vSphere 認証

Update 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

vmware
by Broadcom

VMware by Broadcom の Web サイトで最新の技術ドキュメントを確認できます

https://docs.vmware.com/jp/

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

目次

vSphere の認証について　7

1 vSphere 証明書の管理と認証の概要　9

vCenter Server 証明書の管理　11

vSphere Client を使用した vCenter Server 証明書の管理　11

CLI を使用した vCenter Server 証明書の管理　12

vCenter Server 認証サービスの管理　13

vSphere Client を使用した vCenter Server 認証サービスの管理　13

スクリプトを使用した vCenter Server 認証サービスの管理　14

vCenter Server の管理　14

管理インターフェイスを使用した vCenter Server の管理　15

vCenter Server シェルを使用した vCenter Server の管理　15

Active Directory ドメインへの vCenter Server の追加　16

2 vSphere セキュリティ証明書　17

異なるソリューション パスに対する vSphere 証明書の要件　18

vSphere 証明書管理　22

vSphere 証明書の置き換え　24

vSphere で証明書を使用する場合　27

VMware Certificate Authority と VMware Core Identity Services　30

VMware Endpoint Certificate Store　30

vSphere 証明書の失効の管理　32

大規模環境での vSphere 証明書の置き換え　32

vSphere Client を使用した証明書の管理　34

vSphere Client を使用した証明書ストアの検索　35

vSphere Client を使用した vCenter Server 証明書の有効期限の警告に対するしきい値の設定　35

vSphere Client を使用した新しい VMCA 署名付き証明書への VMCA 証明書の更新　36

vSphere Client を使用したカスタム証明書による証明書の置き換え　36

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　37

vSphere Client を使用した証明書ストアへの信頼できるルート証明書の追加　38

vSphere Client を使用したカスタム証明書の追加　39

VMCA リーフ証明書の生成　40

vSphere Certificate Manager ユーティリティを使用した証明書の管理　41

Certificate Manager を使用した新しい 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　42

Certificate Manager を使用して VMCA を中間認証局にする　43

Certificate Manager を使用した CSR の生成とルート証明書（中間 CA）の用意　44

Certificate Manager を使用した VMCA ルート証明書のカスタム署名証明書への置き換えと、すべての証明書の置き換え 46
Certificate Manager を使用したマシン SSL 証明書の VMCA 証明書（中間 CA）への置き換え 47
Certificate Manager を使用したソリューション ユーザー証明書の VMCA 証明書（中間 CA）への置き換え 48
Certificate Manager を使用したすべての証明書のカスタム証明書への置き換え 49
Certificate Manager を使用した証明書署名リクエストの生成（カスタム証明書） 50
Certificate Manager を使用したマシン SSL 証明書のカスタム証明書への置き換え 51
Certificate Manager を使用したソリューション ユーザー証明書のカスタム証明書への置き換え 52
Certificate Manager を使用した古い証明書の再発行による直近の操作の取り消し 53
Certificate Manager を使用したすべての証明書のリセット 54
手動での vSphere 証明書の置き換え 54
vCenter Server サービスの停止と開始のガイドライン 54
CLI を使用した既存の VMCA 署名証明書の新しい VMCA 署名証明書への置き換え 55
CLI を使用した新しい VMCA 署名付きルート証明書の生成 55
CLI を使用したマシン SSL 証明書の VMCA 署名証明書への置き換え 56
CLI を使用した新規 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 59
CLI を使用して VMCA を中間認証局にする 64
CLI を使用したルート証明書（中間 CA）の置き換え 64
CLI を使用したマシン SSL 証明書（中間 CA）の置き換え 67
CLI を使用したソリューション ユーザー証明書（中間 CA）の置き換え 69
CLI を使用したカスタム証明書による証明書の置き換え 74
CLI を使用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 74
CLI を使用したマシン SSL 証明書のカスタム証明書への置き換え 76

3 vSphere 証明書とサービス CLI コマンド リファレンス 78
certool 初期化コマンド リファレンス 81
certool 管理コマンド リファレンス 84
vecs-cli コマンド リファレンス 86
dir-cli コマンド リファレンス 92

4 vCenter Single Sign-On による vSphere 認証 100
vCenter Single Sign-On によって環境を保護する方法 101
vCenter Server ID プロバイダ フェデレーション 105
vCenter Server ID プロバイダ フェデレーションの機能 105
vCenter Server ID プロバイダ フェデレーションに関する注意事項と相互運用性 109
vCenter Server ID プロバイダ フェデレーションのライフサイクル 111
vCenter Server ID プロバイダ フェデレーションと拡張リンク モード 112
拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセス 117
vCenter Server ID プロバイダ フェデレーションの設定 119
vCenter Server ID プロバイダ フェデレーション設定プロセス フロー 119
JRE トラストストアの代替としての信頼済みルート証明書ストアの使用 122

AD FS に対する vCenter Server ID プロバイダ フェデレーションの構成 123
Okta に対する vCenter Server ID プロバイダ フェデレーションの構成 127
Microsoft Entra ID に対する vCenter Server ID プロバイダ フェデレーションの構成 131
PingFederate の vCenter Server ID プロバイダの構成 135
範囲の作成 137
PingFederate ワークフローの共通構成の作成 138
パスワード付与フロー構成の作成 141
認可コード フロー構成の作成 144
SCIM Provisioner のインストール 147
PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成 148
SCIM アプリケーション（SP 接続）の作成 150
PingFederate 認証用の vCenter Server の構成 154
VMware Single Sign-On の構成 154
VMware Identity Services の管理 156
VMware Identity Services の停止と起動 156
vCenter Server での SCIM トークンの再生成 157
削除された SCIM ユーザーおよびグループのリストア 158
vCenter Single Sign-On 158
vCenter Single Sign-On コンポーネント 158
vSphere での vCenter Single Sign-On の使用 159
vCenter Single Sign-On ドメイン内のグループ 161
vCenter Single Sign-On ID ソースの設定 164
vCenter Single Sign-On による vCenter Server の ID ソース 164
vCenter Single Sign-On 用のデフォルト ドメインの設定 165
vCenter Single Sign-On ID ソースの追加または編集 166
LDAP [Lightweight Directory Access Protocol] を介した Active Directory および OpenLDAP Server ID ソースの設定 167
Active Directory ID ソースの設定 170
CLI を使用した ID ソースの追加または削除 171
vCenter Server Security Token Service の管理 172
vSphere Client を使用した vCenter Server STS 証明書の更新 173
vSphere Client を使用した vCenter Server STS 証明書のインポートと置き換え 175
コマンド ラインを使用した vCenter Server STS 証明書の置き換え 176
vSphere Client を使用したアクティブな vCenter Server STS 署名証明書チェーンの表示 177
コマンド ラインを使用した LDAPS SSL 証明書の有効期限の特定 178
vCenter Single Sign-On ポリシーの管理 178
vCenter Single Sign-On のパスワード ポリシーの編集 179
vCenter Single Sign-On のロックアウト ポリシーの編集 180
vCenter Single Sign-On のトークン ポリシーの編集 181
Active Directory（統合 Windows 認証）ユーザーへのパスワード有効期限の通知の編集 182
vCenter Single Sign-On ユーザーおよびグループの管理 183
vCenter Single Sign-On ユーザーの追加 183

vCenter Single Sign-On ユーザーの無効化と有効化　184
vCenter Single Sign-On ユーザーの削除　185
vCenter Single Sign-On ユーザーの編集　185
vCenter Single Sign-On グループの追加　186
vCenter Single Sign-On グループへのメンバーの追加　187
vCenter Single Sign-On グループからのメンバーの削除　188
vCenter Single Sign-On パスワードの変更　188
その他の vSphere の認証オプション　189
スマート カード認証ログイン　190
スマート カード認証の設定と使用　191
クライアント証明書を要求するための vCenter Server の構成　191
vSphere Client を使用したスマート カード認証の管理　193
CLI を使用したスマート カード認証の管理　195
スマート カード認証の失効ポリシーの設定　198
RSA SecurID 認証の設定　199
vSphere Client ログイン画面のログイン メッセージの管理　202
vSphere Client ログイン画面のログイン メッセージの管理　202
vCenter Single Sign-On のセキュリティのベスト プラクティス　202

5 vCenter Server 認証のトラブルシューティング　204
Lookup Service エラーの原因の特定　204
Active Directory ドメイン認証を使用してログインできない　205
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　207
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　207
vCenter Server サポート バンドルのエクスポート　208
vCenter Server 認証サービス ログのリファレンス　208

vSphere の認証について

『vSphere の認証』ドキュメントでは、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。

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

『vSphere の認証』では、vCenter Server の証明書および関連するサービスを管理し、vCenter Single Sign-On を使用して認証を設定する方法について説明します。

表 1-1. vSphere の認証の特徴

トピック	内容
認証の基本操作	■ 認証サービスの管理。 ■ vCenter Server 管理インターフェイスを使用した vCenter Server 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。
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。 ■ vCenter Server ID プロバイダ フェデレーション

Platform Services Controller に対する変更点

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

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

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

対象読者

本書は、vCenter Server 認証の設定および証明書を管理する管理者を対象にしています。ここに記載の情報は、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 証明書の管理と認証の概要 1

vSphere は、vCenter Server と ESXi の両方のコンポーネントに関する証明書の管理と、vCenter Single Sign-On による認証の管理のための共通インフラストラクチャ サービスを提供します。

vSphere 証明書の管理方法

デフォルトでは、vSphere によって VMware Certificate Authority (VMCA) 証明書を使用して vCenter Server コンポーネントおよび ESXi ホストをプロビジョニングできます。VMware Endpoint Certificate Store (VECS) に格納されているカスタム証明書を使用することもできます。詳細については、『vSphere 証明書の管理に必要なオプション』を参照してください。

vCenter Single Sign-On について

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 では独自の用語と定義が使用されており、これらを理解することが重要です。

表 1-1. vCenter Single Sign-On 用語集

用語	定義
プリンシパル	ユーザーなどの認証可能なエンティティ。
ID プロバイダ	ID ソースを管理し、プリンシパルを認証するサービス。例：Microsoft Active Directory フェデレーション サービス (AD FS) および vCenter Single Sign-On。
ID ソース（ディレクトリ サービス）	プリンシパルを格納および管理します。プリンシパルは、ユーザーまたはサービス アカウントに関する属性（名前、アドレス、E メール、グループ メンバーシップなど）のコレクションで構成されます。例：Microsoft Active Directory および VMware Directory Service (vmdir)。
認証	誰かまたは何かが、実際に自身で宣言しているとおりの人または物であるかどうかを判断するための手段。たとえば、ユーザーは、スマート カード、ユーザー名、正しいパスワードなどの認証情報を入力すると認証されます。
認可	プリンシパルがアクセスできるオブジェクトを確認するプロセス。

表 1-1. vCenter Single Sign-On 用語集 （続き）

用語	定義
トークン	特定のプリンシパルの ID 情報を構成するデータの署名付きコレクション。トークンには、そのタイプによってはメール アドレスやフル ネームなどのプリンシパルに関する基本的な情報だけでなく、プリンシパルのグループとロールも含まれることがあります。
vmdir	VMware Directory Service。ユーザー ID、グループ、および設定データを格納する vCenter Server 内の内部（ローカル）LDAP リポジトリ。
OAuth 2.0	プリンシパルの認証情報を公開することなく、プリンシパルと Web サービス間で情報を交換できるようにする認可のオープン スタンダード。
OpenID Connect (OIDC)	OAuth をユーザー識別情報で強化する、OAuth 2.0 に基づく認証プロトコル。これは、OAuth 認証中に認証サーバからアクセス トークンと一緒に返される ID トークンで表されます。vCenter Server では、Active Directory フェデレーション サービス (AD FS)、Okta、Microsoft Entra ID、PingFederate とのやり取りに OIDC 機能が使用されます。
クロスドメイン ID 管理 (SCIM) のシステム	ID ドメイン間または IT システム間でユーザー ID 情報の交換を自動化するための標準。
VMware Identity Services	バージョン 8.0 Update 1 以降では、VMware Identity Services は、外部 ID プロバイダへの ID フェデレーションに使用できる vCenter Server 内の組み込みコンテナです。vCenter Server 内の独立した ID ブローカとして機能し、独自の API セットが付属しています。現在、VMware Identity Services では Okta、Microsoft Entra ID、PingFederate が外部 ID プロバイダとしてサポートされています。
テナント	VMware Identity Services の概念。テナントにより、同一の仮想環境内で、データは他のテナントのデータから論理的に分離されます。
JSON Web トークン (JWT)	OAuth 2.0 仕様によって定義されたトークン形式。JWT トークンは、プリンシパルに関する認証および認可情報を伝送します。
証明書利用者	証明書利用者は、ID 管理に認可サーバ（VMware Identity Services または AD FS）を「利用」します。たとえば、vCenter Server はフェデレーションを介して、VMware Identity Services または AD FS に対する証明書利用者の信頼を確立します。
Security Assertion Markup Language (SAML)	vCenter Server で使用される、関係者間で認証および認可データを交換するための XML ベースのオープン標準。プリンシパルが vCenter Single Sign-On から SAML トークンを取得し、セッション ID 用の vSphere Automation API エンドポイントに送信します。

vCenter Single Sign-On 認証タイプについて

vCenter Single Sign-On では、組み込みの vCenter Server ID プロバイダと外部 ID プロバイダのどちらが関係するかに応じて、異なるタイプの認証が使用されます。

表 1-2. vCenter Single Sign-On 認証タイプ

認証タイプ	ID プロバイダとして機能するもの	vCenter Server はパスワードを処理するか	説明
トークンベースの認証	外部 ID プロバイダ。たとえば、AD FS です。	なし	vCenter Server は、特定のプロトコルを介して外部の ID プロバイダと通信し、特定のユーザーを識別するトークンを取得します。
単純な認証	vCenter Server	はい	ユーザー名とパスワードが vCenter Server に直接渡され、そこで ID ソースによって認証情報が検証されます。

次のトピックを参照してください。

- vCenter Server 証明書の管理
- vCenter Server 認証サービスの管理
- vCenter Server の管理

vCenter Server 証明書の管理

vCenter Server 証明書は vSphere Client から管理するか、API、スクリプト、または CLI を使用して管理します。

次の表に、vCenter Server 証明書の管理に使用できるインターフェイスを示します。

表 1-3. vSphere 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	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 を使用した証明書の管理を参照してください。
vSphere Automation API	『VMware vSphere Automation SDKs Programming Guide』を参照してください。
証明書管理ユーティリティ	証明書署名リクエスト (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 ユーティリティを使用した証明書の管理を参照してください。
証明書およびディレクトリの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。3 章 vSphere 証明書とサービス CLI コマンド リファレンスを参照してください。

vSphere Client を使用した vCenter Server 証明書の管理

vSphere Client から vCenter Server 証明書を管理することができます。

手順

1 ローカルの vCenter Single Sign-On ドメインの管理者権限を持つユーザーとして vCenter Server にログインします。

デフォルトのドメインは vsphere.local です。

2 [管理] を選択します。

3 [証明書] で、[証明書の管理] をクリックします。

さまざまなタイプの証明書の証明書タブが表示されます。

4 証明書の詳細の表示、証明書の更新、信頼できるルート証明書の追加などの証明書タスクを実行します。

詳細については、『vSphere Client を使用した証明書の管理』を参照してください。

CLI を使用した vCenter Server 証明書の管理

vCenter Server には、証明書署名リクエスト (CSR) の生成、証明書の管理、およびサービスの管理を行うための CLI が用意されています。

たとえば、`certool` コマンドを使用して CSR を生成し、証明書を置き換えることができます。

vSphere Client 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. vCenter Server 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。VMware Certificate Authority (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。VMware Authentication Framework Daemon (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`	Security Token Service (STS) 証明書を更新します。	コマンド ラインを使用した vCenter Server STS 証明書の置き換え
`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。

前提条件

vCenter Server への SSH ログインを有効にします。vCenter Server 管理インターフェイス (`https://vcenter_server_ip:5480`) の [アクセス] タブを使用して、SSH ログインの有効化や無効化を設定できます。

手順

1 vCenter Server シェルにログインします。

通常、root ユーザーまたは管理者ユーザーの権限が必要です。詳細については、vSphere 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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

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

詳細については、『手動での vSphere 証明書の置き換え』を参照してください。

vCenter Server 認証サービスの管理

認証サービスは、vSphere Client から、または CLI を使用して管理します。API を使用して vCenter Server ID プロバイダ フェデレーション構成プロセスを管理することもできます。

さまざまなインターフェイスを使用して vCenter Server 認証を管理できます。

表 1-5. vCenter Server 認証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）。
API	vCenter Server ID プロバイダのフェデレーション構成プロセスを管理します。
`sso-config`	vCenter Server の組み込み ID プロバイダを設定するためのコマンドライン ユーティリティ。

vSphere Client を使用した vCenter Server 認証サービスの管理

vSphere Client から vCenter Server 認証サービスを管理できます。

手順

1 ローカルの vCenter Single Sign-On ドメインの管理者権限を持つユーザーとして vCenter Server にログインします。

デフォルトのドメインは vsphere.local です。

2 [管理] を選択します。

3 [Single Sign On] で [設定] をクリックして ID プロバイダを管理し、パスワードとロックアウト ポリシーを設定します。

詳細については、『4 章 vCenter Single Sign-On による vSphere 認証』を参照してください。

スクリプトを使用した vCenter Server 認証サービスの管理

vCenter Server には、認証サービスを管理するためのユーティリティである `sso-config` が含まれています。

vSphere Client でサポートされていない管理タスクに対して、または自社環境用のカスタム スクリプトを作成する場合は、`sso-config` ユーティリティを使用します。

表 1-6. 認証および関連サービスを管理するための CLI

CLI	説明	リンク
`sso-config`	vCenter Server の組み込み ID プロバイダを設定するためのコマンドライン ユーティリティ。	`sso-config.sh -help` を実行して `sso-config` のヘルプを参照するか、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/67304) で使用例を参照してください。
`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。`service-control` コマンドでパスを指定する必要はありません。

前提条件

vCenter Server への SSH ログインを有効にします。vCenter Server 管理インターフェイス (`https://vcenter_server_ip:5480`) の [アクセス設定] タブを使用して、SSH ログインの有効化や無効化を設定できます。

手順

1 vCenter Server シェルにログインします。

通常、root ユーザーまたは管理者ユーザーの権限が必要です。詳細については、vSphere CLI の実行に必要な権限を参照してください。

2 次のデフォルトの場所にある `sso-config` ユーティリティにアクセスします。

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

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。

vCenter Server の管理

vCenter Server は、vCenter Server 管理インターフェイスまたは vCenter Server シェルを使用して管理できます。

vCenter Server の管理の詳細については、『vCenter Server の構成』を参照してください。

表 1-7. vCenter Server 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
vCenter Server 管理インターフェイス	このインターフェイスを使用して、システムを再設定します。管理インターフェイスを使用した vCenter Server の管理 を参照してください。
vCenter Server 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 ユーティリティを使用した証明書の管理および 3 章 vSphere 証明書とサービス CLI コマンド リファレンスを参照してください。

管理インターフェイスを使用した vCenter Server の管理

vCenter Server 管理インターフェイスを使用して、システムを設定できます。

vCenter Server 管理インターフェイスでの設定には、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。

注： [ネットワーク] ペインでは、仮想 NIC 0 が管理トラフィック用に予約されています。NIC 0 から別の NIC にトラフィックを再割り当てすることはできません。VCHA を使用している場合、このトラフィックでは NIC 1 を使用します。NIC を vCenter Server Appliance に追加できます。詳細については、VMware のナレッジベースの記事 (https://kb.vmware.com/article/2147155) を参照してください。

手順

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

2 信頼されていない 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、vCenter Server のデプロイ時に設定したパスワードです。

結果

vCenter Server 管理インターフェイスの [サマリ] ページが表示されます。

vCenter Server シェルを使用した vCenter Server の管理

vCenter Server 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://*vcenter_server_ip*:5480 にある vCenter Server 管理インターフェイスにログインします。

   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、vCenter Server の Bash シェルを有効にします。

2 シェルにアクセスします。

   - vCenter Server 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、vCenter Server へのセッションを開始します。

