Platform Services Controller の管理

Update 2
変更日：2022 年 5 月 02 日
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

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

Platform Services Controller の管理について

Platform Services Controller の管理ドキュメントでは、VMware® Platform Services Controller ™ を個々の vSphere 環境に組み込む方法について説明します。また、証明書管理や vCenter Single Sign-On の設定などの一般的なタスクを実行するための情報を提供します。

『Platform Services Controller の管理』では、vCenter Single Sign-On による認証を設定する方法と、vCenter Server および関連サービスの証明書を管理する方法について説明します。

表 1-1. Platform Services Controller の管理の特徴

トピック	内容
Platform Services Controller の導入方法	■ vCenter Server および Platform Services Controller の導入モデル。注：この情報は、製品のリリースごとに変更されます。 ■ Linux および Windows の Platform Services Controller サービス。 ■ Platform Services Controller サービスの管理。 ■ VAMI を使用した Platform Services Controller アプライアンスの管理。
vCenter Single Sign-On による vSphere 認証	■ 認証プロセスのアーキテクチャ。 ■ ドメイン内のユーザー認証用に ID ソースを追加する方法。 ■ 2 要素認証。 ■ ユーザー、グループ、およびポリシーの管理。
vSphere セキュリティ証明書	■ 証明書モデル、および証明書の置き換えのオプション。 ■ ユーザー インターフェイスで証明書を置き換え（単純なケース）。 ■ Certificate Manager ユーティリティを使用した証明書を置き換え。 ■ CLI を使用した証明書を置き換え（複雑なケース）。 ■ 証明書管理 CLI リファレンス。

関連ドキュメント

『vSphere のセキュリティ』では、使用可能なセキュリティ機能と、環境を攻撃から保護するための対策について説明しています。このドキュメントには、権限を設定する方法についての説明と、コマンドの実行に必要な権限情報が含まれています。

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 Security Configuration Guide」（旧称「セキュリティ強化ガイド」）を公開しており、http://www.vmware.com/security/hardening-guides.html 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。

対象読者

本書は、Platform Services Controller および関連するサービスを設定する管理者を対象にしています。ここに記載の情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジーおよびデータセンターの運用に詳しい方を想定しています。

vSphere Client および vSphere Web Client

本書の説明は、vSphere Client（HTML5 ベースの GUI）に対応しています。ここに記載のガイダンスは、vSphere Web Client（Flex ベースの GUI）を使用したタスクで使用できます。

vSphere Client と vSphere Web Client でワークフローが大きく異なるタスクでは、各クライアント インターフェイスに応じたステップが提供され、手順が重複しています。vSphere Web Client に関連する手順は、タイトルに vSphere Web Client が含まれています。

注： vSphere 6.7 Update 1 では、vSphere Web Client 機能のほぼすべてが vSphere Client に実装されています。サポート対象外の残りの機能を記載した最新のリストについては、「vSphere Client の機能の更新」を参照してください。

更新情報

『Platform Services Controller の管理』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。

『Platform Services Controller の管理』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 5 月 02 日	■ vCenter Single Sign-On によって環境を保護する方法の誤記を訂正しました。 ■ Active Directory LDAP Server および OpenLDAP Server ID ソースの設定へのマイナー更新。 ■ アプライアンスでの新しい STS 署名証明書の生成へのマイナー更新。 ■ LDAPS SSL 証明書の有効期限日の判断内の手順を修正しました。 ■ 異なるソリューション パスの証明書の要件へのマイナー更新。 ■ 新しい VMCA ルート証明書の再生成およびすべての証明書の置き換えへのマイナー更新。
2021 年 10 月 08 日	■ 証明書の要件となる否認防止をドキュメントから削除。 ■ Platform Services Controller サービスへのマイナー更新。 ■ Active Directory LDAP Server および OpenLDAP Server ID ソースの設定に記載されているユーザー名とプライマリ サーバの URL の説明を更新。 ■ RSA SecurID 認証の設定に記載されている、`-securIDAuthn` にダッシュが含まれている場合に発生する問題を修正。コピー時にこのコマンドを実行すると、適切に実行されませんでした。 ■ カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換えの誤記を修正。 ■ サービスの停止と開始についてへのマイナー更新。 ■ VMCA 署名付き証明書によるマシン SSL 証明書の置き換えの誤記を修正。 ■ dir-cli コマンド リファレンスの誤記を修正。
2020 年 8 月 12 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。
2020 年 5 月 11 日	■ ユーザーのベース DN とグループのベース DN に関する情報を Active Directory LDAP Server および OpenLDAP Server ID ソースの設定 に追加しました。 ■ Windows 版 vCenter Server のログの場所を Platform Services Controller サービス ログのリファレンス に追加しました。 ■ 証明書の要求およびカスタム ルート証明書のインポートへのマイナー更新。 ■ certool 初期化コマンド リファレンス を更新して、`--gencsr` オプションが `--initcsr` の代わりに使用されるようになりました。 ■ vpxd 証明書ストアが vCenter Server Appliance にのみ存在することを示すように ソリューション ユーザー証明書の置き換え（中間 CA） を更新しました。 ■ イベント ID 2889 に関する情報を Active Directory ID ソースの設定 に追加しました。
2019 年 8 月 26 日	■ certool 構成オプションの変更 の `certool.cfg` ファイルの場所を修正しました。 ■ RSA SecurID 認証の設定 の userPrincipalName 属性の使用に関する情報を更新しました。
2019 年 4 月 11 日	初期リリース。

Platform Services Controller の導入方法

1

Platform Services Controller は vSphere 環境に一般的なインフラストラクチャ サービスを提供します。サービスには、ライセンス、証明書管理、および vCenter Single Sign-On との認証が含まれます。

Platform Services Controller インターフェイスの機能向上 (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_qcyuyhrt/uiConfId/49694343/)

この章には、次のトピックが含まれています。

- vCenter Server および Platform Services Controller のデプロイ タイプ
- 外部の Platform Services Controller インスタンスと高可用性を使用したデプロイ トポロジ
- vSphere ドメイン、ドメイン名、サイトについて
- Platform Services Controller の機能
- Platform Services Controller サービスの管理
- Platform Services Controller アプライアンスの管理

vCenter Server および Platform Services Controller のデプロイ タイプ

組み込みのまたは外部の Platform Services Controller を使用する vCenter Server Appliance をデプロイすることも、 vCenter Server for Windows をインストールすることもできます。また、Platform Services Controller は、アプライアンスとしてデプロイすることも、Windows にインストールすることもできます。必要に応じて、オペレーティング システムの混在環境を使用できます。

vCenter Server Appliance のデプロイまたは vCenter Server for Windows のインストールを行う前に、ご使用の環境に適したデプロイ モデルを判断する必要があります。デプロイまたはインストールごとに、3 つのデプロイ タイプのいずれかを選択する必要があります。

表 1-1. vCenter Server および Platform Services Controller のデプロイ タイプ

デプロイ タイプ	説明
Platform Services Controller が組み込まれた vCenter Server	Platform Services Controller にバンドルされているすべてのサービスが、同じ仮想マシンまたは物理サーバで vCenter Server サービスと共にデプロイされます。
Platform Services Controller	Platform Services Controller にバンドルされているサービスのみが仮想マシンまたは物理サーバにデプロイされます。
外部の Platform Services Controller を使用する vCenter Server （外部の Platform Services Controller が必要）	vCenter Server サービスのみが仮想マシンまたは物理サーバにデプロイされます。 このような vCenter Server インスタンスは、以前にデプロイまたはインストールされた Platform Services Controller インスタンスに登録する必要があります。

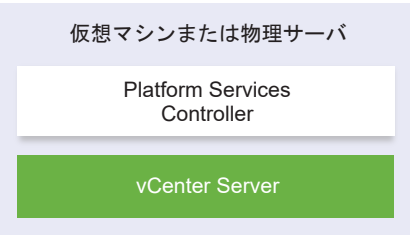
注： 外部の Platform Services Controller を使用する vCenter Server 展開環境は、今後の vSphere リリースではサポート対象外となる予定です。vCenter Server 展開環境への展開またはアップグレードには、組み込みの Platform Services Controller を使用してください。詳細については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/60229) を参照してください。

Platform Services Controller が組み込まれた vCenter Server

組み込みの Platform Services Controller を使用すると、単一のサイトに独自の vCenter Single Sign-On ドメインを持つスタンドアロン デプロイになります。

vSphere 6.5 Update 2 以降では、Platform Services Controller が組み込まれた vCenter Server の他のインスタンスを参加させて拡張リンク モードを有効にすることができます。

図 1-1. Platform Services Controller が組み込まれた vCenter Server



Platform Services Controller が組み込まれている vCenter Server をインストールすることには、次のようなメリットがあります。

- vCenter Server と Platform Services Controller がネットワークを介して接続されておらず、vCenter Server と Platform Services Controller の間の接続性問題や名前解決問題が原因で vCenter Server が停止することがなくなります。
- Windows 仮想マシンまたは物理サーバに vCenter Server をインストールする場合、必要な Windows ライセンスの数が少なくて済みます。
- 管理する仮想マシンまたは物理サーバの数が少なくて済みます。

Platform Services Controller が組み込まれている vCenter Server Appliance は、vCenter High Availability 構成で実行できます。詳細については、『vSphere の可用性』を参照してください。

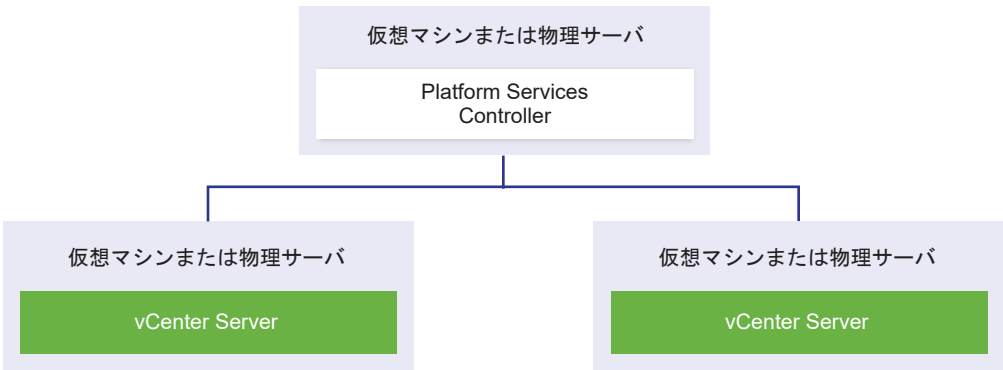
Platform Services Controller と、外部の Platform Services Controller を使用する vCenter Server

Platform Services Controller インスタンスをデプロイまたはインストールする場合、vCenter Single Sign-On ドメインの作成や、既存の vCenter Single Sign-On ドメインへの参加を行うことができます。ドメインに参加した Platform Services Controller インスタンスは、インフラストラクチャ データ（認証および情報）をレプリケートし、複数の vCenter Single Sign-On サイトにまたがることができます。詳細については、vSphere ドメイン、ドメイン名、サイトについてを参照してください。

注： 外部の Platform Services Controller を使用する vCenter Server 展開環境は、今後の vSphere リリースではサポート対象外となる予定です。vCenter Server 展開環境への展開またはアップグレードには、組み込みの Platform Services Controller を使用してください。詳細については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/60229) を参照してください。

複数の vCenter Server インスタンスを単独の共通外部 Platform Services Controller インスタンスに登録できます。vCenter Server インスタンスでは、その登録先の Platform Services Controller インスタンスの vCenter Single Sign-On サイトが想定されます。1 つの共通または異なる参加済み Platform Services Controller インスタンスに登録されているすべての vCenter Server インスタンスは、拡張リンク モードで接続されます。

図 1-2. 共通の外部 Platform Services Controller を使用する 2 つの vCenter Server インスタンスの例



外部 Platform Services Controller を使用する vCenter Server をインストールすることには、次のようなデメリットがあります。

- vCenter Server と Platform Services Controller の間の接続において接続の問題および名前解決の問題が発生する可能性があります。
- Windows 仮想マシンまたは物理サーバに vCenter Server をインストールする場合、必要な Windows ライセンスの数が多くなります。
- 多くの仮想マシンまたは物理サーバを管理する必要があります。

Platform Services Controller および vCenter Server の上限については、『構成の上限』を参照してください。

外部の Platform Services Controller を使用する vCenter Server Appliance を vCenter High Availability 構成で構成する方法については、『vSphere の可用性』を参照してください。

注： 外部 Platform Services Controller を使用する vCenter Server をデプロイまたはインストールした後、デプロイ タイプを再構成して、組み込みの Platform Services Controller を使用する vCenter Server に切り替えることができます。

オペレーティング システムの混在環境

Windows 上にインストールされた vCenter Server インスタンスは、Windows 上にインストールされた Platform Services Controller または Platform Services Controller アプライアンスに登録することができます。vCenter Server Appliance は、Windows 上にインストールされた Platform Services Controller または Platform Services Controller アプライアンスに登録することができます。vCenter Server と vCenter Server Appliance の両方を同じ Platform Services Controller に登録できます。

図 1-3. Windows 上の外部 Platform Services Controller との混在オペレーティング システム環境の例

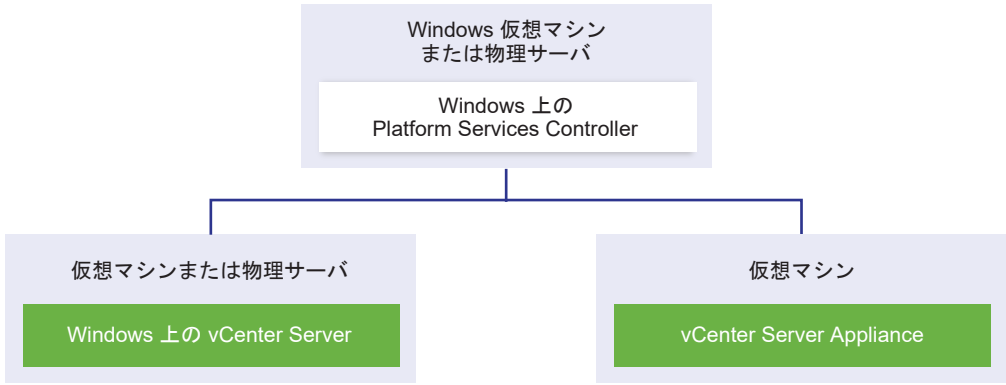
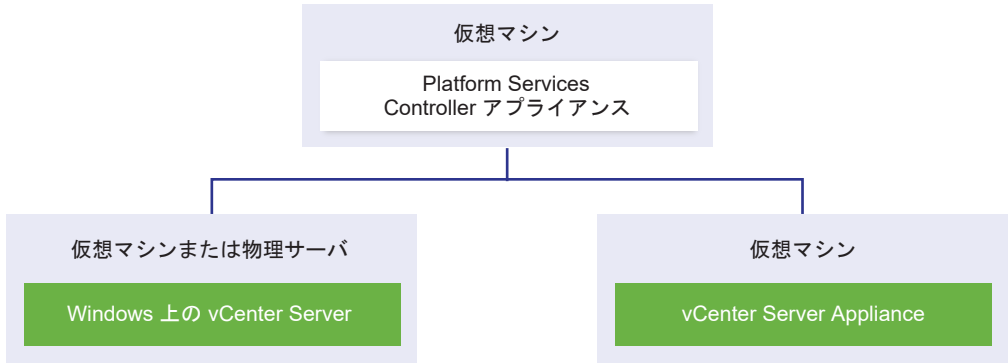


図 1-4. 外部 Platform Services Controller アプライアンスとの混在オペレーティング システム環境の例



注： 管理とメンテナンスを容易にするには、vCenter Server および Platform Services Controller のアプライアンスのみまたは Windows インストールのみを使用します。

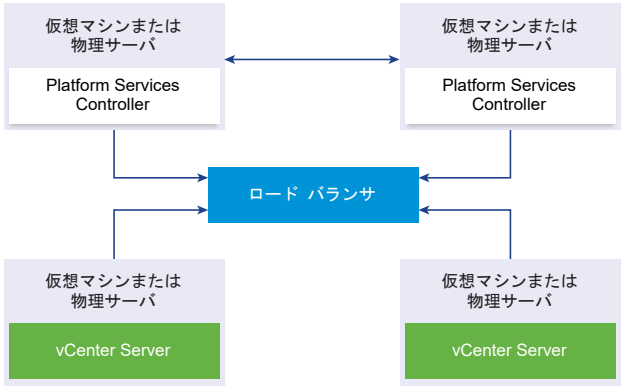
外部の Platform Services Controller インスタンスと高可用性を使用したデプロイ トポロジ

外部のデプロイで Platform Services Controller の高可用性を確保するには、vCenter Single Sign-On ドメインに、2 つ以上の参加済み Platform Services Controller インスタンスをインストールするかデプロイする必要があります。サードパーティのロード バランサを使用する場合は、ダウンタイムのなしの自動フェイルオーバーを確実に実行することができます。

注： 外部の Platform Services Controller を使用する vCenter Server 展開環境は、今後の vSphere リリースではサポート対象外となる予定です。vCenter Server 展開環境への展開またはアップグレードには、組み込みの Platform Services Controller を使用してください。詳細については、ナレッジベースの記事 KB60229 を参照してください。

ロード バランサを使用する Platform Services Controller

図 1-5. Platform Services Controller インスタンスのロード バランシングされたペアの例



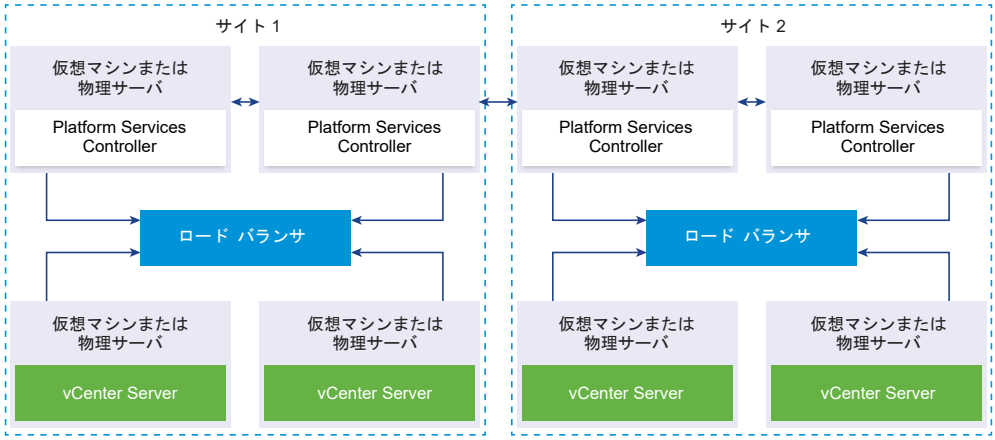
サイトごとにサードパーティのロード バランサを使用して、そのサイトに対して自動フェイルオーバーに対応する Platform Services Controller 高可用性を構成することができます。ロード バランサの背後の Platform Services Controller インスタンスの最大数については、『構成の上限』ドキュメントを参照してください。

重要： ロード バランサの背後で Platform Services Controller の高可用性を構成するには、Platform Services Controller インスタンスが同じオペレーティング システム タイプである必要があります。ロード バランサの背後では、オペレーティング システム タイプが異なる Platform Services Controller インスタンスはサポートされていません。

vCenter Server インスタンスはロード バランサに接続されます。Platform Services Controller インスタンスが応答を停止した場合、ロード バランサはその他の機能する Platform Services Controller インスタンス間で負荷を自動的に分散し、ダウンタイムを発生させません。

vCenter Single Sign-On サイト間でロード バランサを使用する Platform Services Controller

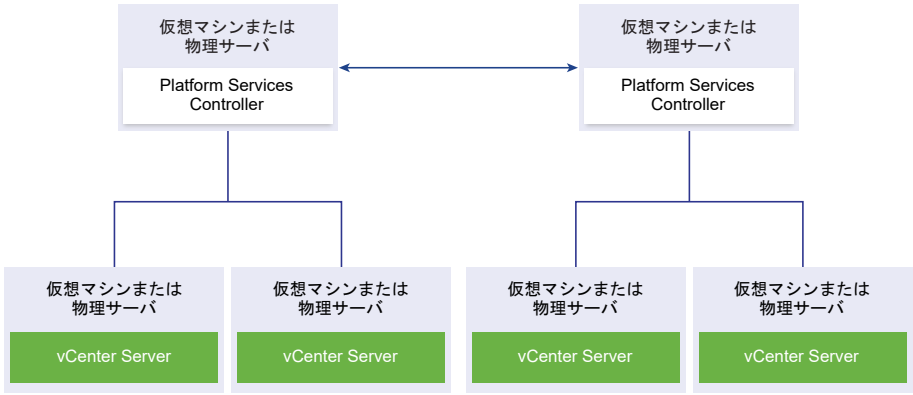
図 1-6. 2 つのサイト間でロード バランシングされる 2 ペアの Platform Services Controller インスタンスの例



vCenter Single Sign-on ドメインが複数のサイトにまたがる場合があります。自動フェイルオーバーに対応する Platform Services Controller 高可用性をドメイン全体で確保するには、各サイトに個別のロード バランサを構成する必要があります。

ロード バランサを使用しない Platform Services Controller

図 1-7. ロード バランサを使用しない 2 つの参加済み Platform Services Controller インスタンスの例



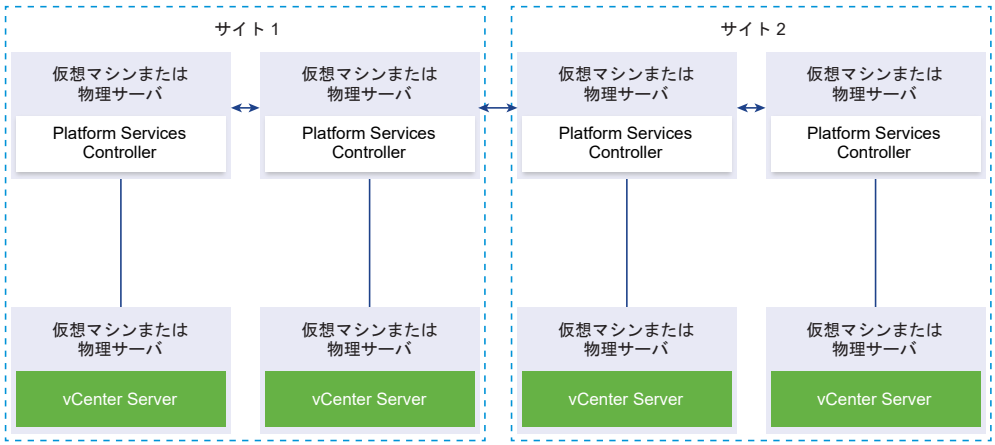
ロード バランサがない同一のサイトに複数の Platform Services Controller インスタンスを参加させる場合、そのサイトに対して、手動フェイルオーバーに対応する Platform Services Controller 高可用性を構成します。

Platform Services Controller インスタンスが応答を停止した場合は、サイトに登録した vCenter Server インスタンスを手動でフェイルオーバーする必要があります。インスタンスをフェイルオーバーするには、同じサイト内で機能する他の Platform Services Controller インスタンスに、該当のインスタンスを指定し直します。vCenter Server インスタンスを別の外部の Platform Services Controller に指定し直す方法については、『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。

注： vCenter Single Sign-On ドメインに 3 つ以上の Platform Services Controller インスタンスがある場合は、リング トポロジを手動で作成できます。リング トポロジがあると、いずれかのインスタンスに障害が発生したときに Platform Services Controller の信頼性が確保されます。リング トポロジを作成するには、デプロイした最初と最後の Platform Services Controller インスタンスに対して `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` コマンドを実行します。

vCenter Single Sign-On サイト間でロード バランサを使用しない Platform Services Controller

図 1-8. ロード バランサがない 2 つのサイトに置かれた 2 ペアの参加済み Platform Services Controller インスタンスの例



vCenter Single Sign-on ドメインが複数のサイトにまたがる場合があります。ロード バランサが使用できない場合は、同じサイト内で障害が発生した Platform Services Controller から、機能するものに vCenter Server を手動で指定し直すことができます。vCenter Server インスタンスを別の外部の Platform Services Controller に指定し直す方法については、『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。

vSphere ドメイン、ドメイン名、サイトについて

各 Platform Services Controller は vCenter Single Sign-On ドメインに関連付けられています。ドメイン名のデフォルトは vsphere.local ですが、最初の Platform Services Controller のインストール中に変更できます。ドメインによって、ローカルの認証スペースが決まります。ドメインを複数のサイトに分割して、それぞれの Platform Services Controller と vCenter Server インスタンスをサイトに割り当てることができます。サイトは論理的な構築概念ですが、通常、地理的な場所に対応します。

Platform Services Controller ドメイン

Platform Services Controller をインストールすると、vCenter Single Sign-On ドメインを作成するか、または既存のドメインに参加するか確認を求められます。

ドメイン名は、すべての Lightweight Directory Access Protocol (LDAP) の内部構造に対応する VMware Directory Service (vmdir) によって使用されます。

vSphere 6.0 以降では、vSphere ドメインに一意の名前を付けることができます。認証が競合しないように、OpenLDAP や Microsoft Active Directory、その他のディレクトリ サービスで使用されていない名前を使用してください。

注： Platform Services Controller または vCenter Server インスタンスが属するドメインは変更できません。

ドメインの名前を指定すると、ユーザーとグループを追加できます。通常、Active Directory または LDAP ID ソースを追加し、その ID ソースでユーザーとグループを認証できるようにするのが合理的です。vCenter Server または Platform Services Controller のインスタンス、あるいは vRealize Operations などの VMware 製品をドメインに追加することもできます。

Platform Services Controller サイト

Platform Services Controller ドメインを論理的なサイトに編成することができます。VMware Directory Service のサイトは、vCenter Single Sign-On ドメイン内の Platform Services Controller インスタンスをグループ分けする論理的なコンテナです。

vSphere 6.5 から、サイトは重要になりました。Platform Services Controller のフェイルオーバー中、vCenter Server インスタンスは同じサイトの別の Platform Services Controller にアフィニティ化されます。vCenter Server インスタンスが、地理的に離れた場所の Platform Services Controller にアフィニティ化されないようにするために複数のサイトを使用できます。

Platform Services Controller をインストールまたはアップグレードすると、サイト名を入力するように求められます。『vCenter Server のインストールとセットアップ』ドキュメントを参照してください。

Platform Services Controller の機能

Platform Services Controller は、vSphere で ID 管理、証明書管理、ライセンス管理などのサービスをサポートします。

主な機能

Platform Services Controller には Platform Services Controller サービスに説明されている複数のサービスが含まれており、主な機能は次のとおりです。

- vCenter Single Sign-On による認証
- VMware Certificate Manager (VMCA) 証明書を使用したデフォルトでの vCenter Server コンポーネントおよび ESXi ホストのプロビジョニング
- VMware Endpoint 証明書ストア (VECS) に格納されているカスタム証明書の使用

デプロイ モデル

Platform Services Controller を Windows システムにインストールするか、Platform Services Controller アプライアンスをデプロイできます。

デプロイ モデルは、使用している Platform Services Controller のバージョンによって異なります。 vCenter Server および Platform Services Controller のデプロイ タイプを参照してください。

vSphere 6.7 Update 1 以降、外部 Platform Services Controller に接続された vCenter Server インスタンスを展開またはインストールし、それを Platform Services Controller が組み込まれた vCenter Server インスタンスに変換する場合は、既存の vCenter Server に組み込まれた新しい Platform Services Controller を複製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。

vSphere 6.7 Update 1 以降、組み込み Platform Services Controller を持つ vCenter Server をある vSphere ドメインから別の vSphere ドメインに移動することができます。タグ付け、ライセンス付与などのサービスは保持され、新しいドメインに移行されます。『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。

Platform Services Controller サービスの管理

Platform Services Controller サービスは、vSphere Client から管理するか、あるいは利用可能なスクリプトおよび CLI を使用して管理できます。

それぞれの Platform Services Controller サービスは異なるインターフェイスをサポートします。

表 1-2. Platform Services Controller サービスを管理するためのインターフェイス

インターフェイス	説明
vSphere Client	Web インターフェイス（HTML5 ベース クライアント）。vSphere Client のユーザー インターフェイスの用語、トポロジ、およびワークフローは、vSphere Web Client ユーザー インターフェイスの同じ要素や項目とほとんど一致しています。
vSphere Web Client	一部のサービスを管理するための Web インターフェイス。
証明書管理ユーティリティ	CSR の生成および証明書の置き換えをサポートするコマンドライン ツールです。vSphere Certificate Manager ユーティリティによる証明書の管理を参照してください。
Platform Services Controller サービスを管理するための CLI	VMware Endpoint Certificate Store (VECS) と VMware Directory Service (vmdir) の証明書を管理するためのコマンド セットです。4 章 CLI コマンドを使用したサービスと証明書の管理を参照してください。

Platform Services Controller サービス

Platform Services Controller を使用することで、同じ環境内のすべての VMware 製品が認証ドメインおよびその他のサービスを共有できます。サービスには、証明書管理、認証、ライセンスが含まれます。

Platform Services Controller には、次のコア インフラストラクチャ サービスが含まれます。

表 1-3. Platform Services Controller サービス

サービス	説明
applmgmt (VMware Appliance Management Service)	アプライアンスの構成を処理し、アプライアンスのライフサイクル管理用の公開 API エンドポイントを提供します。Platform Services Controller アプライアンスに含まれています。
vmware-cis-license (VMware License Service)	各 Platform Services Controller には、使用環境の VMware 製品に統合ライセンス管理とレポート作成機能を提供する VMware License Service が含まれています。 License Service インベントリでは、ドメイン内のすべての Platform Services Controller を 30 秒間隔でレプリケートします。
vmware-stsd (VMware Security Token Service)	vCenter Single Sign-On 機能の背後にあるサービスで、VMware ソフトウェア コンポーネントとユーザーにセキュアな認証サービスを提供します。 vCenter Single Sign-On を使用することで、VMware コンポーネントはセキュアな SAML トークン交換メカニズムを使用して通信することができます。vCenter Single Sign-On は、インストールまたはアップグレード中に VMware ソフトウェア コンポーネントが登録される内部セキュリティ ドメイン（デフォルトでは vsphere.local）を構築します。
vmware-rhttpproxy (VMware HTTP Reverse Proxy)	リバース プロキシは各 Platform Services Controller ノードおよび各 vCenter Server システムで実行されます。ノードへの単一のエントリ ポイントで、ノードで実行されるサービスが安全に通信できるようにします。
vmware-sca (VMware Service Control Agent)	サービス設定を管理します。service-control CLI を使用して、個別のサービス設定を管理できます。
vmware-statsmonitor (VMware Appliance Monitoring Service)	vCenter Server Appliance のゲスト OS のリソース使用量を監視します。
vmware-vapi-endpoint (VMware vAPI Endpoint)	vSphere Automation API エンドポイントは、vAPI サービスへの単一のアクセス ポイントを提供します。vAPI Endpoint サービスのプロパティは vSphere Client から変更できます。vAPI エンドポイントの詳細については、「vSphere Automation SDKs Programming Guide」を参照してください。
vmafdd VMware Authentication Framework	vmdir 認証用のクライアント側フレームワークを提供し、VMware Endpoint Certificate Store (VECS) を提供するサービス。
vmcad VMware 証明書サービス	vmafd クライアント ライブラリを持つ各 VMware ソフトウェア コンポーネントと各 ESXi ホストを、VMware 認証局 (VMCA) をルート認証局とする署名付き証明書を使用してプロビジョニングします。Certificate Manager ユーティリティを使用して、デフォルトの証明書を変更できます。 VMware Certificate Service は VMware Endpoint Certificate Store (VECS) を使用して、すべての Platform Services Controller インスタンスで証明書のローカル リポジトリとして機能します。VMCA を使用せず、代わりにカスタム証明書を使用することもできますが、VECS に証明書を追加する必要があります。

