIG) の実装を開発し、普及させ、義務付けることです。つまり、STIG は、システムを強化するための標準ベースのポータブル ガイドです。STIG は、DoD の IT システムに必須であるため、DoD 以外のエンティティにとっても、精査されたセキュアなベースラインとなり、セキュリティ状態を測定することができます。

VMware などのベンダーは、DISA プロトコルとフィードバックに基づいて、推奨されるセキュリティ強化ガイダンスを DISA に送信して、評価を受けています。このプロセスが完了すると、DISA 組織の Web サイト https://public.cyber.mil/stigs/に公式の STIG が公開されます。VMware は『vSphere セキュリティ設定ガイド』の一部として、vSphere のセキュリティ ベースラインおよびセキュリティ強化のガイダンスを提供しています。https://core.vmware.com/security を参照してください。

VMware のセキュリティ開発ライフサイクルについて

VMware のセキュリティ開発ライフサイクル (SDL) プログラムは、VMware ソフトウェア製品の開発フェーズでのセキュリティ リスクを特定および軽減します。また、VMware は、VMware Security Response Center (VSRC) を運営し、VMware 製品で発生するソフトウェア セキュリティの問題を分析および修正します。

SDL は、VMware Security Engineering, Communication, and Response (vSECR) グループと VMware 製品開発グループが、セキュリティの問題の特定と軽減に使用するソフトウェア開発手法です。VMware セキュリティ開発ライフサイクルの詳細については、https://www.vmware.com/security/sdl.html の Web ページを参照してください。

VSRC は、お客様やセキュリティ研究コミュニティと連携して、セキュリティの問題に対処し、セキュリティに関する実用的な情報を適切なタイミングで顧客に提供するという目標の達成に取り組んでいます。VMware Security Response Center の詳細については、https://www.vmware.com/security/vsrc.html の Web ページを参照してください。

監査ログの記録

ネットワーク トラフィック、コンプライアンス アラート、ファイアウォール アクティビティ、オペレーティング システムの変更、およびプロビジョニング アクティビティの監査ログを記録することは、どの IT 環境でもセキュリティを維持するためのベスト プラクティスと見なされます。さらに、ログ記録は、多くの規制や標準で明確な要件になっています。

インフラストラクチャの変更を確実に認識するために実施する最初のステップの 1 つは、環境を監査することです。vSphere には、変更の表示および追跡を可能にするツールがデフォルトで含まれています。たとえば、vSphere Client の [タスクとイベント] タブを使用して、vSphere 階層内の任意のオブジェクトでどのような変更が発生したかを確認できます。PowerCLI を使用して、イベントやタスクを取得することもできます。また、vRealize Log Insight の監査ログ記録機能では、重要なシステム イベントの収集と保持がサポートされます。さらに、多くのサードパーティ製のツールで、vCenter Server の監査機能が提供されています。

ログ ファイルが示す監査証跡は、ホストや仮想マシンなどに誰または何がアクセスしているかを判断するために役立ちます。詳細については、ESXi ログ ファイルの場所を参照してください。

Single Sign-On 監査イベント

Single Sign-On (SSO) の監査イベントは、SSO サービスにアクセスする際のユーザーまたはシステムのアクションの記録です。

vCenter Server 6.7 Update 2 以降では、次の操作のイベントを追加することで、VMware vCenter Single Sign-On 監査機能が向上しています。

- ユーザー管理
- ログイン
- グループの作成
- ID ソース
- ポリシーの更新

サポートされている ID ソースは vsphere.local、統合 Wiindows 認証 (IWA)、および LDAP を介した Active Directory です。

Single Sign-On を使用して vCenter Server にログインしたり、SSO に影響する変更を加えた場合、SSO 監査ログ ファイルに次の監査イベントが書き込まれます。

- [ログインおよびログアウトの試行：]成功または失敗したログインおよびログアウト操作すべてに関するイベント
- [権限の変更：]ユーザー ロールまたは権限の変更に関するイベント
- [アカウントの変更：]ユーザーのアカウント情報（ユーザー名、パスワード、その他のアカウント情報）の変更に関するイベント
- [セキュリティの変更：]セキュリティ設定、パラメータ、ポリシーの変更に関するイベント
- [アカウントの有効化または無効化：]アカウントの有効と無効の切り替えに関するイベント
- [ID ソース：]ID ソースの追加、削除、編集に関するイベント

vSphere Client の [監視] タブに、イベント データが表示されます。『vSphere の監視とパフォーマンス』を参照してください。

SSO 監査イベント データには、次の詳細事項が含まれます。

- イベントが発生した時点のタイムスタンプ
- アクションを実行したユーザー
- イベントの説明
- イベントの重要度
- vCenter Server への接続に使用されるクライアントの IP アドレス（該当する場合）