3 最初に vCenter Server 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 vCenter Server の追加

Active Directory の ID ソースを vCenter Server に追加する場合は、Active Directory ドメインに vCenter Server を参加させる必要があります。

vCenter Server ID プロバイダ フェデレーション、または LDAPS を介した Active Directory を使用できない場合、vCenter Server は統合 Windows 認証 (IWA) をサポートします。IWA を使用するには、vCenter Server を Active Directory ドメインに参加させる必要があります。

手順

1 vSphere Client を使用して、ローカルの vCenter Single Sign-On ドメイン（デフォルトは vsphere.local）の管理者権限を持つユーザーとして vCenter Server にログインします。

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 [ID プロバイダ] タブで、[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入力して、[参加] をクリックします。

6 vCenter Server を再起動してください。

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-On ID ソースの追加または編集を参照してください。

vSphere セキュリティ証明書

2

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 での証明書の使用方法

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 台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。

VMware 認証局について

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 vCenter Server ホストそれぞれにインストールされ、何らかの変更を加えなくてもすぐにソリューションを保護します。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。

vSphere 証明書の管理に必要なオプション

証明書管理には、次のオプションが推奨されます。

表 2-1. vSphere 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）	vCenter Server 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。

vSphere 証明書の置き換えに使用できるツール

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 2-2. vSphere 証明書を置き換えるための各種アプローチ

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 Client を使用した証明書の管理
vSphere Automation API を使用して、証明書のライフサイクルを管理します。	VMware vSphere Automation SDKs Programming Guide
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 ユーティリティを使用した証明書の管理
CLI コマンドを使用して証明書を手動で置き換える。	3 章 vSphere 証明書とサービス CLI コマンド リファレンス

次のトピックを参照してください。

- 異なるソリューション パスに対する vSphere 証明書の要件
- vSphere 証明書管理
- vSphere Client を使用した証明書の管理
- vSphere Certificate Manager ユーティリティを使用した証明書の管理
- 手動での vSphere 証明書の置き換え

異なるソリューション パスに対する vSphere 証明書の要件

証明書の要件は、VMware 認証局 (VMCA) を中間認証局として使用するか、カスタム証明書を使用するかによって異なります。マシン証明書の要件も異なります。

証明書の変更を開始する前に、vSphere 環境内の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。

注： vSphere は、サーバ認証に RSA 証明書のみをデプロイし、ECDSA 証明書の生成をサポートしません。vSphere は、他のサーバによって提示された ECDSA 証明書を検証します。たとえば、vSphere が Syslog サーバに接続していて、Syslog サーバに ECDSA 証明書がある場合、vSphere はその証明書の検証をサポートします。

すべてのインポートされた vSphere 証明書の要件

- キー サイズ：2,048 ビット（最小）から 8,192 ビット（最大）（PEM エンコード）。vSphere Client および API は、証明書署名リクエストの生成時に、引き続き最大 16,384 ビットのキー サイズを受け入れます。

  注： vSphere 8.0 では、vSphere Client または vSphere Certificate Manager を使用する場合、最小キー長が 3,072 ビットの CSR のみ生成できます。vCenter Server は、キーの長さが 2,048 ビットのカスタム証明書を引き続き受け入れます。vSphere 8.0 Update 1 以降では、vSphere Client を使用して、キーの長さが 2,048 ビットの CSR を生成できます。

  注： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。
- 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。
- vpxd-extension ソリューション ユーザーの証明書を除外して、[拡張キー使用] を空にするか、[サーバ認証] を含めることができます。

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。
- アルゴリズム md2WithRSAEncryption、md5WithRSAEncryption、RSASSA-PSS、dsaWithSHA1、ecdsa_with_SHA1、sha1WithRSAEncryption はサポートされていません。
- vCenter Server 用のカスタム マシン SSL 証明書を作成する場合、サーバ認証とクライアント認証はサポートされません。Microsoft 認証局 (CA) テンプレートを使用する場合は、これらの認証を削除する必要があります。詳細については、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/2112009) を参照してください。

RFC 2253 に対する vSphere 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 vSphere 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 vSphere 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、vSphere 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。
- vSphere 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。
  - vSphere Certificate Manager を実行する vCenter Server ノードの IP アドレス。

注： OU (organizationalUnitName) フィールドは必須ではなくなりました。

VMCA を中間認証局として使用する場合の証明書の要件

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。Certificate Manager を使用した CSR の生成とルート証明書（中間 CA）の用意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（最小）から 8,192 ビット（最大）（PEM エンコード）
	■ PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
	■ x509 バージョン 3
	■ ルート証明書に対しては、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。例：
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ 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 認証局の使用例については、VMware ナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x」(https://kb.vmware.com/s/article/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 を作成することができます。 CSR を手動で作成する場合は、上記の「すべてのインポートされた vSphere 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。 vpxd-extension ソリューション ユーザーの場合は、[拡張キー使用] を空のままにするか、「TLS WWW クライアント認証」を使用できます。

カスタム証明書を使用する場合の要件

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 vSphere 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。 ■ 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 vSphere 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。 **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。 vpxd-extension ソリューション ユーザーの場合は、[拡張キー使用] を空のままにするか、「TLS WWW クライアント認証」を使用できます。

vSphere 証明書管理

vSphere 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。

VMware Certificate Authority 証明書を使用する環境

VMware Certificate Authority (VMCA) はすべての証明書管理を処理できます。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 6.0 以降にアップグレードしている場合、すべての自己署名証明書は 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。

カスタム証明書を使用する環境

企業ポリシーでサードパーティ認証局またはエンタープライズ認証局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 VMware Certificate Endpoint Store (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、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。
- シンプルな vCenter Server の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。既存の vCenter Server および vCenter Single Sign-On の証明書を維持します。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。VMware では、ソリューション ユーザー証明書の置き換えを推奨していません。

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 2-3. 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 Automation API	『VMware vSphere Automation SDKs Programming Guide』を参照してください。
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。
vSphere 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。

表 2-3. vCenter Server 証明書を管理するためのインターフェイス （続き）

インターフェイス	用途
`sso-config` ユーティリティ	STS 証明書管理は、vCenter Server インストールのコマンド ラインから実行します。
PowerCLI 12.4 以降（vSphere 7.0 以降も必要）	信頼されている証明書ストアの管理、vCenter Server マシン SSL 証明書の管理、および ESXi マシン SSL 証明書の管理を実行します。

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 Server 証明書

vCenter Server 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。

vSphere 証明書の置き換え

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。vSphere Client 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。

VMware Certificate Authority (VMCA) は、各 vCenter Server 環境に含まれています。VMware 認証局 (VMCA) は、VMCA を認証局として署名した証明書を使用して、各ノード、各 vCenter Server ソリューション ユーザー、および各 ESXi ホストをプロビジョニングします。

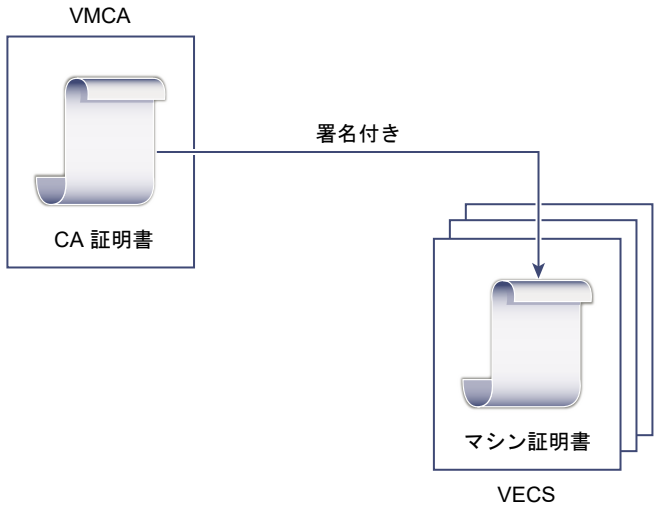
デフォルトの証明書は、置き換えることができます。vCenter Server のコンポーネントの場合は、インストール製品に組み込まれているコマンドライン ツール セットを使用できます。いくつかのオプションが用意されています。

注： vCenter Server が NSX-T Manager にリンクされていて、vCenter Server 証明書を置き換える場合は、vCenter Server コンピュート マネージャのサムプリントを更新する必要があります。『NSX-T Data Center Migration Coordinator ガイド』の「コンピュート マネージャの追加」というタイトル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証明書の置き換え

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 2-1. 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

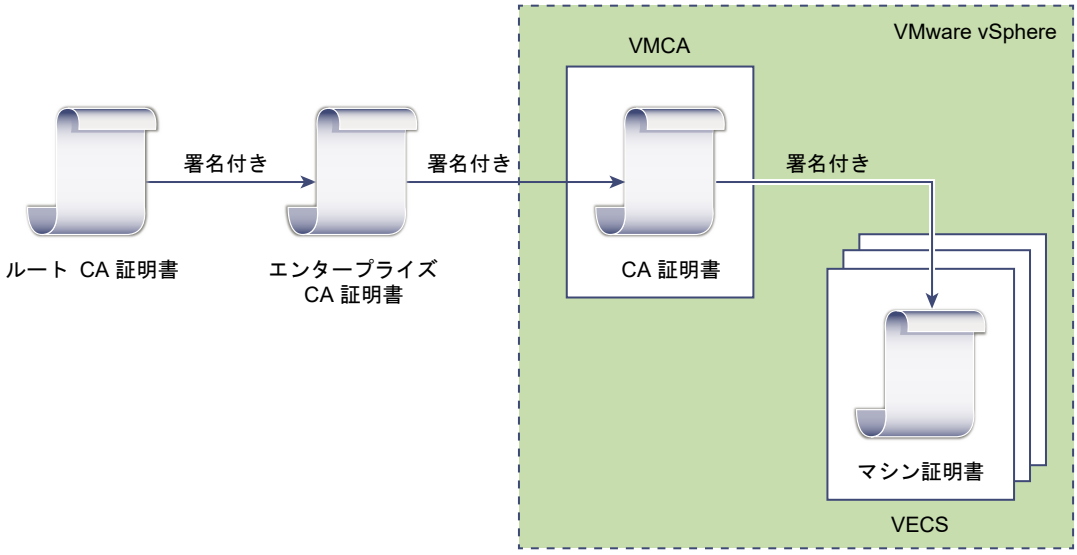
証明書の置き換えの詳細については、「CLI を使用した既存の VMCA 署名証明書の新しい VMCA 署名証明書への置き換え」を参照してください。

VMCA を中間認証局にする

VMCA のルート証明書は、企業認証局 (CA) やサードパーティ CA によって署名された証明書に置き換えることができます。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： vCenter Server 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 2-2. 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。

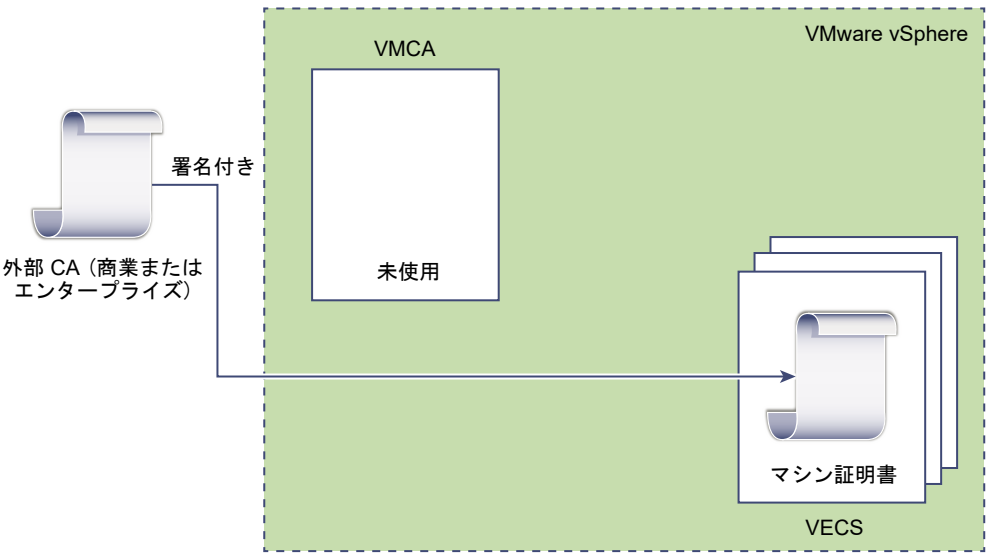
- カスタム署名証明書による VMCA ルート証明書の置き換えと、すべての証明書の置き換え
- マシンの SSL 証明書を VMCA 証明書で置き換える（複数ノード拡張リンク モード デプロイ）
- ソリューション ユーザー証明書を VMCA 証明書で置き換える（複数ノード拡張リンク モード デプロイ）

証明書の置き換えの詳細については、「CLI を使用して VMCA を中間認証局にする」を参照してください。

カスタム証明書による VMCA 署名付き証明書の置き換え

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 2-3. 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、「CLI を使用したカスタム証明書による証明書の置き換え」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 アプローチを使用した証明書の展開

ハイブリッド アプローチでは、証明書の一部は VMCA で提供し、インフラストラクチャのその他の部分に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。

詳細については、「New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement」というブログ記事 (http://vmware.com/go/hybridvmca) を参照してください。

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 2-4. 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 によって署名または発行されていない証明書を、手動で更新して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

Vmware 認証局 (VMCA) は、証明書を使用して環境をプロビジョニングします。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 2-5. vSphere 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）	VMware Endpoint Certificate Store (VECS) に保存されます。
ソリューション ユーザー証明書	VMCA（デフォルト）	VECS に保存されます。
vCenter Single Sign-On SSL 署名証明書	インストール中にプロビジョニングされます。	この証明書はコマンドラインから管理します。 **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、マシン SSL 証明書は vmdir 証明書として使用されます。
SMS 自己署名証明書	IOFilter プロバイダの登録中にプロビジョニングされます。	vSphere 7.0 以降、SMS 自己署名証明書は `/etc/vmware/ssl/iofiltervp_castore.pem` に保存されます。vSphere 7.0 より前のリリースでは、SMS 自己署名証明書は `/etc/vmware/ssl/castore.pem` に保存されます。また、retainVasaProviderCertificate=True の場合、SMS ストアは VVOL VASA プロバイダ（バージョン 4.0 以前）の自己署名証明書を保存することもできます。

ESXi 証明書

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。詳細については、『vSphere のセキュリティ』を参照してください。

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。

vCenter Server ノードごとに専用のマシン SSL 証明書があります。vCenter Server 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。

- 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。
- vCenter Server サービス (vpxd)。
- 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 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 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`：vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに保存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 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。
- `wcp`：VMware vSphere® with VMware Tanzu™ ストア。vSphere クラスタ サービスにも使用されます。

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。

この証明書は CLI から置き換えることができます。コマンド ラインを使用した vCenter Server STS 証明書の置き換え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、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。vSphere の以前のバージョンについては、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 仮想マシン暗号化ソリューションは、キー サーバに接続します。ソリューションがキー サーバに対してどのように認証を行うかによっては、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。

VMware Certificate Authority と VMware Core Identity Services

コア ID サービスは、各 vCenter Server システムの一部です。VMware Certificate Authority (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 2-6. コア ID サービス

サービス	説明
VMware Directory Service (vmdir)	vCenter Single Sign-On を使用した認証の SAML 証明書管理を扱う ID ソース。
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。
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。

VMware Endpoint Certificate Store

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、vCenter Server ノードそれぞれで実行されます。VECS には、証明書とキーが含まれるキーストアが保持されます。

VECS は、更新のため定期的に VMware ディレクトリ サービス (vmdir) を信頼されたルート 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 2-7. 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。 ■ 各 vCenter Server 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。
ソリューション ユーザー ストア ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp	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、他の証明書属性は確認しません。 次のソリューション ユーザー証明書ストアが 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：vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに保存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 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。 ■ wcp：VMware vSphere® with VMware Tanzu™ ストア。vSphere クラスタ サービスにも使用されます。 各 vCenter Server ノードには machine 証明書が含まれます。
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 2-7. 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、CLI 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。

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。

vSphere 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 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 vSphere 証明書の置き換え

多数の vCenter Server ホストが含まれている環境で証明書を置き換える場合は、vSphere 証明書管理ユーティリティを使用するか、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。どちらを選択するかは、いくつかのベスト プラクティスに基づいて決定します。

複数の vCenter Server システムが含まれる環境でのマシン SSL 証明書の置き換え

複数の vCenter Server システム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マシンの SSL 証明書を置き換えるか、CLI コマンドを使用して証明書を手動で置き換えることができます。

vSphere Certificate Manager を使用した複数の vCenter Server システムでのマシン SSL 証明書の置き換え

vSphere Certificate Manager を各マシンで実行します。実行するタスクによっては、証明書情報も求められます。詳細については、次のトピックを参照してください。

- Certificate Manager を使用した VMCA ルート証明書のカスタム署名証明書への置き換えと、すべての証明書の置き換え
- Certificate Manager を使用したマシン SSL 証明書の VMCA 証明書（中間 CA）への置き換え
- Certificate Manager を使用したソリューション ユーザー証明書の VMCA 証明書（中間 CA）への置き換え

CLI を使用した複数の vCenter Server システムでのマシン SSL 証明書の手動による置き換え

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 CLI コマンドを実行します。詳細については、次のトピックを参照してください。

- CLI を使用したマシン SSL 証明書の VMCA 署名証明書への置き換え
- CLI を使用したマシン SSL 証明書（中間 CA）の置き換え
- CLI を使用したマシン SSL 証明書のカスタム証明書への置き換え

拡張リンク モードの複数の vCenter Server システムがある環境でのソリューション ユーザー証明書の置き換え

拡張リンク モードの複数の vCenter Server システムが環境に含まれている場合は、次の手順を実行してソリューション ユーザー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、`/usr/lib/vmware-vmafd/bin/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。`/usr/lib/vmware-vmafd/bin/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 を使用した ELM の vCenter Server システムでのマシン SSL 証明書の置き換え

vSphere Certificate Manager を各マシンで実行します。実行するタスクによっては、証明書情報も求められます。vSphere Certificate Manager ユーティリティを使用した証明書の管理を参照してください。

CLI を使用した ELM の vCenter Server システムでのマシン SSL 証明書の手動による置き換え

ELM の vCenter Server でマシン SSL 証明書を手動で置き換える手順の概要は次のとおりです。

1 証明書を生成または要求します。

  次の証明書が必要です。

  - 各 vCenter Server のマシン ソリューション ユーザーの証明書。
  - 各ノードの、次のソリューション ユーザーそれぞれの証明書。
    - `vpxd` ソリューション ユーザー
    - `vpxd-extension` ソリューション ユーザー

- `vsphere-webclient` ソリューション ユーザー
- `wcp` ソリューション ユーザー

2 CLI コマンドを使用して、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。詳細については、次のトピックを参照してください。

- CLI を使用した新規 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
- CLI を使用したソリューション ユーザー証明書（中間 CA）の置き換え
- Certificate Manager を使用したソリューション ユーザー証明書のカスタム証明書への置き換え

外部ソリューションが含まれる VMware 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 システムとは別のマシンにインストールされます。vCenter Server システム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。VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/2109074) を参照してください。

vSphere Client を使用した証明書の管理

vSphere Client を使用して証明書を管理および表示できます。

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

- マシン SSL 証明書、VMware Certificate Authority (VMCA) ルート証明書、信頼できるルート証明書、および Security Token Service (STS) 証明書を表示します。
- 新しい信頼できるルート証明書を追加し、既存のマシン SSL 証明書および STS 証明書を更新または置き換えます。
- 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。他の証明書の置き換えワークフローは、vSphere Certificate Manager ユーティリティでサポートされています。vSphere Certificate Manager ユーティリティを使用した証明書の管理を参照してください。

デフォルトの証明書を置き換えるオプションの詳細については、vSphere 証明書の置き換えを参照してください。

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。

vSphere Client を使用した証明書ストアの検索

VMware Endpoint Certificate Store (VECS) のインスタンスは、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探索できます（マシン SSL、STS、信頼できるルート証明書など）。

VECS 内のさまざまなストアの詳細については、VMware Endpoint Certificate Store 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 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

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 Certificate Store を参照してください。