表 1-3. Platform Services Controller サービス （続き）

サービス	説明
vmdird VMware Directory Service	認証、証明書、ルックアップ、およびライセンスの情報を保管するマルチテナントのピア複製 LDAP ディレクトリ サービスを提供します。LDAP ブラウザを使用して vmdird でデータを更新しないでください。 ドメインに Platform Services Controller の複数のインスタンスが含まれる場合、1 つの vmdir インスタンスで更新された vmdir の内容は、他のすべての vmdir インスタンスに伝達されます。
vmdnsd VMware Domain Name Service	vSphere 6.x では使用されません。
vmonapi VMware Lifecycle Manager API vmware-vmon VMware Service Lifecycle Manager	vCenter Server サービスを起動および停止して、サービス API の健全性を監視します。vmware-vmon サービスは、Platform Services Controller と vCenter Server のライフサイクルを管理する、プラットフォームに依存しない一元化されたサービスです。API と CLI をサードパーティ アプリケーションに公開します。
lwsmd Likewise Service Manager	Likewise を使用すると、ホストを Active Directory ドメインおよびその後のユーザー認証に参加させることができます。
pschealth VMware Platform Services Controller 健全性監視	すべての Platform Services Controller のコア インフラストラクチャ サービスの健全性およびステータスを監視します。
vmware-analytics VMware 分析サービス	テレメトリ データをさまざまな vSphere コンポーネントから収集して VMware 分析クラウドにアップロードし、カスタマ エクスペリエンス改善プログラム (CEIP) を管理するコンポーネントから構成されます。

vSphere Client からの Platform Services Controller サービスの管理

vSphere Client で、vCenter Server のアクセス制御、ライセンス、ソリューション、リンク先のドメイン、証明書、および Single Sign-On を管理できます。

手順

1 ローカルの vCenter Single Sign-On ドメイン（デフォルトは vsphere.local）で、Platform Services Controller に関連付けられた vCenter Server に、管理者権限を持つユーザーとしてログインします。

2 [管理] を選択して、管理する項目をクリックします。

vSphere Web Client からの Platform Services Controller サービスの管理

vSphere Web Client から vCenter Single Sign-On とライセンス サービスを管理できます。

vSphere Web Client の代わりに、vSphere Client または CLI を使用して次のサービスを管理します。

- 証明書
- VMware Endpoint Certificate Store (VECS)
- Common Access Card 認証などの 2 要素認証
- ログイン バナー

手順

1 ローカルの vCenter Single Sign-On ドメイン（デフォルトは vsphere.local）で、Platform Services Controller に関連付けられた vCenter Server に、管理者権限を持つユーザーとしてログインします。

2 [管理] を選択して、管理する項目をクリックします。

オプション	説明
[Single Sign-On]	vCenter Single Sign-On の構成 ■ ポリシーを設定します。 ■ ID ソースを管理します。 ■ STS 署名証明書を管理します。 ■ SAML サービス プロバイダを管理します。 ■ ユーザーとグループを管理します。
[ライセンス]	ライセンスを構成します。

スクリプトを使用した Platform Services Controller サービスの管理

Platform Services Controller には、CSR の生成、証明書の管理、およびサービスの管理を行うスクリプトが含まれています。

たとえば、`certool` ユーティリティを使用して、CSR の生成および証明書の置き換えを行うことができます。これらの操作は、どちらも組み込みの Platform Services Controller を使用するシナリオと外部の Platform Services Controller を使用するシナリオで行うことができます。vSphere Certificate Manager ユーティリティによる証明書の管理を参照してください。

Web インターフェイスでサポートされていない管理タスクや自社環境用のカスタム スクリプトの作成には CLI を使用します。

表 1-4. 証明書および関連サービスを管理するための CLI

CLI	説明	リンク
`certool`	証明書およびキーを生成および管理します。VMCA の一部です。	certool 初期化コマンド リファレンス
`vecs-cli`	VMware 証明書ストア インスタンスのコンテンツを管理します。VMAFD の一部です。	vecs-cli コマンド リファレンス
`dir-cli`	VMware Directory Service に証明書を作成し更新します。VMAFD の一部です。	dir-cli コマンド リファレンス
`sso-config`	スマート カード認証を構成するためのユーティリティ。	vCenter Server の 2 要素認証について
`service-control`	サービスの起動、停止およびリストを表示するコマンド。	このコマンドを実行して、他の CLI コマンドを実行する前にサービスを停止します。

手順

1 Platform Services Controller シェルにログインします。

ほとんどの場合、操作するには root ユーザーか管理者ユーザーである必要があります。詳細については、CLI の実行に必要な権限を参照してください。

2 次のいずれかのデフォルトの場所で、CLI にアクセスします。

必要な権限は、実行するタスクによって異なります。機密情報を保護するために、パスワードの入力を 2 回求められる場合があります。

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
```

Linux では、`service-control` コマンドでパスを指定する必要はありません。

Platform Services Controller アプライアンスの管理

Platform Services Controller アプライアンスは、仮想アプライアンス管理インターフェイスまたはアプライアンス シェルを使用して管理できます。

組み込みの Platform Services Controller を含む環境を使用している場合は、Platform Services Controller と vCenter Server の両方を含む単一のアプライアンスを管理します。vCenter Server Appliance の構成 を参照してください。

表 1-5. Platform Services Controller アプライアンスを管理するためのインターフェイス

インターフェイス	説明
Platform Services Controller 仮想アプライアンス管理インターフェイス (VAMI)	このインターフェイスは、Platform Services Controller デプロイのシステム設定を再構成するために使用します。
Platform Services Controller アプライアンス シェル	このコマンドライン インターフェイスは、VMCA、VECS、および VMDIR でサービス管理操作を実行するために使用します。vSphere Certificate Manager ユーティリティによる証明書の管理および 4 章 CLI コマンドを使用したサービスと証明書の管理を参照してください。

Platform Services Controller 仮想アプライアンスの管理インターフェイスによるアプライアンスの管理

外部の Platform Services Controller が設定された環境では、Platform Services Controller 仮想アプライアンスの管理インターフェイス (VAMI) を使用してアプライアンス システムを設定することができます。設定には、時

刻同期、ネットワーク設定、および SSH ログイン設定が含まれます。また、root パスワードを変更したり、Active Directory ドメインにアプライアンスを参加させたり、Active Directory ドメインへの参加を解除したりすることができます。

組み込みの Platform Services Controller が設定された環境では、Platform Services Controller と vCenter Server の両方を含むアプライアンスを管理します。

手順

1 Web ブラウザで、https://*platform_services_controller_ip*:5480 の Web インターフェイスに移動します。

2 信頼されない SSL 証明書に関する警告メッセージが表示された場合は、会社のセキュリティ ポリシーおよび使用している Web ブラウザに基づいて問題を解決します。

3 root としてログインします。

デフォルトの root パスワードは、仮想アプライアンスをデプロイするときに設定した仮想アプライアンスの root パスワードです。

結果

Platform Services Controller アプライアンス管理インターフェイスの [システム情報] ページを参照できます。

アプライアンス シェルからのアプライアンスの管理

アプライアンス シェルからサービス管理ユーティリティおよび CLI を使用することができます。TTY1 を使用してコンソールにログインするか、SSH を使用してシェルに接続することができます。

手順

1 必要であれば SSH ログインを有効にします。

a https://*platform_services_controller_ip*:5480 から、アプライアンス管理インターフェイス (VAMI) にログインします。

b ナビゲータで、[アクセス] を選択して [編集] をクリックします。

c [SSH ログインの有効化] に切り替えて、[OK] をクリックします。

同じ手順を使用して、アプライアンスの Bash シェルを有効にします。

2 アプライアンス シェルにアクセスします。

- アプライアンス コンソールに直接アクセスできる場合は、[ログイン] を選択して Enter キーを押します。
- リモート接続するには、SSH などのリモート コンソール接続を使用して、アプライアンスへのセッションを開始します。

3 最初にアプライアンスをデプロイしたときに設定したパスワードを使用して root としてログインします。

root パスワードを変更した場合は、新しいパスワードを使用します。

Active Directory ドメインへの Platform Services Controller アプライアンスの追加

Active Directory の ID ソースを Platform Services Controller に追加する場合は、Active Directory ドメインに Platform Services Controller アプライアンスを参加させる必要があります。

Windows にインストールされた Platform Services Controller インスタンスを使用している場合、そのマシンが属するドメインを使用することができます。

手順

1. vSphere Client を使用して、Platform Services Controller に関連付けられた vCenter Server に、ローカルの vCenter Single Sign-On ドメイン（デフォルトで vsphere.local）の管理者権限を持つユーザーとしてログインします。
2. [管理] を選択します。
3. [Single Sign-On] を展開し、[構成] をクリックします。
4. [Active Directory ドメイン] をクリックします。
5. [Active Directory に参加] をクリックし、ドメイン、オプションの組織単位、およびユーザー名とパスワードを指定して、[参加] をクリックします。

次のステップ

参加した Active Directory ドメインからユーザーとグループを接続するには、参加したドメインを vCenter Single Sign-On の ID ソースとして追加します。 vCenter Single Sign-OnID ソースの追加または編集を参照してください。

vCenter Single Sign-On による vSphere 認証

2

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

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

vSphere 6.0 以降では、vCenter Single Sign-On は Platform Services Controller に含まれています。Platform Services Controller には、vCenter Server および vCenter Server コンポーネントをサポートする共有サービスが用意されています。これらのサービスには、vCenter Single Sign-On、VMware Certificate Authority、License Service が含まれます。Platform Services Controller の詳細については、『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。

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

次の手順は、特定のタスクを実行するために認証を受けることができるユーザーを認証することです。多くの場合、通常はロールを持つグループにユーザーを割り当てることで vCenter Server 権限を割り当てます。vSphere は、グローバル権限などその他の権限モデルを含みます。『vSphere のセキュリティ』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。

vCenter Single Sign-On について

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

vCenter Single Sign-On 6.0 ドメインとサイト (https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

vCenter Single Sign-On によって環境を保護する方法

vCenter Single Sign-On を使用すると、vSphere コンポーネントの安全なトークン メカニズムを介した相互通信が可能になります。

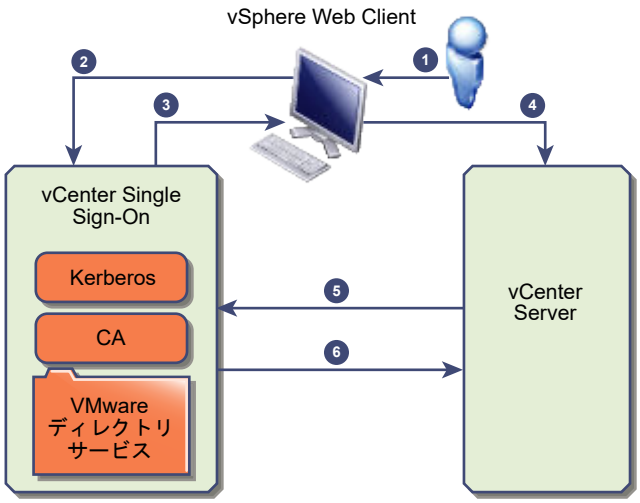
vCenter Single Sign-On は次のサービスを使用します。

- STS (Security Token Service)。
- トラフィックを保護するための SSL。
- Active Directory または OpenLDAP を介した人間のユーザー認証。
- 証明書を介したソリューション ユーザー認証。

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

次の図に、ユーザー（人）のハンドシェイクを示します。

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



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

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

2 vSphere Client は、ログイン情報を vCenter Single Sign-On サービスに渡します。このサービスにより、vSphere Client の SAML トークンがチェックされます。vSphere Client に有効なトークンがある場合、vCenter Single Sign-On により、ユーザーが構成済み ID ソース（Active Directory など）に存在するかどうかがチェックされます。

   - ユーザー名のみが使用されている場合は、vCenter Single Sign-On によってデフォルト ドメイン内がチェックされます。
   - ドメイン名がユーザー名に含まれている場合（*DOMAIN*\user1 または user1@*DOMAIN*）、vCenter Single Sign-On によってそのドメインがチェックされます。

3 ユーザーが ID ソースの認証を受けることができる場合、そのユーザーを vSphere Client に示すトークンが vCenter Single Sign-On によって返されます。

4 vSphere Client はトークンを vCenter Server システムに渡します。

5 vCenter Server は、トークンが有効で期限切れになっていないことを、vCenter Single Sign-On サーバでチェックします。

6 vCenter Single Sign-On サーバにより、トークンが vCenter Server システムに返され、vCenter Server 認可フレームワークを使用してユーザーのアクセスを許可します。

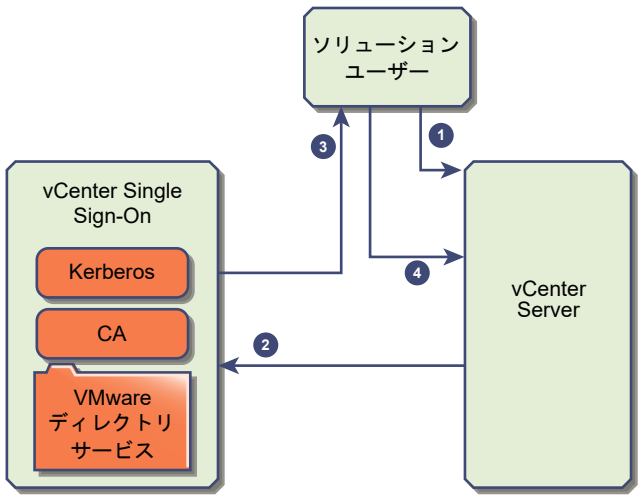
これで、ユーザーは認証を受けて、自分のロールに権限があるすべてのオブジェクトを表示および変更できます。

注： まず、各ユーザーにアクセスなしロールが割り当てられます。vCenter Server の管理者は、ユーザーがログインできるように少なくとも読み取り専用ロールを割り当てる必要があります。『vSphere のセキュリティ』ドキュメントを参照してください。

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

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

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



ソリューション ユーザーの場合、やりとりは、次のように行われます。

1 ソリューション ユーザーが vCenter サービスに接続しようとします。

2 ソリューション ユーザーは vCenter Single Sign-On にリダイレクトされます。ソリューション ユーザーが vCenter Single Sign-On を初めて使用する場合、有効な証明書を提供する必要があります。

3 証明書が有効であれば、vCenter Single Sign-On は SAML トークン（ベアラ トークン）をソリューション ユーザーに割り当てます。このトークンは、vCenter Single Sign-On によって署名されます。

4 ソリューション ユーザーは vCenter Single Sign-On にリダイレクトされ、そのアクセス許可に基づいてタスクを実行できます。

5 次にソリューション ユーザーが認証を受ける必要があるときは、SAML トークンを使用して vCenter Server にログインできます。

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

サポートされている暗号化

最高レベルの暗号化である AES 暗号化がサポートされています。サポートされている暗号化は、vCenter Single Sign-On が ID ソースとして Active Directory を使用するときにセキュリティに影響します。

また、ESXi ホストまたは vCenter Server が Active Directory に参加するときにもセキュリティに影響を与えます。

vCenter Single Sign-On コンポーネント

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

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

STS （Security Token Service）

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

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

管理サーバ

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

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) は、インストール時に指定したドメインに関連付けられ、組み込みの各デプロイおよび各 Platform Services Controller に含まれます。これは、ポート 389 で LDAP ディレクトリを使用可能にするマルチテナント、マルチマスターのディレクトリ サービスです。このサービスでは、vSphere 5.5 以前のシステムとの下位互換性を確保するためにポート 11711 が引き続き使用されています。

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

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

ID 管理サービス

ID ソースおよび STS 認証要求を処理します。

vCenter Single Sign-On がインストールに与える影響

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

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

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

インストールの順序は重要です。

最初のインストール

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

後続のインストール

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

デプロイ モデル、および各デプロイ タイプのメリットとデメリットの詳細については、「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。

vSphere での vCenter Single Sign-On の使用

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

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

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

  ユーザーが表示できるオブジェクトと実行できる内容は、通常、vCenter Server の権限設定で決まります。vCenter Server 管理者は、vCenter Single Sign-On からではなく、vSphere Web Client または vSphere Client の [権限] インターフェイスから権限を割り当てます。『vSphere のセキュリティ』ドキュメントを参照してください。

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

ユーザーはログイン ページで認証情報を入力して、vCenter Single Sign-On に対して認証を行います。vCenter Server への接続後、認証済みユーザーは、ロールによって権限が与えられているすべての vCenter Server インスタンスまたは他の vSphere オブジェクトを表示することができます。それ以上の認証は不要です。

インストール後に、vCenter Single Sign-On ドメインの管理者（デフォルトは administrator@vsphere.local）は、vCenter Single Sign-On と vCenter Server の両方の管理者権限を持ちます。そのユーザーは次に、vCenter Single Sign-On ドメインで ID ソースを追加してデフォルトの ID ソースを設定し、ユーザーとグループを管理できます。

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

注： vSphere Client から Software-Defined Data Center (SDDC) のパスワードを変更すると、新しいパスワードとデフォルトの vCenter Server の認証情報ページに表示されるパスワードは同期されません。ページでは、デフォルトの認証情報のみが表示されます。認証情報を変更した場合、新しいパスワードの保管と管理はユーザーの責任となります。テクニカル サポートに連絡し、パスワードの変更を要求します。

vCenter Single Sign-On 管理者ユーザー

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

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

注： vCenter Single Sign-On 管理者ユーザー（デフォルトは administrator@vsphere.local。インストール中に別のドメインを指定した場合は administrator@*mydomain*）の名前は変更できません。セキュリティを高めるには、vCenter Single Sign-On ドメインに追加で名前付きユーザーを作成し、管理者権限を割り当てることを検討します。その後、管理者アカウントを使用して停止することができます。

ESXi ユーザー

スタンドアローンの ESXi ホストには vCenter Single Sign-On や Platform Services Controller は組み込まれません。ESXi ホストの Active Directory への追加については、vSphere のセキュリティ を参照してください。

VMware Host Client、vCLI、PowerCLI を使用して管理対象の ESXi ホストの ローカル ESXi ユーザーを作成しても、vCenter Server はこれらのユーザーを認識しません。そのため、ローカル ユーザーの作成は、特に同じユーザー名を使用する場合に混乱する原因となります。vCenter Single Sign-On で認証可能なユーザーは、ESXi ホスト オブジェクトの対応する権限がある場合、ESXi ホストを確認および管理できます。

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

vCenter Server コンポーネントへのログイン方法

vSphere Client または vSphere Web Client に接続してログインできます。

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

- デフォルト ドメインに所属しているユーザーはユーザー名とパスワードでログインできます。

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

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

注： vSphere 6.0 Update 2 以降、2 要素認証がサポートされています。 vCenter Server の 2 要素認証についてを参照してください。

vCenter Single Sign-On ドメイン内のグループ

vCenter Single Sign-On ドメイン（デフォルトでは vsphere.local）には、複数の事前定義されたグループが含まれます。それらのグループのいずれかにユーザーを追加して、対応するアクションを実行できるようにします。

vCenter Single Sign-On ユーザーおよびグループの管理を参照してください。

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

vCenter Server が直接管理しない一部のサービスについては、vCenter Single Sign-On グループのいずれかのメンバーシップによって権限が決定します。たとえば、管理者グループのメンバー ユーザーは、vCenter Single Sign-On を管理できます。CAAdmins グループのメンバー ユーザーは VMware 認証局を管理することができ、License Service.Administrators グループのユーザーはライセンスを管理できます。

vsphere.local には次のグループが事前定義されています。

注： これらのグループの多くは、vsphere.local の内部グループですが、ユーザーに高いレベルの管理権限を付与できます。リスクについて慎重に考慮した後にのみ、これらのグループのいずれかにユーザーを追加してください。

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

表 2-1. vsphere.local ドメイン内のグループ

権限	説明
ユーザー	vCenter Single Sign-On ドメイン内のユーザー（デフォルトでは vsphere.local）。
SolutionUsers	ソリューション ユーザー グループの vCenter サービス。各ソリューション ユーザーは、証明書により vCenter Single Sign-On に対して個別に認証します。デフォルトでは、VMCA が証明書を使用してソリューション ユーザーをプロビジョニングします。このグループには、メンバーを明示的に追加しないでください。

表 2-1. vsphere.local ドメイン内のグループ （続き）

権限	説明
CAAdmins	CAAdmins グループのメンバーには、VMCA の管理権限があります。明確な理由がある場合を除き、このグループにメンバーを追加しないでください。
DCAdmins	DCAdmins グループのメンバーは、VMware ディレクトリ サービスでドメイン コントローラ管理者のアクションを実行できます。 **注：** ドメイン コントローラは、直接管理しないでください。代わりに、`vmdir` CLI または vSphere Client を使用して対応するタスクを実行してください。
SystemConfiguration.BashShellAdministrators	このグループは、vCenter Server Appliance のデプロイの場合にのみ使用できます。 このグループのユーザーは、BASH シェルへのアクセスを有効および無効にすることができます。SSH を使用して vCenter Server Appliance に接続するユーザーは、デフォルトで、制約されたシェルのコマンドにのみアクセスできます。このグループのユーザーは、BASH シェルにアクセスできます。
ActAsUsers	Act-As ユーザーのメンバーは、vCenter Single Sign-On から Act-As トークンを取得できます。
ExternalIPDUsers	この内部グループは、vSphere では使用されません。VMware vCloud Air には、このグループが必要です。
SystemConfiguration.Administrators	SystemConfiguration.Administrators グループのメンバーは、vSphere Client でシステム構成を表示および管理できます。これらのユーザーは、サービスを表示、起動、および再起動し、サービスのトラブルシューティングを行い、使用可能なノードを表示し、それらのノードを管理することができます。
DCClients	このグループは、管理ノードに VMware ディレクトリ サービス内のデータへのアクセスを許可するために内部で使用されます。 **注：** このグループは変更しないでください。変更を加えると、証明書インフラストラクチャが侵害される可能性があります。
ComponentManager.Administrators	ComponentManager.Administrators グループのメンバーは、サービスを登録または登録解除するコンポーネント マネージャ API を呼び出す（つまり、サービスを変更する）ことができます。このグループのメンバーシップは、サービスでの読み取りアクセスでは不要です。
LicenseService.Administrators	LicenseService.Administrators のメンバーには、すべてのライセンス関連データに対する完全な書き込みアクセス権限が付与されており、ライセンス サービスで登録されているすべての製品資産のシリアル キーを追加、削除、割り当て、および割り当て解除することができます。
管理者	VMware ディレクトリ サービス (vmdir) の管理者。このグループのメンバーは、vCenter Single Sign-On の管理タスクを実行できます。正当な理由があり、問題が発生した場合の影響を理解している場合を除き、このグループにメンバーを追加しないでください。

vCenter Single Sign-OnID ソースの設定

ユーザーがユーザー名のみでログインすると、vCenter Single Sign-On はデフォルトの ID ソースで、そのユーザーが認証可能であるかを確認します。ユーザーがログイン時にログイン画面でドメイン名を入力すると、vCenter Single Sign-On は入力されたドメインが ID ソースとして追加されているかを確認します。ID ソースは、追加および削除ができるほか、デフォルト設定を変更できます。

vSphere Client から vCenter Single Sign-On を設定します。vCenter Single Sign-On を設定するには、vCenter Single Sign-On 管理者権限が必要です。vCenter Single Sign-On 管理者権限があることは、vCenter Server または ESXi の管理者ロールが割り当てられていることとは異なります。新規インストールでは、vCenter Single Sign-On 管理者（デフォルトでは administrator@vsphere.local）のみが vCenter Single Sign-On の認証を受けることができます。

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

  ID ソースを使用すると、vCenter Single Sign-On に 1 つ以上のドメインを接続できます。ドメインは vCenter Single Sign-On サーバがユーザー認証に使用できるユーザーまたはグループのリポジトリです。

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

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

- vCenter Single Sign-OnID ソースの追加または編集

  ユーザーは、vCenter Single Sign-On ID ソースとして追加されたドメインに属している場合のみ vCenter Server にログインできます。vCenter Single Sign-On の管理者ユーザーは、ID ソースの追加や、追加した ID ソースの設定を変更することができます。

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

  vCenter Single Sign-On で Windows セッション認証 （SSPI） を使用できます。SSPI を使用するには、Platform Services Controller を Active Directory ドメインに参加させる必要があります。

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

ID ソースを使用すると、vCenter Single Sign-On に 1 つ以上のドメインを接続できます。ドメインは vCenter Single Sign-On サーバがユーザー認証に使用できるユーザーまたはグループのリポジトリです。

管理者は、ID ソースの追加、デフォルトの ID ソースの設定、vsphere.local ID ソースのユーザーおよびグループの作成を実行できます。

ユーザーおよびグループのデータは、Active Directory、OpenLDAP、またはローカルで vCenter Single Sign-On がインストールされたマシンのオペレーティング システムに格納されます。インストールが完了すると、vCenter Single Sign-On のすべてのインスタンスに *your_domain_name* の ID ソース（vsphere.local など）があります。この ID ソースは vCenter Single Sign-On の内部のものです。

バージョン 5.1 より前の vCenter Server バージョンは、Active Directory およびローカル オペレーティング システムのユーザーをユーザー リポジトリとしてサポートしていました。このため、ローカル オペレーティング システムのユーザーは常に vCenter Server システムから認証可能でした。vCenter Server バージョン 5.1 およびバージョン 5.5 では、認証に vCenter Single Sign-On を使用します。vCenter Single Sign-On 5.1 がサポートしている ID ソースのリストについては、vSphere 5.1 のドキュメントを参照してください。vCenter Single Sign-On 5.5 は以下のタイプのユーザー リポジトリを ID ソースとしてサポートしていますが、デフォルトでサポートする ID ソースは 1 つだけです。

- Active Directory バージョン 2003 以降。vSphere Client では、[Active Directory (統合 Windows 認証)] として表示されます。vCenter Single Sign-On では、単一の Active Directory ドメインを ID ソースとして指定できます。ドメインに子ドメインを持たせたり、フォレスト ルート ドメインにすることができます。VMware のナレッジベースの記事 KB2064250 では、vCenter Single Sign-On でサポートされている Microsoft Active Directory の信頼関係についての解説しています。
- LDAP を用いた Active Directory。vCenter Single Sign-On は LDAP を用いた Active Directory の複数の ID ソースをサポートします。この ID ソース タイプは、vSphere 5.1 に含まれる vCenter Single Sign-On サービスとの互換性を維持するためのものです。vSphere Client には、[LDAP サーバとしての Active Directory] として表示されます。
- OpenLDAP バージョン 2.4 以降。vCenter Single Sign-On は複数の OpenLDAP ID ソースをサポートします。vSphere Client には、[OpenLDAP] として表示されます。
- ローカル オペレーティング システム ユーザー。ローカル オペレーティング システム ユーザーは、vCenter Single Sign-On サーバが実行されているオペレーティング システムのローカル ユーザーです。ローカル オペレーティング システムの ID ソースは、基本的な vCenter Single Sign-On サーバの展開にのみ使用でき、複数の vCenter Single Sign-On インスタンスを用いた展開では使用できません。1 つのローカル オペレーティング システム ID ソースのみが許可されます。vSphere Client には、[localos] として表示されます。

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

- vCenter Single Sign-On のシステム ユーザー。vCenter Single Sign-On のインストール時に、単一のシステム ID ソースのみが作成されます。

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

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

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

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

- デフォルト ドメインに所属しているユーザーはユーザー名とパスワードでログインできます。

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ID ソース] をクリックし、ID ソースを選択して、[デフォルトに設定] をクリックします。

ドメイン表示では、デフォルトのドメインのドメイン列に （デフォルト） と表示されます。

vCenter Single Sign-OnID ソースの追加または編集

ユーザーは、vCenter Single Sign-On ID ソースとして追加されたドメインに属している場合のみ vCenter Server にログインできます。vCenter Single Sign-On の管理者ユーザーは、ID ソースの追加や、追加した ID ソースの設定を変更することができます。

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

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

localos

すべてのローカル オペレーティング システム ユーザー。アップグレードする場合、すでに認証が可能な `localos` ユーザーは、引き続き認証することができます。組み込みの Platform Services Controller を使用している環境で `localos` ID ソースを使用しても意味がありません。

vsphere.local

vCenter Single Sign-On の内部ユーザーを含みます。

前提条件

Active Directory ID ソースを追加する場合は、vCenter Server または vCenter Server Appliance の Windows マシンを Active Directory ドメイン内に配置する必要があります。「Active Directory ドメインへの Platform Services Controller アプライアンスの追加」を参照してください。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ID ソース]、[ID ソースの追加] の順にクリックします。

5 ID ソースを選択し、ID ソース設定を入力します。

オプション	説明
Active Directory (統合 Windows 認証)	ネイティブの Active Directory 実装にこのオプションを使用します。このオプションを使用する場合は、vCenter Single Sign-On サービスが稼動しているマシンが Active Directory ドメインに属している必要があります。 「Active Directory ID ソースの設定」を参照してください。
LDAP を介した Active Directory	このオプションは後方互換性用に使用できます。ドメイン コントローラと他の情報を指定する必要があります。Active Directory LDAP Server および OpenLDAP Server ID ソースの設定を参照してください。
OpenLDAP	OpenLDAP ID ソースにこのオプションを使用します。Active Directory LDAP Server および OpenLDAP Server ID ソースの設定を参照してください。
SSO サーバのローカル オペレーティング システム	SSO サーバのローカル オペレーティング システムには、このオプションを使用します。

注： ユーザー アカウントがロックされているか、無効になっていると、Active Directory ドメイン内の認証およびグループとユーザーの検索が失敗します。ユーザー アカウントは、ユーザーとグループの OU への読み取り専用アクセス権を持ち、ユーザーとグループの属性を読み取ることができる必要があります。Active Directory はデフォルトでこのアクセスを提供します。セキュリティの向上のために、特別なサービス ユーザーを使用します。

6 [追加] をクリックします。

次のステップ

ID ソースが追加されると、すべてのユーザーは認証可能になりますが、アクセスなしロールが付与されます。vCenter Server の「権限の変更」権限を持つユーザーは、ユーザーまたはユーザー グループに権限を付与できます。権限が付与されたユーザーまたはグループは、vCenter Server にログインし、オブジェクトを表示したり管理したりできます。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。『vSphere のセキュリティ』ドキュメントを参照してください。

Active Directory ID ソースの設定

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

Active Directory アイデンティティ ソース使用の前提条件

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

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

注： Active Directory （統合 Windows 認証）は、Active Directory ドメイン フォレストのルートを常に使用します。Active Directory フォレスト内の子ドメインを使用して統合 Windows 認証 ID ソースを構成する方法については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/2070433) を参照してください。

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

注： vSphere 5.5 の場合、SPN を指定しても vCenter Single Sign-On はマシン アカウントを使用します。詳細については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/2087978) を参照してください。

セキュリティ強化が必要になる可能性のある場所の特定のために Active Directory で診断イベント ログを有効にしていると、そのディレクトリ サーバにイベント ID 2889 のログ イベントが表示されることがあります。統合 Windows 認証を使用している場合、イベント ID 2889 はセキュリティ リスクではなく、異常として生成されます。イベント ID 2889 の詳細については、https://kb.vmware.com/s/article/78644 にある VMware ナレッジベースの記事を参照してください。

表 2-2. ID ソース設定の追加

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

Active Directory LDAP Server および OpenLDAP Server ID ソースの設定

LDAP [Lightweight Directory Access Protocol] を介した Active Directory ID ソースは、Active Directory (統合 Windows 認証) オプションより優先されます。OpenLDAP Server ID ソースは、OpenLDAP を使用する環境で使用できます。

OpenLDAP の ID ソースを設定する場合は、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2064977) で追加要件を確認してください。

注： Microsoft Windows の今後の更新では、強力な認証と暗号化を必須とするように、Active Directory のデフォルトの動作が変更されます。この変更は、vCenter Server が Active Directory に対してどのように認証を行うかに影響します。vCenter Server の ID ソースとして Active Directory を使用する場合は、LDAPS を有効にすることを検討する必要があります。この Microsoft セキュリティ アップデートの詳細については、https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 および https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html を参照してください。

表 2-3. LDAP サーバとしての Active Directory および OpenLDAP の設定

オプション	説明
名前	ID ソースの名前。
ユーザーのベース DN	ユーザーのベース識別名。ユーザー検索を開始する DN を入力します。たとえば、cn = Users、dc = myCorp、dc = com のように入力します。
グループのベース DN	グループのベース識別名。グループ検索を開始する DN を入力します。たとえば、cn = Groups、dc = myCorp、dc = com のように入力します。
ドメイン名	ドメインの FQDN。
ドメイン エイリアス	Active Directory の ID ソースの場合、ドメインの NetBIOS 名。SSPI 認証を使用する場合は、ID ソースの別名として Active Directory ドメインの NetBIOS 名を追加します。 OpenLDAP の ID ソースの場合、別名を指定しないと、大文字で表記されたドメイン名が追加されます。
ユーザー名	ユーザーおよびグループの BaseDN に対して、最低限の読み取り専用アクセス権を持つドメイン内のユーザーの ID。ID は次のいずれかの形式にすることができます。 ■ UPN (user@domain.com) ■ NetBIOS（ドメイン\ユーザー） ■ DN (cn=user,cn=Users,dc=domain,dc=com) ユーザー名は完全修飾名にする必要があります。「user」という入力は機能しません。
パスワード	[ユーザー名] で指定したユーザーのパスワード。
接続先	接続先のドメイン コントローラ。ドメイン内の任意のドメイン コントローラ、または特定のコントローラを指定できます。
プライマリ サーバの URL	ドメインのプライマリ ドメイン コントローラ LDAP サーバ。 **`ldap://hostname_or_IPaddress:port`** の形式または **`ldaps://hostname_or_IPaddress:port`** の形式を使用します。通常のポートは、LDAP 接続では 389、LDAPS 接続では 636 です。Active Directory のマルチドメイン コントローラ デプロイの場合、通常のポートは LDAP 接続では 3268、LDAPS 接続では 3269 です。 プライマリまたはセカンダリ LDAP の URL に **`ldaps://`** を使用する場合は、Active Directory サーバの LDAPS エンドポイントに対する信頼を確立する証明書が必要です。
セカンダリ サーバの URL	フェイルオーバーに使用されるセカンダリ ドメイン コントローラ LDAP サーバのアドレス。
SSL 証明書	Active Directory LDAP Server または OpenLDAP Server の ID ソースで LDAPS を使用する場合、**参照** をクリックして証明書を選択します。Active Directory からルート CA 証明書をエクスポートするには、Microsoft のドキュメントを参照してください。

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

vCenter Single Sign-On で Windows セッション認証 （SSPI） を使用できます。SSPI を使用するには、Platform Services Controller を Active Directory ドメインに参加させる必要があります。

SSPI を使用すると、現在マシンにログインしているユーザーのログイン プロセスの速度が上がります。

前提条件

- Platform Services Controller アプライアンス または Platform Services Controller が稼動する Windows マシンを Active Directory ドメインに参加させます。「Active Directory ドメインへの Platform Services Controller アプライアンスの追加」を参照してください。
- ドメインが正常に設定されていることを確認します。詳細については、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2064250) を参照してください。
- vSphere 6.0 またはそれ以前のバージョンを使用している場合は、クライアント統合プラグインがインストールされていることを確認します。
- vSphere 6.5 以降を使用している場合は、拡張認証プラグインがインストールされていることを確認します。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。

手順

1. vSphere Client の [ログイン] ページに移動します。
2. [Windows セッション認証を使用する] チェック ボックスを選択します。
3. Active Directory のユーザー名とパスワードを使用してログインします。
   - Active Directory ドメインがデフォルトの ID ソースである場合は、jlee などのユーザー名でログインします。
   - そうでない場合は、jlee@example.com のようにドメイン名を含めます。

vCenter Server の 2 要素認証について

vCenter Single Sign-On では、vCenter Single Sign-On で認識されている ID ソース内のユーザーとして認証するか、Windows セッション認証を使用して認証できます。また、スマート カード（UPN ベースの Common Access Card (CAC)）を使用して、または RSA SecurID トークンを使用して認証を行うことができます。

2 要素認証方法

2 要素認証方法は、一般的に行政機関および大規模企業で利用されます。

スマート カード認証

スマート カード認証を使用すると、ログインしているコンピュータの USB ドライブに物理カードを接続しているユーザーにのみアクセスが許可されます。例として、Common Access Card (CAC) 認証があります。

管理者は公開鍵基盤 (PKI) を展開し、認証局が発行する唯一のクライアント証明書としてスマート カード証明書を設定できます。このようなデプロイでは、スマート カード証明書のみがユーザーに提示されます。ユーザーが証明書を選択すると、PIN を入力するよう求められます。物理カードおよび PIN （証明書と一致するもの）の両方を持っているユーザーのみがログインできます。

RSA SecureID 認証

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

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

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

デフォルト以外の認証方法の指定

管理者は vSphere Client から、または `sso-config` スクリプトを使用して、デフォルト以外の認証方法を設定できます。

- スマート カード認証の場合、vSphere Client から、または `sso-config` を使用して vCenter Single Sign-On の設定を実行できます。設定には、スマート カード認証の有効にしたり証明書の失効ポリシーを設定する作業も含まれます。
- RSA SecurID の場合、`sso-config` スクリプトを使用してドメインの RSA 認証マネージャを構成し、RSA トークン認証を有効にします。RSA SecurID 認証は、vSphere Client からは設定できません。ただし、RSA SecurID を有効にした場合、その認証方法が vSphere Client に表示されます。

認証方法の組み合わせ

`sso-config` を使用することで、各認証方法を個別に有効または無効にできます。2 要素認証方法のテスト中は、最初に有効にしたユーザー名およびパスワードによる認証方法のままにしておき、テスト後に 1 つの認証方法のみを有効にします。

スマート カード認証ログイン

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

vCenter Server または Platform Services Controller システムにログインするユーザーは、次のようにスマート カードと PIN を組み合わせて認証を行うよう求められます。

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

2 vCenter Single Sign-On は、ユーザーに証明書の選択とその証明書の PIN の入力を求めます。

3 また、スマート カード上の証明書が既存のものかどうか、さらに PIN が正しいかどうかを確認します。失効チェックが有効な場合、vCenter Single Sign-On は証明書が失効しているかどうかを確認します。

4 証明書が既存のものであり、失効していなければ、ユーザーが認証され、権限を与えられたタスクを実行することができます。

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

スマート カード認証の設定と使用

ユーザーが vSphere Client または vSphere Web Client から vCenter Server または関連する Platform Services Controller に接続する場合にスマート カード認証を要求するよう環境を設定することができます。

スマート カード認証の設定方法は、使用している vSphere のバージョンによって異なります。

vSphere バージョン	手順	リンク
6.0 Update 2 vSphere 6.0 の以降のバージョン	1 Tomcat サーバを設定します。 2 スマート カード認証を有効にして、設定します。	vSphere 6.0 ドキュメント センター。
6.5 以降	1 リバース プロキシを設定します。 2 スマート カード認証を有効にして、設定します。	クライアント証明書を要求するリバース プロキシの設定 コマンド ラインを使用したスマート カード認証の管理 スマート カード認証の管理

クライアント証明書を要求するリバース プロキシの設定

スマート カード認証を有効にするには、Platform Services Controller システムでリバース プロキシを設定する必要があります。お使いの環境で組み込みの Platform Services Controller を使用している場合、vCenter Server と Platform Services Controller の両方が実行されているシステムでこのタスクを実行します。

リバース プロキシの設定は、vSphere 6.5 以降で必要です。

前提条件

CA 証明書を Platform Services Controller システムにコピーします。

手順

1 Platform Services Controller にログインします。

OS	説明
アプライアンス	アプライアンス シェルに root ユーザーとしてログインします。
Windows	Windows コマンド プロンプトに管理者ユーザーとしてログインします。

2 信頼できるクライアント認証局 (CA) ストアを作成します。

このストアには、クライアント証明書用の信頼できる発行元の認証局の証明書が含まれます。ここでは、クライアントとは、スマート カード プロセスでエンド ユーザーに情報の入力を求めるメッセージが表示されるブラウザを指します。

次の例は、Platform Services Controller アプライアンスで証明書ストアを作成する方法を示しています。

単一の証明書の場合：

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

複数の証明書の場合：

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

注： Windows の Platform Services Controller で `C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\conf\` を使用し、バックスラッシュを使用するようにコマンドを変更します。

3 リバース プロキシ定義を含む `config.xml` ファイルのバックアップを作成して、エディタで `config.xml` を開きます。

OS	説明
アプライアンス	`/etc/vmware-rhttpproxy/config.xml`
Windows	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml`

4 次の変更を加えて、ファイルを保存します。