SSO 監査イベント ログの概要

vSphere Single-Sign On 処理で、監査イベントが `/var/log/audit/sso-events/` ディレクトリの `audit_events.log` ファイルに書き込まれます。

注意： `audit_events.log` ファイルは、手動で編集しないでください。監査ログを記録できなくなる可能性があります。

`audit_events.log` ファイルを使用する場合は、次の点に注意してください。

- ログ ファイルは、50 MB に達するとアーカイブされます。
- 最大 10 個のアーカイブ ファイルが保存されます。上限に達すると、新しいアーカイブの作成時に最も古いファイルが消去されます。
- アーカイブ ファイルの名前は `audit_events-` <インデックス>`.log.gz` です。このインデックスは 1 から 10 までの数字です。最初に作成されたアーカイブは、インデックス 1 です。以降、アーカイブが作成されるごとに数字が増えていきます。
- 最も古いイベントは、アーカイブ インデックス 1 です。最も大きい数字のインデックス ファイルが最新のアーカイブです。

セキュリティとコンプライアンスの段取りについて

まず始めに、インフラストラクチャのすべての脆弱性を把握するために、セキュリティ評価を実行します。セキュリティ評価は、セキュリティ監査の一環として行われます。セキュリティ コンプライアンスなどの制度と遵守状態の両方を対象とします。

セキュリティ評価とは、通常、組織の物理インフラストラクチャ（ファイアウォール、ネットワーク、ハードウェアなど）の脆弱性と欠陥を識別するスキャンを指します。セキュリティ評価は、セキュリティ監査と同じではありません。セキュリティ監査には、物理インフラストラクチャの確認だけでなく、セキュリティ コンプライアンスなどのポリシーおよび標準操作手順など、他の要素も含まれます。監査を行うと、システムで発生した問題を解決する手順を判断できます。

セキュリティ監査を実施する場合は、以下の一般的な問題点を把握する必要があります。

1 組織でコンプライアンスの遵守が義務付けられているか。義務付けられている場合、遵守する必要があるコンプライアンス。

2 監査の間隔。

3 内部自己評価の間隔。

4 以前の監査結果を確認したか。

5 監査にサードパーティの監査組織を利用しているか。その場合、仮想化の最適レベル。

6 システムおよびアプリケーションに対して脆弱性スキャンを実行するか。スキャンはどのタイミングで、どれくらいの頻度で実行するか。

7 内部のサイバーセキュリティ ポリシー。

8 監査ログをニーズに合わせて設定しているか。監査ログの記録を参照してください。

何から始めれたらいいか、具体的な案や指示がない場合は、とりあえず次の方法で vSphere 環境を保護できます。

- 最新のソフトウェアおよびファームウェアのパッチを適用して、環境を最新の状態に保つ
- すべてのアカウントにおいて適切なパスワード管理および検疫を維持する
- ベンダー承認のセキュリティ推奨事項を確認する
- VMware のセキュリティ構成ガイド（vSphere セキュリティ設定ガイドについて）を参照する
- NIST、ISO などのポリシー フレームワークから容易に使用できる実証済みガイダンスを用いる
- PCI、DISA、FedRAMP などのコンプライアンス フレームワークのガイダンスを実行する

vCenter Server および FIPS

vSphere 7.0 Update 2 以降では、vCenter Server Appliance で FIPS 検証済み暗号化を有効にできます。

FIPS 140-2 は、暗号化モジュールのセキュリティ要件を指定する、米国およびカナダの政府規格です。vSphere は、FIPS 検証済みの暗号化モジュールを使用して、FIPS 140-2 標準で指定された暗号化モジュールと一致します。vSphere FIPS サポートは、規制の厳しいさまざまな環境でのコンプライアンスとセキュリティのアクティビティを容易にすることを目的としています。

vSphere 6.7 以降では、ESXi および vCenter Server は FIPS 検証済み暗号化を使用して管理インターフェイスと VMware Certificate Authority (VMCA) を保護します。

vSphere 7.0 Update 2 以降では、vCenter Server Appliance に FIPS 検証済みの暗号化が追加されています。デフォルトでは、この FIPS 検証オプションは無効になっています。