6 証明書の詳細を表示するには、適切な証明書タブを選択し、証明書を選択し、証明書を展開して詳細を表示します。

vSphere Client を使用した vCenter Server 証明書の有効期限の警告に対するしきい値の設定

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、vSphere Client の `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 を使用した新しい VMCA 署名付き証明書への VMCA 証明書の更新

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 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。
5. ローカル システムの VMCA 署名付きマシン SSL 証明書を更新します。
   a. [マシン SSL 証明書] タブで目的の証明書を選択し、[更新] をクリックします。
   b. 証明書の有効期間を日数で指定します。
   c. チェックボックスをクリックして、vCenter Server とそのデータベースをバックアップしたことを確認します。
   d. [更新] をクリックします。

      証明書が更新され、成功を示すメッセージが表示されます。
   e. 証明書が変更されたというメッセージが表示されたら、[更新] をクリックしてブラウザ画面を更新します。

vSphere Client を使用したカスタム証明書による証明書の置き換え

vSphere Client を使用して、デフォルト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。

vSphere Client を使用して、各マシンの CSR を生成し、内部またはサードパーティの認証局 (CA) から証明書を受け取ったときに証明書を置き換えることができます。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。vSphere Client 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 vCenter Server ノードでリバース 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（最小）から 8,192 ビット（最大）（PEM エンコード）。vSphere Client および API は、証明書署名リクエストの生成時に、引き続き最大 16,384 ビットのキー サイズを受け入れます。
- 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： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。

手順

1. vSphere Client を使用して 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. [マシン SSL] タブで目的の証明書を選択し、[証明書署名要求 (CSR) の生成] をクリックします。
   b. 証明書情報を入力し、[次へ] をクリックします。

      キー サイズのデフォルト値は 2,048 ビットです。この値は必要に応じて変更してください。

      注： vCenter Server を使用してキー サイズの大きい CSR を生成する場合、この処理は CPU への負荷が大きいため、生成までに数分かかります。
   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。vSphere Client を使用したカスタム証明書の追加を参照してください。

vSphere Client を使用した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。これは、vSphere Client を使用して実行できます。

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。

vSphere は、インポートに有効な CA 証明書のみを受け入れます。CA 証明書を有効にするには、基本制約とキー使用法 X.509 v3 証明書拡張で CA ビットと keyCertSign ビットをそれぞれ設定する必要があります。これは、証明書が CA であり、その目的が証明書署名であることを意味します。詳細については、https://www.rfc-editor.org/rfc/rfc5280 を参照してください。

チェーン内のすべての証明書について keyCertSign ビットが設定されていることを確認します。

手順

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

2 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [信頼されたルート] タブで、[信頼できるルート証明書の追加] 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。

注： vSphere 8.0 Update 2 以降では、[vCenter Server ホストへのルート証明書のプッシュの開始] チェック ボックスが削除されます。証明書が追加されると、vCenter Server によって、インベントリ内の接続されているすべてのホストにルート証明書がプッシュされます。vCenter Server とは異なるルート証明書を持つホストが接続されると、この違いを修正するために、vCenter Server によってルート証明書がプッシュされます。この場合、ホスト上のルート証明書は vCenter Server のルート証明書で上書きされるので、インベントリ全体で必要なカスタム ルート証明書があれば、管理者は vCenter Server に対して確実に追加することができます。

vSphere Client を使用したカスタム証明書の追加

vSphere Client を使用して、証明書ストアにカスタム マシン SSL 証明書を追加できます。

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。

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。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。vCenter Server 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 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [マシン SSL] タブで証明書を選択し、[証明書をインポートして置き換え] をクリックします。

6 該当する証明書の置き換えのオプションをクリックし、[次へ] をクリックします。

オプション	説明
VMCA 証明書に置き換え	VMCA で生成された CSR を作成して、現在の証明書を置き換えます。
vCenter Server から CSR が生成される外部 CA 証明書に置き換え（プライベート キーは組み込み）	vCenter Server で生成された CSR を使用して署名された証明書を使用して、現在の証明書を置き換えます。
外部 CA 証明書に置き換え（プライベート キーが必要）	外部 CA によって署名された証明書を使用して、現在の証明書を置き換えます。

7 CSR 情報を入力するか、該当する証明書をアップロードします。

8 チェックボックスをクリックして、vCenter Server とそのデータベースをバックアップしたことを確認します。

9 情報を確認し、[終了] をクリックします。

証明書が置き換えられ、成功メッセージが表示されます。

10 証明書が変更されたというメッセージが表示されたら、[更新] をクリックしてブラウザ画面を更新します。

VMCA リーフ証明書の生成

VMware インフラストラクチャで使用するために、VMware Certificate Authority (VMCA) によって署名されたリーフ証明書を生成できます。

VMware Certificate Authority (VMCA) は、すべての証明書管理を処理することに加え、リーフ証明書を生成することもできます。リーフ証明書は VMCA によって署名され、他の VMware リソースを識別するために使用されます。VMCA によって生成されたリーフ証明書は VECS には保存されません。また、vCenter Server はこれらのリーフ証明書の有効期限を追跡しません。

前提条件

リーフ証明書をインストールする VMware インフラストラクチャ内のホストで証明書署名リクエスト (CSR) を生成します。

手順

1 vSphere Client を使用して 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [信頼できるルート] タブで VMCA ルート証明書を選択し、[新しいリーフ証明書の発行] をクリックします。

6 以前に生成した CSR を参照し、期間を指定して、[次へ] をクリックします。

7 [証明書のダウンロード] をクリックしてリーフ証明書とルート証明書を保存します。

結果

リーフ証明書とルート証明書が生成され、指定した場所にダウンロードされます。

次のステップ

リーフ証明書とルート証明書を VMware インフラストラクチャ内のターゲット ホストにインポートします。

vSphere Certificate Manager ユーティリティを使用した証明書の管理

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。

デフォルトの証明書を置き換えるオプションの詳細については、vSphere 証明書の置き換えを参照してください。

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。

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 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。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。

vSphere Certificate Manager ユーティリティの場所

vSphere Certificate Manager ユーティリティは次の場所にあります。

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

注： vSphere Certificate Manager を実行すると、いくつかのオプションで次のようにプロンプトが表示されます。

```
Enter proper value for VMCA 'Name':
```

この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。

vSphere Certificate Manager ユーティリティのワークフロー

次の表に、vSphere Certificate Manager ユーティリティを使用して実行できる証明書の置き換えワークフローの概要を示します。

表 2-8. vSphere Certificate Management ユーティリティのワークフロー

ワークフロー	説明	詳細については、ドキュメント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	VMCA ルート証明書を生成してすべての証明書を置き換えるには、オプション 4 [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] を使用します。	Certificate Manager を使用した新しい 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 を中間認証局にする	VMCA を中間 CA にするには、vSphere Certificate Manager ユーティリティを数回実行し、複数のオプションを使用する必要があります。このワークフローは、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。	Certificate Manager を使用して VMCA を中間認証局にする
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で置き換えるには、vSphere Certificate Manager ユーティリティを複数回実行し、複数のオプションを使用する必要があります。このワークフローは、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。	Certificate Manager を使用したすべての証明書のカスタム証明書への置き換え
最後に実行した操作の取り消し	最後に実行した証明書操作を元の状態に戻し、前の状態に戻すには、オプション 7 [古い証明書の再発行による直近の操作の取り消し] を使用します。	Certificate Manager を使用した古い証明書の再発行による直近の操作の取り消し
すべての証明書のリセット	既存のすべての vCenter Server 証明書を VMCA によって署名された証明書に置き換えるには、オプション 8 [すべての証明書のリセット] を使用します。	Certificate Manager を使用したすべての証明書のリセット

Certificate Manager を使用した新しい 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

vSphere Certificate Manager ユーティリティを使用して VMCA ルート証明書を再生成し、ローカルのマシン SSL 証明書およびローカルのソリューション 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。複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている場合は、各 vCenter Server で証明書を置き換える必要があります。

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、vCenter Server 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。
- vCenter Server の IP アドレス
- 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。

注： OU (organizationalUnitName) フィールドは必須ではなくなりました。

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 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 オプション 4 [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] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 プロンプトに応答します。

vSphere Certificate Manager は入力に基づいて新しい VMCA ルート証明書を生成し、vSphere Certificate Manager を実行しているシステム上のすべての証明書を置き換えます。置き換えプロセスは、vSphere Certificate Manager がサービスを再起動した後で実行されます。

5 マシン SSL 証明書を置き換えるには、vSphere Certificate Manager をオプション 3 [マシンの SSL 証明書の VMCA 証明書での置き換え] で実行します。

6 ソリューション ユーザー証明書を置き換えるには、オプション 6 [VMCA 証明書によるソリューション ユーザー証明書の置き換え] を使用して Certificate Manager を実行します。

Certificate Manager を使用して VMCA を中間認証局にする

vSphere Certificate Manager ユーティリティを使用して、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、vSphere Certificate Manager を使用して、既存のすべての証明書を新しい VMCA 署名付き証明書に置き換えることができます。

VMCA を中間 CA にするには、vSphere Certificate Manager を複数回実行する必要があります。マシン SSL 証明書とソリューション ユーザー証明書の両方を置き換える手順の概要は次のとおりです。

1 vSphere Certificate Manager ユーティリティを起動しています。

2 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] を実行して CSR を生成します。証明書についての情報が必要になる場合があります。もう一度オプションの入力を求められたら、オプション 1 の [VMCA ルート署名証明書の証明書署名リクエストとキーの生成] を選択します。

3 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。

4 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。

5 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] を実行してすべての証明書を置き換えてプロンプトに従います。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。

6 (オプション) 複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている場合に、各ノードの証明書を次の方法で置き換えます。

   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 [マシンの SSL 証明書の VMCA 証明書での置き換え])。

   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 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])。

Certificate Manager を使用した CSR の生成とルート証明書（中間 CA）の用意

vSphere Certificate Manager ユーティリティを使用して証明書署名リクエスト (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。

  注： vSphere 8.0 以降では、vSphere Certificate Manager を使用して CSR を生成すると、最小キー サイズが 2,048 ビットから 3,072 ビットに変更されます。vSphere 8.0 Update 1 以降では、vSphere Client を使用して、キー サイズが 2,048 ビットの CSR が生成されます。

  注： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。

- 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（最小）から 8,192 ビット（最大）（PEM エンコード）
  - PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
  - x509 バージョン 3

- ルート証明書に対しては、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。例：

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- 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 認証局の使用例については、VMware ナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x」(https://kb.vmware.com/s/article/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 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 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。

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 管理者ユーザーとパスワードを入力します。

4 オプション 1 の [VMCA ルート署名証明書の証明書署名リクエストとキーの生成] 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、vSphere 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。Certificate Manager を使用した VMCA ルート証明書のカスタム署名証明書への置き換えと、すべての証明書の置き換えを参照してください。

Certificate Manager を使用した VMCA ルート証明書のカスタム署名証明書への置き換えと、すべての証明書の置き換え

vSphere Certificate Manager ユーティリティを使用すると、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。

vCenter Server 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、Certificate Manager を使用した CSR の生成とルート証明書（中間 CA）の用意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 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 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。

3 管理者ユーザーとパスワードを入力します。

4 オプション 2 の [カスタム証明書とキーをインポートして既存の VMCA ルート証明書を置き換え] を選択し、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。

Certificate Manager を使用したマシン SSL 証明書の VMCA 証明書（中間 CA）への置き換え

VMCA を中間 CA として使用する場合は、vSphere Certificate Manager ユーティリティを使用してマシン SSL 証明書を明示的に置き換えることができます。最初に、vCenter Server の VMCA ルート証明書を置き換えます。次に、マシン SSL 証明書を置き換えて、VMCA の新しいルートで署名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、vCenter Server 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。
- vCenter Server の IP アドレス

- 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。

注： OU (organizationalUnitName) フィールドは必須ではなくなりました。

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。
  - vCenter Server システムのホスト名または IP アドレス。

手順

1. vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2. オプション 3 の [マシンの SSL 証明書の VMCA 証明書での置き換え] を選択します。
3. 管理者ユーザーとパスワードを入力します。
4. プロンプトに応答します。

   vSphere Certificate Manager によって情報は `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。

Certificate Manager を使用したソリューション ユーザー証明書の VMCA 証明書（中間 CA）への置き換え

VMCA を中間 CA として使用する場合は、vSphere Certificate Manager ユーティリティを使用してソリューション 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、vCenter Server の VMCA ルート証明書を置き換えます。次に、ソリューション ユーザー証明書を置き換えて、VMCA の新しいルートで署名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証明書を置き換える際も使用できます。

前提条件

- 複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている環境で 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 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
  - vCenter Server システムのホスト名または IP アドレス

手順

1 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 オプション 6 [VMCA 証明書によるソリューション ユーザー証明書の置き換え] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 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 (https://kb.vmware.com/s/article/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。

Certificate Manager を使用したすべての証明書のカスタム証明書への置き換え

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、認証局 (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で置き換えるには、vSphere Certificate Manager ユーティリティを複数回実行する必要があります。マシン SSL 証明書とソリューション ユーザー証明書の両方を置き換える手順の概要は次のとおりです。

1 vSphere Certificate Manager ユーティリティを起動しています。

2 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 の [カスタム証明書によるマシン SSL 証明書の置き換え] を選択します。もう一度オプションの入力を求められたら、オプション 1 の [マシン SSL 証明書の証明書署名リクエストおよびキーの生成] 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 の [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] を選択します。

3 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。

4 署名付き証明書とルート証明書を CA から受け取ったら、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] を使用して、各マシンのマシン SSL 証明書を置き換えます。

5 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 の [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] を選択します。

6 最後に、複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている場合は、各ノードでこのプロセスを繰り返します。

Certificate Manager を使用した証明書署名リクエストの生成（カスタム証明書）

vSphere Certificate Manager ユーティリティを使用すると、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リクエスト (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。

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。
- vCenter Server のホスト名または IP アドレスを入力するように求められます。
- 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。

注： vSphere 8.0 以降では、vSphere Certificate Manager を使用して CSR を生成すると、最小キー サイズが 2,048 ビットから 3,072 ビットに変更されます。vSphere 8.0 Update 1 以降では、vSphere Client を使用して、キー サイズが 2,048 ビットの CSR が生成されます。

注： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。

手順

1 環境内の各 vCenter Server（vCenter Server シェル）にログインし、vSphere Certificate Manager を起動します。

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

2 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] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 オプション 1 の [マシン SSL 証明書の証明書署名リクエストおよびキーの生成] を選択して CSR を生成し、プロンプトに応答して vSphere 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。vSphere Certificate Manager は、ディレクトリに証明書とキー ファイルを配置します。

5 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、vSphere Certificate Manager を再起動し、オプション 5 の [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] 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、vCenter Server 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 の [ソリューション ユーザー証明書の証明書署名リクエストおよびキーの生成] を選択して CSR を生成し、プロンプトに応答して vSphere 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。

次のステップ

証明書の置き換えを実行するには、Certificate Manager を使用したマシン SSL 証明書のカスタム証明書への置き換えを参照してください。

Certificate Manager を使用したマシン SSL 証明書のカスタム証明書への置き換え

vSphere Certificate Manager ユーティリティを使用して、各ノードのマシン SSL 証明書をカスタム証明書に置き換えることができます。 マシン SSL 証明書は、各 vCenter Server ノードでリバース 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。

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、Certificate Manager を使用した証明書署名リクエストの生成（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（最小）から 8,192 ビット（最大）（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

VMware ナレッジベースの記事「Obtaining vSphere certificates from a Microsoft Certificate Authority」(https://kb.vmware.com/s/article/2112014) も参照してください。

手順

1 vCenter Server にログインし、vSphere Certificate Manager を起動します。

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

2 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] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 オプション 2 [カスタム証明書とキーをインポートして既存のマシン SSL 証明書を置き換え] を選択して、証明書の置き換えを開始して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）
- vCenter Server の IP アドレス

Certificate Manager を使用したソリューション ユーザー証明書のカスタム証明書への置き換え

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、vSphere 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 ユーザーとは、サービスのコレクション（vSphere Client に関連付けられているすべてのサービスなど）です。

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。

形式は次のようになります。

```
-----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、Certificate Manager を使用した証明書署名リクエストの生成（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（最小）から 8,192 ビット（最大）（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 vCenter Server にログインし、vSphere Certificate Manager を起動します。

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

2 オプション 5 の [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] を選択します。

3 シングル サインオン (SSO) ユーザーとパスワードを入力します。

4 オプション 2 の [カスタム証明書とキーをインポートして既存のソリューション ユーザー証明書を置き換え] を選択し、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
- 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`）
- すべてのソリューション ユーザーの証明書とキー（`vpxd.crt` および `vpxd.key`）の完全なセット

Certificate Manager を使用した古い証明書の再発行による直近の操作の取り消し

vSphere Certificate Manager ユーティリティ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 VECS の 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。

手順

1 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 オプション 7 [古い証明書の再発行による直近の操作の取り消し] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 続行するには、**Y** と入力します。

Certificate Manager を使用したすべての証明書のリセット

既存の vCenter Server 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、vSphere Certificate Manager ユーティリティを使用できます。

このオプションを使用すると、現在 VMware Endpoint Certificate Store (VECS) にあるすべてのカスタム証明書を上書きします。

vSphere Certificate Manager では、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。

手順

1 vCenter Server シェルにログインし、vSphere Certificate Manager を起動します。

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

2 オプション 8 [すべての証明書のリセット] を選択します。

3 管理者ユーザーとパスワードを入力します。

4 プロンプトが表示されたら、証明書情報を入力します。

次のステップ

証明書が置き換えられ、サービスが再起動されたら、証明書情報を確認します。

手動での vSphere 証明書の置き換え

一部の特殊な証明書の置き換えでは、vSphere Certificate Manager ユーティリティを使用できません。代わりに、インストールに含まれている CLI を証明書の置き換えのために使用します。

vCenter Server サービスの停止と開始のガイドライン

手動による証明書置き換え手順の一部では、すべての vCenter Server 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。

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。
- VECS (VMware Endpoint Certificate Store) でマシン SSL 証明書を削除する直前に、サービスを停止します。

CLI を使用した既存の VMCA 署名証明書の新しい VMCA 署名証明書への置き換え

VMware Certificate Authority (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、CLI を使用して新しいルート証明書を生成し、VMware Directory Service 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。

CLI を使用した新しい VMCA 署名付きルート証明書の生成

`certool` CLI を使用して新しい VMCA 署名付き証明書を生成し、証明書を vmdir に発行できます。

手順

1 vCenter Server で、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。

```
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）vCenter Server で、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。

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

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。

```
/usr/lib/vmware-vmafd/bin/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。

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/
certool.cfg
```

CLI を使用したマシン SSL 証明書の VMCA 署名証明書への置き換え

VMCA 署名付きルート証明書を新しく生成したら、`vecs-cli` コマンドを使用して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。複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている場合は、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。

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` ファイルは `/usr/lib/vmware-vmca/share/config/` ディレクトリにあります。

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。

```
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-<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。拡張リンク モード構成で接続された複数の vCenter Server インスタンスの展開では、このコマンドを vCenter Server ノードごとに実行します。

```
/usr/lib/vmware-vmca/bin/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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- vCenter Server のサンプル出力：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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。

- 各 vCenter Server 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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/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。

CLI を使用した新規 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、`dir-cli` コマンドを使用して、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 vCenter Server システムのマシン ソリューション ユーザー証明書とソリューション ユーザー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、`/usr/lib/vmware-vmafd/bin/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。`/usr/lib/vmware-vmafd/bin/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：

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
/usr/lib/vmware-vmca/bin/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。

```
/usr/lib/vmware-vmafd/bin/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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

拡張リンク モード構成で接続された複数の vCenter Server インスタンスの展開では、`/usr/lib/vmware-vmafd/bin/dir-cli service list` の出力にはすべてのノードのすべてのソリューション ユーザーが含まれます。`/usr/lib/vmware-vmafd/bin/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。