```
<http>
<maxConnections> 2048 </maxConnections>
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

`config.xml` ファイルには、これらの要素が含まれます。必要に応じて、コメントを解除する、更新する、または構成要素を追加します。

5 サービスを再起動してください。

OS	説明
アプライアンス	`/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy`

Windows	OS を再起動するか、次の手順で VMware HTTP Reverse Proxy を再起動します。
	a 管理者権限を使用して、コマンド プロンプトを開きます。
	b 次のコマンドを実行します。
	`cd C:\Program Files\VMware\vCenter Server\bin`
	`service-control --stop vmware-rhttpproxy`
	`service-control --start vmware-rhttpproxy`

コマンド ラインを使用したスマート カード認証の管理

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

`sso-config` スクリプトは次の場所にあります。

Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat`
Linux	`/opt/vmware/bin/sso-config.sh`

サポートされる認証タイプおよび失効の設定は VMware Directory Service に保存され、vCenter Single Sign-On ドメインのすべての Platform Services Controller インスタンスにわたって複製されます。

ユーザー名とパスワードの認証が無効で、スマート カード認証に問題が発生した場合、ユーザーはログインできません。その場合、root ユーザーまたは管理者ユーザーは Platform Services Controller コマンド ラインを使用して、ユーザー名とパスワードの認証を有効にできます。次のコマンドで、ユーザー名とパスワードの認証を有効にします。

OS	コマンド
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` デフォルトのテナントを使用する場合は、テナント名として vsphere.local を使用します。
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` デフォルトのテナントを使用する場合は、テナント名として vsphere.local を使用します。

失効確認のために OCSP を使用する場合は、スマート カード証明書 AIA 拡張機能に指定されたデフォルトの OCSP を使用できます。1 つ以上の代替 OCSP レスポンダを設定して、デフォルトをオーバーライドすることもできます。たとえば、vCenter Single Sign-On サイトに対してローカルの OCSP レスポンダを設定して、失効確認要求を処理できます。

注： 証明書に OCSP が定義されていない場合は、代わりに CRL（証明書失効リスト）を有効にします。

前提条件

- 導入環境内で Platform Services Controller バージョン 6.5 以降および vCenter Server バージョン 6.0 以降を使用していることを確認します。Platform Services Controller バージョン 6.0 Update 2 は、スマート カード認証をサポートしますが、セットアップの手順が異なります。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - ユーザー プリンシパル名 (UPN) は、Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応する必要があります。
  - 証明書では、アプリケーション ポリシーまたは拡張キー使用法のフィールドにクライアント認証を指定する必要があります。設定しない場合、ブラウザに証明書が表示されません。
- Platform Services Controller の証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザは認証を試行しません。
- vCenter Single Sign-On に Active Directory ID ソースを追加します。
- vCenter Server 管理者ロールを、Active Directory ID ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、認証を受けることができ、vCenter Server 管理者権限を保有しているので、管理タスクを実行できます。

  注： vCenter Single Sign-On ドメインの管理者（デフォルトは administrator@vsphere.local）はスマート カード認証を実行できません。

- リバース プロキシを設定し、物理マシンまたは仮想マシンを再起動します。

手順

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

オプション	説明
Windows	Platform Services Controller Windows 環境にログインし、WinSCP または類似のユーティリティを使用してファイルをコピーします。

アプライアンス	a 直接または SSH を使用してアプライアンス コンソールにログインします。
	b アプライアンス シェルを次のように有効にします。
	`shell`
	`chsh -s "/bin/bash" root`
	c WinSCP または類似のユーティリティを使用して、証明書を Platform Services Controller 上の `/usr/lib/vmware-sso/vmware-sts/conf` にコピーします。
	d 必要に応じて、アプライアンス シェルを次のように無効にします。
	`chsh -s "/bin/appliancesh" root`

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

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

例：

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

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

3 他の認証方法をすべて無効にするには、次のコマンドを実行します。

```
sso-config.[bat|sh] -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 （オプション） 証明書ポリシーのホワイト リストを設定するには、次のコマンドを実行します。

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

複数のポリシーを指定するには、次のようにコンマでポリシーを区切ります。

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

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

5 （オプション） OCSP を使用して失効確認を有効にし、設定します。

a OCSP を使用して失効確認を有効にします。

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

b 証明書の AIA 拡張機能によって OCSP レスポンダのリンクが提供されていない場合、オーバーライドする OCSP レスポンダ URL と OCSP 認証局証明書を指定します。

各 vCenter Single Sign-On サイトには代替の OCSP が設定されます。vCenter Single Sign-On サイトに対して 1 つ以上の代替 OCSP レスポンダを指定し、フェイルオーバーを使用することができます。

```
sso-config.[bat|sh] -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl
http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

注： この設定は、デフォルトで現在の vCenter Single Sign-On サイトに適用されます。他の vCenter Single Sign-On サイトに対して代替 OCSP を設定する場合にのみ、`siteID` パラメータを指定します。

次の例を想定します。

```
 .sso-config.[bat|sh] -t vsphere.local -add_alt_ocsp -ocspUrl http://
failover.ocsp.nsn0.rcvs.nit.disa.mil/ -ocspSigningCert ./
DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c 現在の代替 OCSP レスポンダ設定を表示するには、次のコマンドを実行します。

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

d 現在の代替 OCSP レスポンダ設定を削除するには、次のコマンドを実行します。

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

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

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

スマート カード認証の管理

vSphere Client から、スマート カード認証の有効と無効の切り替え、ログイン バナーのカスタマイズ、失効ポリシーの設定を行うことができます。

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

ユーザー名とパスワードの認証が無効で、スマート カード認証に問題が発生した場合、ユーザーはログインできません。その場合、root ユーザーまたは管理者ユーザーは Platform Services Controller コマンド ラインを使用して、ユーザー名とパスワードの認証を有効にできます。次のコマンドで、ユーザー名とパスワードの認証を有効にします。

OS	コマンド
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` デフォルトのテナントを使用する場合は、テナント名として vsphere.local を使用します。
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` デフォルトのテナントを使用する場合は、テナント名として vsphere.local を使用します。

前提条件

- 導入環境内で Platform Services Controller バージョン 6.5 以降および vCenter Server バージョン 6.0 以降を使用していることを確認します。Platform Services Controller バージョン 6.0 Update 2 は、スマート カード認証をサポートしますが、セットアップの手順が異なります。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - ユーザー プリンシパル名 (UPN) は、Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応する必要があります。
  - 証明書では、アプリケーション ポリシーまたは拡張キー使用法のフィールドにクライアント認証を指定する必要があります。設定しない場合、ブラウザに証明書が表示されません。
- Platform Services Controller の証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザは認証を試行しません。
- vCenter Single Sign-On に Active Directory ID ソースを追加します。

- vCenter Server 管理者ロールを、Active Directory ID ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、認証を受けることができ、vCenter Server 管理者権限を保有しているので、管理タスクを実行できます。

  注： vCenter Single Sign-On ドメインの管理者（デフォルトは administrator@vsphere.local）はスマート カード認証を実行できません。

- リバース プロキシを設定し、物理マシンまたは仮想マシンを再起動します。

手順

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

オプション	説明
Windows	Platform Services ControllerWindows 環境にログインし、WinSCP または類似のユーティリティを使用してファイルをコピーします。

アプライアンス	a 直接または SSH を使用してアプライアンス コンソールにログインします。
	b アプライアンス シェルを次のように有効にします。
	`shell`
	`chsh -s "/bin/bash" root`
	`csh -s "bin/appliance/sh" root`
	c WinSCP または類似のユーティリティを使用して、証明書を Platform Services Controller 上の `/usr/lib/vmware-sso/vmware-sts/conf` にコピーします。
	d 必要に応じて、アプライアンス シェルを次のように無効にします。
	`chsh -s "/bin/appliancesh" root`

2 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

4 [構成] ユーザー インターフェイスに移動します。

  a [ホーム] メニューから [管理] を選択します。

  b [Single Sign-On] で、[構成] をクリックします。

5 [スマート カード認証] で [編集] をクリックします。

6 認証方法を選択するか、または選択を解除して、[保存] をクリックします。

  スマート カード認証を単独で選択するか、スマート カード認容とパスワードおよび Windows セッション認証を両方選択することができます。

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

[信頼できる CA 証明書] が表示されます。

7 [信頼できる CA 証明書] タブで [追加] をクリックし、[参照] をクリックします。

8 信頼できる認証局 (CA) からの証明書をすべて選択して、[追加] をクリックします。

次のステップ

環境に、拡張 OCSP 構成が必要である場合があります。

- OCSP 応答が、スマート カードの署名 CA とは異なる CA によって発行されている場合、OCSP による署名 CA 証明書を提供します。
- 複数サイトのデプロイでは、Platform Services Controller サイトごとに 1 つ以上のローカル OCSP レスポンダを構成できます。CLI を使用して、このような代替 OCSP レスポンダを構成できます。コマンド ラインを使用したスマート カード認証の管理を参照してください。

スマート カード認証の失効ポリシーの設定

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

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

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

  OCSP のみ

  発行元の認証局で OCSP レスポンダがサポートされている場合、[OCSP] が有効になり、[OCSP のフェイルオーバーとしての CRL] が無効になります。

  CRL のみ

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

  OSCP と CRL の両方の利用

  発行元の認証局で OCSP レスポンダと CRL の両方がサポートされている場合、vCenter Single Sign-On によって OCSP レスポンダが最初にチェックされます。レスポンダによって不明なステータスが返されるか、使用可能でない場合は、vCenter Single Sign-On によって CRL がチェックされます。この場合、[OCSP チェック] および [CRL チェック] の両方が有効になり、[OCSP のフェイルオーバーとしての CRL] が有効になります。

- 失効チェックが有効な場合、上級ユーザーは次の追加設定を指定できます。

  OSCP URL

  vCenter Single Sign-On は、デフォルトで、検証されている証明書内で定義される OCSP レスポンダの場所を確認します。Authority Information Access 拡張領域が証明書内にない場合、または拡張領域にオーバーライドする場合には、明示的に場所を指定できます。

  証明書の CRL を使用

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

  CRL の場所

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

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

前提条件

- 導入環境内で Platform Services Controller バージョン 6.5 以降および vCenter Server バージョン 6.0 以降を使用していることを確認します。Platform Services Controller バージョン 6.0 Update 2 は、スマート カード認証をサポートしますが、セットアップの手順が異なります。
- エンタープライズの公開鍵基盤 (PKI) が環境内に設定されていること、および証明書が次の要件を満たしていることを確認します。
  - ユーザー プリンシパル名 (UPN) は、Subject Alternative Names (SAN) 拡張の Active Directory アカウントに対応する必要があります。
  - 証明書では、アプリケーション ポリシーまたは拡張キー使用法のフィールドにクライアント認証を指定する必要があります。設定しない場合、ブラウザに証明書が表示されません。
- Platform Services Controller の証明書がエンド ユーザーのワークステーションによって信頼されていることを確認します。信頼されていない場合、ブラウザは認証を試行しません。
- vCenter Single Sign-On に Active Directory ID ソースを追加します。
- vCenter Server 管理者ロールを、Active Directory ID ソースの 1 人以上のユーザーに割り当てます。これらのユーザーは、認証を受けることができ、vCenter Server 管理者権限を保有しているので、管理タスクを実行できます。

注： vCenter Single Sign-On ドメインの管理者（デフォルトは administrator@vsphere.local）はスマート カード認証を実行できません。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [スマート カード認証] をクリックします。

5 [証明書の失効] をクリックし、[編集] をクリックして、失効チェックを有効または無効にします。

6 環境内で証明書ポリシーが有効になっている場合、[証明書ポリシー] ペインにポリシーを追加できます。

RSA SecurID 認証の設定

RSA SecurID トークンを使用したログインをユーザーに要求するように環境を設定できます。SecurID の設定はコマンド ラインからのみサポートされています。

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

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

前提条件

- RSA SecurID の構成時に、vCenter Single Sign-On (SSO) ではユーザー プリンシパル名（userPrincipalName 属性）をユーザー ID として使用できます。これは、統合 Windows 認証 (IWA) が RSA ユーザーに対し ID ソースとして構成されている場合のみです。
- 導入環境内で Platform Services Controller バージョン 6.5 以降および vCenter Server バージョン 6.0 以降を使用していることを確認します。Platform Services Controller バージョン 6.0 Update 2 は、スマート カード認証をサポートしますが、セットアップの手順が異なります。
- 環境内に正しく構成された RSA 認証マネージャが配備され、ユーザーに RSA トークンが提供されていることを確認します。RSA 認証マネージャのバージョン 8.0 以降が必要です。
- RSA マネージャが使用する ID ソースが、vCenter Single Sign-On に追加されていることを確認します。vCenter Single Sign-OnID ソースの追加または編集を参照してください。
- RSA 認証マネージャのシステムが Platform Services Controller ホスト名を解決でき、Platform Services Controller システムが RSA 認証マネージャのホスト名を解決できることを確認します。
- [アクセス] - [認証エージェント] - [構成ファイルを生成] を選択して、`sdconf.rec` ファイルを RSA マネージャからエクスポートします。生成された `AM_Config.zip` ファイルを解凍し、`sdconf.rec` ファイルを見つけます。
- `sdconf.rec` ファイルを Platform Services Controller ノードにコピーします。

手順

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

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

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

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

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

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

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

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

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

例：

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

次のオプションを指定できます。

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

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

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

通常、デフォルト値が適切です。次に例を示します。

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

6 （オプション） ID ソースでユーザー プリンシパル名がユーザー ID として使用されていない場合、ID ソースの userID 属性を設定します（LDAP アイデンティティ ソース上の Active Directory でのみサポートされます）。

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

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

例：

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

7 現在の設定を表示するには、次のコマンドを実行します。

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

結果

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

注： ユーザー名の形式は、***userID@domainName*** または ***userID@domain_upn_suffix*** です。

ログイン メッセージの管理

ご利用の環境にログイン メッセージを表示できます。ログイン メッセージの有効と無効を切り替えたり、明示的な承諾を得る際にユーザーがチェック ボックスをクリックするように求めたりできます。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ログイン メッセージ] タブをクリックします。

5 [編集] をクリックし、ログイン メッセージを設定します。

オプション	説明
ログイン メッセージの表示	ログイン メッセージを有効にするには、[ログイン メッセージの表示] のスイッチを切り替えます。このスイッチを有効にしないと、ログイン メッセージを変更することはできません。
ログイン メッセージ	メッセージのタイトル。デフォルトでは、[承諾チェックボックス] が選択されているとき、ログイン メッセージのテキストは `I agree to Terms and Conditions` です。`Terms and Conditions` を独自のテキストに置き換える必要があります。[承諾チェックボックス] を選択解除すると `Login message` が表示され、メッセージを入力することができます。
承諾チェックボックス	ログインする前にチェック ボックスをクリックするようユーザーに求める場合は、[承諾チェックボックス] を選択します。また、チェック ボックスを使用せずにメッセージを表示することもできます。
ログイン メッセージの詳細	ユーザーがログイン メッセージをクリックしたときに表示されるメッセージ。たとえば、使用条件の文章などです。このテキスト ボックスに詳細情報を入力する必要があります。

6 [[保存]] をクリックします。

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

vSphere Web Client は、信頼される SAML 2.0 サービス プロバイダ (SP) として自動的に vCenter Single Sign-On に登録されます。他の信頼されるサービス プロバイダを、vCenter Single Sign-On が SAML ID プロバイダ (IDP) として動作する ID フェデレーションに追加することができます。サービス プロバイダは SAML 2.0 プロトコルに適合する必要があります。フェデレーションを設定した後、ユーザーが vCenter Single Sign-On の認証を受けることができれば、サービス プロバイダはそのユーザーにアクセス権を付与します。

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

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

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

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

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

2 SP メタデータをエクスポートし、IDP にインポートします。

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

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

ID フェデレーションへの SAML サービス プロバイダの参加

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

前提条件

ターゲット サービスは SAML 2.0 標準を完全サポートし、SP メタデータには `SPSSODescriptor` 要素が含まれている必要があります。

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

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

手順

1. サービス プロバイダのメタデータをファイルにエクスポートします。
2. vSphere Web Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。
3. [構成] ユーザー インターフェイスに移動します。
   a. [ホーム] メニューから [管理] を選択します。
   b. [Single Sign-On] で、[構成] をクリックします。
4. SP メタデータを vCenter Single Sign-On にインポートします。
   a. [SAML サービス プロバイダ] タブを選択します。
   b. [SAML サービス プロバイダのメタデータ] ダイアログ ボックスで XML 文字列を貼り付けるか、ファイルをインポートしてメタデータをインポートします。
5. vCenter Single Sign-On IDP メタデータをエクスポートします。
   a. [SAML サービス プロバイダのメタデータ] テキスト ボックスで [ダウンロード] をクリックします。
   b. ファイルの場所を指定します。

6 SAML SP（たとえば VMware vRealize Automation 7.0）にログインし、SP の指示に従って vCenter Single Sign-On メタデータをそのサービス プロバイダに追加します。

製品へのメタデータのインポートに関する詳細については、vRealize Automation のドキュメントを参照してください。

Security Token Service (STS)

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

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

ユーザー

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

アプリケーション ユーザー

有効な証明書

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

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

Security Token Service 証明書の更新

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

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

ソリューション ユーザー

有効な証明書

その他のユーザー

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

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

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

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

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

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

前提条件

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

Platform Services Controller アプライアンス

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

例：

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

Windows インストール

certificate_location\root-trust.jks

例：

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

手順

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

vCenter Single Sign-On 管理者権限を保有するユーザーは、ローカルの vCenter Single Sign-On ドメインの管理者グループに含まれます（デフォルトは vsphere.local）。

2 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

3 [証明書] タブを選択して、[STS 署名] サブタブを選択し、[STS 署名証明書の追加] アイコンをクリックします。

4 証明書を追加します。

a [参照] をクリックして、新しい証明書を含むキー ストア JKS ファイルを参照し、[開く] をクリックします。

b パスワードの入力が求められた場合は、入力します。

c STS エイリアス チェーンの最上部をクリックし、[OK] をクリックします。

d パスワードの入力が求められた場合は、再び入力します。

5 [OK] をクリックします。

6 Platform Services Controller ノードを再起動し、STS サービスと vSphere Web Client の両方を起動します。

再起動するまで認証は正しく機能しません。そのため、再起動は必須です。

アプライアンスでの新しい STS 署名証明書の生成

vCenter Single Sign-On Security Token Service (STS) 署名証明書は内部的な VMware 証明書であるため、会社が内部証明書の置き換えを必要としている場合を除き、置き換えないでください。デフォルトの STS 署名証明書を置き換える場合は、新しい証明書を生成し、Java キーストアに追加する必要があります。ここでは、組み込まれたデプロイ アプライアンスまたは外部の Platform Services Controller アプライアンスに対する手順について説明します。

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

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

手順

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

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

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

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

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

国は必須で、次の例に示すように 2 文字で指定する必要があります。

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

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

4 キーを生成します。

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

5 証明書を生成します

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

6 証明書を PK12 形式に変換します。

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key
-certfile /var/lib/vmware/vmca/root.cer -name "newstssigning" -passout pass:testpassword
-out newsts.p12
```