注： vSphere は FIPS よりも互換性を優先するため、コンポーネントによっては注意すべき点があります。FIPS を使用する場合の考慮事項を参照してください。

FIPS モジュール

暗号化モジュールは、セキュリティ機能を実装するハードウェア、ソフトウェア、またはファームウェアのセットです。ESXi では、FIPS 140-2 検証済みの暗号化モジュールがいくつか使用されます。

次の表に、ESXi で使用されている FIPS 140-2 検証済みの暗号化モジュールのセットを示します。

表 17-3. FIPS モジュール

暗号化モジュール	セキュリティ ポリシー バージョン	アルゴリズム (CAVP)	暗号化モジュール検証プログラム
Vmkernel 暗号化モジュール	1.0	AES、SHS、DRBG、HMAC (C 1172)	証明書 #3073
Vmkernel 暗号化モジュール ローダー	該当なし	HMAC、SHS (C 1171)	証明書 #3073
Vmkernel DRBG 暗号化モジュール	該当なし	AES、DRBG (C 499)	なし
VMware OpenSSL FIPS オブジェクト モジュール	2.0.20-vmw	DRBG、AES、SHS、HMAC、DSA、RSA、ECDSA、KAS-FFC、KAS-ECC (C 470)	証明書 #3550 および #3857

vCenter Server Appliance で FIPS を有効または無効にする

HTTP 要求を使用して、vCenter Server Appliance で FIPS 検証済みの暗号化を有効または無効にできます。

さまざまな方法を使用して HTTP 要求を実行できます。このタスクでは、vSphere Client のデベロッパー センターを使用して vCenter Server Appliance で FIPS を有効または無効にする方法を示します。API を使用して vCenter Server Appliance を操作する方法の詳細については、『VMware vCenter Server 管理プログラミング ガイド』を参照してください。

手順

1. vSphere Client で vCenter Server にログインします。
2. メニューから、[デベロッパー センター] を選択します。
3. [API Explorer] をクリックします。
4. [API を選択] ドロップダウン メニューで、[アプライアンス] を選択します。
5. カテゴリを下にスクロールして、[system/security/global_fips] を展開します。
6. [GET] を展開し、[実行する] の下の [実行] をクリックします。

   現在の設定は、[応答] で確認できます。

7 設定を変更します。

a FIPS を有効にするには、[PUT] を展開し、`request_body` に以下を入力して、[実行] をクリックします。

```
{
"enabled":true
}
```

b FIPS を無効にするには、[PUT] を展開し、`request_body` に以下を入力して、[実行] をクリックします。

```
{
"enabled":false
}
```

結果

FIPS を有効または無効にした後に、vCenter Server Appliance が再起動します。

FIPS を使用する場合の考慮事項

vCenter Server Appliance で FIPS を有効にする場合、現在、一部のコンポーネントには機能上の制約があります。

vCenter Server で FIPS を有効にした後は違いは見られませんが、注意すべき考慮事項がいくつかあります。

表 17-4. FIPS に関する検討事項

製品またはコンポーネント	検討事項	回避策
vSphere Single Sign-On	FIPS を有効にすると、vCenter Server はフェデレーション認証用の暗号化モジュールのみをサポートします。その結果、RSA SecureID および一部の CAC カードは機能しなくなります。	フェデレーション認証を使用します。詳細については、『vSphere 認証』ドキュメントを参照してください。
VMware 以外およびパートナーの vSphere Client UI プラグイン	これらのプラグインは、FIPS が有効になっていると機能しない場合があります。	プラグインをアップグレードして、準拠する暗号化ライブラリを使用します。詳細については、https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance の「FIPS コンプライアンスのためのローカル プラグインの準備」を参照してください。
vCenter Server ファイルベースのバックアップおよびリストアのメカニズム	SMB を使用したファイルベースのバックアップとリストアは FIPS に準拠していません。	バックアップとリストアには別のプロトコルを使用します（FTP、FTPS、HTTP、HTTPS、SFTP、または NFS）。