```
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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --
cert ./vpxd.crt
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/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 拡張リンク モード構成で、各 vCenter Server ノード上のソリューション ユーザーごとにパブリック キーとプライベート キーのペアを生成します。これには、マシン ソリューション用のペアと、追加のソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient、wcp) ごとのペアが含まれます。

a 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。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b 各ノードの vpxd ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c 各ノードの vpxd-extension ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d 各ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

e 各ノードの wcp ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 マシン ソリューション ユーザーと、各 vCenter Server ノードの追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient、wcp) ごとに、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 `/usr/lib/vmware-vmca/share/config/certool.cfg` ファイルのコピーを 1 つ作成し、必要に応じて名前、IP アドレス、DNS 名、E メールの各フィールドを変更または削除して、ファイルの名前を `sol_usr.cfg` などに変更します。

b 各ノードのマシン ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --config sol_usr.cfg
```

c 各ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv
--Name=vpxd --config sol_usr.cfg
```

d 各ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension --config sol_usr.cfg
```

e 次のコマンドを実行して、各ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
```

f 次のコマンドを実行して、各ノードで wcp ソリューション ユーザーの証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp --config sol_usr.cfg
```

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 以下のように、各ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b 各ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c 各ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d 各ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e 各ノードの wcp ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 `/usr/lib/vmware-vmafd/bin/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、vCenter Server システム上で実行できます。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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、`/usr/lib/vmware-vmafd/bin/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。`/usr/lib/vmware-vmafd/bin/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 各 vCenter Server 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f 各ノードの wcp 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、wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e が wcp 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

次のステップ

各 vCenter Server ノードのすべてのサービスを再起動します。

CLI を使用して VMCA を中間認証局にする

CLI を使用して、VMCA ルート証明書を、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。

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、「New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement」というブログ記事 (http://vmware.com/go/hybridvmca) を参照してください。

CLI を使用したルート証明書（中間 CA）の置き換え

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、CLI を使用し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（最小）から 8,192 ビット（最大）（PEM エンコード）
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- ルート証明書に対しては、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。例：

```
basicConstraints        = critical,CA:true
keyUsage                = critical,digitalSignature,keyCertSign
```

- 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 認証局の使用例については、VMware ナレッジベースの記事「Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.x」(https://kb.vmware.com/s/article/2112009) を参照してください。

注： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。

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 サイズ：2,048 ビット（最小）から 8,192 ビット（最大）。
- 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。

```
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。

たとえば、チェーン内に証明書が 1 つしかない場合は、次のようになります。

```
dir-cli trustedcert publish --cert rootca1.crt
```

チェーン内に複数の証明書を持つ場合、次のようになります。

```
dir-cli trustedcert publish --cert rootca1.crt --chain
```

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。

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/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。コマンド ラインを使用した vCenter Server STS 証明書の置き換えを参照してください。

CLI を使用したマシン SSL 証明書（中間 CA）の置き換え

CA から署名付き証明書を受信したら、CLI を使用してそれを VMCA ルート証明書にし、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。複数の vCenter Server インスタンスが拡張リンク モード構成で接続されている場合は、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。

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` ファイルは、 `/usr/lib/vmware-vmca/share/config/` ディレクトリにあります。

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。

```
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-<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。拡張リンク モード構成で接続された複数の vCenter Server インスタンスの展開では、このコマンドを vCenter Server ノードごとに実行します。

```
/usr/lib/vmware-vmca/bin/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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

- vCenter Server のサンプル出力：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

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。

- 各 vCenter Server 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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

CLI を使用したソリューション ユーザー証明書（中間 CA）の置き換え

マシン SSL 証明書を置き換えたら、CLI を使用してソリューション 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 vCenter Server システムのマシン ソリューション ユーザー証明書とソリューション ユーザー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、/usr/lib/vmware-vmafd/bin/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。/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost を実行して、各ホストのローカル マシン ID を検索します。各ソリューション ユーザーの名前には、マシン ID が含まれています。

前提条件

各ソリューション ユーザー証明書には異なる Subject が指定されている必要があります。たとえば、ソリューション ユーザー名（例： vpxd）などの一意の識別子を含めることができます。

手順

1 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。

```
/usr/lib/vmware-vmafd/bin/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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

拡張リンク モード構成で接続された複数の vCenter Server インスタンスの展開では、`/usr/lib/vmware-vmafd/bin/dir-cli service list` の出力にはすべてのノードのすべてのソリューション ユーザーが含まれます。`/usr/lib/vmware-vmafd/bin/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。

```
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 拡張リンク モード構成で、各 vCenter Server ノード上のソリューション ユーザーごとにパブリック キーとプライベート キーのペアを生成します。これには、マシン ソリューション用のペアと、追加のソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient、wcp) ごとのペアが含まれます。

a 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。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

b 各ノードの vpxd ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

c 各ノードの vpxd-extension ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-extension-key.priv --pubkey=vpxd-extension-key.pub
```

d 各ノードの vsphere-webclient ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

e 各ノードの wcp ソリューション ユーザーにキー ペアを生成します。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

2 マシン ソリューション ユーザーと、各 vCenter Server ノードの追加ソリューション ユーザー (vpxd、vpxd-extension、vsphere-webclient、wcp) ごとに、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 `/usr/lib/vmware-vmca/share/config/certool.cfg` ファイルのコピーを 1 つ作成し、必要に応じて名前、IP アドレス、DNS 名、E メールの各フィールドを変更または削除して、ファイルの名前を `sol_usr.cfg` などに変更します。

b 各ノードのマシン ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --config sol_usr.cfg
```

c 各ノードの vpxd ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --config sol_usr.cfg
```

d 各ノードの vpxd-extensions ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --
privkey=vpxd-extension-key.priv --Name=vpxd-extension --config sol_usr.cfg
```

e 次のコマンドを実行して、各ノードの vsphere-webclient ソリューション ユーザーに証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --config sol_usr.cfg
```

f 次のコマンドを実行して、各ノードで wcp ソリューション ユーザーの証明書を生成します。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp --config sol_usr.cfg
```

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 以下のように、各ノードのマシン ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine.crt --key machine-key.priv
```

b 各ノードの vpxd ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c 各ノードの vpxd-extension ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d 各ノードの vsphere-webclient ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e 各ノードの wcp ソリューション ユーザー証明書を置き換えます。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 `/usr/lib/vmware-vmafd/bin/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、vCenter Server システム上で実行できます。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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、`/usr/lib/vmware-vmafd/bin/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。`/usr/lib/vmware-vmafd/bin/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 各 vCenter Server 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine.crt
```

c 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

d 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

e 各ノードの 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

f 各ノードの wcp 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、wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e が wcp 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。

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e --cert new-wcp.crt
```

CLI を使用したカスタム証明書による証明書の置き換え

企業ポリシーで規定されている場合は、CLI を使用して、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。vCenter Server では、ソリューション ユーザー証明書は内部での通信にのみ使用されます。ソリューション ユーザー証明書は、外部との通信には使用されません。

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。Certificate Manager を使用したすべての証明書のカスタム証明書への置き換え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 (https://kb.vmware.com/s/article/2000988) を参照してください。

CLI を使用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

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、次に CLI を使用してルート証明書を 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（最小）から 8,192 ビット（最大）（PEM エンコード）
- PEM 形式。VMware では、PKCS8 および PKCS1（RSA キー）がサポートされます。VECS に追加されたキーは、PKCS8 に変換されます。
- x509 バージョン 3
- ルート証明書の場合、認証局の拡張を true に設定する必要があり、証明書の署名を要件の一覧に含める必要があります。
- SubjectAltName には DNS Name=<machine_FQDN> が含まれている必要があります。

- CRT 形式
- キー使用法として、デジタル署名、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）

注： vSphere の FIPS 証明書は、2,048 ビットと 3,072 ビットの RSA キー サイズのみを検証します。

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。
   - オプションで、ノードごとに 5 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 アドレスを含める必要はありません。証明書の Subject は、各証明書で異なっている必要があります。

   通常、その結果は信頼されたチェーンの PEM ファイルと、vCenter Server ノードごとの署名付き SSL 証明書です。

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、証明書情報を表示して、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。

```
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。コマンド ラインを使用した vCenter Server STS 証明書の置き換えを参照してください。

CLI を使用したマシン SSL 証明書のカスタム証明書への置き換え

カスタム証明書を取得したら、CLI を使用して各マシン証明書を置き換えることができます。

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）

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（最小）から 8,192 ビット（最大）（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

各 vCenter Server ホストで手順を実行します。

手順

1 現在のマシン SSL 証明書をバックアップします。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias
__MACHINE_CERT > oldmachine.crt
/usr/lib/vmware-vmafd/bin/vecs-cli entry getkey --store MACHINE_SSL_CERT --alias
__MACHINE_CERT > oldmachinekey.key
```

2 各ホストにログインし、認証局から取得した新しいマシン証明書を VECS に追加します。

SSL を介して通信するには、すべてのホストのローカル証明書ストアに新しい証明書が必要です。

a 既存の証明書を削除します。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
```

b 新しい証明書を追加します。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert <cert-file-path> --key <key-file-path>
```

3 置き換える古い証明書のハッシュを抽出します。

```
openssl x509 -in <path_to_old_machinessl_certificate> -noout -sha1 -fingerprint
```

次のような出力が表示されます。

```
SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88
```

4 Lookup Service 登録エンドポイントを手動で更新します。

```
/usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/
lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --
password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
```

`ls_update_certs.py` の実行中に問題が発生した場合は、https://kb.vmware.com/s/article/95982 にある VMware ナレッジベースの記事を参照してください。

5 すべてのサービスを再起動します。

```
service-control --stop --all && service-control --start --all
```

vSphere 証明書とサービス CLI コマンド リファレンス

3

CLI のセットを使用すると、VMCA (VMware Certificate Authority)、VECS (VMware Endpoint Certificate Store)、VMware Directory Service (vmdir)、および Security Token Service (STS) 証明書を管理できます。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 (https://kb.vmware.com/s/article/2100508) を参照してください。

手動での vSphere 証明書の置き換えでは、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 3-1. 証明書および関連サービスを管理する vSphere 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。VMware Authentication Framework Daemon (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.sh`	STS 証明書を管理します。	コマンドライン ヘルプ。オプションなしで `sso-config.sh` を入力すると、コマンドライン ヘルプが表示されます。
`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。

vSphere CLI の場所

デフォルトでは、CLI は次の場所にあります。

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

```
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

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

vSphere 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を行うには、ローカルの vCenter Single Sign-On ドメイン（デフォルトは vsphere.local）の管理者であることが必要です。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。管理者グループのユーザーには、包括的なアクセス権限があります。

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、デフォルトでは /usr/lib/vmware-vmca/share/config/ ディレクトリにあります。

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
```

注： OU (organizationalUnitName) フィールドは必須ではなくなりました。

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。
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/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。

  ```
  /usr/lib/vmware-vmca/bin/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。

次のトピックを参照してください。

- 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
  ```

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、VMware Certificate Authority (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、「CLI を使用した既存の VMCA 署名証明書の新しい VMCA 署名証明書への置き換え」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>	構成ファイルの名前。サンプル構成ファイルが /usr/lib/vmware-vmca/share/config/certool.cfg にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。

例：

```
certool --gencsr --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。CLI を使用して VMCA を中間認証局にする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。

オプション	説明
`--config <config_file>`	構成ファイルの名前。サンプル構成ファイルが `/usr/lib/vmware-vmca/share/config/certool.cfg` にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。
`--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：

```
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。他のオプションと共に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。
--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>	構成ファイルの名前。サンプル構成ファイルが /usr/lib/vmware-vmca/share/config/certool.cfg にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。
--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 --gencert --privkey=<filename> --cert=<filename> --config=<config_file>
```

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。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>`	構成ファイルの名前。サンプル構成ファイルが `/usr/lib/vmware-vmca/share/config/certool.cfg` にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。

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>`	構成ファイルの名前。サンプル構成ファイルが `/usr/lib/vmware-vmca/share/config/certool.cfg` にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。
`--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 --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>`	構成ファイルの名前。サンプル構成ファイルが `/usr/lib/vmware-vmca/share/config/certool.cfg` にあります。ベスト プラクティスとしては、デフォルトの構成ファイルのコピーを作成してから、必須フィールドを置き換えます。

例：

```
certool --genselfcert --privkey=<filename> --cert=<filename> --config=<config_file>
```

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認証サービスを管理するには、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 3-2. 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。 ■ 各 vCenter Server 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。
ソリューション ユーザー ストア ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp	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、他の証明書属性は確認しません。 次のソリューション ユーザー証明書ストアが 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：vCenter サービス デーモン (vpxd) ストア。vpxd は、このストアに保存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 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。 ■ wcp：VMware vSphere® with VMware Tanzu™ ストア。vSphere クラスタ サービスにも使用されます。 各 vCenter Server ノードには machine 証明書が含まれます。
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 3-2. 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。

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。

注： このコマンドを使用して TRUSTED_ROOTS ストアにルート証明書を追加しないでください。代わりに、`dir-cli` コマンドを使用してルート証明書を公開します。

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。
`--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。
`--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。

オプション	説明
`--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。vCenter Server 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

拡張リンク モードで接続されているすべての vCenter Server システムを一覧表示します。

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>`	このオプションを使用すると、別の vCenter Server に接続して、そのレプリケーション パートナーを表示できます。

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。

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>`	vCenter Server 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。
`--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した後で、`vecs-cli entry create` コマンドを実行して、VECS のソリューション ユーザー証明書エントリを更新します。vecs-cli コマンド リファレンスを参照してください。

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。
`--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`	vCenter Server 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変更し、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さい。
`--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>`	検索する 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

既存の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。このコマンドを実行すると、1 分後に VECS によって証明書の変更が取得されます。または、`vecs-cli force-refresh` コマンドを実行して証明書をすぐに同期することもできます。

注： vSphere 8.0 Update 3 以降では、vSphere Client または API のいずれかを使用して信頼できるルート証明書を公開し、サービスの再起動を不要にします。

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。

注： vSphere 8.0 Update 3 以降では、vSphere Client または API のいずれかを使用して信頼できるルート証明書を非公開にし、サービスの再起動を不要にします。

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。

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 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。

vCenter Single Sign-On による vSphere 認証

4

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。vCenter Single Sign-On は、ユーザーが認証を行うときにトークンを発行します。ユーザーはその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。

ユーザーおよびサービス アカウントは、トークン、またはユーザー名とパスワードを使用して認証します。ソリューション ユーザーは、証明書を使用して認証します。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、2 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。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。

次のトピックを参照してください。

- vCenter Single Sign-On によって環境を保護する方法
- vCenter Server ID プロバイダ フェデレーション
- vCenter Server ID プロバイダ フェデレーションと拡張リンク モード
- vCenter Server ID プロバイダ フェデレーションの設定
- vCenter Single Sign-On
- vCenter Single Sign-On ID ソースの設定
- vCenter Server Security Token Service の管理
- vCenter Single Sign-On ポリシーの管理
- vCenter Single Sign-On ユーザーおよびグループの管理
- その他の vSphere の認証オプション
- vSphere Client ログイン画面のログイン メッセージの管理
- vCenter Single Sign-On のセキュリティのベスト プラクティス

vCenter Single Sign-On 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。

- 外部 ID プロバイダ フェデレーションまたは vCenter Server 組み込み ID プロバイダを介したユーザーの認証。組み込み ID プロバイダでは、ローカル アカウント、Active Directory または OpenLDAP、統合 Windows 認証 (IWA)、その他の認証メカニズム（スマート カードおよび RSA SecurID）がサポートされます。
- 証明書を介したソリューション ユーザー認証。
- Security Token Service (STS)。
- トラフィックを保護するための SSL。

vCenter Server の組み込み ID プロバイダ

vCenter Server には、組み込みの ID プロバイダが含まれています。デフォルトでは、vCenter Server では ID ソースとして vsphere.local ドメインが使用されます。ただし、ドメインはインストール時に変更できます。LDAP/S、OpenLDAP/S、または統合 Windows 認証 (IWA) を使用して、vCenter Server 組み込み ID プロバイダが ID ソースとして Active Directory (AD) を使用するように構成できます。この設定では、ユーザーは AD アカウントを使用して vCenter Server にログインできます。

vCenter Server と外部 ID プロバイダ

vSphere 7.0 以降では、フェデレーション認証を使用して外部 ID プロバイダの vCenter Server を構成できます。この設定では、vCenter Server を ID プロバイダとして置き換えます。

vSphere は、次の ID プロバイダをサポートしています。

- vSphere 7.0 以降：Active Directory フェデレーション サービス (AD FS)
- vSphere 8.0 Update 1 以降：Okta
- vSphere 8.0 Update 2 以降：Microsoft Entra ID（旧称 Azure AD）
- vSphere 8.0 Update 3 以降：PingFederate

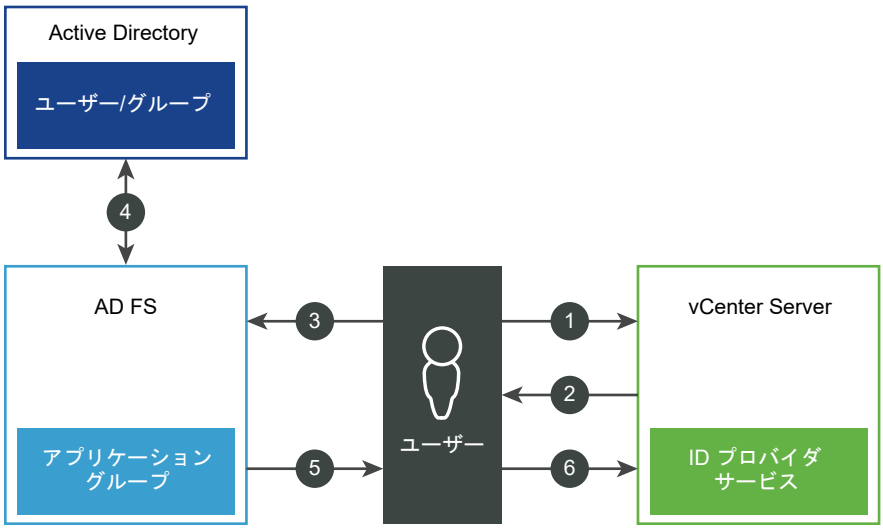
外部 ID プロバイダを使用するように vSphere を構成すると、外部 ID プロバイダは vCenter Server の代わりに ID ソースと通信します。

vCenter Server ID プロバイダ フェデレーション認証を使用したユーザー ログイン

外部 ID プロバイダを使用して vCenter Server で認証する場合、vCenter Server はログイン要求を外部 ID プロバイダにリダイレクトします。外部 ID プロバイダは、ディレクトリ サービスを使用してユーザーを認証し、ユーザーのログインに使用する vCenter Server のトークンを発行します。

たとえば、次の図は、AD FS を使用した vCenter Server ID プロバイダ フェデレーションのユーザー ログイン フローの詳細を示しています。

図 4-1. AD FS ID プロバイダ フェデレーションを使用した vCenter Server ユーザーのログイン



vCenter Server、AD FS、および Active Directory は、次のようにやりとりを行います。

1 ユーザーが vCenter Server のトップ ページでユーザー名を入力することで、フローが開始されます。

2 ユーザー名がフェデレーション ドメイン用の場合、vCenter Server は認証要求を AD FS にリダイレクトします。

3 必要に応じて、Active Directory 認証情報を使用してログインするようにユーザーに求めます。

4 AD FS が Active Directory を使用してユーザーを認証します。

5 AD FS が Active Directory からのグループ情報を含むセキュリティ トークンを発行します。

6 vCenter Server がトークンを使用してユーザーをログインさせます。

これで、ユーザーは認証を受け、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。

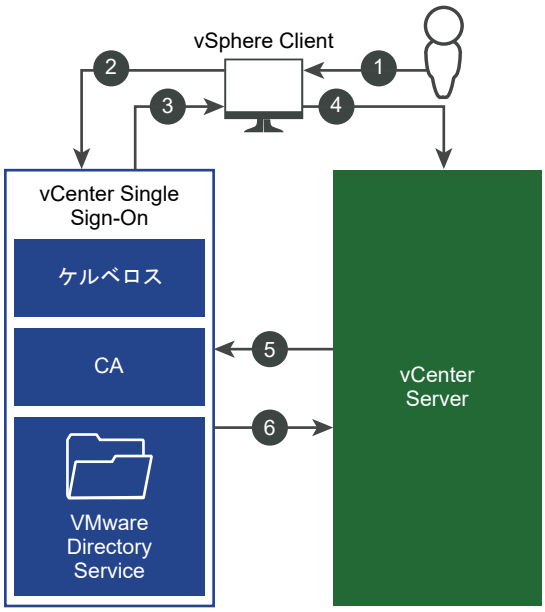
外部 ID プロバイダにアクセスできない場合、ログイン プロセスは vCenter Server のトップ ページに戻り、適切な情報メッセージが表示されます。ユーザーは、引き続き vsphere.local ID ソースのローカル アカウントを使用してログインできます。

vCenter Server と Okta、Microsoft Entra ID、PingFederate との間の相互作用は、AD FS の場合と同様ですが、vCenter Server では VMware Identity Services が使用される点が異なります。VMware Identity Services の認証プロセスを参照してください。

vCenter Server 組み込み ID プロバイダを使用したユーザー ログイン

次の図に、vCenter Server が ID プロバイダとして機能する場合のユーザー ログイン フローを示します。

図 4-2. vCenter Server 組み込み ID プロバイダを使用したユーザー ログイン



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。

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、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。