7 Java キーストア (JKS) に証明書を追加します。

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype
pkcs12 -srcstorepass testpassword -srcalias newstssigning -destkeystore root-trust.jks
-deststoretype JKS -deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype
JKS -storepass testpassword -keypass testpassword -file /var/lib/vmware/vmca/root.cer
-alias root-ca
```

使用可能なすべてのコマンドのリストについては、`keytool -help` を使用します。

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

次のステップ

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

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

vCenter Single Sign-On Security Token Service (STS) 署名証明書は内部的な VMware 証明書であるため、会社が内部証明書の置き換えを必要としている場合を除き、置き換えないでください。デフォルトの STS 署名証明

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

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

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

手順

1 新しい証明書を保持するためのディレクトリを作成します。

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

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

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

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

国は必須で、2 文字で指定する必要があります。以下に例を示します。

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

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

4 キーを生成します。

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

5 証明書を生成します

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

6 証明書を PK12 形式に変換します。

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

7 Java キーストア (JKS) に証明書を追加します。

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

次のステップ

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

LDAPS SSL 証明書の有効期限日の判断

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

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

手順

1 vSphere Web Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ID ソース] タブをクリックします。

5 画面の上部で、LDAPS 証明書を表示する ID ソースを選択します。

6 画面の下部で証明書の詳細を表示し、[有効期限の終了日] フィールドで有効期限を確認します。

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

vCenter Single Sign-On ポリシーの管理

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

vCenter Single Sign-On のパスワード ポリシーの編集

vCenter Single Sign-On のパスワード ポリシーは、パスワードの形式と有効期限を決定します。パスワード ポリシーは vCenter Single Sign-On ドメイン（vsphere.local または vmc.local）内のユーザーにのみ適用されます。

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

vCenter Single Sign-On パスワードの変更 を参照してください。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ポリシー] をクリックして [パスワード ポリシー] を選択し、[編集] をクリックします。

5 パスワード ポリシーを編集します。

オプション	説明
説明	パスワード ポリシーの説明。
最長有効期間	ユーザーが変更するまでのパスワードの最大有効期間。入力できる日数の最大値は 999999999 です。ゼロ (0) を指定すると、パスワードは期限切れになりません。
再利用を制限	再利用できない過去に設定したパスワードの数。たとえば 6 と入力すると、ユーザーは過去に使用した直近 6 つのいずれのパスワードも再利用できません。
最大長	パスワードで使用できる最大文字数。
最小長	パスワードに必要な最小文字数。最小長は、アルファベット、数字、および特殊文字の最小要件を組み合わせた文字数以上であることが必要です。

オプション	説明
文字要件	パスワードに必要なさまざまな文字タイプの最小数。各タイプの文字の数は、次のように指定できます。 ■ 特殊： & # % ■ アルファベット： A b c D ■ 大文字： A B C ■ 小文字： a b c ■ 数字： 1 2 3 アルファベット文字の最小数は、大文字および小文字で指定した数の合計以上にする必要があります。 ASCII 以外の文字もパスワードに使用できます。以前のバージョンの vCenter Single Sign-On には、サポートされる文字に制限があります。
隣接した同一文字	パスワードで使用できる隣接した同一文字の最大数。たとえば 1 と入力すると、「p@$$word」というパスワードは許可されません。 値は 0 より大きくする必要があります。

6 [保存] をクリックします。

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

vCenter Single Sign-On のロックアウト ポリシーを使用すると、ユーザーが誤った認証情報でログインしようとしたときに、そのユーザーの vCenter Single Sign-On アカウントをロックするタイミングを指定できます。管理者はロックアウト ポリシーを編集できます。

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

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [ロックアウト ポリシー] を選択し、[編集] をクリックします。

5 パラメータを編集します。

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

6 [保存] をクリックします。

vCenter Single Sign-On のトークン ポリシーの編集

vCenter Single Sign-On トークン ポリシーには、クロック トレランス、更新数などのトークンのプロパティを指定します。トークンの仕様が企業のセキュリティ標準に準拠するように、トークン ポリシーを編集できます。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [構成] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[構成] をクリックします。

4 [トークン ポリシー] を選択し、[編集] をクリックします。

5 トークン ポリシー構成パラメータを編集します。

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

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

6 [保存] をクリックします。

Active Directory ユーザーへのパスワード有効期限の通知の編集

Active Directory のパスワード有効期限の通知は、vCenter Server SSO パスワードの有効期限とは別のものです。Active Directory ユーザーへのデフォルトのパスワード有効期限の通知期間は 30 日ですが、実際のパスワード有効期限は、Active Directory システムによって異なります。有効期限の通知は、vSphere Client と vSphere Web Client で制御します。デフォルトの有効期限の通知は、自社のセキュリティ標準に合わせて変更できます。

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。

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 ディレクトリを `webclient.properties` ファイルの場所に変更します。

OS	コマンド

Linux	■ vSphere Client：
	`cd /etc/vmware/vsphere-ui`
	■ vSphere Web Client：
	`cd /etc/vmware/vsphere-client`

Windows	■ vSphere Client：
	`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-ui`
	■ vSphere Web Client：
	`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-client`

3 テキスト エディタで `webclient.properties` ファイルを開きます。

4 次の変数を編集します。

```
sso.pending.password.expiration.notification.days = 30
```

5 クライアントを再起動します。

OS	コマンド

Linux	■ vSphere Client：
	`service-control --stop vsphere-ui`
	`service-control --start vsphere-ui`
	■ vSphere Web Client：
	`service-control --stop vsphere-client`
	`service-control --start vsphere-client`

Windows	■ vSphere Client：
	`cd "C:\Program Files\VMware\vCenter Server\bin\"`
	`service-control --stop vsphere-ui`
	`service-control --start vsphere-ui`
	■ vSphere Web Client：
	`cd "C:\Program Files\VMware\vCenter Server\bin\"`
	`service-control --stop vspherewebclientsvc`
	`service-control --start vspherewebclientsvc`

vCenter Single Sign-On ユーザーおよびグループの管理

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

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

- vCenter Single Sign-On ユーザーの追加

  vSphere Client の [ユーザー] タブには、vsphere.local ドメインに属している vCenter Single Sign-On の内部ユーザーが表示されます。vCenter Single Sign-On 管理インターフェイスのいずれかを使用して、このドメインにユーザーを追加します。

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

  vCenter Single Sign-On ユーザー アカウントを無効にすると、管理者がアカウントを有効にするまで、そのユーザーは vCenter Single Sign-On サーバにログインできなくなります。アカウントは、いずれかの vCenter Single Sign-On 管理インターフェイスで有効および無効にできます。

- vCenter Single Sign-On ユーザーの削除

  vsphere.local ドメインのユーザーは、vCenter Single Sign-On 管理インターフェイスから削除できます。ローカル オペレーティング システムのユーザーまたは別のドメインのユーザーを vCenter Single Sign-On 管理インターフェイスから削除することはできません。

- vCenter Single Sign-On ユーザーの編集

  vCenter Single Sign-On 管理インターフェイスから vCenter Single Sign-On ユーザーのパスワードまたはその他の詳細を変更できます。vsphere.local ドメインではユーザーの名前を変更できません。つまり、administrator@vsphere.local の名前は変更できません。

- vCenter Single Sign-On グループの追加

  vCenter Single Sign-On [グループ] タブには、ローカル ドメインのグループが表示されます（デフォルトでは vsphere.local）。グループ メンバー（プリンシパル）のコンテナが必要な場合は、グループを追加します。

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

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

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

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

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

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

- vCenter Single Sign-On パスワードの変更

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

vCenter Single Sign-On ユーザーの追加

vSphere Client の [ユーザー] タブには、vsphere.local ドメインに属している vCenter Single Sign-On の内部ユーザーが表示されます。vCenter Single Sign-On 管理インターフェイスのいずれかを使用して、このドメインにユーザーを追加します。

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

手順

1. vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。
2. administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 ドメインに vsphere.local が選択されていない場合は、ドロップダウン メニューから vsphere.local を選択します。

ユーザーを他のドメインに追加することはできません。

5 [ユーザー] タブで [ユーザーの追加] をクリックします。

6 新規ユーザーのユーザー名とパスワードを入力します。

ユーザーの作成後、ユーザー名は変更できません。パスワードは、システムのパスワード ポリシー要件を満たしている必要があります。

7 （オプション） 新規ユーザーの姓名を入力します。

8 （オプション） ユーザーのメール アドレスと説明を入力します。

9 [追加] をクリックします。

結果

追加した当初、ユーザーには管理操作を実行する権限がありません。

次のステップ

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

vCenter Single Sign-On ユーザーの無効化および有効化

vCenter Single Sign-On ユーザー アカウントを無効にすると、管理者がアカウントを有効にするまで、そのユーザーは vCenter Single Sign-On サーバにログインできなくなります。アカウントは、いずれかの vCenter Single Sign-On 管理インターフェイスで有効および無効にできます。

無効なユーザー アカウントは引き続き vCenter Single Sign-On システムで使用可能ですが、そのユーザーはログインできず、サーバでの操作を実行できません。管理者権限を保有するユーザーは、vCenter Server の [ユーザーおよびグループ] ページからユーザーを無効および有効にできます。

前提条件

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 ユーザー名を選択して縦の省略符号アイコンをクリックし、[無効] をクリックします。

5 [OK] をクリックします。

6 ユーザーを再度有効にするには、縦の省略符号アイコンをクリックして [有効] をクリックし、[OK] をクリックします。

vCenter Single Sign-On ユーザーの削除

vsphere.local ドメインのユーザーは、vCenter Single Sign-On 管理インターフェイスから削除できます。ローカル オペレーティング システムのユーザーまたは別のドメインのユーザーを vCenter Single Sign-On 管理インターフェイスから削除することはできません。

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [ユーザー] を選択し、ドロップダウン メニューから vsphere.local ドメインを選択します。

5 削除するユーザーをユーザーのリストで選択して、縦の省略符号アイコンをクリックします。

6 [削除] をクリックします。

操作は慎重に行ってください。この操作を取り消すことはできません。

vCenter Single Sign-On ユーザーの編集

vCenter Single Sign-On 管理インターフェイスから vCenter Single Sign-On ユーザーのパスワードまたはその他の詳細を変更できます。vsphere.local ドメインではユーザーの名前を変更できません。つまり、administrator@vsphere.local の名前は変更できません。

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

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

vCenter Single Sign-On のパスワード ポリシーは、vSphere Client で確認できます。administrator@vsphere.local として [管理] メニューからログインし、[構成] - [ポリシー] - [パスワード ポリシー] の順に選択します。

vCenter Single Sign-On のパスワード ポリシーの編集も参照してください。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [ユーザー] をクリックします。

5 縦の省略符号アイコンをクリックし、[編集] を選択します。

6 ユーザーの属性を編集します。

ユーザー名は変更できません。

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

7 [OK] をクリックします。

vCenter Single Sign-On グループの追加

vCenter Single Sign-On [グループ] タブには、ローカル ドメインのグループが表示されます（デフォルトでは vsphere.local）。グループ メンバー（プリンシパル）のコンテナが必要な場合は、グループを追加します。

vCenter Single Sign-On [グループ] タブでは、他のドメイン（Active Directory ドメインなど）にグループを追加することはできません。

ID ソースを vCenter Single Sign-On に追加しない場合は、グループを作成してユーザーを追加することで、ローカル ドメインを編成できます。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [グループ] を選択し、[グループの追加] をクリックします。

5 グループの名前と説明を入力します。

グループを作成した後は、グループ名を変更できません。

6 [追加] をクリックします。

次のステップ

- メンバーをグループに追加します。

vCenter Single Sign-On グループへのメンバーの追加

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

背景情報については、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2095342) を参照してください。

Web インターフェイスの [グループ] タブに表示されるグループは、vsphere.local ドメインに属しています。vCenter Single Sign-On ドメイン内のグループを参照してください。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [グループ] をクリックしてから、グループ（管理者など）をクリックします。

5 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。

6 グループに追加するメンバーを含む ID ソースを選択します。

7 （オプション） 検索用語を入力し、[検索] をクリックします。

8 メンバーを選択します。

複数のメンバーを追加できます。

9 [OK] をクリックします。

vCenter Single Sign-On グループからのメンバーの削除

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [グループ] を選択し、グループをクリックします。

5 グループ メンバーのリストで、削除するユーザーまたはグループを選択し、垂直方向の省略記号アイコンをクリックします。

6 [メンバーの削除] をクリックします。

7 [削除] をクリックします。

結果

ユーザーはグループから削除されますが、その後もシステムで使用可能です。

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

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

vCenter Server ソリューション ユーザーまたはサードパーティ製ソリューション ユーザーに関連付けられている一連のサービスを使用環境から削除すると、ソリューション ユーザーが vSphere Web Client の表示から削除されます。ソリューション ユーザーがまだシステム内にいるときにアプリケーションを強制的に削除した場合、またはシステムが回復不能になった場合は、ソリューション ユーザーを vSphere Web Client から明示的に削除できます。

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

手順

1 vSphere Web Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 vCenter Single Sign-On ユーザーの設定を行うユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [Single Sign-On] で、[ユーザーおよびグループ] をクリックします。

4 [ソリューション ユーザー] タブをクリックして、ソリューション ユーザー名をクリックします。

5 [ソリューション ユーザーの削除] アイコンをクリックします。

6 [はい] をクリックします。

結果

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

vCenter Single Sign-On パスワードの変更

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

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

注： パスワードは有効期限内の場合にのみ変更できます。

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

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

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

4 [パスワードの変更] を選択し、現在のパスワードを入力します。

5 新しいパスワードを入力して確定します。

パスワードはパスワード ポリシーに従っている必要があります。

6 [OK] をクリックします。

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

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

vSphere の認証インフラストラクチャにより、vSphere 環境のセキュリティが強化されます。インフラストラクチャが危険にさらされないようにするために、vCenter Single Sign-On のベスト プラクティスを遵守してください。

パスワードの有効期限の確認

vCenter Single Sign-On のデフォルトのパスワード ポリシーの有効期限は 90 日です。90 日後にパスワードの有効期限が切れ、ログインできなくなります。有効期限を確認して、適宜パスワードを更新してください。

NTP の構成

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

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

vSphere セキュリティ証明書

3

vSphere では、通信の暗号化、サービスの認証、トークンへの署名に証明書を使用してセキュリティを提供します。

vSphere は、次の処理に証明書を使用します。

- vCenter Server ホストや ESXi ホストなどの 2 つのノード間の通信を暗号化します。
- vSphere サービスを認証します。
- トークンへの署名などの内部のアクションを実行する。

vSphere の内部認証局 (CA)、VMware 認証局 (VMCA) は、vCenter Server および ESXi に必要なすべての証明書を提供します。VMCA は各 Platform Services Controller にインストールされると、他の変更を加えずに直ちにソリューションのセキュリティを強化します。このデフォルトの構成を維持することで、証明書管理の運用上のオーバーヘッドが最小に抑えられます。vSphere には、証明書の期限が切れるイベントで証明書を更新するメカニズムがあります。

vSphere には、特定の証明書を独自の証明書で置き換えるメカニズムもあります。ただし、証明書管理のオーバーヘッドを低く抑えるために、ノード間の暗号化を提供している SSL 証明書のみを置き換えます。

証明書管理には、次のオプションが推奨されます。

表 3-1. 証明書管理の推奨オプション

モード	説明	メリット
VMCA のデフォルト証明書	VMCA は、vCenter Server および ESXi ホストのすべての証明書を提供します。	最もシンプルで、オーバーヘッドが最小になります。VMCA は、vCenter Server および ESXi ホストのすべての証明書のライフサイクルを管理します。
VMCA のデフォルト証明書と外部 SSL 証明書（ハイブリッド モード）	Platform Services Controller および vCenter Server Appliance の SSL 証明書を置き換え、VMCA でソリューション ユーザーおよび ESXi ホストの証明書を管理できるようにします。高度なセキュリティに対応したデプロイでは、必要に応じて、ESXi ホストの SSL 証明書も置き換えることができます。	シンプルでセキュアです。VMCA で内部証明書を管理しますが、企業で承認した SSL 証明書を使用できるため、ブラウザに証明書を信頼させることができるという利点があります。

VMware では、ソリューション ユーザー証明書または STS 証明書を置き換えることも、VMCA の代わりに従属 CA を使用することも推奨していません。これらのオプションのいずれかを選択すると、著しい複雑さとセキュリティに対する好ましくない影響が潜在的に発生し、運用上のリスクが無用に増大する可能性があります。vSphere 環境内での証明書管理の詳細については、http://vmware.com/go/hybridvmca で「New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement」というブログ記事を参照してください。

既存の証明書を置き換えるには、次のオプションを使用します。

表 3-2. 証明書を置き換えるための異なるアプローチ

オプション	詳細については、ドキュメントを参照してください。
vSphere Client を使用する。vSphere 6.7 以降では、Platform Services Controller は vSphere Client を使用して管理します。	vSphere Client での証明書の管理
コマンド ラインから vSphere Certificate Manager ユーティリティを使用する。	vSphere Certificate Manager ユーティリティによる証明書の管理
CLI コマンドを使用して証明書を手動で置き換える。	4 章 CLI コマンドを使用したサービスと証明書の管理

vSphere 証明書管理
(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

この章には、次のトピックが含まれています。

- 異なるソリューション パスの証明書の要件
- 証明書管理の概要
- vSphere Client での証明書の管理
- vSphere Web Client からの証明書の管理
- vSphere Certificate Manager ユーティリティによる証明書の管理
- 証明書の手動での置き換え

異なるソリューション パスの証明書の要件

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

開始する前に、環境内ですべてのノードの時刻が確実に同期されるようにします。

すべてのインポートされた証明書の要件

- キー サイズ：2,048 ビット以上（PEM エンコード）
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加したキーは、PKCS8 に変換されます。
- x509 バージョン 3
- SubjectAltName には DNS Name=*machine_FQDN* が含まれている必要があります。

- CRT 形式
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります。
- [拡張キー使用] は、空白にするかサーバ認証を指定します。

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。
- 推奨されていないアルゴリズムは、md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4、および sha1WithRSAEncryption 1.2.840.113549.1.1.5 です。
- OID が 1.2.840.113549.1.1.10 のアルゴリズム RSASSA-PSS はサポートされていません。

RFC 2253 に対する証明書のコンプライアンス

証明書は、RFC 2253 に準拠している必要があります。

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

文字列	X.500 属性のタイプ
CN	`commonName`
L	`localityName`
ST	`stateOrProvinceName`
O	`organizationName`
OU	`organizationalUnitName`
C	`countryName`
STREET	`streetAddress`
DC	`domainComponent`
UID	`userid`

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

- administrator@vsphere.local ユーザー、つまり接続している vCenter Single Sign-On ドメインの管理者のパスワード。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- Certificate Manager によって `Certool.cfg` ファイルに保存される情報。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。
  - administrator@vsphere.local のパスワード。
  - 2 文字の国名コード
  - 会社名

- 組織名
- 部門名
- 都道府県
- 市区町村
- IP アドレス（オプション）
- E メール
- ホスト名、すなわち証明書を置き換えるマシンの完全修飾ドメイン名 (FQDN)「ホスト名が FQDN と一致しない場合、証明書の置き換えは正しく完了せず、環境が不安定な状態になる可能性があります。
- Platform Services Controller の IP アドレス（コマンドを vCenter Server（管理）ノード上で実行している場合）。

VMCA を中間 CA として使用する場合の要件

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

証明書タイプ	証明書の要件
ルート証明書	■ CSR は vSphere Certificate Manager を使用して作成できます。vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意するを参照してください。 ■ CSR を手動で作成する場合、署名のために送付する証明書は以下の要件を満たしている必要があります。 ■ キー サイズ： 2,048 ビット以上 ■ PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。 ■ x509 バージョン 3 ■ カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。 ■ CRL の署名は有効にしてください。 ■ [拡張キー使用] は、空にするか、[サーバ認証] を指定します。 ■ 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。 ■ ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。 ■ VMCA の従属認証局は作成できません。 Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (2112009)」(http://kb.vmware.com/kb/2112009) を参照してください。
マシン SSL 証明書	vSphere Certificate Manager を使用して CSR を作成するか、手動で CSR を作成できます。 CSR を手動で作成する場合は、「すべてのインポートされた証明書の要件」に記載されている要件を満たす必要があります。ホストの FQDN を指定する必要もあります。
ソリューション ユーザー証明書	vSphere Certificate Manager を使用して CSR を作成するか、手動で CSR を作成することができます。 **注：** 各ソリューション ユーザーの名前には異なる値を使用する必要があります。証明書を手動で生成する場合、使用するツールに応じて、[サブジェクト] の [CN] として表示される可能性があります。 vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、`certool.cfg` に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。

カスタム 証明書の要件

カスタム証明書を使用する場合、証明書は次の要件を満たす必要があります。

証明書タイプ	証明書の要件
マシン SSL 証明書	各ノード上のマシン SSL 証明書には、サードパーティまたはエンタープライズ CA からの個別の証明書が必要です。 ■ vSphere Client または vSphere Certificate Manager を使用して CSR を生成することも、手動で CSR を作成することもできます。CSR は、上記の「すべてのインポートされた証明書の要件」に記載されている要件を満たす必要があります。 ■ vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、`certool.cfg` に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。 ■ ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。
ソリューション ユーザー証明書	各ノード上の各ソリューション ユーザーには、サードパーティまたはエンタープライズ CA からの個別の証明書が必要です。 ■ CSR は、vSphere Certificate Manager を使用して生成することも、CSR を自分で準備することもできます。CSR は、上記の「すべてのインポートされた証明書の要件」に記載されている要件を満たす必要があります。 ■ vSphere Certificate Manager を使用する場合、各ソリューション ユーザーの証明書情報を求められます。vSphere Certificate Manager によって、`certool.cfg` に情報が保存されます。「Information that Certificate Manager Prompts For」を参照してください。 **注：** 各ソリューション ユーザーの名前には異なる値を使用する必要があります。手動で生成された証明書は、使用するツールに応じて、[サブジェクト] の [CN] として表示される可能性があります。 後でソリューション ユーザー証明書をカスタム証明書と置き換える場合、サードパーティの CA の署名証明書チェーンすべてを指定します。

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

証明書管理の概要

証明書インフラストラクチャの設定や更新に必要な作業は、環境の要件によって異なります。新規インストールとアップグレードのどちらを実行しているのか、ESXi と vCenter Server のどちらを検討しているのか、などを考慮する必要があります。

管理者が VMware 証明書を置き換えない場合

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

VMware 証明書を置き換えない場合、環境では自己署名証明書の代わりに VMCA 署名付き証明書が使用されます。

管理者が VMware 証明書をカスタム証明書に置き換える場合

企業ポリシーでサード パーティ認証局 (CA) またはエンタープライズ CA によって署名された証明書の使用が規定されている場合、またはカスタム証明書の情報が要求される場合、新規インストールには複数の選択肢があります。

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

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

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

  vSphere 6.0 以降にアップグレードした後で、証明書モードを [カスタム] に設定できます。証明書モードが VMCA（デフォルト）で、ユーザーが vSphere Client から証明書の更新を実行する場合、VMCA 署名付き証明書によってカスタム証明書が置き換えられます。
- vCenter Server コンポーネントでは、既存の環境によって処理が異なります。
  - シンプルなインストールを組み込みデプロイにアップグレードする場合、vCenter Server はカスタム証明書を維持します。アップグレード後の環境は、以前と同様に動作します。
  - 複数サイトのデプロイのアップグレードの場合、vCenter Single Sign-On が vCenter Server コンポーネントとは別のマシンに配置される場合があります。この場合は、アップグレード プロセスによって複数ノードのデプロイが作成され、Platform Services Controller ノードと 1 つ以上の管理ノードが含まれます。

    このシナリオでは、既存の vCenter Server 証明書および vCenter Single Sign-On 証明書が維持されます。これらの証明書は、マシン SSL 証明書として使用されます。

    さらに、VMCA 署名付き証明書が、VMCA によって各ソリューション ユーザー（vCenter サービスのコレクション）に割り当てられます。ソリューション ユーザーは、vCenter Single Sign-On への認証でのみこの証明書を使用します。通常、ソリューション ユーザー証明書の置き換えが企業ポリシーで規定されていることはありません。

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

vSphere 証明書インターフェイス

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

表 3-3. vCenter Server 証明書を管理するためのインターフェイス

インターフェイス	用途
vSphere Client	グラフィカル ユーザー インターフェイスを使用して、証明書に関連する一般的なタスクを実行します。
vSphere Certificate Manager ユーティリティ	vCenter Server インストールのコマンド ラインから証明書置き換えに関連する一般的なタスクを実行します。
証明書管理 CLI	すべての証明書管理タスクを `dir-cli`、`certool`、および `vecs-cli` を使用して実行します。
vSphere Web Client	証明書を表示します（有効期限情報を含む）。

ESXi では、vSphere Client から証明書管理を実行します。VMCA は、証明書をプロビジョニングして、ESXi ホストのローカルに保存します。VMDIR または VECS には ESXi ホスト証明書を保存しません。『vSphere のセキュリティ』ドキュメントを参照してください。

サポートされる vCenter 証明書

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

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

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

証明書の置き換えの概要

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

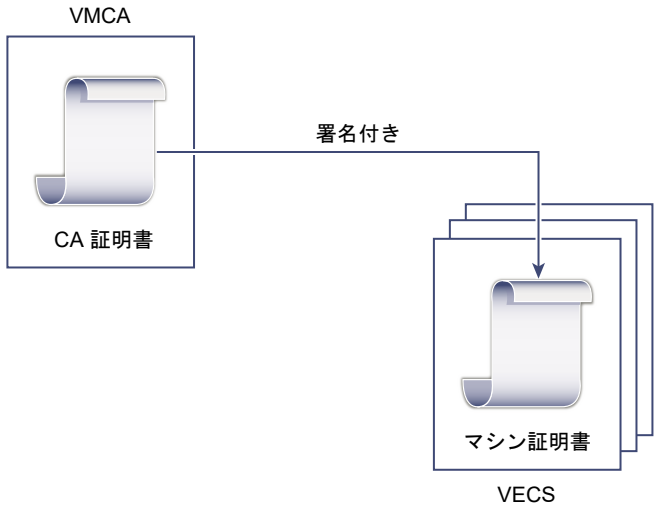
VMCA は、各 Platform Services Controller およびに環境に組み込まれています。VMCA は、各ノード、各 vCenter Server ソリューション ユーザー、および各 ESXi ホストに、VMCA が認証局として署名した証明書をプロビジョニングします。vCenter Server ソリューション ユーザーは、vCenter Server サービスのグループです。

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

VMware 認証局 (VMCA) によって署名された証明書との置き換え

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

図 3-1. VMCA によって署名された証明書の VECS への保存



次の vSphere Certificate Manager のオプションを使用できます。

- マシンの SSL 証明書を VMCA 証明書で置き換える
- ソリューション ユーザーの証明書を VMCA 証明書で置き換える

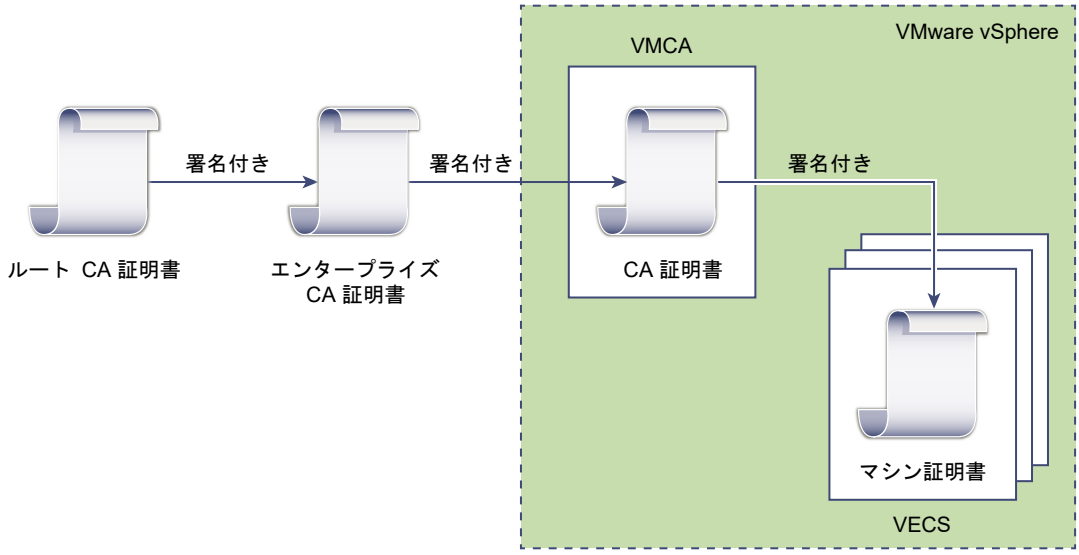
証明書の置き換えの詳細については、「新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え」を参照してください。

VMCA を中間 CA にする

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

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

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



次の vSphere Certificate Manager のオプションを使用できます。

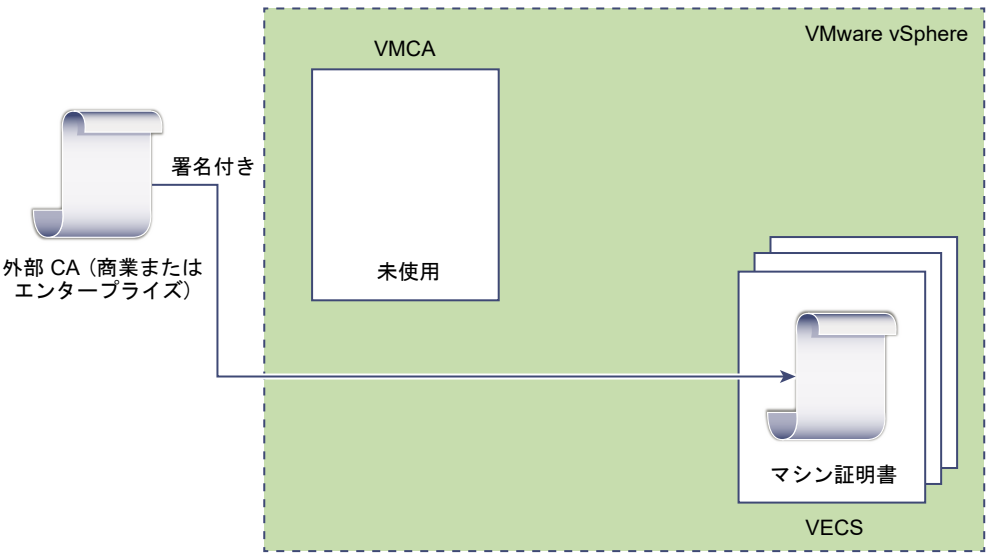
- カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え
- マシンの SSL 証明書を VMCA 証明書で置き換える（複数ノード デプロイ）
- ソリューション ユーザーの証明書を VMCA 証明書で置き換える（複数ノード デプロイ）

証明書の置き換えの詳細については、「中間認証局としての VMCA の使用」を参照してください。

VMCA を使用しない、カスタム証明書によるプロビジョニング

既存の VMCA 署名付き証明書は、カスタム証明書と置き換えることができます。この方法を使用する場合は、証明書のプロビジョニングと監視については、すべて自己責任となります。

図 3-3. 外部証明書を VMware Endpoint Certificate Store (VECS) に直接保存



次の vSphere Certificate Manager のオプションを使用できます。

- カスタム証明書によるマシン SSL 証明書の置き換え
- カスタム証明書によるソリューション ユーザー証明書の置き換え

証明書の置き換えの詳細については、「vSphere でのカスタム証明書の使用」を参照してください。

vSphere Client を使用して、マシン SSL 証明書（カスタム）の CSR を生成し、証明書が CA から返された後で置き換えることもできます。vSphere Client（カスタム証明書）を使用したマシン SSL 証明書の証明書署名リクエストの生成を参照してください。

ハイブリッド デプロイ

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

多くの場合、企業ポリシーでは中間 CA が許可されていません。そのような場合は、ハイブリッド デプロイが適切なソリューションとなります。これにより、置き換える証明書の数は最小限に抑えられ、すべてのトラフィックが保護されます。ハイブリッド デプロイでは、内部のトラフィック、つまりソリューション ユーザーのトラフィックにのみデフォルトの VMCA 署名付き証明書が使用されます。

ESXi 証明書の置き換え

ESXi ホストの場合は、vSphere Client から証明書のプロビジョニング処理を変更することができます。詳細については、『vSphere のセキュリティ』を参照してください。

表 3-4. ESXi 証明書の置き換えのオプション

オプション	説明
VMware 認証局モード（デフォルト）	vSphere Client からの証明書を更新する場合、VMCA はホストの証明書を発行します。VMCA ルート証明書を変更して証明書チェーンを含めるようにする場合、ホストの証明書には完全な証明書チェーンが含められます。
カスタム認証局モード	VMCA による署名がないか、または発行されていない証明書を、手動で更新して証明書を使用することができます。
サムプリント モード	更新中に 5.5 証明書を維持するために使用できます。このモードは、デバッグ状況のときに一時的にのみ使用してください。

vSphere で証明書を使用する場合

vSphere 6.0 以降では、VMware 認証局 (VMCA) が証明書を使用して環境のプロビジョニングを行います。証明書には、安全な接続のための SSL 証明書、vCenter Single Sign-On へのサービスの認証のためのソリューション ユーザー証明書、および ESXi ホスト用の証明書があります。

次の証明書が使用されます。

表 3-5. vSphere 6.0 以降の証明書

証明書	プロビジョニング済み	コメント
ESXi 証明書	VMCA（デフォルト）	ESXi ホスト上にローカルに保存されます
マシン SSL 証明書	VMCA（デフォルト）	VECS に保存
ソリューション ユーザー証明書	VMCA（デフォルト）	VMware Endpoint Certificate Store (VECS) に保存されます
vCenter Single Sign-OnSSL 署名証明書	インストール中にプロビジョニングされます。	この証明書は、vSphere Web Client から管理します。 **注：** 予期しない動作の発生を避けるため、ファイルシステム内でこの証明書を変更しないでください。
VMware Directory Service (VMDIR) SSL 証明書	インストール中にプロビジョニングされます。	vSphere 6.5 以降では、マシン SSL 証明書は vmdir 証明書として使用されます。

ESXi

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

マシン SSL 証明書

各ノードのマシン SSL 証明書は、サーバ側の SSL ソケットの作成に使用されます。SSL クライアントは、この SSL ソケットに接続します。この証明書は、サーバの検証と、HTTPS や LDAPS などのセキュアな通信に使われます。

ノードごとに専用のマシン SSL 証明書があります。ノードには、vCenter Server インスタンス、Platform Services Controller インスタンス、または組み込みのデプロイ インスタンスが含まれています。ノードで実行中のすべてのサービスが、マシン SSL 証明書を使用して SSL エンドポイントを公開します。

マシン SSL 証明書を使用するサービスは次のとおりです。

- 各 Platform Services Controller ノードのリバース プロキシ サービス。個々の vCenter サービスへの SSL 接続では、常にリバース プロキシに接続します。サービス自体にトラフィックが送られることはありません。
- 管理ノードと組み込みノード上の vCenter サービス (vpxd)。
- インフラストラクチャ ノードと組み込みノード上の VMware Directory Service (vmdir)。

VMware 製品では、標準の X.509 バージョン 3 (X.509v3) 証明書を使用して、セッション情報を暗号化します。セッション情報は、SSL を介してコンポーネント間で送信されます。

ソリューション ユーザー証明書

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

ソリューション ユーザーは、最初に認証が必要になった時、再起動の後、およびタイムアウト時間の終了後に、vCenter Single Sign-On に証明書を提供します。タイムアウト（Holder-of-Key (HOK) タイムアウト）は、vSphere Web Client から設定することができ、デフォルト値は 2,592,000 秒（30 日）です。

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

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

- `machine`：License Server およびログ サービスにより使用されます。

  注： マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は、SAML トークン交換に使用されます。マシン SSL 証明書は、マシン向けのセキュア SSL 接続に使用されます。

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

各 Platform Services Controller ノードには `machine` 証明書が含まれます。

内部証明書

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

vCenter Single Sign-On 署名証明書

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

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

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

VMware ディレクトリ サービス SSL 証明書

vSphere 6.5 以降では、マシン SSL 証明書は VMware ディレクトリ証明書として使用されます。以前のバージョンの vSphere の場合は、対応する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の証明書

vSphere 仮想マシンの暗号化ソリューションは、外部のキー管理サーバ (KMS) と接続します。ソリューションに対する KMS の認証方法によっては、証明書が生成されて VMware Endpoint Certificate Store (VECS) に保存される場合があります。『vSphere のセキュリティ』ドキュメントを参照してください。

VMCA および VMware コア ID サービス

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

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

表 3-6. コア ID サービス

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

VMware Endpoint 証明書ストアの概要

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

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

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

VECS には、次のストアが含まれます。

表 3-7. VECS 内のストア

ストア	説明
マシン SSL ストア (MACHINE_SSL_CERT)	■ 各 vSphere ノード上のリバースプロキシ サービスによって使用されます。 ■ 組み込みデプロイおよび各 Platform Services Controller ノード上の VMware Directory Service (vmdir) によって使用されます。 vSphere 6.0 以降のすべてのサービスは、マシン SSL 証明書を使用するリバース プロキシを介して通信されます。下位互換性を保つため、5.x サービスでは特定のポートが引き続き使用されています。その結果、vpxd などの一部のサービスのポートが開かれたままになります。
信頼されたルート ストア (TRUSTED_ROOTS)	すべての信頼済みルート証明書を含みます。
ソリューション ユーザー ストア ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient	VECS には、ソリューション ユーザーごとに 1 つのストアが含まれます。各ソリューション ユーザー証明書の件名は一意でなければなりません。たとえば、マシン証明書には vpxd 証明書と同じ件名を指定できません。 ソリューション ユーザー証明書は、vCenter Single Sign-On での認証に使用されます。vCenter Single Sign-On は、証明書が有効であることを確認しますが、その他の証明書の属性は確認しません。組み込みのデプロイでは、すべてのソリューション ユーザー証明書が同じシステム上に存在します。 次のソリューション ユーザー証明書ストアが、各管理ノードと各組み込みデプロイの VECS に含まれています。 ■ machine：License Server およびログ サービスにより使用されます。 **注：** マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は、SAML トークン交換に使用されます。マシン SSL 証明書は、マシン向けのセキュア SSL 接続に使用されます。 ■ vpxd：管理ノードおよび組み込みデプロイ上の、vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに格納されているソリューション ユーザー証明書を使用して、vCenter Single Sign-On への認証を行います。 ■ vpxd-extension：vCenter Server 拡張機能のストア。Auto Deploy サービス、Inventory Service、およびその他のソリューション ユーザーに含まれないその他のサービス。 ■ vsphere-webclient：vSphere Web Client ストア。パフォーマンス チャート サービスなどの一部の追加サービスも含まれます。 各 Platform Services Controller ノードには machine 証明書が含まれます。

表 3-7. VECS 内のストア （続き）

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

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

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

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

証明書の失効の管理

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

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

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

大規模環境での証明書の置き換え

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

ロード バランサが含まれる高可用性環境での証明書の置き換え

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

複数の管理ノードが含まれる環境でのマシン SSL 証明書の置き換え

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

vSphere Certificate Manager

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

手動での証明書の置き換え

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

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

複数の管理ノードが含まれる環境でのソリューション ユーザー証明書の置き換え

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

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

vSphere Certificate Manager

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

手動での証明書の置き換え

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

- 各管理ノードの、次のソリューション ユーザーそれぞれの証明書。
  - `vpxd solution` ユーザー
  - `vpxd-extension` ソリューション ユーザー
  - `vsphere-webclient` ソリューション ユーザー

2 各ノードの証明書を置き換えます。正確なプロセスは、実行している証明書置き換えのタイプに応じて異なります。vSphere Certificate Manager ユーティリティによる証明書の管理を参照してください。

詳細については、次のトピックを参照してください。

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

外部ソリューションが含まれる環境での証明書の置き換え

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

この問題は、`ls_update_certs` スクリプトを実行して解決できます。詳細については、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2109074) を参照してください。

vSphere Client での証明書の管理

vSphere Client を使用して証明書を管理および表示できます。また、vSphere Certificate Manager ユーティリティを使用することで多数の証明書管理タスクを実行することもできます。

vSphere Client では、次の管理タスクを実行することができます。

- 信頼できるルート証明書および SSL 証明書の表示。
- 既存の証明書の更新または証明書の置き換え。
- マシン SSL 証明書のカスタム証明書署名リクエスト (CSR) を生成し、認証局から返されたら証明書を置き換えます。

証明書の置き換えワークフローの大部分は、vSphere Client で完全にサポートされています。マシン SSL 証明書の CSR を生成する場合は、vSphere Client または Certificate Manager ユーティリティを使用できます。

サポートされているワークフロー

Platform Services Controller のインストール後、このノード上の VMware 認証局は、デフォルトの証明書を使用して環境内の他のすべてのノードをプロビジョニングします。現在の証明書管理の推奨については、3 章 vSphere セキュリティ証明書を参照してください。

次のワークフローのいずれかを使用して、証明書を更新または置き換えることができます。

証明書の更新

使用環境内の SSL 証明書およびソリューション ユーザー証明書を更新するように、vSphere Client から VMCA に指示することができます。

VMCA を中間 CA にする

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

カスタム証明書による証明書の置き換え

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

注： VMCA を中間認証局として使用している場合、またはカスタム証明書を使用している場合は、複雑さが著しく高まり、セキュリティに悪影響が及ぶ可能性が生じて、運用上のリスクが不必要に増大することがあります。vSphere 環境内での証明書管理の詳細については、http://vmware.com/go/hybridvmca で「New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement」というブログ記事を参照してください。

混合モード環境では、CLI コマンドを使用して、他の証明書を置き換えた後に vCenter Single Sign-On 証明書を置き換えることができます。混合モード環境での VMware ディレクトリ サービス証明書の置き換えを参照してください。

vSphere Client からの証明書ストアの検索

VMware Endpoint Certificate Store (VECS) のインスタンスは、各 Platform Services Controller ノードおよび各 vCenter Server ノードに含まれます。vSphere Client から VMware Endpoint Certificate Store 内のさまざまなストアを検索できます。

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

前提条件

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

手順

1. vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。
2. administrator@vsphere.local または vCenter Single Sign-On 管理者グループの別のメンバーのユーザー名とパスワードを指定します。

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

3 [証明書の管理] ユーザー インターフェイスに移動します。

   a [ホーム] メニューから [管理] を選択します。

   b [証明書] で、[証明書の管理] をクリックします。

4 vCenter Server の認証情報を入力します。

5 VMware Endpoint Certificate Store (VECS) 内に格納されている証明書を検索します。

   各ストアの格納している内容については、VMware Endpoint 証明書ストアの概要を参照してください。

6 証明書の詳細を表示するには、証明書を選択し、[詳細表示] アイコンをクリックします。

7 [アクション] メニューから、証明書の更新または置き換えを実行します。

   たとえば、既存の証明書を置き換える場合は、古いルート証明書を後で削除できます。その証明書がすでに使用されていないことが確認できた場合にのみ、証明書を削除してください。

vCenter Server 証明書の有効期限の警告に対するしきい値の設定

vSphere 6.0 以降では、vCenter Server は VMware Endpoint Certificate Store (VECS) にあるすべての証明書を監視し、証明書が有効期限まで 30 日以内になるとアラームを発行します。警告を受けるタイミングは `vpxd.cert.threshold` 詳細オプションを使用して変更できます。

手順

1 vSphere Client にログインします。

2 vCenter Server オブジェクトをクリックして [構成] をクリックします。

3 [[詳細設定]] をクリックします。

4 [設定の編集] をクリックして、**しきい値** をフィルタリングします。

5 `vpxd.cert.threshold` の設定を任意の値に変更し、[保存] をクリックします。

vSphere Client からの新しい VMCA 署名付き証明書への証明書の置き換え

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

前提条件

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

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [証明書の管理] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [証明書] で、[証明書の管理] をクリックします。

4 vCenter Server の認証情報を入力します。

5 ローカル システムのマシン SSL 証明書を更新します。

a [マシン SSL 証明書] を選択します。

b [アクション] - [更新] の順にクリックします。

c [更新] をクリックします。

証明書が更新されるというメッセージが表示されます。

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

a [ソリューション証明書] で、証明書を選択します。

b [アクション] - [更新] の順にクリックし、選択した証明書を個別に更新するか、[すべてを更新] をクリックして、すべてのソリューション ユーザー証明書を更新します。

証明書が更新されるというメッセージが表示されます。

7 環境に外部 Platform Services Controller が含まれている場合は、その後に各 vCenter Server システムの証明書を更新できます。

a [証明書の管理] パネルで [ログアウト] ボタンをクリックします。

b プロンプトが表示されたら、vCenter Server システムの IP アドレスまたは FQDN と、vCenter Single Sign-On に対して認証できる vCenter Server 管理者のユーザー名とパスワードを指定します。

c vCenter Server でマシン SSL 証明書を更新し、オプションで各ソリューション ユーザー証明書を更新します。

d 環境内に複数の vCenter Server システムがある場合は、システムごとにこのプロセスを繰り返します。

次のステップ

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

Windows

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

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

vCenter Server Appliance

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

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

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

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

vSphere Client（カスタム証明書）を使用したマシン SSL 証明書の証明書署名リクエストの生成

マシン SSL 証明書は、各管理ノード、Platform Services Controller、および組み込みデプロイのリバース プロキシ サービスによって使用されます。他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。vSphere Client を使用すると、マシン SSL 証明書の証明書署名リクエスト (CSR) を生成し、準備が整ったら、証明書を置き換えることができます。

前提条件

証明書は次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）
- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります

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

マシン SSL 証明書の CSR の生成は、vCenter Server Appliance でのみサポートされます。Windows にインストールされている vCenter Server ではサポートされません。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [証明書の管理] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [証明書] で、[証明書の管理] をクリックします。

4 vCenter Server の認証情報を入力します。

5 CSR を生成します。

a 置換対象の証明書の [マシン SSL 証明書] で、[アクション] - [証明書署名要求 (CSR) の生成] の順にクリックします。

b 証明書情報を入力し、[次へ] をクリックします。

c CSR をコピーまたはダウンロードします。

d [終了] をクリックします。

e 認証局に CSR を提供します。

次のステップ

認証局から証明書が返されたら、証明書ストアにある既存の証明書を置き換えます。 Platform Services Controller からのカスタム証明書の追加を参照してください。

vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）

vSphere Certificate Manager を使用すると、エンタープライズ CA で使用したり外部認証局に送信したりできる証明書署名要求 (CSR) を生成できます。サポートされているさまざまな証明書置き換えプロセスで、証明書を使用できます。

Certificate Manager ツールは、次に示すようにコマンド ラインから実行できます。

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

- CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者が求められます。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- マシン SSL 証明書の CSR を生成するには、`certool.cfg` ファイルに保存されている証明書プロパティが求められます。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。

手順

1. 環境内の各マシンで、vSphere Certificate Manager を起動してオプション 1 を選択します。
2. パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
3. オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。

   プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。
4. すべてのソリューション ユーザー証明書も置き換える場合は、Certificate Manager を再起動します。
5. オプション 5 を選択します。
6. パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。
7. オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。

   プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。

   Platform Services Controller ノードごとに、Certificate Manager により 1 つの証明書と鍵のペアが生成されます。vCenter Server ノードごとに、Certificate Manager により 4 つの証明書と鍵のペアが生成されます。

次のステップ

証明書の置き換えを実行します。

証明書ストアへの信頼できるルート証明書の追加

環境内でサードパーティ証明書を使用する場合は、信頼できるルート証明書を証明書ストアに追加する必要があります。

前提条件

サードパーティまたは内部の認証局 (CA) からカスタム ルート証明書を取得します。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [証明書の管理] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [証明書] で、[証明書の管理] をクリックします。

4 vCenter Server の認証情報を入力します。

5 [信頼できるルート証明書] で [追加] をクリックします。

6 [参照] をクリックし、証明書チェーンの配置場所を選択します。

CER、PEM、または CRT の各ファイル タイプを使用できます。

7 [追加] をクリックします。

証明書がストアに追加されます。

次のステップ

マシンの SSL 証明書と、必要に応じてソリューション ユーザー証明書を、この認証局の署名付き証明書と置き換えます。

Platform Services Controller からのカスタム証明書の追加

Platform Services Controller から、カスタム マシン SSL 証明書およびカスタム ソリューション ユーザー証明書を証明書ストアに追加できます。

通常は、各コンポーネントのマシン SSL 証明書を置き換えるだけで十分です。ソリューション ユーザー証明書はプロキシに置いたままにします。

前提条件

置き換える各証明書の証明書署名要求 (CSR) を生成します。CSR を生成するには、Certificate Manager ユーティリティを使用します。vSphere Client を使用して、マシン SSL 証明書の CSR を生成することもできます。Platform Services Controller がアクセスできる場所に証明書およびプライベート キーを格納します。

手順

1 vSphere Client を使用して、Platform Services Controller に接続している vCenter Server にログインします。

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

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

3 [証明書の管理] ユーザー インターフェイスに移動します。

a [ホーム] メニューから [管理] を選択します。

b [証明書] で、[証明書の管理] をクリックします。

4 vCenter Server の認証情報を入力します。

5 マシン SSL 証明書を置き換えるには、次の手順を実行します。

a [マシン SSL 証明書] で、置き換える証明書に対して [アクション] - [置き換え] の順にクリックします。

b マシン SSL 証明書（.cer、.pem、または .crt ファイル）とプライベート キー（.key ファイル）を参照します。

c [置き換え] をクリックします。

6 ソリューション ユーザー証明書を置き換えるには、次の手順を実行します。

a [ソリューション証明書]で、コンポーネントの最初の証明書（[マシン] など）で [アクション] - [置き換え] の順にクリックします。

b [参照] をクリックして証明書チェーンを置き換え、[参照] をクリックしてプライベート キーを置き換えます。

c [置き換え] をクリックします。

d 同じコンポーネントの他の証明書に対して、この手順を繰り返します。

結果

証明書の置き換えが完了したことを示すメッセージが表示されます。

次のステップ

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

Windows

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

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

vCenter Server Appliance

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

vSphere Web Client からの証明書の管理

vSphere Web Client から証明書を確認することができます。vSphere Client から、その他のすべてのタスクを実行します。

vSphere Client での証明書の管理を参照してください。

vSphere Web Client での vCenter 証明書の表示

vCenter Certificate Authority (VMCA) に認識されている証明書を表示して、有効な証明書の有効期限が近付いているかどうかを確認したり、期限切れの証明書を参照したり、ルート証明書のステータスを確認したりできます。すべての証明書管理タスクは、証明書管理 CLI を使用して実行します。

組み込みデプロイまたは Platform Services Controller に含まれている VMCA インスタンスに関連付けられた証明書を表示します。証明書の情報は VMware Directory Service (vmdir) のインスタンス全体にレプリケートされます。

vSphere Web Client で証明書を表示しようとすると、ユーザー名とパスワードを求められます。VMware 認証局の権限を持つユーザー、すなわち CAAdmins vCenter Single Sign-On グループのユーザーのユーザー名とパスワードを指定します。

手順

1 vSphere Web Client を使用して、vCenter Server に administrator@vsphere.local または CAAdmins vCenter Single Sign-On グループの他のユーザーとしてログインします。

2 [ホーム] メニューから [管理] を選択します。

3 [デプロイ] - [システム設定] の順にクリックします。

4 [ノード] をクリックし、[ノード] リストでホストを選択します。

5 [管理] タブをクリックし、[認証局] をクリックします。

6 証明書情報を表示する証明書のタイプをクリックします。

オプション	説明
有効な証明書	有効な証明書を、検証情報とともに表示します。緑の [有効期間の終了] アイコンは、証明書の有効期限が近付くと変化します。
失効した証明書	失効した証明書のリストを表示します。今回のリリースではサポートされていません。
期限の切れた証明書	期限の切れた証明書を表示します。
ルート証明書	vCenter Certificate Authority の、このインスタンスで使用可能なルート証明書を表示します。

7 証明書を選択して [証明書の詳細の表示] ボタンをクリックして証明書の詳細を表示します。

詳細には Subject Name、Issuer、Validity および Algorithm が含まれています。

vSphere Certificate Manager ユーティリティによる証明書の管理

vSphere Certificate Manager ユーティリティを使用すると、ほとんどの証明書管理タスクをコマンド ラインから対話形式で実行することができます。vSphere Certificate Manager では、実行するタスクや証明書の場所などの情報を入力する画面が必要に応じて表示され、その後サービスがいったん停止されてから起動され、証明書が置き換えられます。

vSphere Certificate Manager を使用する場合、ユーザーが VECS（VMware Endpoint 証明書ストア）に証明書を配置したり、サービスの起動と停止を行う必要はありません。

vSphere Certificate Manager を実行する前に、必ず置き換えプロセスについて理解すると共に、使用する証明書を入手してください。

注意： vSphere Certificate Manager では、1 レベルの取り消しがサポートされます。vSphere Certificate Manager を 2 回実行し、誤って環境を壊したことに気付いた場合、2 回の実行のうちの最初の実行は取り消すことができません。

Certificate Manager ユーティリティの場所

このツールは、次に示すようにコマンド ラインで実行できます。

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

手順

1 このドキュメントに含まれる Certificate Manager オプションおよびワークフロー

Certificate Manager オプションを順に実行することで、1 つのワークフローが完成します。たとえば、証明書署名要求 (CSR) を生成する一部のオプションは、さまざまなワークフローで使用されます。

2 新しい VMCA ルート証明書の再生成およびすべての証明書の置き換え

VMCA ルート証明書を再生成し、ローカル マシンの SSL 証明書およびローカル ソリューションのユーザー証明書を VMCA 署名付き証明書に置き換えることができます。マルチノード環境では、このオプションで vSphere Certificate Manager を Platform Services Controller 上で実行してから、再度このユーティリティを他のすべてのノード上で実行し、
[`Replace Machine SSL certificate with VMCA Certificate`] および
[`Replace Solution user certificates with VMCA certificates`] を選択します。

3 VMCA を中間認証局にする (Certificate Manager)

Certificate Manager ユーティリティからプロンプトに従って、VMCA を中間 CA にすることができます。プロセスの完了後、VMCA はすべての新規証明書に完全なチェーンで署名します。必要な場合は、Certificate Manager を使用して、既存のすべての証明書を VMCA 署名付き証明書に置き換えることができます。

4 カスタム証明書によるすべての証明書の置き換え (Certificate Manager)

vSphere Certificate Manager ユーティリティを使用して、すべての証明書をカスタム証明書に置き換えることができます。プロセスを始める前に、CA に CSR を送信する必要があります。Certificate Manager を使用して CSR を生成できます。

5 古い証明書の再発行による、最後に実行された操作の取り消し

vSphere Certificate Manager を使用して証明書の管理操作を実行する際に、証明書が置き換えられる前に、現在の証明書の状態が BACKUP_STORE ストアに格納されます。最後に実行した処理を取り消して、以前の状態に戻すことができます。

6 すべての証明書のリセット

既存の vCenter 証明書すべてを VMCA によって署名された証明書に置き換えるには、すべての証明書をリセット オプションを使用します。

このドキュメントに含まれる Certificate Manager オプションおよびワークフロー

Certificate Manager オプションを順に実行することで、1 つのワークフローが完成します。たとえば、証明書署名要求 (CSR) を生成する一部のオプションは、さまざまなワークフローで使用されます。

カスタム署名証明書による VMware 認証局 (VMCA) のルート証明書の置き換えと、すべての証明書の置き換え

これは単一オプションのワークフロー（オプション 2）であり、単体で使用することも、中間証明書ワークフローで使用することもできます。新しい VMCA ルート証明書の再生成およびすべての証明書の置き換えを参照してください。

VMware 認証局 (VMCA) を中間認証局にする

VMware 認証局 (VMCA) を中間認証局にするには、Certificate Manager を複数回実行する必要があります。ワークフローは、マシン SSL 証明書とソリューション ユーザー証明書を両方とも置き換えるために必要な一連の手順を提供します。これには、組み込みの Platform Services Controller または外部の Platform Services Controller を使用した環境で必要な作業が含まれます。

1 CSR を生成するには、オプション 2 の [カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え] を選択します。証明書についての情報が必要になる場合があります。もう 1 度オプションを入力するよう求められたら、オプション 1 を選択します。

CSR を外部またはエンタープライズ認証局 (CA) に送信します。署名付き証明書とルート証明書を認証局 (CA) から受信します。

2 VMware 認証局 (VMCA) のルート証明書と認証局 (CA) のルート証明書を結合してファイルを保存します。

3 オプション 2 の [カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え] を選択します。このプロセスにより、ローカル マシン上のすべての証明書が置き換えられます。

4 マルチノード環境では、各ノードで証明書を置き換える必要があります。

a まず、マシン SSL 証明書を（新しい）VMCA 証明書に置き換えます（オプション 3）。

b 次に、ソリューション ユーザー証明書を（新しい）VMCA 証明書に置き換えます（オプション 6）。

「VMCA を中間認証局にする (Certificate Manager)」を参照してください。

カスタム証明書によるすべての証明書の置き換え

すべての証明書をカスタム証明書に置き換えるには、Certificate Manager を複数回実行する必要があります。ワークフローは、マシン SSL 証明書とソリューション ユーザー証明書を両方とも置き換えるために必要な一連の手順を提供します。これには、組み込みの Platform Services Controller または外部の Platform Services Controller を使用した環境で必要な作業が含まれます。

1 マシン SSL 証明書とソリューション ユーザー証明書の証明書署名要求を、各マシンで個別に生成します。

   a マシン SSL 証明書の CSR を生成するには、オプション 1 を選択します。

   b 企業のポリシーで、すべての証明書を置き換える必要がある場合は、オプション 5 も選択します。

2 認証局 (CA) から署名付き証明書とルート証明書を受信したら、オプション 1 を使用して、各マシンのマシン SSL 証明書を置き換えます。

3 ソリューション ユーザー証明書も置き換える場合は、オプション 5 を選択します。

4 マルチノード環境では、このプロセスを各ノードで繰り返す必要があります。

カスタム証明書によるすべての証明書の置き換え (Certificate Manager)を参照してください。

注： vSphere 6.5 以降では、Certificate Manager ユーティリティの実行時に次のプロンプトが表示されます。

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

プロンプトの指示に従って、証明書構成を実行しているマシンの完全修飾ドメイン名を入力します。

新しい VMCA ルート証明書の再生成およびすべての証明書の置き換え

VMCA ルート証明書を再生成し、ローカル マシンの SSL 証明書およびローカル ソリューションのユーザー証明書を VMCA 署名付き証明書に置き換えることができます。マルチノード環境では、このオプションで vSphere Certificate Manager を Platform Services Controller 上で実行してから、再度このユーティリティを他のすべてのノード上で実行し、[`Replace Machine SSL certificate with VMCA Certificate`] および [`Replace Solution user certificates with VMCA certificates`] を選択します。

既存のマシン SSL 証明書を新しい VMCA 署名付きの証明書に置き換えると、vSphere Certificate Manager により次の情報が求められ、Platform Services Controller のパスワードと IP アドレスを除くすべての値が `certool.cfg` ファイルに入力されます。

- administrator@vsphere.local のパスワード。
- 2 文字の国名コード
- 会社名
- 組織名
- 部門名
- 都道府県
- 市区町村

- IP アドレス（オプション）
- E メール
- ホスト名、すなわち証明書を置き換えるマシンの完全修飾ドメイン名 (FQDN)「ホスト名が FQDN と一致しない場合、証明書の置き換えは正しく完了せず、環境が不安定な状態になる可能性があります。
- Platform Services Controller の IP アドレス（管理ノード上でコマンドを実行している場合）。
- VMCA 名、すなわち証明書の設定を実行しているマシンの完全修飾ドメイン名。

前提条件

このオプションを指定して vSphere Certificate Manager を実行する場合は、次の情報を把握している必要があります。

- administrator@vsphere.local のパスワード。
- 新しい VMCA 署名付き証明書を生成するマシンの FQDN。他のすべてのプロパティは事前定義された値にデフォルト設定されますが、変更が可能です。

手順

1 組み込みデプロイまたは Platform Services Controller の vCenter Server にログインし、vSphere Certificate Manager を開始します。

OS	コマンド
Linux	`/usr/lib/vmware-vmca/bin/certificate-manager`
Windows	`C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat`

2 オプション 4 の `Regenerate a new VMCA Root Certificate and replace all certificates` を選択します。

3 プロンプトに応答します。

入力した情報に基づいて、Certificate Manager によって新しい VMCA ルート証明書が生成され、Certificate Manager が実行されているシステム上のすべての証明書が置き換えられます。組み込みの導入環境の場合は、Certificate Manager がサービスを再起動した後で置き換えプロセスが実行されます。

4 環境に外部 Platform Services Controller が含まれている場合は、各 vCenter Server システムで証明書を置き換える必要があります。

a vCenter Server システムにログインします。

b すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

Windows

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

vCenter Server Appliance

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

c すべてのサービスを再開します。

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

d マシン SSL 証明書を置き換えるには、オプション 3 の [`Replace Machine SSL certificate with VMCA Certificate`] を使用して vSphere Certificate Manager を実行します。

e ソリューション ユーザー証明書を置き換えるには、オプション 6 の [` Replace Solution user certificates with VMCA certificates`] を使用して Certificate Manager を実行します。

VMCA を中間認証局にする (Certificate Manager)

Certificate Manager ユーティリティからプロンプトに従って、VMCA を中間 CA にすることができます。プロセスの完了後、VMCA はすべての新規証明書に完全なチェーンで署名します。必要な場合は、Certificate Manager を使用して、既存のすべての証明書を VMCA 署名付き証明書に置き換えることができます。

VMware 認証局 (VMCA) を中間認証局にするには、Certificate Manager を複数回実行する必要があります。ワークフローでは、マシン SSL 証明書とソリューション ユーザー証明書を両方とも置き換えるために必要な一連の手順が提供されます。組み込みの Platform Services Controller または外部の Platform Services Controller を使用した環境で何を実行すべきかが説明されています。

1 CSR を生成するには、オプション 1 の [カスタム証明書によるマシン SSL 証明書の置き換え] を選択した後、オプション 1 を選択します。

署名付き証明書とルート証明書を認証局 (CA) から受信します。

2 VMware 認証局 (VMCA) のルート証明書と認証局 (CA) のルート証明書を結合してファイルを保存します。

3 オプション 2 の [カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え] を選択します。このプロセスにより、ローカル マシン上のすべての証明書が置き換えられます。

4 マルチノード デプロイでは、各ノードで証明書を置き換える必要があります。

   a まず、マシン SSL 証明書を（新しい）VMCA 証明書に置き換えます（オプション 3）。

   b 次に、ソリューション ユーザー証明書を（新しい）VMCA 証明書に置き換えます（オプション 6）。

手順

1 vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する

   vSphere Certificate Manager を使用して証明書署名要求 (CSR) を生成できます。この CSR をエンタープライズまたは外部の認証局 (CA) に送信して署名を要求します。署名付きの証明書は、サポートされているさまざまな証明書置き換えプロセスで使用できます。

2 カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え

   vSphere Certificate Manager を使用すると、CSR を生成して、署名のためにエンタープライズまたはサードパーティの CA に CSR を送信できます。続いて、VMware 認証局 (VMCA) ルート証明書をカスタム署名証明書に置換し、既存のすべての証明書を、カスタム CA が署名した証明書に置き換えます。

3 VMCA 証明書によるマシンの SSL 証明書の置き換え（中間 CA）

   VMCA を中間 CA として使用するマルチノード環境では、マシン SSL 証明書を明示的に置き換える必要があります。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったマシンの SSL 証明書を置き換える際も使用できます。

4 VMCA 証明書によるソリューション ユーザー証明書の置き換え（中間 CA）

   VMCA を中間 CA として使用するマルチノード環境では、ソリューション ユーザー証明書を明示的に置き換えることができます。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったソリューション ユーザー証明書を置き換えるためにも使用できます。

vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意する

vSphere Certificate Manager を使用して証明書署名要求 (CSR) を生成できます。この CSR をエンタープライズまたは外部の認証局 (CA) に送信して署名を要求します。署名付きの証明書は、サポートされているさまざまな証明書置き換えプロセスで使用できます。

- CSR は vSphere Certificate Manager を使用して作成できます。
- CSR を手動で作成する場合、署名のために送付する証明書は以下の要件を満たしている必要があります。
  - キー サイズ： 2,048 ビット以上
  - PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
  - x509 バージョン 3

- カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。
- CRL の署名は有効にしてください。
- [拡張キー使用] は、空にするか、[サーバ認証] を指定します。
- 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。
- ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。
- VMCA の従属認証局は作成できません。

  Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (2112009)」(http://kb.vmware.com/kb/2112009) を参照してください。

前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者のパスワードが求められます。

手順

1 vSphere Certificate Manager を実行します。

OS	コマンド
Windows	`cd "C:\Program Files\VMware\vCenter Server\vmcad"` `certificate-manager`
Linux	`/usr/lib/vmware-vmca/bin/certificate-manager`

2 オプション 2 を選択します。

最初はこのオプションを使用して証明書の置き換えではなく CSR の生成を行います。

3 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。

4 オプション 1 を選択して CSR を生成し、プロンプトに応答します。

プロセスの一部として、ディレクトリを指定する必要があります。署名対象の証明書（`*.csr` ファイル）と対応するキー ファイル（`*.key` ファイル）は、Certificate Manager によってディレクトリ内に配置されます。

5 証明書署名リクエスト (CSR) の名前を `root_signing_cert.csr` とします。

6 署名のために CSR を組織または外部の認証局 (CA) に送信し、署名された証明書の名前を `root_signing_cert.cer` とします。

7 テキスト エディタで次のように証明書を結合します。

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 ファイルを `root_signing_chain.cer` という名前で保存します。

次のステップ

既存のルート証明書をチェーン ルート証明書に置き換えます。カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換えを参照してください。

カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え

vSphere Certificate Manager を使用すると、CSR を生成して、署名のためにエンタープライズまたはサードパーティの CA に CSR を送信できます。続いて、VMware 認証局 (VMCA) ルート証明書をカスタム署名証明書に置換し、既存のすべての証明書を、カスタム CA が署名した証明書に置き換えます。

組み込みインストールや外部 Platform Services Controller で vSphere Certificate Manager を実行して、VMCA ルート証明書をカスタム署名証明書に置き換えます。

前提条件

- 証明書チェーンを生成します。
  - vSphere Certificate Manager を使用して CSR を作成するか、手動で CSR を作成することができます。
  - 署名証明書をサードパーティ CA またはエンタープライズ CA から受信した後、その証明書を最初の VMCA ルート証明書と組み合わせて完全なチェーンを作成します。

    証明書の要件と証明書を組み合わせる処理については、vSphere Certificate Manager で CSR を生成し、ルート証明書（中間認証局）を用意するを参照してください。
- 必要な情報を収集します。
  - administrator@vsphere.local のパスワード。
  - ルートの有効なカスタム証明書（`.crt` ファイル）。
  - ルートの有効なカスタム キー（`.key` ファイル）。

手順

1 Platform Services Controller の組み込みインストールまたは外部 Platform Services Controller 上で vSphere Certificate Manager を起動し、オプション 2 を選択します。

2 もう一度、オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。

   a 指示に従い、ルート証明書のフルパスを指定します。

   b 証明書を初めて置き換えるときには、マシン SSL 証明書に使用される情報の入力を求められます。

   この情報は、マシンの必須 FQDN を含み、`certool.cfg` ファイルに保存されます。

3 マルチノード デプロイで、Platform Services Controller のルート証明書を置き換える場合は、各 vCenter Server ノードに対して次の手順を行います。

   a vCenter Server ノードのサービスを再起動します。

   b 3 (`Replace Machine SSL certificate with VMCA Certificate`) および 6 (`Replace Solution user certificates with VMCA certificates`) オプションを使用して、vCenter Server インスタンス上ですべての証明書を再生成します。

   証明書を置き換えると、VMCA が完全なチェーンで署名します。

次のステップ

vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。混合モード環境での VMware ディレクトリ サービス証明書の置き換えを参照してください。

VMCA 証明書によるマシンの SSL 証明書の置き換え（中間 CA）

VMCA を中間 CA として使用するマルチノード環境では、マシン SSL 証明書を明示的に置き換える必要があります。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったマシンの SSL 証明書を置き換える際も使用できます。

既存のマシン SSL 証明書を新しい VMCA 署名付きの証明書に置き換えると、vSphere Certificate Manager により次の情報が求められ、Platform Services Controller のパスワードと IP アドレスを除くすべての値が `certool.cfg` ファイルに入力されます。

- administrator@vsphere.local のパスワード。
- 2 文字の国名コード
- 会社名
- 組織名
- 部門名
- 都道府県
- 市区町村
- IP アドレス（オプション）
- E メール
- ホスト名、すなわち証明書を置き換えるマシンの完全修飾ドメイン名 (FQDN)「ホスト名が FQDN と一致しない場合、証明書の置き換えは正しく完了せず、環境が不安定な状態になる可能性があります。
- Platform Services Controller の IP アドレス（管理ノード上でコマンドを実行している場合）。

- VMCA 名、すなわち証明書の設定を実行しているマシンの完全修飾ドメイン名。

前提条件

- マルチノード環境で VMCA ルート証明書を置き換えた場合は、すべての vCenter Server ノードを明示的に再起動します。
- このオプションを指定して Certificate Manager を実行する場合は、次の情報を把握している必要があります。
  - administrator@vsphere.local のパスワード。
  - 新しい VMCA 署名付き証明書を生成するマシンの FQDN。他のすべてのプロパティは事前定義された値にデフォルト設定されますが、変更が可能です。
  - 外部 Platform Services Controller を使用した vCenter Server システムで実行する場合は、Platform Services Controller のホスト名または IP アドレス。

手順

1 vSphere Certificate Manager を起動して、オプション 3 を選択します。

2 プロンプトに応答します。

情報は `certool.cfg` ファイルに保存されます。

結果

vSphere Certificate Manager はマシン SSL 証明書を置き換えます。

VMCA 証明書によるソリューション ユーザー証明書の置き換え（中間 CA）

VMCA を中間 CA として使用するマルチノード環境では、ソリューション ユーザー証明書を明示的に置き換えることができます。最初に、Platform Services Controller ノードの VMCA ルート証明書を置き換えます。次に、vCenter Server ノード上の証明書を置き換えて、完全なチェーンで署名された証明書にすることができます。このオプションは、破損したり、期限切れ間近となったソリューション ユーザー証明書を置き換えるためにも使用できます。

前提条件

- マルチノード環境で VMCA ルート証明書を置き換えた場合は、すべての vCenter Server ノードを明示的に再起動します。
- このオプションを指定して Certificate Manager を実行する場合は、次の情報を把握している必要があります。
  - administrator@vsphere.local のパスワード。
  - 外部 Platform Services Controller を使用した vCenter Server システムで実行する場合は、Platform Services Controller のホスト名または IP アドレス。

手順

1 vSphere Certificate Manager を起動して、オプション 6 を選択します。

2 プロンプトに応答します。

詳細については、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2112281) を参照してください。

結果

vSphere Certificate Manager によって、すべてのソリューション ユーザー証明書が置き換えられます。

カスタム証明書によるすべての証明書の置き換え (Certificate Manager)

vSphere Certificate Manager ユーティリティを使用して、すべての証明書をカスタム証明書に置き換えることができます。プロセスを始める前に、CA に CSR を送信する必要があります。Certificate Manager を使用して CSR を生成できます。

マシン SSL 証明書のみを置き換えて、VMCA によってプロビジョニングされたソリューション ユーザー証明書を使用することもできます。ソリューション ユーザー証明書は、vSphere コンポーネント間の通信にのみ使用されます。

カスタム証明書を使用する場合は、VMCA によって署名された証明書をカスタム証明書に置き換えます。vSphere Client、vSphere Certificate Manager ユーティリティ、または CLI を使用して手動で証明書を置き換えることができます。証明書は VECS に保存されます。

すべての証明書をカスタム証明書に置き換えるには、Certificate Manager を複数回実行する必要があります。ワークフローでは、マシン SSL 証明書とソリューション ユーザー証明書を両方とも置き換えるために必要な一連の手順が提供されます。組み込みの Platform Services Controller または外部の Platform Services Controller を使用した環境で何を実行すべきかが説明されています。

1 マシン SSL 証明書とソリューション ユーザー証明書の証明書署名要求を、各マシンで個別に生成します。

   a マシン SSL 証明書の CSR を生成するには、オプション 1 を選択します。

   b 会社のポリシーでハイブリッド デプロイが許可されていない場合は、オプション 5 を選択します。

2 認証局 (CA) から署名付き証明書とルート証明書を受信したら、オプション 1 を使用して、各マシンのマシン SSL 証明書を置き換えます。

3 ソリューション ユーザー証明書も置き換える場合は、オプション 5 を選択します。

4 最後に、マルチノード デプロイでは、このプロセスを各ノードで繰り返す必要があります。

手順

1 vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）

   vSphere Certificate Manager を使用すると、エンタープライズ CA で使用したり外部認証局に送信したりできる証明書署名要求 (CSR) を生成できます。サポートされているさまざまな証明書置き換えプロセスで、証明書を使用できます。

2 カスタム証明書によるマシン SSL 証明書の置き換え

   マシン SSL 証明書は、各管理ノード、Platform Services Controller、および組み込みデプロイのリバース プロキシ サービスによって使用されます。他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。各ノードの証明書をカスタム証明書に置き換えることができます。

3 カスタム証明書によるソリューション ユーザー証明書の置き換え

多くの企業では、置き換えが必要となるのは外部からアクセス可能なサービスの証明書のみです。ただし、Certificate Manager では、ソリューション ユーザー証明書の置き換えもサポートしています。ソリューション ユーザーはサービスのコレクションです。たとえば、vSphere Client に関連付けられたすべてのサービスもソリューション ユーザーになります。複数ノードを展開している場合は、Platform Services Controller 上のマシン ソリューション ユーザー証明書および各管理ノード上のすべてのソリューション ユーザーを置き換えます。

vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）

vSphere Certificate Manager を使用すると、エンタープライズ CA で使用したり外部認証局に送信したりできる証明書署名要求 (CSR) を生成できます。サポートされているさまざまな証明書置き換えプロセスで、証明書を使用できます。

Certificate Manager ツールは、次に示すようにコマンド ラインから実行できます。

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

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

前提条件

情報を指定するよう求めるプロンプトが vSphere Certificate Manager から表示されます。表示されるプロンプトは、使用環境と、置き換える証明書のタイプによって異なります。

- CSR の生成全般では、administrator@vsphere.local ユーザーのパスワード、または接続先の vCenter Single Sign-On ドメインの管理者が求められます。
- 外部 Platform Services Controller が存在する環境で CSR を生成している場合、その Platform Services Controller のホスト名または IP アドレスを求められます。
- マシン SSL 証明書の CSR を生成するには、`certool.cfg` ファイルに保存されている証明書プロパティが求められます。ほとんどのフィールドで、デフォルト値を受け入れたり、サイト固有の値を指定したりできます。マシンの FQDN が必要です。

手順

1 環境内の各マシンで、vSphere Certificate Manager を起動してオプション 1 を選択します。

2 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。

3 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。

プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。

4 すべてのソリューション ユーザー証明書も置き換える場合は、Certificate Manager を再起動します。

5 オプション 5 を選択します。

6 パスワードを指定します。また、要求された場合は、Platform Services Controller の IP アドレスまたはホスト名を指定します。

7 オプション 1 を選択して CSR を生成し、プロンプトに応答して Certificate Manager を終了します。

プロセスの一部として、ディレクトリを指定する必要があります。Certificate Manager は、このディレクトリに証明書とキー ファイルを配置します。

Platform Services Controller ノードごとに、Certificate Manager により 1 つの証明書と鍵のペアが生成されます。vCenter Server ノードごとに、Certificate Manager により 4 つの証明書と鍵のペアが生成されます。

次のステップ

証明書の置き換えを実行します。

カスタム証明書によるマシン SSL 証明書の置き換え

マシン SSL 証明書は、各管理ノード、Platform Services Controller、および組み込みデプロイのリバース プロキシ サービスによって使用されます。他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。各ノードの証明書をカスタム証明書に置き換えることができます。

前提条件

開始する前に、環境内のマシンごとに CSR が存在している必要があります。CSR は、vSphere Certificate Manager を使用して生成することも、明示的に生成することもできます。

1 vSphere Certificate Manager を使用して CSR を生成するには、vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）を参照してください。

2 CSR を明示的に生成するには、サードパーティまたはエンタープライズ CA に各マシンの証明書を要求します。証明書は次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）
- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります

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

VMware のナレッジベースの記事「Obtaining vSphere certificates from a Microsoft Certificate Authority」(http://kb.vmware.com/kb/2112014) も参照してください。

手順

1 vSphere Certificate Manager を起動して、オプション 1 を選択します。

2 オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。

vSphere Certificate Manager により、次の情報を指定するように求められます。

- administrator@vsphere.local のパスワード。
- 有効なマシン SSL カスタム証明書（.crt ファイル）。
- 有効なマシン SSL カスタム キー（.key ファイル）。
- カスタム マシン SSL 証明書の有効な署名証明書（.crt ファイル）。
- マルチノード デプロイの管理ノードでコマンドを実行している場合は、Platform Services Controller の IP アドレス。

次のステップ

vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。混合モード環境での VMware ディレクトリ サービス証明書の置き換えを参照してください。

カスタム証明書によるソリューション ユーザー証明書の置き換え

多くの企業では、置き換えが必要となるのは外部からアクセス可能なサービスの証明書のみです。ただし、Certificate Manager では、ソリューション ユーザー証明書の置き換えもサポートしています。ソリューション ユーザーはサービスのコレクションです。たとえば、vSphere Client に関連付けられたすべてのサービスもソリューション ユーザーになります。複数ノードを展開している場合は、Platform Services Controller 上のマシン ソリューション ユーザー証明書および各管理ノード上のすべてのソリューション ユーザーを置き換えます。

ソリューション ユーザー証明書を求められたら、サードパーティ CA の完全な署名証明書チェーンを提供します。

次のような形式になります。

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

前提条件

開始する前に、環境内のマシンごとに CSR が存在している必要があります。CSR は、vSphere Certificate Manager を使用して生成することも、明示的に生成することもできます。

1 vSphere Certificate Manager を使用して CSR を生成するには、vSphere Certificate Manager による証明書署名要求の生成（カスタム証明書）を参照してください。

2 各ノードのソリューション ユーザーごとに、サードパーティ CA またはエンタープライズ CA の証明書を要求します。CSR は、vSphere Certificate Manager を使用して生成することも、管理者自身が準備することもできます。CSR は次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）

- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- 各ソリューション ユーザー証明書には異なる `Subject` が指定されている必要があります。たとえば、ソリューション ユーザー名（例： vpxd）などの一意の識別子を含めることができます。
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります

VMware のナレッジベースの記事「Obtaining vSphere certificates from a Microsoft Certificate Authority」(http://kb.vmware.com/kb/2112014) も参照してください。

手順

1 vSphere Certificate Manager を起動して、オプション 5 を選択します。

2 オプション 2 を選択して証明書の置き換えを開始し、プロンプトに応答します。

vSphere Certificate Manager により、次の情報を指定するように求められます。

- administrator@vsphere.local のパスワード。
- マシン ソリューション ユーザーの証明書およびキー。
- vSphere Certificate Manager を Platform Services Controller ノード上で実行している場合は、マシン ソリューション ユーザーの証明書とキー（`vpxd.crt` および `vpxd.key`）を求めるメッセージが表示されます。
- vSphere Certificate Manager を管理ノードまたは組み込みデプロイで実行している場合は、すべてのソリューション ユーザーの証明書およびキー（`vpxd.crt` および `vpxd.key`）のフル セットを求めるメッセージが表示されます。

次のステップ

vSphere 5.x 環境からアップグレードする場合は、必要に応じて vmdir 内の vCenter Single Sign-On 証明書を置き換えます。混合モード環境での VMware ディレクトリ サービス証明書の置き換えを参照してください。

古い証明書の再発行による、最後に実行された操作の取り消し

vSphere Certificate Manager を使用して証明書の管理操作を実行する際に、証明書が置き換えられる前に、現在の証明書の状態が BACKUP_STORE ストアに格納されます。最後に実行した処理を取り消して、以前の状態に戻すことができます。

注： 取り消し操作により、現在 BACKUP_STORE 内にあるものがリストアされます。2 つの異なるオプションを使用して vSphere Certificate Manager を実行していて、取り消しを行う場合は、最後の操作のみが取り消されます。

すべての証明書のリセット

既存の vCenter 証明書すべてを VMCA によって署名された証明書に置き換えるには、**すべての証明書をリセット** オプションを使用します。

このオプションを使用すると、現在 VECS にあるカスタム証明書がすべて上書きされます。

- Platform Services Controller ノードでは、vSphere Certificate Manager を使用して、ルート証明書の再生成と、マシン SSL 証明書およびマシン ソリューション ユーザー証明書の置き換えを行えます。
- 管理ノードでは、vSphere Certificate Manager を使用して、マシン SSL 証明書とすべてのソリューション ユーザー証明書を置き換えることができます。
- 組み込みデプロイでは、vSphere Certificate Manager を使用してすべての証明書を置き換えることができます。

どの証明書が置き換えられるかは、選択するオプションによって異なります。

証明書の手動での置き換え

一部の特殊な場合、たとえば、1 種類のソリューション ユーザー証明書のみを置き換える場合などでは、vSphere Certificate Manager ユーティリティは使用できません。この場合、証明書の置き換えのインストールに含まれた CLI を使用できます。

サービスの停止と開始について

手動による証明書置き換え手順の一部では、すべてのサービスを停止してから、証明書インフラストラクチャを管理するサービスのみを開始する必要があります。必要なときにだけサービスを停止すると、ダウンタイムを最小化できます。

証明書の置き換えプロセスの一部として、サービスを停止し、開始する必要があります。`service-control` コマンドを使用して、サービスを開始および停止できます。すべてのサービスまたは個々のサービスを開始および停止できます。詳細については、コマンドラインのヘルプを参照してください。

- 組み込みの Platform Services Controller を使用している環境では、本書で説明するとおり、すべてのサービスを停止して開始する必要があります。
- 外部の Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) の停止および開始を行う必要はありません。これらのサービスは、Platform Services Controller 上で実行されます。

次のガイドラインに従ってください。

- パブリック キーとプライベート キーのペアや証明書を新しく生成するためにサービスを停止することはしません。
- 管理者が 1 人しかいない場合、新しいルート証明書を追加するときにサービスを停止する必要はありません。古いルート証明書は使用可能なままで、その証明書を使用して引き続きすべてのサービスを認証できます。ホストとの間で問題が発生することを回避するため、ルート証明書を追加し終えたらすべてのサービスを停止し、すぐに再開します。
- 環境内に複数の管理者がいる場合は、新しいルート証明書を追加する前にサービスを停止し、追加が終わったらサービスを再開します。
- 次のタスクを実行する直前にサービスを停止します。
  - VECS でマシン SSL 証明書または任意のソリューション ユーザー証明書を削除します。

- vmdir（VMware ディレクトリ サービス）でソリューション ユーザー証明書を置き換えます。

新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え

VMCA ルート証明書の有効期限が近付いているか、またはその他の理由で証明書を置き換える場合には、新しいルート証明書を生成し、VMware ディレクトリ サービスに追加できます。新しいルート証明書を使用すれば、新しいマシン SSL 証明書およびソリューション ユーザー証明書を生成することもできます。

多くの場合、vSphere Certificate Manager ユーティリティを使用して証明書を置き換えます。

詳細な制御が必要な場合には、このシナリオを参照すると、CLI コマンドを使用して証明書のセットをすべて置き換える具体的な手順が詳細に分かります。あるいは、該当するタスクの手順を使用して、個別の証明書のみを置き換えることもできます。

前提条件

administrator@vsphere.local または CAAdmins グループ内の他のユーザーのみが証明書管理タスクを実行できます。 vCenter Single Sign-On グループへのメンバーの追加 を参照してください。

手順

1 新規の VMCA 署名付きルート証明書の生成

   `certool` CLI または vSphere Certificate Manager ユーティリティを使用して新しい VMware 認証局 (VMCA) 署名証明書を生成し、証明書を vmdir に公開します。

2 VMCA 署名付き証明書によるマシン SSL 証明書の置き換え

   VMCA 署名付きルート証明書を新しく生成したら、環境内のすべてのマシン SSL 証明書を置き換えることができます。

3 新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え

   マシン SSL 証明書を置き換えたら、すべてのソリューション ユーザー証明書を置き換えることができます。ソリューション ユーザー証明書は有効である必要があります。ここでの「有効」とは、有効期限が切れておらず、証明書に含まれるその他の情報が証明書インフラストラクチャで使用されていないことを意味します。

4 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

   アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

新規の VMCA 署名付きルート証明書の生成

`certool` CLI または vSphere Certificate Manager ユーティリティを使用して新しい VMware 認証局 (VMCA) 署名証明書を生成し、証明書を vmdir に公開します。

マルチノード デプロイでは、Platform Services Controller でルート証明書の生成コマンドを実行します。

手順

1 新しい自己署名証明書およびプライベート キーを生成します。

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 既存のルート証明書を新しい証明書に置き換えます。

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

このコマンドは、証明書を生成し、その証明書を vmdir に追加して、VECS に追加します。

3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

4 （オプション） 新しいルート証明書を vmdir に発行します。

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

コマンドは、vmdir のインスタンスを即座に更新します。コマンドを実行しない場合、すべてのノードへ新しい証明書を伝達するのに時間がかかる場合があります。

5 すべてのサービスを再開します。

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

例： 新規の VMCA 署名付きルート証明書の生成

次の例は、現在のルート CA 情報を確認し、ルート証明書を再生成するための手順を示します。

1 （オプション）VMCA ルート証明書を一覧表示し、証明書ストア内に含まれていることを確認します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- 管理ノードで、次のように実行します（外部インストール）。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
```