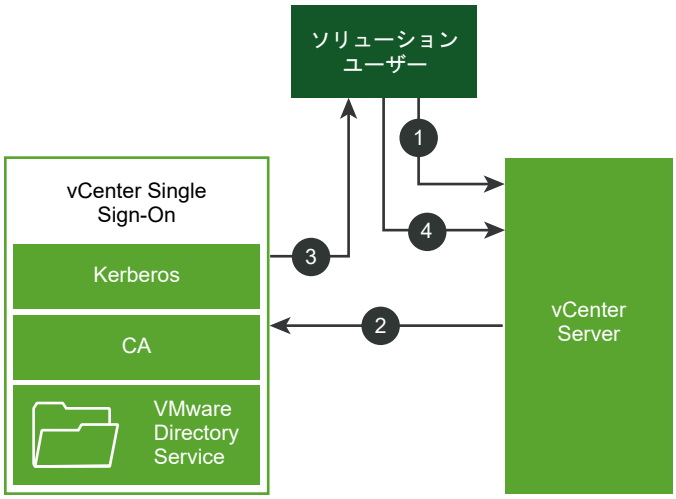
ソリューション ユーザーのログイン

ソリューション ユーザーとは、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 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。

注： vCenter Server では、ソリューション ユーザー証明書は内部での通信にのみ使用されます。ソリューション ユーザー証明書は、外部との通信には使用されません。

次の図に、ソリューション ユーザーのログイン フローを示します。

図 4-3. ソリューション ユーザーのログイン



1 ソリューション ユーザーが vCenter Server サービスへの接続を試みます。

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。

   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。
Certificate Manager を使用したソリューション ユーザー証明書のカスタム証明書への置き換えを参照してください。

vSphere でサポートされる暗号化

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 Server ID プロバイダ フェデレーション

vSphere 7.0 以降では、vCenter Server はフェデレーション認証を使用して vCenter Server にログインすることができます。

vCenter Server へのフェデレーション認証を有効にするには、外部 ID プロバイダへの接続を設定します。設定した ID プロバイダ インスタンスにより、ID プロバイダとしての vCenter Server が置き換えられます。現在、vCenter Server は、外部 ID プロバイダとして Active Directory フェデレーション サービス (AD FS)、Okta、Microsoft Entra ID（旧称 Azure AD）、PingFederate をサポートしています。vCenter Server は、AD FS（vSphere 7.0 以降）、Okta（vSphere 8.0 Update 1 以降）、Microsoft Entra ID（vSphere 8.0 Update 2 以降）、PingFederate（vSphere 8.0 Update 3 以降）をサポートしています。

注： vSphere がトークンベースの認証に移行することに伴い、VMware はフェデレーション認証の使用を推奨します。vCenter Server は引き続き、管理アクセスとエラー リカバリのためにローカル アカウントを使用します。

vCenter Server ID プロバイダ フェデレーションの機能

vCenter Server の ID プロバイダ フェデレーションにより、フェデレーション認証用に外部 ID プロバイダを構成できます。この構成では、外部 ID プロバイダが vCenter Server の代わりに ID ソースと通信します。

vCenter Server ID プロバイダ フェデレーションの基本

vSphere 7.0 以降では、vCenter Server はフェデレーション認証をサポートします。このシナリオでは、ユーザーが vCenter Server にログインすると、vCenter Server はユーザー ログインを外部の ID プロバイダにリダイレクトします。ユーザー認証情報が直接 vCenter Server に提供されることはなくなりました。代わりに、ユーザーは外部の ID プロバイダに認証情報を提供します。vCenter Server は、認証を実行するために外部 ID プロバイダを信頼します。フェデレーション モデルでは、ユーザーが認証情報をサービスまたはアプリケーションに直接提供することはなく、ID プロバイダのみに提供します。それにより、vCenter Server などのアプリケーションとサービスを ID プロバイダと「フェデレート」します。

vCenter Server の外部 ID プロバイダのサポート

vCenter Server は、次の外部 D プロバイダをサポートしています。

- AD FS（vSphere 7.0 以降）
- Okta（vSphere 8.0 Update 1 以降）
- Microsoft Entra ID（旧称 Azure AD）（vSphere 8.0 Update 2 以降）
- PingFederate（vSphere 8.0 Update 3）

vCenter Server ID プロバイダ フェデレーションの利点

vCenter Server ID プロバイダ フェデレーションには、次の利点があります。

- 既存のフェデレーション インフラストラクチャおよびアプリケーションで Single Sign-On を使用できます。
- vCenter Server ではユーザーの認証情報が処理されないため、データセンターのセキュリティを高めることができます。
- 外部 ID プロバイダでサポートされている多要素認証などの認証メカニズムを使用できます。

vCenter Server ID プロバイダ フェデレーション アーキテクチャ

vCenter Server と外部 ID プロバイダの間で証明書利用者の信頼を確立するには、識別情報と両者の間の共有シークレット キーを確立する必要があります。vCenter Server は OpenID Connect (OIDC) プロトコルを使用して、vCenter Server に対するユーザー認証を行う ID トークンを受け取ります。

vCenter Server を使用して外部 ID プロバイダを構成する手順の概要は、次のとおりです。

1. OIDC 構成を作成して、vCenter Server と外部 ID プロバイダ間の証明書利用者の信頼を確立します。AD FS の場合は、アプリケーション グループ（またはアプリケーション）を作成します。Okta、Microsoft Entra ID、PingFederate の場合は、サインオン方法として OpenID Connect を使用してネイティブ アプリケーションを作成します。OIDC 構成は、サーバ アプリケーションと Web API で構成されます。この 2 つのコンポーネントは、vCenter Server が外部 ID プロバイダを信頼し、これと通信するために使用する情報を指定します。
2. vCenter Server で対応する ID プロバイダを作成します。
3. 外部 ID プロバイダ ドメイン内のユーザーからのログインを承認するために、vCenter Server でグループ メンバーシップを構成します。

ID プロバイダ 管理者は、vCenter Server ID プロバイダの構成を作成するために次の情報を提供する必要があります。

- クライアント識別子：アプリケーション グループ（またはアプリケーション）の作成時に AD FS で生成され、アプリケーション グループ（またはアプリケーション）を識別する UUID 文字列、または OpenID Connect アプリケーションの作成時に Okta、Microsoft Entra ID、PingFederate で生成される UUID 文字列。
- 共有シークレット キー：アプリケーション グループ（またはアプリケーション）の作成時に AD FS で生成されるシークレット キー、または OpenID Connect アプリケーションの作成時に Okta、Microsoft Entra ID、PingFederate で生成され、外部 ID プロバイダで vCenter Server を認証するために使用されるシークレット キー。
- OpenID アドレス：既知のアドレスを指定する、外部 ID プロバイダ サーバの OpenID Provider Discovery のエンドポイント URL。通常は発行者のエンドポイントにパス `/.well-known/openid-configuration` を連結したものです。AD FS 構成の OpenID アドレスの例を次に示します。

  ```
  https://webserver.example.com/adfs/.well-known/openid-configuration
  ```

  同様に、Okta 構成の OpenID アドレスの例を次に示します。

  ```
  https://example.okta.com/oauth2/default/.well-known/openid-configuration
  ```

Microsoft Entra ID 構成の OpenID アドレスの例を次に示します。

```
https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0/.well-known/
openid-configuration
```

PingFederate 構成の OpenID アドレスの例を次に示します。

```
https://pingfederate-fqdn-and-port/.well-known/openid-configuration
```

VMware Identity Services とフェデレーション認証

vSphere 8.0 Update 1 以降では、VMware Identity Services はフェデレーション ID プロバイダとしての外部 ID プロバイダとの統合を提供します。VMware Identity Services は、vSphere に組み込まれている VMware Workspace ONE の「簡易」バージョンと見なすことができます。

vSphere 8.0 Update 1 以降をインストールするか、このバージョンにアップグレードすると、vCenter Server では VMware Identity Services がデフォルトで有効になります。Okta、Microsoft Entra ID、PingFederate を外部 ID プロバイダとして構成した場合、vCenter Server は VMware Identity Services を使用して Okta、Microsoft Entra ID、PingFederate サーバと通信します。

拡張リンク モード構成の場合、vCenter Server は Okta、Microsoft Entra ID、PingFederate を外部 ID プロバイダとしてサポートします。拡張リンク モード構成では、複数の vCenter Server システムが VMware Identity Services を実行していますが、1 つの vCenter Server と、その VMware Identity Services のみが外部 ID プロバイダ サーバと通信します。たとえば、A、B、C の 3 つの vCenter Server システムが拡張リンク モード構成になっている場合、vCenter Server A で Okta 外部 ID プロバイダを構成すると、vCenter Server A はすべての Okta ログインを処理する唯一のシステムになります。vCenter Server B および vCenter Server C は Okta サーバと直接通信しません。外部 IDP サーバと通信するために、ELM 構成の他の vCenter Server で VMware Identity Services を構成するには、「拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセス」を参照してください。

注： Okta を外部 ID プロバイダとして構成する場合、拡張リンク モード構成のすべての vCenter Server システムでは vSphere 8.0 Update 1 以降を実行する必要があります。Microsoft Entra ID の場合、vSphere 8.0 Update 2 以降が必要です。PingFederate の場合、vSphere 8.0 Update 3 以降が必要です。

注意: Okta、Microsoft Entra ID、PingFederate で拡張リンク モード構成を使用している場合、VMware Identity Services を実行し、ID プロバイダと通信する vCenter Server を ELM 構成から削除することはできません。

VMware Identity Services の認証プロセス

VMware Identity Services を使用して外部 ID プロバイダと通信するように vCenter Server を構成すると、次の認証プロセスが発生します。

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

2 vCenter Single Sign-On は、ユーザー認証を委任し、ユーザー要求を VMware Identity Services にリダイレクトします。

3 VMware Identity Services プロセスは、外部 ID プロバイダにトークンを要求して、ユーザー セッションを確立します。

4 外部 ID プロバイダはユーザーを認証し(多要素認証 (MFA) または SSO 認証情報を使用できます)、トークンを VMware Identity Services に返します。

   トークンには、ユーザー要求が含まれています。

5 VMware Identity Services プロセスは、ID プロバイダ トークンを検証し、対応する VMware Identity Services トークンを生成して、VMware Identity Services トークンを vCenter Single Sign-On に送信します。

6 vCenter Single Sign-On はトークンを検証し、ログイン要求を許可します。

注： AD FS では、フェデレーション認証に VMware Identity Services を使用しません。

SCIM によってプッシュされたユーザーおよびグループと vCenter Server が通信する方法

外部 ID プロバイダを構成する場合、vCenter Server はユーザーとグループの管理にクロスドメイン ID 管理 (SCIM) のシステムを使用します。SCIM は、ユーザー ID 情報の交換を自動化するためのオープン スタンダードです。vCenter Server にプッシュする外部 ID プロバイダのユーザーとグループは、外部 IDP サーバに作成した SCIM アプリケーションによって管理されます。vCenter Server は、ユーザーおよびグループを検索するときに SCIM を使用して、vCenter Server オブジェクトに権限を割り当てます。

注： AD FS 構成では、LDAP を使用して Active Directory を検索します。SCIM は使用しません。

vCenter Server ID プロバイダ フェデレーション コンポーネント

vCenter Server ID プロバイダ フェデレーション構成は、次のコンポーネントで構成されます。

- vCenter Server
  - AD FS の場合：vCenter Server 7.0 以降
  - Okta の場合：vCenter Server 8.0 Update 1 以降
  - Microsoft Entra ID の場合：vCenter Server 8.0 Update 2 以降
  - PingFederate の場合：vCenter Server 8.0 Update 3
- vCenter Server 上に構成された ID プロバイダ サービス
- 外部 ID プロバイダ（AD FS、Okta、Microsoft Entra ID、PingFederate）
- OpenID Connect (OIDC) 構成：
  - AD FS の場合：アプリケーション グループ（別名、アプリケーション）
  - Okta、Microsoft Entra ID、PingFederate の場合：OpenID Connect アプリケーション
- ユーザーおよびグループ管理のためのクロスドメイン ID 管理 (SCIM) アプリケーション（Okta、Microsoft Entra ID、PingFederate の場合のみ）
- vCenter Server グループおよびユーザーにマッピングされる 外部 ID プロバイダ グループおよびユーザー
- vCenter Server で有効になっている VMware Identity Services（Okta、Microsoft Entra ID、PingFederate の場合のみ）

- （オプション）PingFederate の場合、PingFederate サーバの SSL 証明書または証明書チェーン（この証明書が既知のパブリック認証局によって発行されていない場合）。PingFederate SSL 証明書を vCenter Server にインポートします。

vCenter Server ID プロバイダ フェデレーションに関する注意事項と相互運用性

vCenter Server ID プロバイダ フェデレーションは、他の多くの VMware 機能と相互運用できます。

vCenter Server ID プロバイダ フェデレーション戦略を検討する際は、相互運用性に伴う制限の可能性を考慮してください。

認証メカニズム

vCenter Server の ID プロバイダ フェデレーション設定では、外部 ID プロバイダは、認証メカニズム（パスワード、多要素認証 (MFA)、生体認証など）を処理します。

AD FS および単一の Active Directory ドメインのサポート

AD FS の vCenter Server ID プロバイダ フェデレーションを構成する際に、メイン ID プロバイダの構成ウィザードで、vCenter Server にアクセスするユーザーとグループを含む単一 Active Directory ドメインの LDAP 情報を入力するよう要求されます。vCenter Server は、ウィザードで指定したユーザー ベース DN から、認可と権限に使用する Active Directory ドメインを導出します。vSphere オブジェクトに対する権限は、この Active Directory ドメインのユーザーおよびグループに対してのみ追加できます。Active Directory の子ドメインまたは Active Directory フォレスト内の他のドメインのユーザーまたはグループは、vCenter Server ID プロバイダ フェデレーションではサポートされません。

Okta、Microsoft Entra ID、および PingFederate による複数ドメインのサポート

Okta、Microsoft Entra ID、または PingFederate の vCenter Server ID プロバイダ フェデレーションを構成する際に、メイン ID プロバイダの構成ウィザードで、vCenter Server にアクセスするユーザーとグループを含む複数のドメインの LDAP 情報を入力することができます。

パスワード、ロックアウト、およびトークン ポリシー

vCenter Server が ID プロバイダとして機能する場合は、デフォルト ドメイン（vsphere.local、または vSphere のインストール時に入力したドメイン名）の vCenter Server パスワード、ロックアウト、およびトークン ポリシーを制御します。vCenter Server でフェデレーション認証を使用する場合は、Active Directory などの ID ソースに保存されているアカウントのパスワード、ロックアウト、およびトークン ポリシーを外部 ID プロバイダが制御します。

監査とコンプライアンス

vCenter Server ID プロバイダ フェデレーションを使用している場合、成功したユーザー ログインについては、vCenter Server でログ エントリが引き続き作成されます。ただし、パスワード入力の失敗やユーザー アカウントのロックアウトなどのアクションは、外部 ID プロバイダが追跡してログに記録します。このようなイベントは vCenter Server で認識されなくなるため、vCenter Server ではログに記録されません。たとえば、AD FS が

ID プロバイダの場合は、AD FS がフェデレーション ログインのエラーを追跡してログに記録します。vCenter Server がローカル ログインの ID プロバイダである場合は、vCenter Server がローカル ログインのエラーを追跡してログに記録します。フェデレーション構成では、vCenter Server はログイン後のユーザー アクションを引き続きログに記録します。

外部 ID プロバイダと既存の VMware 製品の統合

vCenter Server と統合された VMware 製品（VMware Aria Operations、vSAN、NSX など）は、引き続き以前と同様に動作します。

ログイン後に統合される製品

ログイン後に統合される製品（別途ログインする必要がない）は、引き続き以前と同様に動作します。

API、SDK、および CLI アクセスのための単純な認証

単純な認証（ユーザー名とパスワード）を使用する API、SDK、または CLI コマンドに基づく既存のスクリプト、製品、およびその他の機能は引き続き動作します。内部的には、ユーザー名とパスワードを渡して認証が行われます。ユーザー名とパスワードを渡すこの行為により、vCenter Server（およびスクリプト）にパスワードが公開されるため、ID フェデレーションを使用するメリットの一部が損なわれます。可能な場合は、トークンベースの認証への移行を検討してください。

vCenter Server 管理インターフェイスへのアクセス

ユーザーが vCenter Server 管理者グループのメンバーである場合は、vCenter Server 管理インターフェイス（旧称 vCenter Server Appliance 管理インターフェイス (VAMI)）へのアクセスがサポートされます。

AD FS ログイン画面でのユーザー名テキストの入力

AD FS ログイン画面では、ユーザー名テキスト ボックスに事前入力するテキストを渡すことができません。そのため、AD FS を使用したフェデレーション ログイン中に、vCenter Server のトップページでユーザー名を入力し、AD FS ログイン画面にリダイレクトした後、AD FS ログイン画面でユーザー名を再入力する必要があります。vCenter Server のトップページで入力したユーザー名は、該当する ID プロバイダにログインをリダイレクトするために必要で、AD FS ログイン画面のユーザー名は、AD FS での認証に必要です。AD FS ログイン画面にユーザー名を渡すことができないのは、AD FS の制限です。この動作を vCenter Server から直接設定または変更することはできません。

IPv6 アドレスのサポート

AD FS、Microsoft Entra ID、および Ping Federate は IPv6 アドレスをサポートしています。Okta は IPv6 アドレスをサポートしていません。

VMware Identity Services の単一インスタンス構成

デフォルトでは、vSphere 8.0 Update 1 以降をインストールするか、このバージョンにアップグレードすると、vCenter Server で VMware Identity Services が有効になります。拡張リンク モード構成で Okta、Microsoft Entra ID、または PingFederate を構成する場合は、単一の vCenter Server システムで VMware Identity Services を使用します。たとえば、3 つの vCenter Server システムで構成されている拡張モード リンク構成で Okta を使用する場合、Okta サーバとの通信には、1 つの vCenter Server と VMware Identity Services のインスタンスのみが使用されます。

注意: VMware Identity Services を使用する ELM 構成で、外部 ID プロバイダと通信する vCenter Server システムが使用できなくなった場合は、ELM 構成内の他の vCenter Server で、外部 IDP サーバと連携するように VMware Identity Services を構成できます。拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセスを参照してください。