出力は次のようになります。

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 （オプション）VECS TRUSTED_ROOTS ストアの内容を一覧表示し、そこに表示される証明書のシリアル番号と、手順 1 の出力を比較します。

VECS が vmdir をポーリングするため、このコマンドは Platform Services Controller ノードと管理ノードの両方で機能します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS --text
```

ルート証明書が 1 つだけの単純なケースでは、出力は次のようになります。

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 新しい VMCA ルート証明書を生成します。コマンドは、証明書を VECS と vmdir （VMware Directory Service) の TRUSTED_ROOTS ストアに追加します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg"
```

Windows では、コマンドがデフォルトの `certool.cfg` ファイルを使用するため、`--config` はオプションです。

VMCA 署名付き証明書によるマシン SSL 証明書の置き換え

VMCA 署名付きルート証明書を新しく生成したら、環境内のすべてのマシン SSL 証明書を置き換えることができます。

他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

前提条件

すべてのサービスを停止し、証明書の伝達およびストレージを処理するサービスを開始する準備ができている。

手順

1 新しい証明書を必要とするマシンごとに、`certool.cfg` のコピーを 1 つ作成します。

`certool.cfg` は次の場所で見つけることができます。

OS	パス
Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 マシンの完全修飾ドメイン名 (FQDN) を含めるように、各マシンのカスタム構成ファイルを編集します。

マシンの IP アドレスに対して `NSLookup` を実行して、名前の DNS リストを表示し、ファイルのホスト名フィールドでその名前を使用します。

3 各ファイルに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

5 新しい証明書を VECS に追加します。

SSL を介して通信するには、すべてのマシンのローカル証明書ストアに、新しい証明書が必要です。最初に既存のエントリを削除し、次に新しいエントリを追加します。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.crt
 --key machine1.priv
```

6 すべてのサービスを再開します。

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

例： VMCA 署名付き証明書によるマシン証明書の置き換え

1 SSL 証明書用の構成ファイルを作成し、そのファイルを現在のディレクトリに `ssl-config.cfg` として保存します。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 マシン SSL 証明書にキー ペアを生成します。このコマンドを各管理ノードと Platform Services Controller ノードで実行します。`--server` オプションは必要ありません。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

現在のディレクトリに `ssl-key.priv` および `ssl-key.pub` ファイルが作成されます。

3 新しいマシン SSL 証明書を生成します。この証明書は VMCA によって署名されます。VMCA ルート証明書をカスタム証明書で置き換える場合には、VMCA はすべての証明書に完全な証明書チェーンで署名します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server（外部インストール）の場合：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

現在のディレクトリに `new-vmca-ssl.crt` ファイルが作成されます。

4 （オプション）VECS のコンテンツをリスト表示します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Platform Services Controller のサンプル出力：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server のサンプル出力：

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

5 VECS 内のマシン SSL 証明書を新しいマシン SSL 証明書で置き換えます。`--store` と `--alias` の値はデフォルト名と正確に一致させる必要があります。

- Platform Services Controller で、次のコマンドを実行して MACHINE_SSL_CERT ストア内のマシン SSL 証明書を更新します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 各管理ノードまたは組み込みデプロイで、次のコマンドを実行して MACHINE_SSL_CERT ストア内のマシン SSL 証明書を更新します。FQDN はマシンごとに異なるため、各マシンの証明書は別々に更新する必要があります。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

次のステップ

使用している ESXi ホストの証明書を置き換えることもできます。『vSphere のセキュリティ』ドキュメントを参照してください。

マルチノード デプロイでルート証明書を置き換えた後は、外部の Platform Services Controller ノードを使用するすべての vCenter Server 上でサービスを再起動する必要があります。

新規 VMCA 署名付き証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、すべてのソリューション ユーザー証明書を置き換えることができます。ソリューション ユーザー証明書は有効である必要があります。ここでの「有効」とは、有効期限が切れておらず、証明書に含まれるその他の情報が証明書インフラストラクチャで使用されていないことを意味します。

多くの VMware のユーザーの多くがソリューション ユーザー証明書を置き換えていません。マシン SSL 証明書だけがカスタム証明書に置き換えられています。このハイブリッド アプローチによって、セキュリティ チームの要求を満たすことができます。

- 証明書はプロキシの内側に配置されるか、カスタム証明書が使用されます。
- 中間 CA は使用されません。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 `--server` がある管理ノードでコマンドを実行する場合は、Platform Services Controller パラメータを使用して Platform Services Controller を指定します。

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

前提条件

すべてのサービスを停止し、証明書の伝達およびストレージを処理するサービスを開始する準備ができている。

手順

1 `certool.cfg` のコピーを 1 つ作成し、名前、IP アドレス、DNS 名、および E メールのフィールドを削除して、ファイルの名前を `sol_usr.cfg` のような名前に変更します。

生成プロセスの一部として、コマンド ラインから証明書に名前を付けることができます。その他の情報は、ソリューション ユーザーには必要ありません。デフォルトの情報を残すと、生成される証明書により混乱が生じる可能性があります。

2 各ソリューション ユーザーに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次にようになります。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、`dir-cli` リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

5 各ソリューション ユーザーの既存の証明書を、vmdir、VECS の順に置き換えます。

次の例は、vpxd サービスの証明書を置き換える方法を示します。

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

注： vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On への認証ができません。

6 すべてのサービスを再開します。

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

例： VMCA 署名付きソリューション ユーザー証明書の使用

1 各ソリューション ユーザーにパブリック/プライベート キーのペアを生成します。これには、各 Platform Services Controller のマシン ソリューション ユーザーおよび各管理ノードのペアと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) のペアが含まれます。

a 組み込みデプロイのマシン ソリューション ユーザーまたは Platform Services Controller のマシン ソリューション ユーザーのキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b （オプション）外部 Platform Services Controller を使用したデプロイの場合、各管理ノードのマシン ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

c 各管理ノードの vpxd ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

d 各管理ノードの vpxd-extension ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

e 各管理ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

2 各 Platform Services Controller および各管理ノードのマシン ソリューション ユーザーと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) に新しい VMCA ルート証明書によって署名されたソリューション ユーザー証明書を生成します。

注： `--Name` パラメータは一意である必要があります。ソリューション ユーザー ストアの名前も含めると、ソリューション ユーザーごとにどの証明書を適用するのかが確認しやすくなります。例には、それぞれ `vpxd` または `vpxd-extension` のような名前が含まれています。

a 以下のコマンドを Platform Services Controller ノードで実行し、そのノードのマシン ソリューション ユーザーにソリューション ユーザー証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

b 各管理ノードのマシン ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c 各管理ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d 各管理ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e 次のコマンドを実行して、各管理ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --
server=<psc-ip-or-fqdn>
```