プライマリ ネットワーク ID の再構成

vCenter Server のプライマリ ネットワーク識別子 (PNID) を再構成するには、次のように外部 ID プロバイダの構成を更新する必要があります。

- AD FS：新しいリダイレクト URI が AD FS サーバに追加されます。
- Okta: Okta が再構成されます。Okta に対する vCenter Server ID プロバイダ フェデレーションの構成を参照して、vCenter Server に ID プロバイダを作成する手順を実行してください。
- Microsoft Entra ID：Entra ID を再構成します。Microsoft Entra ID に対する vCenter Server ID プロバイダ フェデレーションの構成を参照して、vCenter Server に ID プロバイダを作成する手順を実行してください。
- PingFederate：PingFederate を再構成します。PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成を参照して、vCenter Server に ID プロバイダを作成する手順を実行してください。

vCenter Server ID プロバイダ フェデレーションのライフサイクル

vCenter Server ID プロバイダ フェデレーションのライフサイクルを管理する場合は、いくつかの考慮事項があります。

vCenter Server ID プロバイダ フェデレーションのライフサイクルは、次の方法で管理できます。

Active Directory を使用する方法から既存の ID プロバイダを使用する方法への移行

vCenter Server の ID ソースとして Active Directory を使用している場合、外部 ID プロバイダを使用する方法への移行は簡単です。Active Directory のグループおよびロールが ID プロバイダのグループおよびロールと一致する場合は、追加のアクションを実行する必要はありません。グループおよびロールが一致しない場合は、いくつかの作業を追加で実行する必要があります。vCenter Server がドメイン メンバーである場合は、ドメインから削除することを検討してください。これは ID フェデレーションでは不要であり、使用されないためです。

ドメイン間再ポイントと移行

vCenter Server ID プロバイダ フェデレーションは、ドメイン間再ポイント（vSphere SSO ドメイン間での vCenter Server の移動）をサポートしています。再ポイントされた vCenter Server は、複製された ID プロバイダ構成を vCenter Server システムまたはポイント先システムから受け取ります。

一般的には、次のいずれかの条件に当てはまらないかぎり、ドメイン間再ポイントについて追加の ID プロバイダの再構成を実行する必要はありません。

1 再ポイントされた vCenter Server の ID プロバイダ構成は、ポイントされた vCenter Server の ID プロバイダ構成とは異なります。

2 これは、再ポイントされた vCenter Server が ID プロバイダ構成を受け取る最初の時点です。

これらの場合、いくつかの追加作業が必要です。たとえば、AD FS では、vCenter Server システムのリダイレクト URI を AD FS サーバ上の対応するアプリケーション グループに追加する必要があります。たとえば、AD FS アプリケーション グループ A がある（または AD FS 設定なしの）vCenter Server 1 が、AD FS アプリケーション グループ B がある vCenter Server 2 に再ポイントされている場合、vCenter Server 1 のリダイレクト URI をアプリケーション グループ B に追加する必要があります。

ユーザーとグループの同期および vCenter Server のバックアップとリストア

ユーザーとグループを vCenter Server と同期するタイミング、および vCenter Server をバックアップするタイミングによっては、vCenter Server をリストアするときに、SCIM によってプッシュされた ユーザーとグループの再同期が必要になる場合があります。

削除したユーザーまたはグループをリストアする際に、ユーザーまたはグループを外部 ID プロバイダから vCenter Server にプッシュすることはできません。見つからないユーザーまたはグループを使用して、外部 ID プロバイダの SCIM 2.0 アプリケーションを更新する必要があります。削除された SCIM ユーザーおよびグループのリストア を参照してください。

vCenter Server ID プロバイダ フェデレーションと拡張リンク モード

拡張リンク モードを使用している vCenter Server 環境で ID プロバイダ フェデレーションを有効にしても、認証とワークフローは以前と同様に機能し続けます。

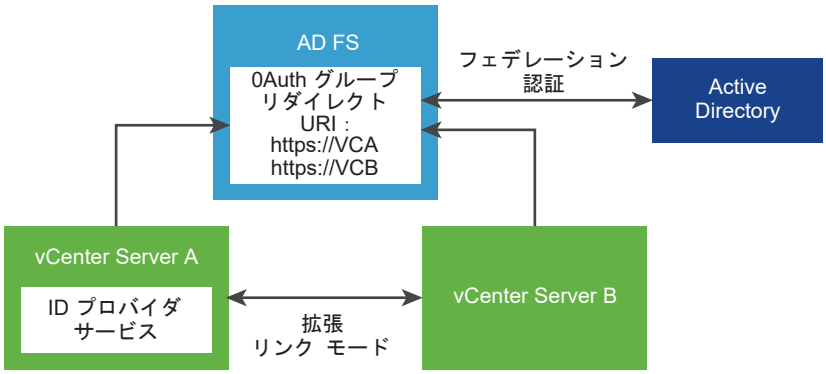
拡張リンク モード構成を使用する場合は、フェデレーション認証を使用して vCenter Server にログインするときに、次の点に注意してください。

- ユーザーには引き続き同じインベントリが表示され、ユーザーは vCenter Server の権限とロール モデルに基づいて同じアクションを実行できます。
- 拡張リンク モードの vCenter Server ホストは、互いの ID プロバイダにアクセスする必要はありません。たとえば、拡張リンク モードを使用する 2 つの vCenter Server システム A と B を想定します。vCenter Server A で承認されたユーザーは、vCenter Server B でも承認されます。

拡張リンク モードと AD FS

次の図は、拡張リンク モードで AD FS を使用する場合の認証ワークフローを示しています。

図 4-4. 拡張リンク モードと AD FS ID プロバイダ フェデレーション



1 拡張リンク モード構成では、2 台の vCenter Server ノードがデプロイされます。

2 AD FS のセットアップは、vCenter Server A で vSphere Client の [ID プロバイダの変更] ウィザードを使用して設定されています。AD FS のユーザーまたはグループに対するグループ メンバーシップと権限も確立されています。

3 vCenter Server A から vCenter Server B に AD FS 設定が複製されます。

4 両方の vCenter Server ノードのすべてのリダイレクト URI が、AD FS の OAuth アプリケーション グループに追加されます。1 つの OAuth アプリケーション グループのみが作成されます。

5 ユーザーが vCenter Server A にログインし、承認されると、そのユーザーは vCenter Server B でも承認されます。ユーザーが最初に vCenter Server B にログインした場合も同様です。

AD FS を使用する拡張リンク モード構成シナリオ

vCenter Server 拡張リンク モードは、AD FS の次の構成シナリオをサポートします。このセクションでは、「AD FS 設定」および「AD FS 構成」という用語は、[ID プロバイダの変更] ウィザードを使用して vSphere Client で実行した設定、および AD FS ユーザーまたはグループに対して確立したグループ メンバーシップまたは権限を示しています。

既存の拡張リンク モード構成での AD FS の有効化

手順の概要：

1 拡張リンク モード構成で、N 個の vCenter Server ノードをデプロイします。

2 リンクされた vCenter Server ノードのいずれかで AD FS を設定します。

3 AD FS 設定が他のすべての (N-1) vCenter Server 個のノードに複製されます。

4 N 個すべての vCenter Server ノードのすべてのリダイレクト URI を、AD FS の設定済み OAuth アプリケーション グループに追加します。

新しい vCenter Server から既存の拡張リンク モード AD FS 構成へのリンク

手順の概要：

1 （前提条件）vCenter Server の N ノード拡張リンク モード構成で AD FS を設定します。

2 独立した新しい vCenter Server ノードをデプロイします。

3 *N* 個のノードのいずれかをレプリケーション パートナーとして使用して、この新しい vCenter Server を N ノード AD FS 拡張リンク モード ドメインに再ポイントします。

4 既存の拡張リンク モード構成のすべての AD FS 設定が新しい vCenter Server に複製されます。

N ノード AD FS 拡張リンク モード ドメインにある AD FS 設定により、新しくリンクされた vCenter Server の既存の AD FS 設定が上書きされます。

5 新しい vCenter Server に関するすべてのリダイレクト URI を、AD FS の設定済み OAuth アプリケーション グループに追加します。

拡張リンク モードの AD FS 構成からの vCenter Server のリンク解除

手順の概要：

1 （前提条件）N ノードの vCenter Server 拡張リンク モード構成で AD FS を設定します。

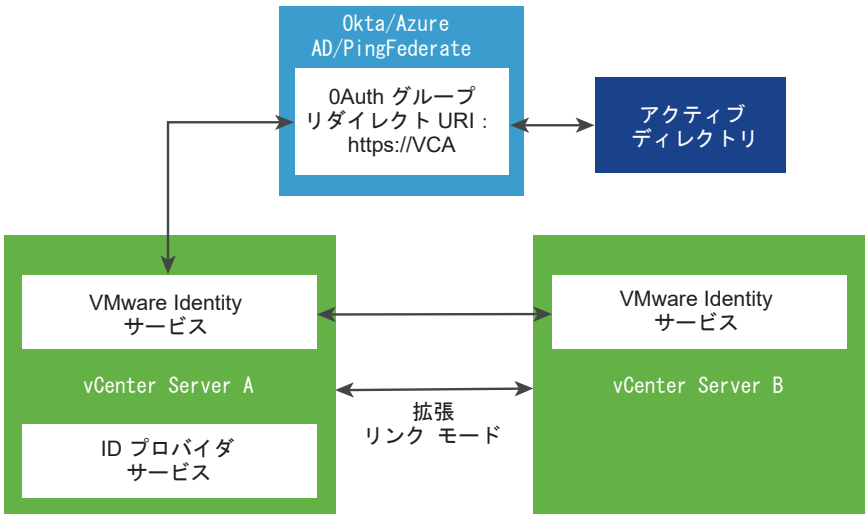
2 N ノード構成のいずれかの vCenter Server ホストを登録解除し、それを新しいドメインに再ポイントすると、N ノード構成からリンクが解除されます。

3 ドメインの再ポイント プロセスでは SSO 設定が保持されないため、リンクが解除された vCenter Server ノードのすべての AD FS 設定は元に戻り、失われます。このリンクが解除された vCenter Server ノードで AD FS を引き続き使用するには、AD FS を最初から設定し直すか、すでに AD FS が設定されている拡張リンク モード構成に vCenter Server を再リンクする必要があります。

拡張リンク モードと Okta、Microsoft Entra ID、または PingFederate ID プロバイダ フェデレーション

次の図は、拡張リンク モードで Okta、Microsoft Entra ID、または PingFederate を使用する場合の認証ワークフローを示しています。

図 4-5. 拡張リンク モードと Okta、Microsoft Entra ID、または PingFederate ID プロバイダ フェデレーション



注： Okta、Microsoft Entra ID、または PingFederate を外部 ID プロバイダとして構成する場合、拡張リンク モード構成のすべての vCenter Server システムで vSphere 8.0 Update 1 以降（Okta の場合）、vSphere 8.0 Update 2（Microsoft Entra ID の場合）、および vSphere 8.0 Update 3（PingFederate の場合）を実行する必要があります。

1 拡張リンク モード構成では、2 台の vCenter Server ノードがデプロイされます。

2 vSphere Client の [ID プロバイダの変更] ウィザードを使用して、vCenter Server A に Okta、Microsoft Entra ID、または PingFederate セットアップが設定されています。また、Okta、Microsoft Entra ID、または PingFederate ユーザーまたはグループに対するグループ メンバーシップと権限も確立されています。

   注： vCenter Server A と B の両方で VMware Identity Services が有効になっていますが、ID プロバイダ サーバと通信するのは vCenter Server A の VMware Identity Services のみです。

3 vCenter Server A で実行されている VMware Identity Services により、vCenter Server B はそのエンドポイントにアクセスできるようになります。

4 vCenter Server A のリダイレクト URI が Okta、Microsoft Entra ID、または PingFederate の OAuth アプリケーションに追加されます。1 つの OAuth アプリケーションのみが作成されます。

5 ユーザーが vCenter Server A にログインし、承認されると、そのユーザーは vCenter Server B でも承認されます。ユーザーが最初に vCenter Server B にログインした場合も同様です。

Okta、Microsoft Entra ID、または PingFederate を使用した拡張リンク モード構成のシナリオ

vCenter Server 拡張リンク モードは、Okta、Microsoft Entra ID、および PingFederate の次の構成シナリオをサポートしています。このセクションでは、「Okta 設定」および「Okta 構成」、「Microsoft Entra ID 設定」および「Microsoft Entra ID 構成」、または「PingFederate 設定」および「PingFederate 構成」という用語は、[ID プロバイダの変更] ウィザードを使用して vSphere Client で実行した設定、および Okta、Microsoft Entra ID、または PingFederate ユーザーまたはグループに対して確立したグループ メンバーシップまたは権限を示しています。

既存の拡張リンク モード構成での Okta、Microsoft Entra ID、または PingFederate の有効化

手順の概要：

1 拡張リンク モード構成で、N 個の vCenter Server ノードをデプロイします。

2 リンクされた vCenter Server ノードのいずれかで Okta、Microsoft Entra ID、または PingFederate を構成します。

3 VMware Identity Services エンドポイントの情報は、他のすべての (N-1) 台の vCenter Server ノードにレプリケートされます。

   Okta、Microsoft Entra ID、または PingFederate の構成（共有クライアント ID など）の情報とユーザー/グループの情報はレプリケートされません。

新しい vCenter Server から既存の拡張リンク モードの Okta、Microsoft Entra ID、または PingFederate 構成へのリンク

手順の概要：

1 （前提条件）vCenter Server の N ノード拡張リンク モード構成で Okta、Microsoft Entra ID、または PingFederate を設定します。

2 独立した新しい vCenter Server ノードをデプロイします。

3 *N* 台のノードのいずれかをレプリケーション パートナーとして使用して、この新しい vCenter Server を N ノードの Okta、Microsoft Entra ID、または PingFederate 拡張リンク モード ドメインに再ポイントします。

4 VMware Identity Services エンドポイントの情報は、他のすべての (N-1) 台の vCenter Server ノードにレプリケートされます。

Okta、Microsoft Entra ID、または PingFederate の構成（共有クライアント ID など）の情報とユーザー/グループの情報はレプリケートされません。

注： 既存の VMware Identity Services 構成を持つ vCenter Server ノードを追加できます。このシナリオでは、既存の VMware Identity Services 構成は、参加している VMware Identity Services 拡張リンク モード構成に置き換えられます。

既存の VMware Identity Services 構成を持つ vCenter Server ノードを、VMware Identity Services で構成されていない ELM 構成に追加することはできません。このシナリオでは、vCenter Server から既存の VMware Identity Services 構成を削除してから、ELM 構成に追加します。

拡張リンク モードの Okta、Microsoft Entra ID、または PingFederate 構成からの vCenter Server のリンク解除

手順の概要：

1 （前提条件）vCenter Server の N ノード拡張リンク モード構成で Okta、Microsoft Entra ID、または PingFederate を設定します。

2 N ノード構成のいずれかの vCenter Server ホストを登録解除し、それを新しいドメインに再ポイントすると、N ノード構成からリンクが解除されます。

3 ドメインの再ポイント プロセスでは SSO 設定が保持されないため、リンクが解除された vCenter Server ノードのすべての Okta、Microsoft Entra ID、または PingFederate の設定は元に戻り、失われます。このリンクが解除された vCenter Server ノードで Okta、Microsoft Entra Id、または PingFederate を引き続き使用するには、Okta、Microsoft Entra ID、または PingFederate を最初から構成し直すか、すでに Okta、Microsoft Entra ID、または PingFederate が設定されている拡張リンク モード構成に vCenter Server を再リンクする必要があります。

注： vCenter Server とアクティブな VMware Identity Services 構成のリンクを解除することはできません。

拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセス

Okta、Microsoft Entra ID、または PingFederate を使用した拡張リンク モード構成の可用性に関する考慮事項の詳細を確認します。

前提条件

- 2 つ以上の vCenter Server システムが拡張リンク モード構成に含まれていること。たとえば、システムには、VC_1、VC_2、VC_3 と VC_N までラベルが付けられます。ここで、N は拡張リンク モード構成の vCenter Server システムの数です。
- Okta および Microsoft Entra ID の場合、すべての vCenter Server システムで vSphere 8.0 Update 2 以降が実行されている必要があります。PingFederate の場合、すべての vCenter Server システムで vSphere 8.0 Update 3 以降が実行されている必要があります。
- Okta、Microsoft Entra ID、または PingFederate が vCenter Server システムのいずれかで外部 ID プロバイダとして構成されていること。たとえば、システムに VC_1 というラベルが付けられます。
- 外部 ID プロバイダが、必要なすべての OAuth2 および SCIM アプリケーションで構成されていること。

手順

1 特定の vCenter Server VC_i（i は 2 ～ N）を有効にするには、次の手順を実行します。

a VC_i へのローカル シェル アクセスを取得して、アクティベーション スクリプトを実行します。

注： 以下の手順を実行するために、管理者権限がある vCenter Server ユーザー アカウントをコマンドラインまたはコンソール プロンプトで指定してください。

b アクティベーション スクリプトから 'status' を実行して、vCenter Server の現在のアクティベーション状態を取得します。

```
python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py status
```

c 'status' コマンドで vCenter Server が有効になっていないことがわかった場合は、アクティベーション スクリプトから 'activate' を実行します。

```
python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py activate
```

d 'status' コマンドで vCenter Server がすでに有効になっていることがわかった場合は、'deactivate' オプションを実行してから、'activate' オプションを実行します。

```
python /usr/lib/vmware-trustmanagement/vmware_identity_services_activation.py
deactivate
```

- たとえば、'activate' オプションを実行します。
- または、'activate' コマンドで '--force-replace' オプションを指定することもできます。

2 ブラウザを開いて vCenter Server VC_i にアクセスし、vCenter Server に管理者としてログインします。

a [ホーム > 管理 > Single Sign-On > 構成] の順に移動します。

b [ユーザー プロビジョニング] の [テナント URL] に VC_i の FQDN が含まれていることを確認します。

c [テナント URL] 文字列をコピーして保存します。この情報は、外部 ID プロバイダで使用します。

d [シークレット トークン] の [生成] をクリックし、生成されたトークン文字列をコピーして保存します。この情報は、外部 ID プロバイダで使用します。

e [OpenID Connect] の [リダイレクト URI] に VC_i の FQDN が含まれていることを確認します。

f [リダイレクト URI] 文字列をコピーして保存します。この情報は、外部 ID プロバイダで使用します。

3 ブラウザを開いて、外部 ID プロバイダの管理ページに移動します。

注： 以下の手順は、外部 ID プロバイダ固有の情報を参照して実行してください。

a 外部 ID プロバイダが最初に VC_1 で構成されたときに設定された OAuth2 登録情報を見つけます。

b OAuth2 登録情報を編集します。先ほど VC_i 用に取得したリダイレクト URI を追加してください。

c 宛先が複数ある SCIM プッシュ構成を外部 ID プロバイダがサポートしている場合は、次の手順を実行します。

- 外部 ID プロバイダが最初に VC_1 で構成されたときに設定された SCIM プッシュ構成を見つけます。
- SCIM プッシュ構成を編集します。先ほど VC_i 用に取得した [テナント URL] と [シークレット トークン] を追加してください。

d 宛先が 1 つのみの SCIM プッシュ構成を外部 ID プロバイダがサポートしている場合は、次のことを行います。

- 先ほど VC_i 用に取得した [テナント URL] と [シークレット トークン] を使用して、新しい SCIM プッシュ構成を作成します。
- 外部 ID プロバイダが最初に VC_1 で構成されたときに設定された SCIM プッシュ構成と同じユーザー/グループ データが、確実に SCIM プッシュ構成によってプッシュされるようにします。

e SCIM プッシュ処理を開始して、VC_i に確実に最新のユーザー データまたはグループ データがポピュレートされるようにします。

vCenter Server ID プロバイダ フェデレーションの設定

最初に vCenter Server をデプロイした後、フェデレーション認証用に外部 ID プロバイダを設定できます。

vSphere 7.0 以降では、Active Directory フェデレーション サービス (AD FS) がサポートされます。vSphere 8.0 Update 1 以降では、Okta がサポートされています。vSphere 8.0 Update 2 以降では、Microsoft Entra ID（旧称 Azure AD）がサポートされています。vSphere 8.0 Update 3 以降では、PingFederate がサポートされています。

vCenter Server ID プロバイダ フェデレーションは vSphere Client または API から設定します。また、外部 ID プロバイダでも設定を行う必要があります。vCenter Server ID プロバイダ フェデレーションを設定するには、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 Server ID プロバイダ フェデレーション設定プロセス フロー

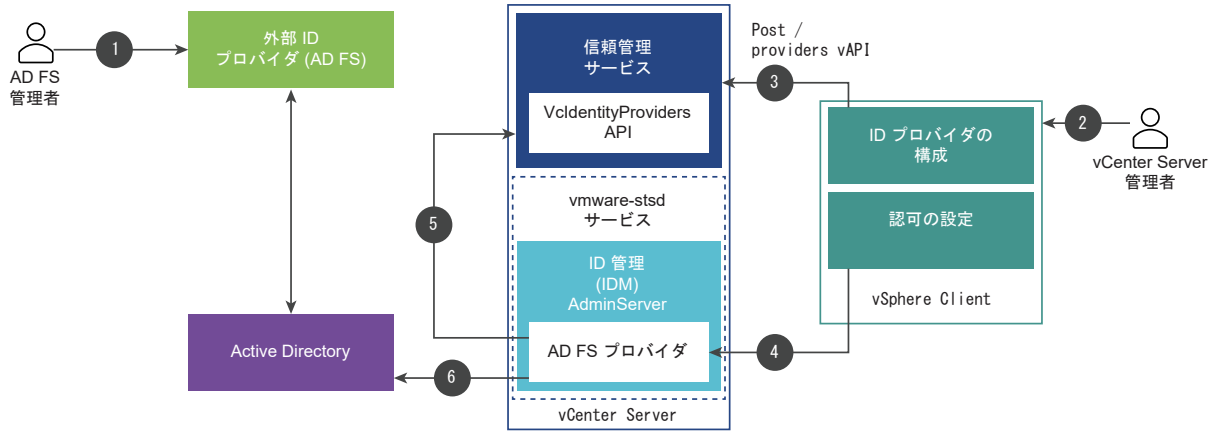
vCenter Server ID プロバイダ フェデレーションを適切に設定するには、実行される通信フローを理解しておく必要があります。

AD FS、Microsoft Entra ID（旧称 Azure AD）、Okta、または PingFederate に vCenter Server ID プロバイダ フェデレーションを構成できます。

AD FS の vCenter Server ID プロバイダ フェデレーション構成プロセス フロー

次の図に、AD FS vCenter Server ID プロバイダ フェデレーションを構成するときに発生するプロセス フローを示します。

図 4-6. AD FS の vCenter Server ID プロバイダ フェデレーション構成プロセス フロー



vCenter Server、AD FS、Active Directory は、次のように相互作用します。

1 AD FS 管理者が vCenter Server 用に AD FS OIDC アプリケーションを構成します。

2 vCenter Server 管理者が vSphere Client を使用して vCenter Server にログインします。

3 vCenter Server 管理者が vCenter Server に AD FS ID プロバイダを追加し、Active Directory ドメインに関する情報も入力します。

vCenter Server は、AD FS サーバの Active Directory ドメインへの LDAP 接続を確立するためにこの情報を必要とします。この接続を使用して vCenter Server はユーザーとグループを検索し、次の手順で vCenter Server ローカル グループに追加します。詳細については、この後の「Active Directory ドメインの検索」セクションを参照してください。

4 vCenter Server 管理者が vCenter Server での AD FS ユーザーの認可権限を設定します。

5 AD FS プロバイダが VcIdentityProviders API にクエリを発行して、Active Directory ソースの LDAP 接続情報を取得します。

6 AD FS プロバイダがクエリで得られたユーザーまたはグループを Active Directory 内で検索して、認可の設定を完了します。

Active Directory ドメインの検索

vSphere Client の [メイン ID プロバイダの設定] ウィザードを使用して、AD FS を vCenter Server の外部 ID プロバイダとして設定します。設定プロセスの一部として、ユーザーとグループの識別名 (DN) 情報を含む、Active Directory ドメインに関する情報を入力する必要があります。認証のために AD FS を設定するには、この Active Directory 接続情報が必要です。この接続は、Active Directory のユーザー名とグループを検索して vCenter Server のロールおよび権限にマッピングするために必要です。また、Active Directory ユーザーの認証には AD FS が使用されます。[メイン ID プロバイダの設定] ウィザードのこの手順では、LDAP を介した Active Directory の ID ソースは作成されません。代わりに vCenter Server はこの情報を使用して、Active Directory ドメインでユーザーとグループを検索できるように、このドメインに対して検索が可能な有効な接続を確立します。

次の識別名 (DN) エントリを使用する例を考えます。

- ユーザーのベース識別名 (DN) : cn=Users,dc=corp,dc=local
- グループのベース識別名 (DN) : dc=corp,dc=local

- ユーザー名：cn=Administrator,cn=Users,dc=corp,dc=local

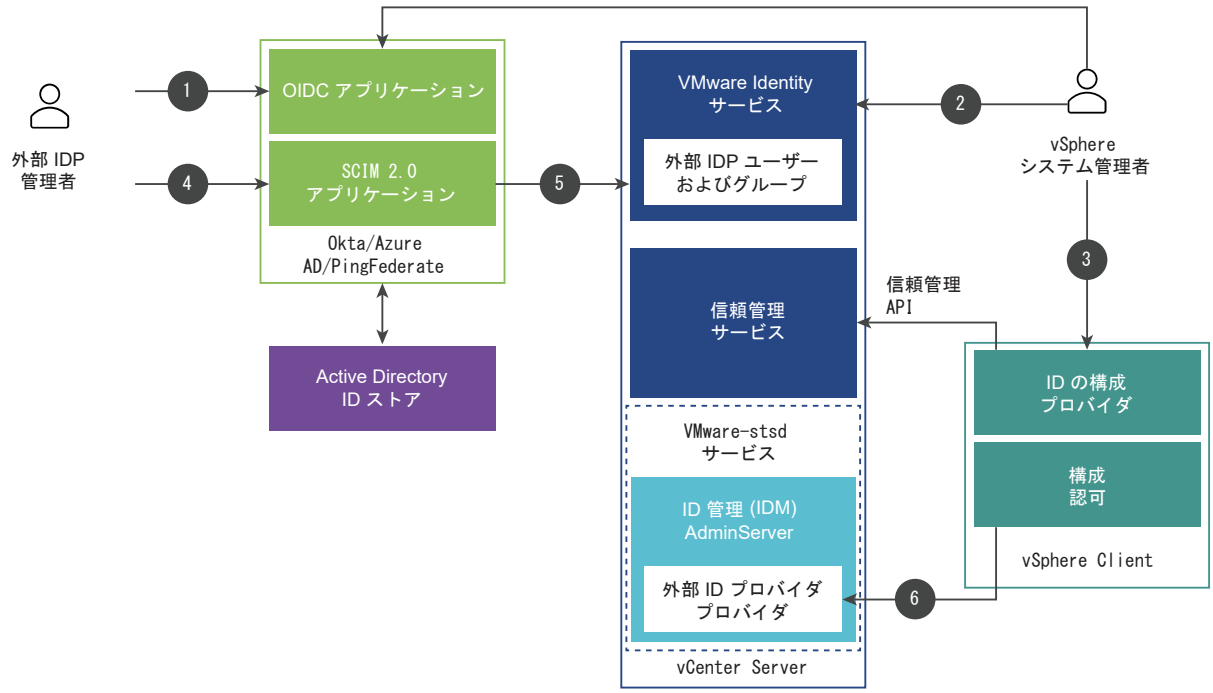
AdfsUser@corp.local ユーザーが ADGroup@corp.local グループのメンバーである場合、vCenter Server 管理者はウィザードでこの情報を入力することにより、ADGroup@corp.local グループを検索して見つけ、それを vCenter Server Administrators@vsphere.local グループに追加できます。その結果、AdfsUser@corp.local ユーザーにはログイン時に vCenter Server の管理者権限が付与されます。

vCenter Server では、Active Directory ユーザーおよびグループのグローバル権限の設定にもこの検索プロセスが使用されます。グローバル権限を設定する場合でもユーザーまたはグループを追加する場合でも、[ドメイン] ドロップダウン メニューから AD FS ID プロバイダに入力したドメインを選択し、Active Directory ドメインからユーザーおよびグループを検索して選択します。

VMware Identity Services を使用した vCenter Server ID プロバイダ フェデレーションの構成プロセス フロー

Okta、Microsoft Entra ID、および PingFederate を構成するには、VMware Identity Services を使用します。次の図に、VMware Identity Services を使用して vCenter Server ID プロバイダ フェデレーションを構成するときに発生するプロセス フローを示します。

図 4-7. VMware Identity Services を使用した vCenter Server ID プロバイダ フェデレーションの構成プロセス フロー



vCenter Server、VMware Identity Services、および Active Directory は、次のように相互作用します。

1 外部 IDP 管理者が vCenter Server 用に OIDC アプリケーションを構成します。

2 vCenter Server 管理者が、vSphere Client を使用して vCenter Server にログインし、ID プロバイダを vCenter Server に追加し、ドメイン情報も入力します。

3 vCenter Server 管理者が、手順 2 で作成した OIDC アプリケーションに追加するために、リダイレクト URI（vSphere Client の ID プロバイダ構成ページから取得）を ID プロバイダ管理者に提供します。

4 外部 IDP 管理者は SCIM 2.0 アプリケーションを構成します。

5 外部 IDP 管理者が SCIM 2.0 アプリケーションにユーザーとグループを割り当てて、ユーザーとグループを vCenter Server にプッシュします。

6 vCenter Server 管理者が vCenter Server での外部 IDP ユーザーの認可権限を設定します。

外部 IDP ユーザーおよびグループ

外部 ID プロバイダはユーザーおよびグループに対してクロスドメイン ID 管理 (SCIM) のシステムを使用するため、これらのユーザーとグループは vCenter Server に配置されます。権限の割り当てなどを行うために外部 ID プロバイダ内のユーザーとグループを検索する場合、検索は vCenter Server でローカルに実行されます。

vCenter Server では、外部 IDP ユーザーおよびグループのグローバル権限の設定にもこの検索プロセスが使用されます。グローバル権限の構成とユーザーまたはグループの追加のいずれを行う場合でも、[ドメイン] ドロップダウン メニューから ID プロバイダに入力したドメインを選択し、ドメインからユーザーおよびグループを検索して選択します。

JRE トラストストアの代替としての信頼済みルート証明書ストアの使用

vSphere 7.0 の JRE トラストストアに独自の内部認証局によって発行されたルート CA 証明書をインポートした場合、vSphere 7.0 Update 1 以降では、信頼済みルート証明書ストアに証明書を登録できます。

vSphere 7.0 で、独自の内部認証局によって発行されたルート CA 証明書を使用して vCenter Server Identity Provider Federation を構成するには、JRE トラスト ストアにインポートする必要があります。vSphere 7.0 Update 1 以降では、証明書を信頼済みルート証明書ストアに登録できます。この変更により、独自の内部認証局によって発行されたルート CA 証明書は信頼済みルート証明書ストア（VMware Endpoint Certificate Store、VECS とも呼ばれます）に追加することが必要になります。JRE トラストストアの証明書は引き続き機能しますが、vCenter Server では信頼済みルート証明書ストアの使用が標準になります。

手順

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

注： 詳細については、vSphere Client を使用した証明書ストアへの信頼できるルート証明書の追加を参照してください。

2 [管理] - [証明書] - [証明書の管理] の順に移動します。

3 [信頼できるルート証明書] の隣にある [追加] をクリックします。

4 AD FS ルート証明書を参照し、[追加] をクリックします。

証明書が [信頼できるルート証明書] の下のパネルに追加されます。

AD FS に対する vCenter Server ID プロバイダ フェデレーションの構成

vSphere 7.0 以降をインストールするか、vSphere 7.0 以降にアップグレードした後、AD FS に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

注： これらの手順は、vSphere 8.0 Update 1 以降を対象にしています。vSphere 8.0 の場合は、『vSphere の認証』ドキュメント (https://docs.vmware.com/jp/VMware-vSphere/8.0/vsphere-documentation-80.zip) の AD FS に対する vCenter Server ID プロバイダ フェデレーションの構成に関するトピックを参照してください。

vCenter Server は、1 つの構成されている外部 ID プロバイダ（1 つのソース）と、vsphere.local ID ソースのみをサポートします。複数の外部 ID プロバイダを使用することはできません。vCenter Server ID プロバイダ フェデレーションは、vCenter Server へのユーザー ログインに OpenID Connect (OIDC) を使用します。

このタスクでは、権限を制御する手段として AD FS グループを vSphere 管理者グループに追加する方法について説明します。また、vCenter Server のグローバル権限またはオブジェクト権限による AD FS 認可を使用して権限を構成することもできます。権限の追加の詳細については、ドキュメント『vSphere のセキュリティ』を参照してください。

注意： AD FS ID ソースの vCenter Server に以前に追加した Active Directory ID ソースを使用する場合は、その既存の ID ソースを vCenter Server から削除しないでください。これを行うと、以前に割り当てられたロールとグループ メンバーシップでリグレッションが発生します。グローバル権限を持つ AD FS ユーザーと管理者グループに追加されたユーザーの両方がログインできなくなります。

回避策：以前に割り当てられたロールとグループ メンバーシップが不要で、以前の Active Directory ID ソースを削除する場合は、AD FS プロバイダを作成して vCenter Server でグループ メンバーシップを構成する前に、ID ソースを削除します。

前提条件

注： AD FS ID プロバイダを構成するこのプロセスでは、vCenter Server と AD FS サーバの両方への管理アクセス権が必要です。構成プロセスでは、vCenter Server、次に AD FS サーバ、その次に vCenter Server の順で情報を入力します。

Active Directory フェデレーション サービスの要件：

- Windows Server 2016 以降の AD FS がすでにデプロイされている必要があります。
- Active Directory に AD FS が接続されている必要があります。
- 設定プロセスの一部として、vCenter Server のアプリケーショングループを AD FS で作成する必要があります。VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/78029) を参照してください。
- 信頼済みルート証明書ストアに追加した AD FS サーバ証明書（または AD FS サーバ証明書に署名した CA/中間証明書）。
- vCenter Server 管理者権限の付与対象となるユーザーを含む vCenter Server 管理者グループを AD FS 内に作成しました。

AD FS の設定の詳細については、Microsoft 社のドキュメントを参照してください。

vCenter Server とその他の要件：

- vSphere 7.0 以降
- vCenter Server は、AD FS 検出エンドポイントに接続可能で、さらに認可、トークン、ログアウト、JWKS および検出エンドポイント メタデータにアドバタイズされているその他のエンドポイントに接続可能である必要があります。
- フェデレーションされた認証に必要な vCenter Server ID プロバイダを作成、更新、作成するには、VcIdentityProviders.Manage 権限が必要です。ユーザーが ID プロバイダの設定情報のみを表示するように制限するには、VcIdentityProviders.Read 権限を割り当てます。

手順

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

2 信頼済みルート証明書ストアに AD FS サーバ証明書（または AD FS サーバ証明書に署名した CA/中間証明書）を追加します。

注： 詳細については、vSphere Client を使用した証明書ストアへの信頼できるルート証明書の追加を参照してください。

a [管理] - [証明書] - [証明書の管理] の順に移動します。

b [信頼されたルート ストア] の横にある [追加] をクリックします。

c AD FS 証明書を参照し、[追加] をクリックします。

証明書が [信頼できるルート証明書] の下のパネルに追加されます。

3 vCenter Server で ID プロバイダの作成を開始します。

a vSphere Client を使用して、vCenter Server に管理者としてログインします。

b [ホーム] - [管理] - [Single Sign-On] - [構成] の順に移動します。

c [プロバイダの変更] をクリックし、[ADFS] を選択します。

[メイン ID プロバイダの構成] ウィザードが開きます。

d [前提条件] パネルで、AD FS と vCenter Server の要件を確認します。

e [事前チェックを実行] をクリックします。

事前チェックでエラーが検出された場合は、[詳細表示] をクリックしてエラーを解決する手順を実行します。

f 事前チェックが終了したら、確認のチェック ボックスをオンにして、[次へ] をクリックします。

g [ユーザーおよびグループ] パネルで、LDAP 経由の Active Directory 接続のユーザーおよびグループ情報を入力して、ユーザーとグループを検索します。

vCenter Server は、認可と権限付与に使用する Active Directory ドメインをユーザーのベース識別名から導出します。vSphere オブジェクトに対する権限は、この Active Directory ドメインのユーザーおよびグループに対してのみ追加できます。Active Directory の子ドメインまたは Active Directory フォレスト内の他のドメインのユーザーまたはグループは、vCenter Server ID プロバイダ フェデレーションではサポートされません。

オプション	説明
ユーザーのベース識別名	ユーザーのベース識別名。
グループのベース識別名	グループのベース識別名。
ユーザー名	ユーザーおよびグループの BaseDN に対して、最低限の読み取り専用アクセス権を持つドメイン内のユーザーの ID。
パスワード	ユーザーおよびグループの 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。
プライマリ サーバ URL	ドメインのプライマリ ドメイン コントローラ LDAP サーバ。 **`ldap://hostname:port`** の形式または **`ldaps://hostname: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。

h [次へ] をクリックします。

i [OpenID Connect] パネルで、リダイレクト URI と ログアウト リダイレクト URI をコピーします。

現時点では、他のフィールドは空白のままにします。次の手順で OpenID Connect 構成を作成すると、[OpenID Connect] パネルに戻ります。

4 AD FS で OpenID Connect 構成を作成し、vCenter Server 用に設定します。

vCenter Server と ID プロバイダの間で証明書利用者の信頼を確立するには、識別情報と両者の間の共有シークレット キーを確立する必要があります。AD FS でこれを実行するには、サーバ アプリケーションと Web API で構成される、アプリケーション グループと呼ばれる OpenID Connect 構成を作成します。この 2 つのコンポーネントは、vCenter Server が AD FS サーバを信頼し、これと通信するために使用する情報を指定します。AD FS で OpenID Connect を有効にするには、https://kb.vmware.com/s/article/78029 にある Vmware のナレッジベースの記事を参照してください。

AD FS アプリケーション グループを作成するときは、次の点に注意してください。

- 前の手順で取得した 2 つの vCenter Server リダイレクト URI が必要です。

- 次の手順で vCenter Server ID プロバイダの作成を完了するときに使用するために、AD FS アプリケーション グループから次の情報をファイルにコピーするかメモします。
  - クライアント識別子
  - 共有シークレット
  - AD FS サーバの OpenID アドレス

注： 必要に応じて、次の PowerShell コマンドを AD FS 管理者として実行して、AD FS サーバの OpenID アドレスを取得します。

```
Get-AdfsEndpoint | Select FullUrl | Select-String openid-configuration
```

返された URL をコピーします（囲んでいるブラケットや最初の `"@{FullUrl="` の部分は含まず、URL 自体のみを選択します）。

5 vCenter Server の [OpenID Connect] パネルで、次の手順を実行します。

a AD FS アプリケーション グループを作成するときに、前の手順で取得した次の情報を入力します。
   - クライアント識別子
   - 共有シークレット
   - OpenID アドレス

   [ID プロバイダ名] には「Microsoft ADFS」が自動的に入力されます。

b [次へ] をクリックします。

6 情報を確認し、[終了] をクリックします。

vCenter Server で AD FS ID プロバイダが作成されて、構成情報が表示されます。

7 AD FS を認可するためのグループ メンバーシップを vCenter Server で構成します。

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。

c [グループ] タブをクリックします。

d [管理者] グループをクリックして、[メンバーの追加] をクリックします。

e ドロップダウン メニューからドメインを選択します。

f ドロップダウン メニューの下のテキスト ボックスに、追加する AD FS グループの最初の数文字を入力し、ドロップダウンの選択肢が表示されるまで待ちます。

   vCenter Server が Active Directory への接続を確立して検索するため、選択肢が表示されるまで数秒かかる場合があります。

g AD FS グループを選択し、管理者グループに追加します。

h [保存] をクリックします。

8 Active Directory ユーザーで vCenter Server にログインしていることを確認します。

Okta に対する vCenter Server ID プロバイダ フェデレーションの構成

vSphere 8.0 Update 1 以降をインストールするか、vSphere 8.0 Update 1 以降にアップグレードした後、Okta に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

vCenter Server は、1 つの構成されている外部 ID プロバイダ（1 つのソース）と、vsphere.local ID ソース（ローカル ソース）のみをサポートします。複数の外部 ID プロバイダを使用することはできません。vCenter Server ID プロバイダ フェデレーションは、vCenter Server へのユーザー ログインに OpenID Connect (OIDC) を使用します。

vCenter Server のグローバル権限またはオブジェクト権限による Okta グループとユーザーを使用して権限を構成できます。権限の追加の詳細については、ドキュメント『vSphere のセキュリティ』を参照してください。