3 VECS のソリューション ユーザー証明書を、新しいソリューション ユーザー証明書で置き換えます。

注： `--store` と `--alias` パラメータは、サービスのデフォルト名と正確に一致させる必要があります。

a Platform Services Controller ノードで、以下のコマンドを実行してマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b 以下のように、各管理ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c 各管理ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d 各管理ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 新しいソリューション ユーザー証明書を使用して VMware ディレクトリ サービス (vmdir) を更新します。vCenter Single Sign-On 管理者パスワードを求められます。

a `dir-cli service list` を実行し、ソリューション ユーザーごとに一意のサービス ID サフィックスを取得します。このコマンドは、Platform Services Controller または vCenter Server システム上で実行できます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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

b Platform Services Controller の vmdir にあるマシン証明書を置き換えます。たとえば、machine-29a45d00-60a7-11e4-96ff-00505689639a が Platform Services Controller のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c 各管理ノードの vmdir にあるマシン証明書を置き換えます。たとえば、machine-6fd7f140-60a9-11e4-9e28-005056895a69 が vCenter Server のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d 各管理ノードの vmdir にある vpxd ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e 各管理ノードの vmdir にある vpxd-extension ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd-extension ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。たとえば、vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 が vsphere-webclient ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

次のステップ

各 Platform Services Controller ノードおよび各管理ノード上のすべてのサービスを再起動します。

混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。

これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。
- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

注： サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

手順

1 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

   a `C:\ProgramData\VMware\CIS\cfg\vmdird` 内のすべてのファイルをバックアップします。

   b 6.x ノード上の `vmdircert.pem` ファイルのコピーを作成し、このコピーの名前を `<sso_node2.domain.com>.pem`（`<sso_node2.domain.com>` は 6.x ノードの FQDN）に変更します。

   c 名前を変更した証明書を `C:\ProgramData\VMware\CIS\cfg\vmdird` にコピーすることにより、既存の複製証明書を置き換えます。

2 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

   サービスを vSphere Client から再起動することも、`service-control` コマンドを使用することもできます。

中間認証局としての VMCA の使用

VMCA ルート証明書は、証明書チェーンに VMCA が含まれるサードパーティの CA 署名付き証明書に置き換えることができます。将来的に、VMCA によって生成されるすべての証明書には、完全な証明書チェーンが含められます。既存の証明書は、新しく生成された証明書に置き換えることができます。

手順

1 ルート証明書の置き換え（中間 CA）

カスタム証明書による VMware 認証局 (VMCA) 証明書の置き換えの最初の手順は、CSR を生成し、署名のために CSR を送信することです。続いて、署名済みの証明書をルート証明書として VMware 認証局 (VMCA) に追加します。

2 マシン SSL 証明書の置き換え（中間 CA）

CA から署名付き証明書を受信し、それを VMCA ルート証明書にした後で、すべてのマシン SSL 証明書を置き換えることができます。

3 ソリューション ユーザー証明書の置き換え（中間 CA）

マシン SSL 証明書を置き換えたら、ソリューション ユーザー証明書を置き換えることができます。

4 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

ルート証明書の置き換え（中間 CA）

カスタム証明書による VMware 認証局 (VMCA) 証明書の置き換えの最初の手順は、CSR を生成し、署名のために CSR を送信することです。続いて、署名済みの証明書をルート証明書として VMware 認証局 (VMCA) に追加します。

Certificate Manager ユーティリティなどのツールを使用して CSR を生成できます。CSR は次の要件を満たす必要があります。

- キー サイズ： 2,048 ビット以上
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- カスタム証明書を使用している場合、ルート証明書の認証局の拡張を true に設定し、証明書の署名を要件の一覧に含める必要があります。
- CRL の署名は有効にしてください。
- [拡張キー使用] は、空にするか、[サーバ認証] を指定します。
- 証明書チェーンの長さに明示的な制限はありません。VMware 認証局 (VMCA) では、デフォルトで OpenSSL が使用されます。この場合、10 個の証明書となります。

- ワイルドカードまたは複数の DNS 名を使用した証明書はサポートされていません。
- VMCA の従属認証局は作成できません。

  Microsoft Certificate Authority の使用例については、VMware のナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x (2112009)」(http://kb.vmware.com/kb/2112009) を参照してください。

VMCA は、ルート証明書を置き換えるときに、証明書の次の属性を検証します。

- キーのサイズ：2,048 ビット以上
- キーの使用：証明書の署名
- 基本制約：サブジェクト タイプ CA

手順

1 CSR を生成して、CA に送ります。

  CA の指示に従います。

2 署名済みの VMware 認証局 (VMCA) 証明書と、サード パーティ CA またはエンタープライズ CA の完全な CA チェーンを含む証明書ファイルを準備します。`rootca1.crt` などの名前でファイルを保存します。

  この手順は、PEM 形式のすべての CA 証明書を単一ファイルにコピーすることで行えます。VMware 認証局 (VMCA) ルート証明書から始まり、最終的にはルート CA PEM 証明書になります。例：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

4 既存の VMCA ルート CA を置き換えます。

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

このコマンドを実行すると、次の処理が行われます。

- ファイル システム内の証明書がある場所に、新しいカスタム ルート証明書が追加されます。
- VECS の TRUSTED_ROOTS ストアに、カスタム ルート証明書が追加されます（一定時間の経過後）。
- vmdir にカスタム ルート証明書が追加されます（一定時間の経過後）。

5 （オプション） vmdir（VMware ディレクトリ サービス）のすべてのインスタンスに変更を伝達するには、新しいルート証明書を vmdir に発行し、各ファイルのフル パスを指定します。

例：

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

vmdir ノード間のレプリケーションは 30 秒おきに実行されます。VECS は vmdir に対する新しいルート証明書ファイルのポーリングを 5 分おきに実行するため、VECS にルート証明書を明示的に追加する必要はありません。

6 （オプション） 必要な場合は、VECS の更新を強制できます。

```
vecs-cli force-refresh
```

7 すべてのサービスを再開します。

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

例： ルート証明書の置き換え

certool コマンドに `--rootca` オプションを指定して、VMCA ルート証明書をカスタムの CA ルート証明書に置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-
certs\root.pem --privkey=C:\custom-certs\root.key
```

このコマンドを実行すると、次の処理が行われます。

- ファイル システム内の証明書がある場所に、新しいカスタム ルート証明書が追加されます。
- VECS の TRUSTED_ROOTS ストアに、カスタム ルート証明書が追加されます。
- vmdir にカスタム ルート証明書が追加されます。

次のステップ

元の VMCA ルート証明書は証明書ストアから削除できます（会社のポリシーで求められている場合）。その場合、vCenter Single Sign-On 署名証明書を置き換える必要があります。Security Token Service 証明書の更新を参照してください。

マシン SSL 証明書の置き換え（中間 CA）

CA から署名付き証明書を受信し、それを VMCA ルート証明書にした後で、すべてのマシン SSL 証明書を置き換えることができます。

これらの手順は、VMCA を認証局として使用する証明書を置き換える場合と基本的に同じです。ただし、この場合、VMCA はすべての証明書に完全な証明書チェーンで署名します。

他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

前提条件

各マシン SSL 証明書の場合、`SubjectAltName` に `DNS Name=<Machine FQDN>` が含まれている必要があります。

手順

1 新しい証明書を必要とするマシンごとに、`certool.cfg` のコピーを 1 つ作成します。

`certool.cfg` は次の場所で見つけることができます。

Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

2 マシンの完全修飾ドメイン名 (FQDN) を含めるように、各マシンのカスタム構成ファイルを編集します。

マシンの IP アドレスに対して `NSLookup` を実行して、名前の DNS リストを表示し、ファイルのホスト名フィールドでその名前を使用します。

3 各マシンにパブリック/プライベート キー ファイル ペアおよび証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

5 新しい証明書を VECS に追加します。

SSL を介して通信するには、すべてのマシンのローカル証明書ストアに、新しい証明書が必要です。最初に既存のエントリを削除し、次に新しいエントリを追加します。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 すべてのサービスを再開します。

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

例： マシン SSL 証明書の置き換え（VMCA が中間 CA）

1 SSL 証明書用の構成ファイルを作成し、そのファイルを現在のディレクトリに `ssl-config.cfg` として保存します。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 マシン SSL 証明書にキー ペアを生成します。このコマンドを各管理ノードと Platform Services Controller ノードで実行します。`--server` オプションは必要ありません。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

現在のディレクトリに `ssl-key.priv` および `ssl-key.pub` ファイルが作成されます。

3 新しいマシン SSL 証明書を生成します。この証明書は VMCA によって署名されます。VMCA ルート証明書をカスタム証明書で置き換える場合には、VMCA はすべての証明書に完全な証明書チェーンで署名します。

- Platform Services Controller ノードまたは組み込みインストールで、次のように実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server（外部インストール）の場合：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-
ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

現在のディレクトリに `new-vmca-ssl.crt` ファイルが作成されます。

4 （オプション）VECS のコンテンツをリスト表示します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Platform Services Controller のサンプル出力：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server のサンプル出力：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
```

```
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 VECS 内のマシン SSL 証明書を新しいマシン SSL 証明書で置き換えます。`--store` と `--alias` の値はデフォルト名と正確に一致させる必要があります。

- Platform Services Controller で、次のコマンドを実行して MACHINE_SSL_CERT ストア内のマシン SSL 証明書を更新します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 各管理ノードまたは組み込みデプロイで、次のコマンドを実行して MACHINE_SSL_CERT ストア内のマシン SSL 証明書を更新します。FQDN はマシンごとに異なるため、各マシンの証明書は別々に更新する必要があります。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

ソリューション ユーザー証明書の置き換え（中間 CA）

マシン SSL 証明書を置き換えたら、ソリューション ユーザー証明書を置き換えることができます。

多くの VMware のユーザーの多くがソリューション ユーザー証明書を置き換えていません。マシン SSL 証明書だけがカスタム証明書に置き換えられています。このハイブリッド アプローチによって、セキュリティ チームの要求を満たすことができます。

- 証明書はプロキシの内側に配置されるか、カスタム証明書が使用されます。
- 中間 CA は使用されません。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 `--server` がある管理ノードでコマンドを実行する場合は、Platform Services Controller パラメータを使用して Platform Services Controller を指定します。

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

前提条件

各ソリューション ユーザー証明書には異なる `Subject` が指定されている必要があります。たとえば、ソリューション ユーザー名（例： vpxd）などの一意の識別子を含めることができます。

注： Vpxd 証明書ストアは、Platform Services Controller ではなく vCenter Server Appliance にのみ存在します。

手順

1 `certool.cfg` のコピーを 1 つ作成し、名前、IP アドレス、DNS 名、および E メールのフィールドを削除して、ファイルの名前を `sol_usr.cfg` のような名前に変更します。

生成プロセスの一部として、コマンド ラインから証明書に名前を付けることができます。その他の情報は、ソリューション ユーザーには必要ありません。デフォルトの情報を残すと、生成される証明書により混乱が生じる可能性があります。

2 各ソリューション ユーザーに、パブリック キーとプライベート キーのファイル ペアと証明書を生成し、カスタマイズした構成ファイルに渡します。

例：

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次にようになります。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、`dir-cli` リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

4 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

5 vmdir 内の既存の証明書を置き換え、次に VECS 内の証明書を置き換えます。

ソリューション ユーザーに対して、その順序で証明書を追加する必要があります。例：

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

注： vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On にログインできません。

6 すべてのサービスを再開します。

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

例： ソリューション ユーザー証明書の置き換え（中間 CA）

1 各ソリューション ユーザーにパブリック/プライベート キーのペアを生成します。これには、各 Platform Services Controller のマシン ソリューション ユーザーおよび各管理ノードのペアと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) のペアが含まれます。

a 組み込みデプロイのマシン ソリューション ユーザーまたは Platform Services Controller のマシン ソリューション ユーザーのキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b （オプション）外部 Platform Services Controller を使用したデプロイの場合、各管理ノードのマシン ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

c 各管理ノードの vpxd ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

d 各管理ノードの vpxd-extension ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

e 各管理ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

2 各 Platform Services Controller および各管理ノードのマシン ソリューション ユーザーと、各管理ノードの各追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient) に新しい VMCA ルート証明書によって署名されたソリューション ユーザー証明書を生成します。

注： `--Name` パラメータは一意である必要があります。ソリューション ユーザー ストアの名前も含めると、ソリューション ユーザーごとにどの証明書を適用するのかが確認しやすくなります。例には、それぞれ `vpxd` または `vpxd-extension` のような名前が含まれています。

a 以下のコマンドを Platform Services Controller ノードで実行し、そのノードのマシン ソリューション ユーザーにソリューション ユーザー証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

b 各管理ノードのマシン ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c 各管理ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d 各管理ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e 次のコマンドを実行して、各管理ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-
vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --
server=<psc-ip-or-fqdn>
```

3 VECS のソリューション ユーザー証明書を、新しいソリューション ユーザー証明書で置き換えます。

注： `--store` と `--alias` パラメータは、サービスのデフォルト名と正確に一致させる必要があります。

a Platform Services Controller ノードで、以下のコマンドを実行してマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b 以下のように、各管理ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c 各管理ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd
--alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd
--alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d 各管理ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-
key.priv
```

e 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key
vsphere-webclient-key.priv
```

4 新しいソリューション ユーザー証明書を使用して VMware ディレクトリ サービス (vmdir) を更新します。vCenter Single Sign-On 管理者パスワードを求められます。

a `dir-cli service list` を実行し、ソリューション ユーザーごとに一意のサービス ID サフィックスを取得します。このコマンドは、Platform Services Controller または vCenter Server システム上で実行できます。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

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

b Platform Services Controller の vmdir にあるマシン証明書を置き換えます。たとえば、machine-29a45d00-60a7-11e4-96ff-00505689639a が Platform Services Controller のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c 各管理ノードの vmdir にあるマシン証明書を置き換えます。たとえば、machine-6fd7f140-60a9-11e4-9e28-005056895a69 が vCenter Server のマシン ソリューション ユーザーの場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d 各管理ノードの vmdir にある vpxd ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e 各管理ノードの vmdir にある vpxd-extension ソリューション ユーザー証明書を置き換えます。たとえば、vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 が vpxd-extension ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f 各管理ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。たとえば、vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 が vsphere-webclient ソリューション ユーザー ID の場合、以下のコマンドを実行します。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。

これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。
- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

注： サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

手順

1 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

a `C:\ProgramData\VMware\CIS\cfg\vmdird` 内のすべてのファイルをバックアップします。

b 6.x ノード上の `vmdircert.pem` ファイルのコピーを作成し、このコピーの名前を `<sso_node2.domain.com>.pem`（`<sso_node2.domain.com>` は 6.x ノードの FQDN）に変更します。

c 名前を変更した証明書を `C:\ProgramData\VMware\CIS\cfg\vmdird` にコピーすることにより、既存の複製証明書を置き換えます。

2 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

サービスを vSphere Client から再起動することも、`service-control` コマンドを使用することもできます。

vSphere でのカスタム証明書の使用

企業ポリシーで規定されている場合は、vSphere で使用されている一部または全部の証明書を、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置き換えることができます。これを行った場合、VMware 認証局 (VMCA) は証明書チェーンには含まれなくなります。すべての vCenter Server 証明書を VECS に格納する必要があります。

すべての証明書を置き換えるか、ハイブリッド ソリューションを使用できます。たとえば、ネットワーク トラフィックに使用されるすべての証明書を置き換え、VMCA 署名付きソリューション ユーザー証明書はそのまま残すことを考えます。ソリューション ユーザー証明書は、vCenter Single Sign-On への認証にのみ使用されます。

注： VMCA を使用しない場合には、証明書を使用して新しいコンポーネントをプロビジョニングしたり、証明書の期限を常に把握するために、すべての証明書を自分自身で置き換える必要があります。

カスタム証明書を使用する場合でも、VMware Certificate Manager ユーティリティを使用して証明書を置き換えることができます。「カスタム証明書によるすべての証明書の置き換え (Certificate Manager)」を参照してください。

証明書の置き換え後に vSphere 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。

手順

1 証明書の要求およびカスタム ルート証明書のインポート

   エンタープライズまたはサードパーティ認証局 (CA) からのカスタム証明書を使用できます。最初の手順は、認証局に証明書を要求し、ルート証明書を VMware Endpoint Certificate Store (VECS) にインポートすることです。

2 カスタム証明書によるマシン SSL 証明書の置き換え

   カスタム証明書を取得したら、各マシン証明書を置き換えることができます。

3 カスタム証明書によるソリューション ユーザー証明書の置き換え

   マシン SSL 証明書を置き換えたら、VMCA 署名付きソリューション ユーザー証明書をサードパーティ証明書またはエンタープライズ証明書に置き換えることができます。

4 混合モード環境での VMware ディレクトリ サービス証明書の置き換え

   アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

証明書の要求およびカスタム ルート証明書のインポート

エンタープライズまたはサードパーティ認証局 (CA) からのカスタム証明書を使用できます。最初の手順は、認証局に証明書を要求し、ルート証明書を VMware Endpoint Certificate Store (VECS) にインポートすることです。

前提条件

証明書は次の要件を満たす必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- ルート証明書の場合、認証局の拡張を true に設定する必要があり、証明書の署名を要件の一覧に含める必要があります。
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- CRT 形式
- キー使用法として、デジタル署名、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）

手順

1 以下の証明書の証明書署名リクエスト (CSR) をエンタープライズまたはサードパーティ証明書プロバイダに送信します。

   - 各マシンのマシン SSL 証明書。マシン SSL 証明書の場合、SubjectAltName フィールドには、完全修飾ドメイン名 (DNS NAME=*machine_ FQDN*) が含まれている必要があります。
   - （オプション）組み込みシステムまたは管理ノードごとに 4 つのソリューション ユーザー証明書。ソリューション ユーザー証明書には IP アドレス、ホスト名、メール アドレスを含めることはできません。証明書の Subject は、各証明書で異なっている必要があります。
   - （オプション）外部 Platform Services Controller インスタンスのマシン ソリューション ユーザーの証明書。この証明書は、Platform Services Controller のマシン SSL 証明書とは異なります。

   通常、その結果は信頼されたチェーンの PEM ファイルで、Platform Services Controller または管理ノードごとの署名付き SSL 証明書も追加されます。

2 TRUSTED_ROOTS およびマシン SSL ストアをリストします。

```
vecs-cli store list
```

   a 現在のルート証明書とすべてのマシン SSL 証明書が VMCA によって署名されていることを確認します。

   b シリアル番号、発行者、Subject の CN フィールドを書き留めておきます。

   c （オプション） Web ブラウザを使用して、証明書を置き換えるノードへの HTTPS 接続を開き、証明書情報を参照して、マシン SSL 証明書と一致していることを確認します。

3 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

4 カスタム ルート証明書を公開します。

```
dir-cli trustedcert publish --cert <my_custom_root>
```

コマンド ラインでユーザー名とパスワードを指定しないと、指定するように求められます。

5 すべてのサービスを再開します。

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

次のステップ

元の VMCA ルート証明書は証明書ストアから削除できます（会社のポリシーで求められている場合）。その場合、vCenter Single Sign-On 証明書を更新する必要があります。Security Token Service 証明書の更新を参照してください。

カスタム証明書によるマシン SSL 証明書の置き換え

カスタム証明書を取得したら、各マシン証明書を置き換えることができます。

他のサービスとの安全な通信を実現するため、各マシンにマシン SSL 証明書が必要です。マルチノード環境では、各ノードでマシン SSL 証明書生成コマンドを実行する必要があります。外部の Platform Services Controller を使用する vCenter Server の Platform Services Controller を参照するには、`--server` パラメータを使用します。

証明書の置き換えを開始する前に、次の情報を確認しておく必要があります。

- administrator@vsphere.local のパスワード。
- 有効なマシン SSL カスタム証明書（`.crt` ファイル）。

- 有効なマシン SSL カスタム キー（.key ファイル）。
- ルートの有効なカスタム証明書（.crt ファイル）。
- マルチノード 環境内の外部の Platform Services Controller を使用する vCenter Server 上でこのコマンドを実行する場合は、Platform Services Controller の IP アドレス。

前提条件

サードパーティまたはエンタープライズ CA から各マシンの証明書を取得している必要があります。

- キー サイズ：2,048 ビット以上（PEM エンコード）
- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります

手順

1 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

サービス名は、Windows 上と vCenter Server Appliance 上で異なります。

注： 外部 Platform Services Controller を使用している環境では、vCenter Server ノード上で VMware Directory Service (vmdird) および VMware Certificate Authority (vmcad) を停止および開始する必要はありません。これらのサービスは、Platform Services Controller で実行されます。

Windows

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

vCenter Server Appliance

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

2 各ノードにログインし、取得した新しいマシン証明書を CA から VECS に追加します。

SSL を介して通信する場合、すべてのマシンのローカル証明書ストアに、新しい証明書が必要となります。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-
path>
--key <key-file-path>
```

3 すべてのサービスを再開します。

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

例： カスタム証明書によるマシン SSL 証明書の置き換え

この例では、Windows のインストール環境でマシンの SSL 証明書をカスタム証明書と置き換える方法について説明します。各ノードのマシン SSL 証明書も同様に置き換えることができます。

1 最初に、VECS にある既存の証明書を削除します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

2 次に置き換える証明書を追加します。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

カスタム証明書によるソリューション ユーザー証明書の置き換え

マシン SSL 証明書を置き換えたら、VMCA 署名付きソリューション ユーザー証明書をサードパーティ証明書またはエンタープライズ証明書に置き換えることができます。

多くの VMware のユーザーの多くがソリューション ユーザー証明書を置き換えていません。マシン SSL 証明書だけがカスタム証明書に置き換えられています。このハイブリッド アプローチによって、セキュリティ チームの要求を満たすことができます。

- 証明書はプロキシの内側に配置されるか、カスタム証明書が使用されます。
- 中間 CA は使用されません。

ソリューション ユーザーは、vCenter Single Sign-On への認証を行うためだけに、証明書を使用します。証明書が有効な場合、vCenter Single Sign-On はソリューション ユーザーに SAML トークンを割り当てます。ソリューション ユーザーは、他の vCenter コンポーネントへの認証を行うために SAML トークンを使用します。

各管理ノードおよび各 Platform Services Controller ノードにあるマシン ソリューション ユーザー証明書を置き換えます。各管理ノードにある他のソリューション ユーザー証明書のみを置き換えます。外部 `--server` がある管理ノードでコマンドを実行する場合は、Platform Services Controller パラメータを使用して Platform Services Controller を指定します。

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

前提条件

- キー サイズ：2,048 ビット以上（PEM エンコード）

- CRT 形式
- x509 バージョン 3
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。
- 各ソリューション ユーザー証明書には異なる `Subject` が指定されている必要があります。たとえば、ソリューション ユーザー名（例： vpxd）などの一意の識別子を含めることができます。
- キー使用法として、デジタル署名、キー暗号化が含まれている必要があります

手順

1 すべてのサービスを停止し、証明書の作成、伝達、およびストレージを処理するサービスを開始します。

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

2 各ソリューション ユーザーの名前を検索します。

```
dir-cli service list
```

証明書を置き換えるときに返される一意の ID を使用できます。入力と出力は次にようになります。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

マルチノード デプロイでソリューション ユーザー証明書の一覧を表示すると、`dir-cli` リストの出力にすべてのノードのすべてのソリューション ユーザーが示されます。`vmafd-cli get-machine-id --server-name localhost` を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

3 各ソリューション ユーザーの既存の証明書を、VECS、vmdir の順に置き換えます。

その順番で証明書を追加する必要があります。

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

注： vmdir の証明書が置き換えられていないと、ソリューション ユーザーは vCenter Single Sign-On への認証ができません。

4 すべてのサービスを再開します。

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

混合モード環境での VMware ディレクトリ サービス証明書の置き換え

アップグレード時に、環境内に一時的に vCenter Single Sign-On バージョン 5.5 と vCenter Single Sign-On バージョン 6.x の両方が含まれた状態になることがあります。その場合、vCenter Single Sign-On サービスが実行されているノードの SSL 証明書を置き換える場合は、追加の手順を実行して VMware Directory Service の SSL 証明書を置き換える必要があります。

VMware Directory Service の SSL 証明書は、vCenter Single Sign-On 複製を実行する Platform Services Controller ノード間のハンドシェイクを実行するために vmdir によって使用されます。

これらの手順は、vSphere 6.0 ノードと vSphere 6.5 ノードを含む混合モード環境では不要です。これらの手順は次の場合にのみ必要です。

- 環境に vCenter Single Sign-On 5.5 サービスと vCenter Single Sign-On 6.x サービスの両方が含まれる場合。
- vmdir データを複製するように vCenter Single Sign-On サービスが設定されている場合。
- vCenter Single Sign-On 6.x サービスが実行されているノードのデフォルトの VMware 認証局 (VMCA) の署名付き証明書をカスタム証明書に置き換える予定である場合。

注： サービスを再起動する前に、環境全体をアップグレードすることをお勧めします。VMware Directory Service の証明書の置き換えは一般にお勧めできません。

手順

1 vCenter Single Sign-On 5.5 サービスが実行されているノードで、vCenter Single Sign-On 6.x サービスが認識されるように環境を設定します。

   a `C:\ProgramData\VMware\CIS\cfg\vmdird` 内のすべてのファイルをバックアップします。

   b 6.x ノード上の `vmdircert.pem` ファイルのコピーを作成し、このコピーの名前を `<sso_node2.domain.com>.pem`（`<sso_node2.domain.com>` は 6.x ノードの FQDN）に変更します。

   c 名前を変更した証明書を `C:\ProgramData\VMware\CIS\cfg\vmdird` にコピーすることにより、既存の複製証明書を置き換えます。

2 証明書を置き換えたすべてのマシン上の VMware ディレクトリ サービスを再起動します。

   サービスを vSphere Client から再起動することも、`service-control` コマンドを使用することもできます。

CLI コマンドを使用したサービスと証明書の管理

4

CLI のセットを使用すると、VMCA (VMware Certificate Authority)、VECS（VMware Endpoint 証明書ストア)、および VMware Directory Service (vmdir) を管理できます。vSphere Certificate Manager ユーティリティでは、多くの関連タスクもサポートしていますが、手動の証明書管理とその他のサービスの管理には CLI が必要になります。

通常、SSH を使用してアプライアンス シェルに接続することによって、証明書および関連サービスを管理するための CLI ツールにアクセスします。詳細については、VMware ナレッジベースの記事 (http://kb.vmware.com/kb/2100508) を参照してください。

証明書の手動での置き換えでは、CLI コマンドを使用して証明書を置き換える方法の例を紹介します。

表 4-1. 証明書および関連サービスを管理する CLI ツール

CLI	説明	詳細については、ドキュメントを参照してください。
certool	証明書およびキーを生成および管理します。VMCAD の一部としての VMware 証明書管理サービス。	certool 初期化コマンド リファレンス
vecs-cli	VMware 証明書ストア インスタンスのコンテンツを管理します。VMAFD の一部です。	vecs-cli コマンド リファレンス
dir-cli	VMware Directory Service に証明書を作成し更新します。VMAFD の一部です。	dir-cli コマンド リファレンス
sso-config	一部の vCenter Single Sign-On の構成です。ほとんどの場合、vSphere Web Client または vSphere Client のいずれかを使用します。2 要素認証の設定にこのコマンドを使用します。	コマンドライン ヘルプ。 vCenter Server の 2 要素認証について
service-control	証明書の置換ワークフローの一部などで、サービスを開始または停止します。	このコマンドを実行して、他の CLI コマンドを実行する前にサービスを停止します。

CLI の場所

デフォルトでは、CLI は各ノードの次の場所にあります。

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
```

```
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
```

```
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
```

Linux では、`service-control` コマンドでパスを指定する必要はありません。

外部の Platform Services Controller を使用する vCenter Server システムからコマンドを実行する場合、`--server` パラメータを使用して Platform Services Controller を指定できます。

この章には、次のトピックが含まれています。

- CLI の実行に必要な権限
- certool 構成オプションの変更
- certool 初期化コマンド リファレンス
- certool 管理コマンド リファレンス
- vecs-cli コマンド リファレンス
- dir-cli コマンド リファレンス

CLI の実行に必要な権限

必要な権限は、使用する CLI と実行するコマンドによって変わります。たとえば、ほとんどの証明書管理の操作には、ローカルの vCenter Single Sign-On ドメイン（デフォルトは vsphere.local）の管理者が必要です。一部のコマンドは、すべてのユーザーが使用できます。

dir-cli

`dir-cli` コマンドを実行するには、ローカル ドメイン（デフォルトは vsphere.local）の管理者グループのメンバーであることが必要です。ユーザー名とパスワードを指定しない場合、ローカルの vCenter Single Sign-On の管理者（デフォルトは administrator@vsphere.local）のパスワードを入力するように求められます。

vecs-cli

最初は、ストアの所有者と包括的なアクセス権を持つユーザーのみストアにアクセスできます。Windows 上では管理者グループのユーザーが、Linux 上では root ユーザーが包括的なアクセス権を持ちます。

MACHINE_SSL_CERT および TRUSTED_ROOTS ストアは特別なストアです。インストールのタイプによっては、root ユーザーまたは管理者ユーザーにのみ完全なアクセス権があります。

certool

ほとんどの `certool` コマンドでは、ユーザーが管理者グループに属している必要があります。以下のコマンドはすべてのユーザーが実行できます。

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

certool 構成オプションの変更

`certool --gencert` または他の特定の証明書の初期化または管理コマンドを実行する場合、コマンドは構成ファイルからすべての値を読み取ります。既存のファイルを編集したり、`--config=<file name>` オプションを使用してデフォルトの構成ファイルにオーバーライドしたり、コマンド ラインの値にオーバーライドしたりできます。

構成ファイル `certool.cfg` はデフォルトで次の場所にあります。

OS	場所
Linux	`/usr/lib/vmware-vmca/share/config/`
Windows	`C:\Program Files\VMware\vCenter Server\vmcad\`

このファイルには、以下のデフォルト値を持つ複数のフィールドがあります。

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

以下に示すように、値を変更するには変更されたファイルをコマンド ラインで指定するか、個別の値をコマンド ラインでオーバーライドします。

- 構成ファイルのコピーを作成し、ファイルを編集します。 `--config` コマンドライン オプションを使用してファイルを指定します。パス名の問題を回避するため、フル パスを指定します。

- ```
  certool --gencert --config C:\Temp\myconfig.cfg
  ```
- コマンド ラインで個別の値をオーバーライドします。たとえば、Locality をオーバーライドするには次のコマンドを実行します。

  ```
  certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

`--Name` を指定して証明書の Subject 名の CN フィールドを置き換えます。

- ソリューション ユーザー証明書の場合、規則に従って名前が <sol_user name>@<domain> になりますが、お使いの環境で別の規則を使用している場合には名前を変更できます。
- マシン SSL 証明書の場合、マシンの完全修飾ドメイン名 (FQDN) が使用されます。

  VMware 認証局 (VMCA) には DNSName（`Hostname` フィールド内）があるのみで他のエイリアス オプションは許容されません。ユーザーによって IP アドレスが指定されていると、SubAltName に同様に格納されます。

`--Hostname` パラメータを使用して証明書の SubAltName の DNSName を指定します。

certool 初期化コマンド リファレンス

`certool` 初期化コマンドにより証明書の署名要求の生成、VMCA によって署名された証明書およびキーの表示および生成、ルート証明書のインポート、およびその他の証明書管理操作を実行することができます。

多くの場合、構成ファイルを `certool` コマンドに渡します。certool 構成オプションの変更を参照してください。使用例については、「新規の VMCA 署名付き証明書による既存の VMCA 署名付き証明書の置き換え」を参照してください。コマンドライン ヘルプは、オプションに関する詳細を提供します。

certool --initcsr

証明書署名要求 (CSR) を生成します。このコマンドは、PKCS10 ファイルとプライベート キーを生成します。

オプション	説明
`--gencsr`	CSR を生成する場合に必要です。
`--privkey <key_file>`	プライベート キー ファイルの名前。
`--pubkey <key_file>`	パブリック キー ファイルの名前。
`--csrfile <csr_file>`	CA プロバイダに送信される CSR ファイルのファイル名。
`--config <config_file>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。

例：

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```
```

certool --selfca

自己署名証明書を作成し、自己署名ルート CA により VMCA サーバをプロビジョニングします。このオプションは、VMCA サーバのプロビジョニングを最も容易に実行する方法の 1 つです。代わりに、サードパーティのルート証明書を使用して VMCA サーバをプロビジョニングすることで、VMCA を中間 CA することができます。中間認証局としての VMCA の使用を参照してください。

このコマンドにより、タイム ゾーンの競合を避けるため、3 日前の日付の証明書が生成されます。

オプション	説明
`--selfca`	自己署名証明書を生成する場合に必要です。
`--predate <number_of_minutes>`	ルート証明書の [有効期間の開始日] フィールドを、現在時刻より前の指定の時間（分単位）に設定することができます。このオプションは、潜在的なタイム ゾーンの問題への対処に役立ちます。最大値は 3 日です。
`--config <config_file>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

ルート証明書をインポートします。指定した証明書およびプライベート キーを VMCA に追加します。VMware 認証局 (VMCA) は最新のルート証明書を署名に使用しますが、その他のルート証明書も、手動で削除するまでは引き続き信頼されます。つまり、一度に 1 段階ずつインフラストラクチャを更新し、最後に使用しなくなった証明書を削除できます。

オプション	説明
`--rootca`	ルート CA をインポートするために必要です。
`--cert <certfile>`	証明書ファイルの名前。
`--privkey <key_file>`	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

vmdir によって使用されるデフォルトのドメイン名を戻します。

オプション	説明
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
`--port <port_num>`	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --getdc
```

certool --waitVMDIR

VMware Directory Service が稼動し始めるか、`--wait` によって指定されたタイムアウト時間が経過するまで待機します。他のオプションと関連付けてこのオプションを使用し、デフォルトのドメイン名を返すなど特定のタスクをスケジュールします。

オプション	説明
`--wait`	オプションで指定する待機時間（分）。デフォルトは 3 です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
`--port <port_num>`	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

VMCA サービスが稼動し始めるか、指定されたタイムアウト時間が経過するまで待機します。他のオプションと関連付けてこのオプションを使用し、証明書を生成するなど特定のタスクをスケジュールします。

オプション	説明
`--wait`	オプションで指定する待機時間（分）。デフォルトは 3 です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。
`--port <port_num>`	オプションのポート番号。デフォルト設定はポート 389 です。

例：

```
certool --waitVMCA --selfca
```

certool --publish-roots

ルート証明書の更新を強制的に実行します。このコマンドには管理権限が必要です。

オプション	説明
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --publish-roots
```

certool 管理コマンド リファレンス

`certool` 管理コマンドを使用すると、証明書の表示、生成、および失効や、証明書情報の表示を行うことができます。

certool --genkey

プライベート キーとパブリック キーのペアを生成します。これらのファイルを使用して、VMCA が署名する証明書を生成できます。

オプション	説明
`--genkey`	プライベート キーとパブリック キーの生成に必要です。
`--privkey <keyfile>`	プライベート キー ファイルの名前。
`--pubkey <keyfile>`	パブリック キー ファイルの名前。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

VMCA サーバからの証明書を生成します。このコマンドでは、`certool.cfg` または指定された構成ファイルの情報が使用されます。証明書を使用して、マシン証明書またはソリューション ユーザー証明書をプロビジョニングすることができます。

オプション	説明
`--gencert`	証明書の生成に必要です。
`--cert <certfile>`	証明書ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。

オプション	説明
`--privkey <keyfile>`	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
`--config <config_file>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

人間が解読可能な形式で、現在のルート CA 証明書を出力します。管理ノードからこのコマンドを実行する場合は、Platform Services Controller ノードのマシン名を使用して、ルート CA を取得します。この出力は証明書として使用できず、人間が解読可能な形式に変換されます。

オプション	説明
`--getrootca`	ルート証明書の出力に必要です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --getrootca --server=remoteserver
```

certool --viewcert

人間が解読可能な形式で、証明書内のすべてのフィールドを出力します。

オプション	説明
`--viewcert`	証明書の表示に必要です。
`--cert <certfile>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。

例：

```
 certool --viewcert --cert=<filename>
```

certool --enumcert

VMCA サーバが認識しているすべての証明書を一覧表示します。必須の `filter` オプションを使用すると、すべての証明書、失効している証明書のみ、アクティブな証明書のみ、または期限切れの証明書のみのリストを表示できます。

オプション	説明
`--enumcert`	すべての証明書のリストの表示に必要です。
`--filter [all | active]`	filter は必須です。all または active を指定します。現在、revoked および expired のオプションはサポートされていません。

例：

```
certool --enumcert --filter=active
```

certool --status

指定された証明書を VMCA サーバに送信して、証明書が失効しているかどうかを確認します。証明書が失効している場合は 証明書:失効 が出力され、それ以外の場合は 証明書:アクティブ が出力されます。

オプション	説明
`--status`	証明書のステータスの確認に必要です。
`--cert <certfile>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。
`--server <server>`	VMCA サーバのオプション名。このコマンドでは、デフォルトで localhost を使用します。

例：

```
certool --status --cert=<filename>
```

certool --genselfcacert

構成ファイルの値に基づいて、自己署名証明書を生成します。このコマンドにより、タイム ゾーンの競合を避けるため、3 日前の日付の証明書が生成されます。

オプション	説明
`--genselfcacert`	自己署名証明書を生成する場合に必要です。
`--outcert <cert_file>`	証明書ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
`--outprivkey <key_file>`	プライベート キー ファイルの名前。このファイルは、PEM エンコード形式にする必要があります。
`--config <config_file>`	構成ファイルのオプション名。デフォルトの名前は `certool.cfg` です。

例：

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

vecs-cli コマンド リファレンス

vecs-cli コマンド セットを使用して、VMware 証明書ストア (VECS) を管理できます。証明書インフラストラクチャとその他の Platform Services Controller サービスを管理する場合は、次のコマンドを dir-cli および certool と併用します。

vecs-cli store create

証明書ストアを作成します。

オプション	説明
--name <name>	証明書ストアの名前。
--server <server-name>	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
--upn <user-name>	--server <server-name> で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

例：

```
vecs-cli store create --name <store>
```

vecs-cli store delete

証明書ストアを削除します。MACHINE_SSL_CERT、TRUSTED_ROOTS、TRUSTED_ROOT_CRLS のシステム ストアは削除できません、必要な権限を持つユーザーは、ソリューション ユーザー ストアを削除できます。

オプション	説明
--name <name>	削除する証明書ストアの名前。
--server <server-name>	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
--upn <user-name>	--server <server-name> で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

例：

```
vecs-cli store delete --name <store>
```

vecs-cli store list

証明書ストアのリストを表示します。

オプション	説明
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

VECS には、次のストアが含まれます。

表 4-2. VECS 内のストア

ストア	説明
マシン SSL ストア (MACHINE_SSL_CERT)	■ 各 vSphere ノード上のリバースプロキシ サービスによって使用されます。 ■ 組み込みデプロイおよび各 Platform Services Controller ノード上の VMware Directory Service (vmdir) によって使用されます。 vSphere 6.0 以降のすべてのサービスは、マシン SSL 証明書を使用するリバース プロキシを介して通信されます。下位互換性を保つため、5.x サービスでは特定のポートが引き続き使用されています。その結果、vpxd などの一部のサービスのポートが開かれたままになります。
信頼されたルート ストア (TRUSTED_ROOTS)	すべての信頼済みルート証明書を含みます。

表 4-2. VECS 内のストア （続き）

ストア	説明
ソリューション ユーザー ストア ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient	VECS には、ソリューション ユーザーごとに 1 つのストアが含まれます。各ソリューション ユーザー証明書の件名は一意でなければなりません。たとえば、マシン証明書には vpxd 証明書と同じ件名を指定できません。 ソリューション ユーザー証明書は、vCenter Single Sign-On での認証に使用されます。vCenter Single Sign-On は、証明書が有効であることを確認しますが、その他の証明書の属性は確認しません。組み込みのデプロイでは、すべてのソリューション ユーザー証明書が同じシステム上に存在します。 次のソリューション ユーザー証明書ストアが、各管理ノードと各組み込みデプロイの VECS に含まれています。 ■ machine：License Server およびログ サービスにより使用されます。 **注：** マシン ソリューション ユーザー証明書は、マシン SSL 証明書とは無関係です。マシン ソリューション ユーザー証明書は、SAML トークン交換に使用されます。マシン SSL 証明書は、マシン向けのセキュア SSL 接続に使用されます。 ■ vpxd：管理ノードおよび組み込みデプロイ上の、vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに格納されているソリューション ユーザー証明書を使用して、vCenter Single Sign-On への認証を行います。 ■ vpxd-extension：vCenter Server 拡張機能のストア。Auto Deploy サービス、Inventory Service、およびその他のソリューション ユーザーに含まれないその他のサービス。 ■ vsphere-webclient：vSphere Web Client ストア。パフォーマンス チャート サービスなどの一部の追加サービスも含まれます。 各 Platform Services Controller ノードには machine 証明書が含まれます。
vSphere Certificate Manager ユーティリティのバックアップ ストア (BACKUP_STORE)	証明書の取り消しをサポートするために、Certificate Manager によって使用されます。最新の状態のみがバックアップとして保存され、1 段階より多く戻ることはできません。
その他のストア	その他のストアが、ソリューションによって追加される場合があります。たとえば、Virtual Volumes ソリューションにより SMS ストアが追加されます。VMware ドキュメントまたは VMware ナレッジベースの記事で指示されないかぎり、ストア内の証明書は変更しないでください。 **注：** TRUSTED_ROOTS_CRLS ストアを削除すると、証明書インフラストラクチャが破損することがあります。TRUSTED_ROOTS_CRLS ストアの削除や修正は行わないでください。

例：

```
vecs-cli store list
```

vecs-cli store permissions

ストアに対するアクセス許可を付与または破棄します。`--grant` オプションまたは `--revoke` オプションを使用します。

ストアの所有者は、権限の付与と破棄を含めすべての操作を実行できます。ローカルの vCenter Single Sign-On ドメインの管理者（デフォルトは administrator@vsphere.local）は、権限の付与と破棄を含め、すべてのストアの全権限を持ちます。

`vecs-cli get-permissions --name <store-name>` を使用して、ストアの現在の設定を取得できます。

オプション	説明
`--name <name>`	証明書ストアの名前。
`--user <username>`	アクセス許可が付与されるユーザーの一意の名前。
`--grant [read|write]`	付与するアクセス許可（読み取りまたは書き込み）。
`--revoke [read|write]`	破棄するアクセス許可(読み取りまたは書き込み)。現在サポートされていません。

vecs-cli store get-permissions

ストアから現在の権限設定を取得します。

オプション	説明
`--name <name>`	証明書ストアの名前。
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

vecs-cli entry create

VECS にエントリを作成します。このコマンドを使用して、プライベート キーまたは証明書をストアに追加します。

オプション	説明
`--store <NameOfStore>`	証明書ストアの名前。
`--alias <Alias>`	証明書のオプションのエイリアス。このオプションは、信頼されたルート ストアでは無視されます。
`--cert <certificate_file_path>`	証明書ファイルのフル パス。
`--key <key-file-path>`	証明書に対応するキーのフル パス。 オプション。
`--password <password>`	プライベート キーを暗号化するための、オプションのパスワードです。

オプション	説明
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

vecs-cli entry list

指定したストア内のすべてのエントリのリストを表示します。

オプション	説明
`--store <NameOfStore>`	証明書ストアの名前。

vecs-cli entry getcert

VECS から証明書を取得します。証明書を出力ファイルに送信するか、人間が解読可能なテキストとして表示できます。

オプション	説明
`--store <NameOfStore>`	証明書ストアの名前。
`--alias <Alias>`	証明書のエイリアス。
`--output <output_file_path>`	証明書を書き込むファイル。
`--text`	人間が解読可能な証明書のバージョンを表示します。
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

vecs-cli entry getkey

VECS に格納されているキーを取得します。キーを出力ファイルに送信するか、人間が解読可能なテキストとして表示できます。

オプション	説明
`--store <NameOfStore>`	証明書ストアの名前。
`--alias <Alias>`	キーのエイリアス。
`--output <output_file_path>`	キーを書き込む出力ファイル。

オプション	説明
`--text`	人間が解読可能なキーのバージョンを表示します。
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

vecs-cli entry delete

証明書ストア内のエントリを削除します。VECS 内のエントリを削除すると、そのエントリは VECS から完全に削除されます。唯一の例外は、現在のルート証明書です。VECS は vmdir をポーリングして、ルート証明書を確認します。

オプション	説明
`--store <NameOfStore>`	証明書ストアの名前。
`--alias <Alias>`	削除するエントリのエイリアス。
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。
`-y`	確認を求めるプロンプトを抑制します。上級ユーザー専用です。

vecs-cli force-refresh

VECS を強制的に更新します。デフォルトでは、VECS は 5 分ごとに vmdir をポーリングして、新しいルート証明書を確認します。vmdir 内の VECS を直ちに更新する場合は、このコマンドを使用します。

オプション	説明
`--server <server-name>`	リモート VECS インスタンスに接続する場合に、サーバ名を指定するために使用します。
`--upn <user-name>`	`--server <server-name>` で指定するサーバ インスタンスにログインするためのユーザー プリンシパル名。ストアは、作成するユーザーの環境で作成されます。したがって、ストアの所有者は必ずしも root ユーザーではなく、現在のユーザーに紐づいています。

dir-cli コマンド リファレンス

dir-cli ユーティリティは、VMware Directory Service (vmdir) におけるソリューション ユーザーの作成と更新、アカウント管理、および証明書とパスワードの管理をサポートします。また、Platform Services Controller インスタンスのドメイン機能レベルの管理およびクエリに、dir-cli を使用できます。

dir-cli nodes list

指定された Platform Services Controller インスタンスのすべての vCenter Server システムをリストします。

オプション	説明
--login <admin_user_id>	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。
--server <psc_ip_or_fqdn>	アフィニティ化された Platform Services Controller を対象にしない場合は、このオプションを使用します。Platform Services Controller の IP アドレスまたは完全修飾ドメイン名 (FQDN) を指定します。

dir-cli computer password-reset

ドメインのマシン アカウントのパスワードをリセットすることができます。このオプションは、Platform Services Controller インスタンスをリストアする場合に役に立ちます。

オプション	説明
--login <admin_user_id>	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
--password <admin_password>	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。
--live-dc-hostname <server name>	Platform Services Controller インスタンスの現在の名前。

dir-cli service create

ソリューション ユーザーを作成します。主にサードパーティ製ソリューションで使用されます。

オプション	説明
--name <name>	作成するソリューション ユーザーの名前。
--cert <cert file>	証明書ファイルへのパス。VMCA で署名された証明書またはサードパーティ証明書を指定できます。
--ssogroups <comma-separated-groupnames>	ソリューション ユーザーを指定されたグループのメンバーにします。
--wstrustrole <ActAsUser>	ソリューション ユーザーを組み込みの管理者またはユーザー グループのメンバーにします。つまり、ソリューション ユーザーに管理者権限を付与するかどうかを決定します。

オプション	説明
`--ssoadminrole <Administrator/User>`	ソリューション ユーザーを ActAsUser グループのメンバーにします。ActAsUser ロールを持つユーザーは、他のユーザーに代わって作業できるようになります。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli service list

`dir-cli` で認識されるソリューション ユーザーをリストします。

オプション	説明
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli service delete

vmdir のソリューション ユーザーを削除します。ソリューション ユーザーを削除すると、vmdir のこのインスタンスを使用するすべての管理ノードで、関連するサービスがすべて使用できなくなります。

オプション	説明
`--name`	削除するソリューション ユーザーの名前。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli service update

指定したソリューション ユーザー（つまり、サービスのコレクション）の証明書を更新します。このコマンドを実行すると、5 分後に VECS によって変更が取得されます。または、`vecs-cli force-refresh` を使用して強制的に更新することもできます。

オプション	説明
`--name <name>`	更新するソリューション ユーザーの名前。
`--cert <cert_file>`	サービスに割り当てる証明書の名前。

オプション	説明
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli user create

vmdir 内に一般ユーザーを作成します。このコマンドは、ユーザー名とパスワードを使用して vCenter Single Sign-On の認証を受けるユーザー（人）に使用できます。このコマンドは、プロトタイピング時にのみ使用します。

オプション	説明
`--account <name>`	作成する vCenter Single Sign-On ユーザーの名前。
`--user-password <password>`	ユーザーの初期パスワード。
`--first-name <name>`	ユーザーの名。
`--last-name <name>`	ユーザーの姓。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli user modify

vmdir 内の指定したユーザーを変更します。

オプション	説明
`--account <name>`	変更する vCenter Single Sign-On ユーザーの名前。
`--password-never-expires`	Platform Services Controller の認証を受ける必要のある自動化タスクにユーザー アカウントを作成し、パスワードの有効期限切れによってタスクの実行を停止しないようにするには、このオプションを True に設定します。 このオプションは慎重に使用してくだい。
`--password-expires`	`--password-never-expires` オプションを元に戻すには、このオプションを True に設定します。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli user delete

vmdir 内の指定したユーザーを削除します。

オプション	説明
`--account <name>`	削除する vCenter Single Sign-On ユーザーの名前。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli user find-by-name

vmdir 内のユーザーを名前で検索します。このコマンドが返す情報は、`--level` オプションでの指定によって異なります。

オプション	説明
`--account <name>`	削除する vCenter Single Sign-On ユーザーの名前。
`--level <info level 0|1|2>`	次の情報を返します。 ■ レベル 0 - アカウントと UPN ■ レベル 1 - レベル 0 の情報と姓名 ■ レベル 2 - レベル 0 とアカウント無効のフラグ、アカウント ロックのフラグ、パスワード無期限のフラグ、パスワード期限切れのフラグ、およびパスワード有効期限のフラグ デフォルト レベルは 0 です。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli group modify

すでに存在するグループにユーザーまたはグループを追加します。

オプション	説明
`--name <name>`	vmdir のグループの名前。
`--add <user_or_group_name>`	追加するユーザーまたはグループの名前。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli group list

指定した vmdir グループをリストします。

オプション	説明
`--name <name>`	vmdir のグループのオプション名。このオプションによって、特定のグループが存在するかどうかを確認することができます。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli ssogroup create

ローカル ドメイン（デフォルトでは vsphere.local）内にグループを作成します。

グループを作成して vCenter Single Sign-On ドメインのユーザー権限を管理するには、このコマンドを使用します。たとえば、グループを作成し、そのグループを vCenter Single Sign-On ドメインの管理者グループに追加する場合、そのグループに追加されるすべてのユーザーはドメインに対する管理者権限を与えられます。

また、vCenter Single Sign-On ドメインのグループに対して、vCenter Server のインベントリ オブジェクトへのアクセス権限を付与することもできます。『vSphere のセキュリティ』ドキュメントを参照してください。

オプション	説明
`--name <name>`	vmdir のグループの名前。最大文字数は 487 文字です。
`--description <description>`	グループの説明（オプション）。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli trustedcert publish

信頼済みルート証明書を vmdir に発行します。

オプション	説明
`--cert <file>`	証明書ファイルへのパス。
`--crl <file>`	このオプションは VMware 認証局 (VMCA) ではサポートされません。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。
`--chain`	チェーン証明書を公開している場合は、このオプションを指定します。オプションの値は必要ありません。

dir-cli trustedcert publish

信頼済みルート証明書を vmdir に発行します。

オプション	説明
`--cert <file>`	証明書ファイルへのパス。
`--crl <file>`	このオプションは VMware 認証局 (VMCA) ではサポートされません。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。
`--chain`	チェーン証明書を公開している場合は、このオプションを指定します。オプションの値は必要ありません。

dir-cli trustedcert unpublish

現在 vmdir にある信頼済みルート証明書を発行解除します。たとえば、現在の使用環境の他のすべての証明書のルート証明書となっている別のルート証明書を vmdir に追加した場合、このコマンドを使用します。使用されなくなった証明書の発行解除は、使用環境の堅牢化に寄与します。

オプション	説明
`--cert-file <file>`	発行解除する証明書ファイルへのパス。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli trustedcert list

すべての信頼済みルート証明書と対応する ID をリストします。`dir-cli trustedcert get` を使用して証明書を取得するには、証明書 ID が必要です。

オプション	説明
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli trustedcert get

vmdir から信頼済みルート証明書を取得し、指定したファイルに書き込みます。

オプション	説明
`--id <cert_ID>`	取得する証明書の ID。 `dir-cli trustedcert list` コマンドは ID を示します。
`--outcert <path>`	証明書ファイルの書き込み先のパス。
`--outcrl <path>`	CRL ファイルの書き込み先のパス。現在使用されていません。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli password create

パスワード要件を満たす、ランダムなパスワードを作成します。このコマンドは、サードパーティ製ソリューションユーザーが使用できます。

オプション	説明
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli password reset

管理者がユーザーのパスワードをリセットできるようにします。管理者以外のユーザーがパスワードをリセットするには、代わりに `dir-cli password change` を使用します。

オプション	説明
`--account`	新しいパスワードを割り当てるアカウントの名前。
`--new`	指定されたユーザーの新しいパスワード。
`--login <admin_user_id>`	デフォルトでは、ローカル vCenter Single Sign-On ドメインの管理者は administrator@vsphere.local です。
`--password <admin_password>`	管理者ユーザーのパスワード。パスワードを指定していない場合、入力を求められます。

dir-cli password change

ユーザーがパスワードを変更できるようにします。この変更を行うアカウントを所有するユーザーである必要があります。管理者は `dir-cli password reset` を使用して、パスワードをリセットできます。

オプション	説明
--account	アカウント名。
--current	アカウントを所有するユーザーの現在のパスワード。
--new	アカウントを所有するユーザーの新しいパスワード。

Platform Services Controller のトラブルシューティング

5

以降のトピックでは、Platform Services Controller のトラブルシューティングを開始するにあたって役立つ情報を提供します。その他の情報については、ドキュメント センターおよび VMware ナレッジ ベースを検索してください。

この章には、次のトピックが含まれています。

Lookup Service エラーの原因の特定

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

問題

vCenter Server および Web Client のインストーラには、エラー「`Could not contact Lookup Service. Please check VM_ssoreg.log...`」が表示されます。

原因

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

解決方法

1. vCenter Single Sign-On、vCenter Server および Web Client を実行しているホスト マシンのクロックが同期していることを確認してください。
2. エラー メッセージに含まれる特定のログ ファイルを確認します。

   メッセージでは、システム一時フォルダが `%TEMP%` を参照します。

3 ログ ファイル内で、次のメッセージを検索します。

ログ ファイルには、すべてのインストールの試みからの出力が含まれます。`Initializing registration provider...` を示す最新のメッセージを見つけます。

メッセージ	原因と解決策
java.net.ConnectException: Connection timed out: connect	IP アドレスが正しくないか、ファイアウォールが vCenter Single Sign-On へのアクセスをブロックしているか、vCenter Single Sign-On に負荷がかかりすぎています。 ファイアウォールが vCenter Single Sign-On ポート（デフォルトで 7444）をブロックしていないことを確認します。vCenter Single Sign-On がインストールされているマシンに、CPU、I/O、および RAM の十分な空き容量があることも確認します。
java.net.ConnectException: Connection refused: connect	IP アドレスまたは FQDN が不正であり、vCenter Single Sign-On サービスが起動していないか、経過分数以内に起動しませんでした。 vCenter Single Sign-On サービスのステータス（Windows）および vmware-sso デーモン（Linux）をチェックして、vCenter Single Sign-On が動作していることを確認してください。 サービスを再起動してください。再起動しても問題が解決しない場合は、『vSphere トラブルシューティング ガイド』のリカバリのセクションを参照してください。
Unexpected status code: 404. SSO Server failed during initialization	vCenter Single Sign-On を再起動してください。再起動しても問題が解決しない場合は、『vSphere トラブルシューティング ガイド』の復旧のセクションを参照してください。
ユーザー インターフェイスに表示されるエラーは「Could not connect to vCenter Single Sign-On」から始まります。	戻りコード `SslHandshakeFailed` が表示される場合もあります。このエラーは、提供された IP アドレスまたは vCenter Single Sign-On ホストを解決する FQDN が、vCenter Single Sign-On のインストール時に使用されたアドレスではないことを示しています。 `%TEMP%\VM_ssoreg.log` で、次のメッセージを含む行を探します。 「`host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>`」。ここで A は vCenter Single Sign-On のインストール時に入力した FQDN であり、B と C はシステムが生成した許容される代替ドメイン名です。 ログ ファイル中の != の記号の右側で、FQDN を使用するよう設定を修正します。ほとんどの場合、vCenter Single Sign-On のインストール時に指定した FQDN を使用してください。 お使いのネットワーク構成でいずれの代案も使用できない場合は、vCenter Single Sign-On の SSL 構成を復旧してください。

Active Directory ドメイン認証を使用してログインできない

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

問題

Active Directory の ID ソースを vCenter Single Sign-On に追加しましたが、ユーザーが vCenter Server にログインできません。

原因

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

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

解決方法

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

Active Directory フォレスト内の子ドメインを使用して統合 Windows 認証 ID ソースを構成する方法については、VMware のナレッジベースの記事 (http://kb.vmware.com/kb/2070433) を参照してください。統合 Windows 認証では、デフォルトで Active Directory フォレストのルート ドメインを使用します。

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

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

2 それぞれのドメイン コントローラに Active Directory ドメイン DNS サービス内のポインタ レコード (PTR) があることを確認します。

ドメイン コントローラの PTR レコード情報が、コントローラの DNS 名と一致することを確認します。vCenter Server Appliance を使用している場合は、次のコマンドを実行してタスクを行います。

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

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

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

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

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

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

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

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

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

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

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

3 問題が解決しない場合は、vCenter Server Appliance を Active Directory ドメインから削除し、再度ドメインに参加させます。『vCenter Server Appliance の構成』ドキュメントを参照してください。

4 vCenter Server Appliance に接続されているすべてのブラウザ セッションを閉じ、すべてのサービスを再起動します。

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

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

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

問題

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

原因

ログイン失敗の最大数を超えました。

解決方法

- システム ドメイン（デフォルトは vsphere.local）のユーザーとしてログインを試みる場合、vCenter Single Sign-On 管理者に問い合わせてアカウントのロックを解除してもらいます。ロックアウト ポリシーでロックの期限が設定されている場合、アカウントのロックが解除されるまで待つことができます。vCenter Single Sign-On 管理者は CLI コマンドを使用してアカウントのロックを解除できます。
- Active Directory または LDAP ドメインのユーザーとしてログインする場合、Active Directory または LDAP 管理者に問い合わせてアカウントのロックを解除してもらいます。

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

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

問題

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

原因

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

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

解決方法

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

Platform Services Controller サポート バンドルのエクスポート

Platform Services Controller サービスのログ ファイルが含まれているサポート バンドルをエクスポートできます。エクスポートの後、ログをローカルで参照するか、バンドルを VMware サポートに送信することができます。

前提条件

Platform Services Controller 仮想アプライアンスが正常にデプロイされ、実行されていることを確認します。

手順

1. Web ブラウザで、https://*platform_services_controller_ip*:5480 の Platform Services Controller 管理インターフェイスに接続します。
2. 仮想アプライアンスの root ユーザーとしてログインします。
3. [アクション] メニューで [サポート バンドルの作成] を選択します。
4. ブラウザの設定で即時ダウンロードが禁止されていなければ、サポート バンドルがローカル マシンに保存されます。

Platform Services Controller サービス ログのリファレンス

Platform Services Controller サービスは、Syslog を記録に使用します。ログ ファイルを確認し、エラーの理由を判断することができます。

次の表に、vCenter Server Appliance のログの場所を示します。Windows のデプロイの場合、ほとんどのログは `C:\ProgramData\VMware\vCenterServer\logs` ディレクトリにあります。

表 5-1. サービス ログ

サービス	説明
VMware Directory Service	デフォルトでは、vmdir のログは /var/log/messages または /var/log/vmware/vmdird/ に記録されます。 デプロイ時の問題については、/var/log/vmware/vmdir/vmafdvmdirclient.log にトラブルシューティングにも有用なデータが含まれている場合があります。
VMware のシングル サインオン	vCenter Single Sign-On のログは /var/log/vmware/sso/ に記録されます。
VMware Certificate Authority (VMCA)	VMCA サービスのログは /var/log/vmware/vmcad/vmcad-syslog.log にあります。
VMware Endpoint Certificate Store (VECS)	VECS サービスのログは /var/log/vmware/vmafdd/vmafdd-syslog.log にあります。
VMware Lookup Service	Lookup Service のログは /var/log/vmware/sso/lookupServer.log にあります。