前提条件

Okta の要件は次のとおりです。

- Okta を使用していて、専用のドメイン領域（例：https://*your-company*.okta.com）を持っている必要があります。
- OIDC ログインを実行し、ユーザーとグループの権限を管理するには、次の Okta アプリケーションを作成する必要があります。
  - サインオン方法として OpenID Connect を使用する Okta ネイティブ アプリケーション。このネイティブ アプリケーションには、認可コード、リフレッシュ トークン、リソース所有者パスワードの付与タイプが含まれている必要があります。
  - OAuth 2.0 ベアラー トークンを使用して Okta サーバと vCenter Server 間のユーザーおよびグループの同期を実行する System for Cross-domain Identity Management (SCIM) 2.0 アプリケーション。

  VMware のナレッジベースの記事 (https://kb.vmware.com/s/article/90835) を参照してください。
- vCenter Server と共有する Okta ユーザーおよびグループを特定しておく必要があります。この共有は SCIM の処理です（OIDC の処理ではありません）。

Okta の接続要件：

- vCenter Server は、Okta 検出エンドポイントに接続可能で、さらに認可、トークン、JWKS、および検出エンドポイント メタデータにアドバタイズされているその他のエンドポイントに接続可能である必要があります。
- Okta も、SCIM プロビジョニング用のユーザーとグループのデータを送信するために vCenter Server に接続できる必要があります。

vCenter Server の要件：

- vSphere 8.0 Update 1 以降

- Okta ID ソースを作成する vCenter Server で、VMware Identity Services が有効になっていることを確認します。

  注： vSphere 8.0 Update 1 以降をインストールするか、vSphere 8.0 Update 1 以降にアップグレードすると、VMware Identity Services がデフォルトで有効になります。vCenter Server 管理インターフェイスを使用して、VMware Identity Services のステータスを確認できます。VMware Identity Services の停止と起動を参照してください。

vSphere の権限の要件：

- フェデレーションされた認証に必要な vCenter Server ID プロバイダを作成、更新、削除するには、VcIdentityProviders.Manage 権限が必要です。ユーザーが ID プロバイダの設定情報のみを表示するように制限するには、VcIdentityProviders.Read 権限を割り当てます。

拡張リンク モードの要件：

- 拡張リンク モード構成では、Okta に対する vCenter Server ID プロバイダ フェデレーションを構成できます。拡張リンク モード構成で Okta を構成する場合は、単一の vCenter Server システムで VMware Identity Services を使用するように Okta ID プロバイダを構成します。たとえば、拡張リンク モード構成が 2 つの vCenter Server システムで構成されている場合、Okta サーバとの通信には 1 台の vCenter Server とその VMware Identity Services のインスタンスが使用されます。この vCenter Server システムが使用できなくなった場合、ELM 構成内の他の vCenter Server 上の VMware Identity Services を Okta サーバと連携させるように構成できます。詳細については、拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセスを参照してください。
- Okta を外部 ID プロバイダとして構成する場合、拡張リンク モード構成のすべての vCenter Server システムでは vSphere 8.0 Update 1 以降を実行する必要があります。

ネットワークの要件：

- ネットワークが公開されていない場合は、vCenter Server システムと Okta サーバ間にネットワーク トンネルを作成し、パブリックにアクセス可能な適切な URL をベース URI として使用します。

手順

1 Okta で OpenID Connect アプリケーションを作成し、グループとユーザーを OpenID Connect アプリケーションに割り当てます。

  OpenID Connect アプリケーションを作成してグループとユーザーを割り当てるには、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/90835) を参照してください。「Create the OpenID Connect Application」セクションの手順に従います。Okta OpenID Connect アプリケーションを作成したら、Okta OpenID Connect アプリケーションから以下の情報をファイルにコピーして、次の手順で vCenter Server ID プロバイダを構成するときに使用します。

  - クライアント識別子
  - クライアント シークレット（vSphere Client では共有シークレットとして表示）
  - Active Directory ドメイン情報または Okta ドメイン情報（Active Directory を実行していない場合）

2 vCenter Server で ID プロバイダを作成するには、次の手順を実行します。

a vSphere Client を使用して、vCenter Server に管理者としてログインします。

b [ホーム] - [管理] - [Single Sign-On] - [構成] の順に移動します。

c [プロバイダの変更] をクリックし、[Okta] を選択します。

[メイン ID プロバイダの構成] ウィザードが開きます。

d [前提条件] パネルで、Okta と vCenter Server の要件を確認します。

e [事前チェックを実行] をクリックします。

事前チェックでエラーが検出された場合は、[詳細表示] をクリックしてエラーを解決する手順を実行します。

f 事前チェックが終了したら、確認のチェックボックスをオンにして、[次へ] をクリックします。

g [ディレクトリ情報] パネルで、次の情報を入力します。

- ディレクトリ名：Okta からプッシュされたユーザーとグループを格納する vCenter Server に作成するローカル ディレクトリの名前。**`vcenter-okta-directory`** のように入力します。
- ドメイン名：vCenter Server と同期する Okta ユーザーおよびグループを含む Okta ドメイン名を入力します。

  Okta ドメイン名を入力したら、プラス記号アイコン (+) をクリックして追加します。複数のドメイン名を入力する場合は、デフォルトのドメインを指定します。

h [次へ] をクリックします。

i [OpenID Connect] パネルで、次の情報を入力します。

- リダイレクト URI：自動的に入力されます。OpenID Connect アプリケーションの作成に使用するリダイレクト URI を Okta 管理者に提供します。
- ID プロバイダ名：「Okta」が自動的に入力されます。
- クライアント識別子：手順 1 で Okta に OpenID Connect アプリケーションを作成したときに取得されます（Okta では、クライアント識別子がクライアント ID と呼ばれます）。
- 共有シークレット：手順 1 で Okta に OpenID Connect アプリケーションを作成したときに取得されます（Okta では、共有シークレットがクライアント シークレットと呼ばれます）。
- OpenID アドレス：https://*Okta ドメイン領域*/oauth2/default/.well-known/openid-configuration という形式になります。

  たとえば、Okta ドメイン領域が example.okta.com の場合、OpenID アドレスは `https://example.okta.com/oauth2/default/.well-known/openid-configuration` です。

  詳細については https://developer.okta.com/docs/reference/api/oidc/#well-known-openid-configuration を参照してください。

j [次へ] をクリックします。

k 情報を確認し、[終了] をクリックします。

vCenter Server で Okta ID プロバイダが作成されて、構成情報が表示されます。

l 必要に応じて、下にスクロールして [リダイレクト URI] の [コピー] アイコンをクリックし、ファイルに保存します。

Okta OpenID Connect アプリケーションでは、このリダイレクト URI を使用します。

m [テナント URL] の [コピー] アイコンをクリックして、ファイルに保存します。

注： ネットワークが公開されていない場合は、vCenter Server システムと Okta サーバ間にネットワーク トンネルを作成する必要があります。ネットワーク トンネルを作成したら、パブリックにアクセス可能な適切な URL をベース URI として使用します。

n [ユーザー プロビジョニング] で [生成] をクリックしてシークレット トークンを作成し、ドロップダウンからトークンの有効期間を選択してから、[クリップボードにコピー] をクリックします。トークンを安全な場所に保存します。

Okta SCIM 2.0 アプリケーションでは、このテナント URL とトークンを使用します。Okta SCIM 2.0 アプリケーションではトークンを使用して、Okta ユーザーとグループを VMware Identity Services に同期します。この情報は、Okta ユーザーとグループを Okta から vCenter Server にプッシュするために必要です。

3 VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/90835) に戻って Okta のリダイレクト URI を更新します。

「Update the Okta Redirect URI」セクションの手順に従います。

4 SCIM 2.0 アプリケーションを作成するには、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/90835) を引き続き参照します。

「Create the SCIM 2.0 Application and Push Users and Groups to vCenter Server」セクションの手順に従います。

ナレッジベースの記事の説明に従って SCIM 2.0 アプリケーションの作成が完了したら、次の手順に進みます。

5 vCenter Server を Okta 認証用に構成します。

Okta ユーザーを vCenter Server グループに割り当てるか、インベントリレベルおよびグローバル権限を Okta ユーザーに割り当てることができます。ログインするために必要な最小権限は、読み取り専用権限です。

Okta ユーザーをグループに割り当てるには、「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。インベントリレベルおよびグローバル権限を Okta ユーザーに割り当てるには、『vSphere のセキュリティ』ドキュメントで vCenter Server コンポーネントの権限の管理に関するトピックを参照してください。

6 Okta ユーザーで vCenter Server にログインしていることを確認します。

Microsoft Entra ID に対する vCenter Server ID プロバイダ フェデレーションの構成

vSphere 8.0 Update 2 以降をインストールするか、vSphere 8.0 Update 2 以降にアップグレードした後、Microsoft Entra ID（旧称 Azure AD）に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

vCenter Server は、1 つの構成されている外部 ID プロバイダ（1 つのソース）と、vsphere.local ID ソース（ローカル ソース）のみをサポートします。複数の外部 ID プロバイダを使用することはできません。vCenter Server ID プロバイダ フェデレーションは、vCenter Server へのユーザー ログインに OpenID Connect (OIDC) を使用します。

vCenter Server のグローバル権限またはオブジェクト権限による Microsoft Entra ID グループとユーザーを使用して権限を構成できます。権限の追加の詳細については、ドキュメント『vSphere のセキュリティ』を参照してください。

構成プロセスの詳細説明については、次のビデオを参照してください。

vCenter Authentication: AzureAD/Entra ID integration | vSphere 8 Update 2

前提条件

Microsoft Entra ID の要件：

- Microsoft のユーザーであり、Microsoft Entra ID アカウントを持っている必要があります。

Microsoft Entra ID の接続要件：

- サインオン方式として OpenID Connect を使用するエンタープライズ（ギャラリー以外の）アプリケーションを作成しておく必要があります。
- 作成されたアプリケーションの付与タイプとして、認可コード、リフレッシュ トークン、リソース所有者パスワードを追加します。
- ユーザーとグループを同期するには、OAuth 2.0 ベアラー トークンを使用して、Microsoft Entra ID における SCIM 2.0 のプロビジョニング用の VMware Identity Services ギャラリー アプリケーションを構成する必要があります。

vCenter Server の要件：

- vSphere 8.0 Update 2 以降で、VMware Identity Services が有効になっている必要があります（デフォルトで有効になっています）。
- Microsoft Entra ID ID ソースを作成する vCenter Server で、VMware Identity Services が有効になっていることを確認します。
- ID プロバイダからユーザーとグループが vCenter Server にプロビジョニングされている必要があります。

vSphere の権限の要件：

- フェデレーション認証に必要な vCenter Server ID プロバイダを作成、更新、削除するには、[VcIdentityProviders.Manage] 権限が必要です。ユーザーが ID プロバイダの構成情報のみを表示するように制限するには、[VcIdentityProviders.Read] 権限を割り当てます。

拡張リンク モードの要件：

- 拡張リンク モード構成では、Microsoft Entra ID に対する vCenter Server ID プロバイダ フェデレーションを構成できます。拡張リンク モード構成で Microsoft Entra ID を構成する場合は、単一の vCenter Server システムで VMware Identity Services を使用するように Microsoft Entra ID ID プロバイダを構成します。たとえば、拡張リンク モード構成が 2 つの vCenter Server システムで構成されている場合、Microsoft Entra ID サーバとの通信には 1 台の vCenter Server とその VMware Identity Services のインスタンスが使用されます。この vCenter Server システムが使用できなくなった場合、ELM 構成内の他の vCenter Server システム上の VMware Identity Services を Microsoft Entra ID サーバと連携させるように構成できます。詳細については、拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセスを参照してください。
- Microsoft Entra ID を外部 ID プロバイダとして構成する場合、拡張リンク モード構成のすべての vCenter Server システムでは vSphere 8.0 Update 2 以降を実行する必要があります。

ネットワークの要件：

- ネットワークが公開されていない場合は、vCenter Server システムと Microsoft Entra ID サーバの間にネットワーク トンネルを作成し、パブリックにアクセス可能な適切な URL をベース URI として使用します。

手順

1 Microsoft Entra ID で OpenID Connect アプリケーションを作成し、グループとユーザーを OpenID Connect アプリケーションに割り当てます。

   OpenID Connect アプリケーションを作成してグループとユーザーを割り当てるには、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/94182) を参照してください。「Create the OpenID Connect Application」セクションの手順に従います。OpenID Connect アプリケーションを作成したら、Microsoft Entra ID OpenID Connect アプリケーションから以下の情報をファイルにコピーして、次の手順で vCenter Server ID プロバイダを構成するときに使用します。

   - クライアント識別子
   - クライアント シークレット（vSphere Client では共有シークレットとして表示）。
   - Active Directory ドメイン情報または Microsoft Entra ID ドメイン情報 (Active Directory を実行していない場合)。

2 vCenter Server で ID プロバイダを作成するには、次の手順を実行します。

   a vSphere Client を使用して、vCenter Server に管理者としてログインします。

   b [ホーム] - [管理] - [Single Sign-On] - [構成] の順に移動します。

   c [プロバイダの変更] をクリックし、[Microsoft Entra ID] を選択します。

      [メイン ID プロバイダの構成] ウィザードが開きます。

   d [前提条件] パネルで、Microsoft Entra ID と vCenter Server の要件を確認します。

   e [事前チェックを実行] をクリックします。

      事前チェックでエラーが検出された場合は、[詳細表示] をクリックしてエラーを解決する手順を実行します。

f 事前チェックが終了したら、確認のチェック ボックスをオンにして、[次へ] をクリックします。

g [ディレクトリ情報] パネルで、次の情報を入力します。

- ディレクトリ名：Microsoft Entra ID からプッシュされたユーザーとグループを格納する vCenter Server に作成するローカル ディレクトリの名前。**`vcenter-entraid-directory`** のように入力します。
- ドメイン名：vCenter Server と同期する Microsoft Entra ID のユーザーとグループを含む Microsoft Entra ID ドメイン名を入力します。

  Microsoft Entra ID ドメイン名を入力したら、プラス記号アイコン (+) をクリックして追加します。複数のドメイン名を入力する場合は、デフォルトのドメインを指定します。

h [次へ] をクリックします。

i [OpenID Connect] パネルで、次の情報を入力します。

- リダイレクト URI：自動的に入力されます。OpenID Connect アプリケーションの作成に使用するリダイレクト URI を Microsoft Entra ID 管理者に提供します。
- ID プロバイダ名：「Microsoft Entra ID」が自動的に入力されます。
- クライアント識別子：手順 1 で Microsoft Entra ID に OpenID Connect アプリケーションを作成したときに取得されます。(Microsoft Entra ID では、クライアント識別子がクライアント ID と呼ばれます)。
- 共有シークレット キー：手順 1 で Microsoft Entra ID に OpenID Connect アプリケーションを作成したときに取得されます。(Microsoft Entra ID では、共有シークレットがクライアント シークレットと呼ばれます)。
- OpenID アドレス：https://*Microsoft Entra ID ドメイン領域*/oauth2/default/.well-known/openid-configuration という形式になります。

  たとえば、Microsoft Entra ID ドメイン領域が example.EntraID.com の場合、OpenID アドレスは `https://example.EntraID.com/oauth2/default/.well-known/openid-configuration` です。

j [次へ] をクリックします。

k 情報を確認し、[終了] をクリックします。

vCenter Server で Microsoft Entra ID ID プロバイダが作成されて、構成情報が表示されます。

l 必要に応じて、下にスクロールして [リダイレクト URI] の [コピー] アイコンをクリックし、ファイルに保存します。

Microsoft Entra ID OpenID Connect アプリケーションでは、このリダイレクト URI を使用します。

m [テナント URL] の [コピー] アイコンをクリックして、ファイルに保存します。

注： ネットワークが公開されていない場合は、vCenter Server システムと Microsoft Entra ID サーバの間にネットワーク トンネルを作成する必要があります。ネットワーク トンネルを作成したら、パブリックにアクセス可能な適切な URL をベース URI として使用します。

n [ユーザー プロビジョニング] で [生成] をクリックしてシークレット トークンを作成し、ドロップダウンからトークンの有効期間を選択してから、[クリップボードにコピー] をクリックします。トークンを安全な場所に保存します。

Microsoft Entra ID SCIM 2.0 アプリケーションでは、このテナント URL とトークンを使用します。Microsoft Entra ID SCIM 2.0 アプリケーションではトークンを使用して、Microsoft Entra ID のユーザーとグループを VMware Identity Services に同期します。この情報は、Microsoft Entra ID のユーザーとグループを Microsoft Entra ID から vCenter Server にプッシュするために必要です。

3 VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/94182) に戻って Microsoft Entra ID のリダイレクト URI を更新します。

「Update the Azure AD Redirect URI」セクションの手順に従います。

4 SCIM 2.0 アプリケーションを作成するには、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/94182) を引き続き参照します。

「Create the SCIM 2.0 Application and Push Users and Groups to vCenter Server」セクションの手順に従います。

ナレッジベースの記事の説明に従って SCIM 2.0 アプリケーションの作成が完了したら、次の手順に進みます。

5 Microsoft Entra ID を認可するためのグループ メンバーシップを vCenter Server で構成します。

Microsoft Entra ID ユーザーが vCenter Server にログインする前に、グループ メンバーシップを構成する必要があります。

a vSphere Client で、ローカル管理者としてログインしているときに、[管理] - [Single Sign-On] - [ユーザーおよびグループ] の順に移動します。

b [グループ] タブをクリックします。

c [管理者] グループをクリックして、[メンバーの追加] をクリックします。

d ドロップダウン メニューから追加する Microsoft Entra ID グループのドメイン名を選択します。

e ドロップダウン メニューの下のテキスト ボックスに、追加する Microsoft Entra ID グループの最初の数文字を入力し、ドロップダウンの選択肢が表示されるまで待ちます。

f Microsoft Entra ID グループを選択し、管理者グループに追加します。

g [保存] をクリックします。

6 Microsoft Entra ID ユーザーで vCenter Server にログインしていることを確認します。

7 インベントリレベルおよびグローバル権限を Microsoft Entra ID ユーザーに割り当てるには、『vSphere のセキュリティ』ドキュメントで vCenter Server コンポーネントの権限の管理に関するトピックを参照してください。

PingFederate の vCenter Server ID プロバイダの構成

vSphere 8.0 Update 3 をインストールするか、vSphere 8.0 Update 3 にアップグレードした後、PingFederate に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

PingFederate の vCenter Server ID プロバイダを構成する手順の概要

PingFederate 用の vCenter Server の構成には、次の手順が含まれます。

1 PingFederate で、PingFederate ワークフローの範囲と一般的な構成などの vCenter Server/VMware Identity Services 固有の構成を作成すること。

2 PingFederate で、パスワード付与フローの構成や認可コード フローの構成などのグローバル項目を作成すること。

3 PingFederate で、SCIM Provisioner をインストールすること。

4 vCenter Server で、PingFederate ID プロバイダを作成すること。

5 PingFederate で、SCIM アプリケーション（SP 接続）を作成すること。

6 vCenter Server で、PingFederate ユーザーを認証すること。

注： このドキュメントの手順では、PingFederate サーバ用の一般的なセットアップを作成します。実際の環境は異なる可能性があるため、別の選択を行うことになる場合があります。

PingFederate 用に vCenter Server ID プロバイダを構成するための前提条件

PingFederate の要件：

- オンプレミスの PingFederate サーバをインストールしてあること。
- PingFederate ID プロバイダを構成する vCenter Server から信頼できるルート証明書を取得して、PingFederate サーバにインポートする必要があります。
- 証明書が自己署名されている場合（既知のパブリック認証局によって発行されていない場合）は、PingFederate SSL 証明書、または証明書チェーンを vCenter Server にインポートすることが必要な場合があります。PingFederate SSL 証明書、またはチェーン内のいずれかの証明書が既知の認証局によって発行されたものである場合、その証明書は vCenter Server によって自動的に信頼されるので、インポートする必要はありません。PingFederate サーバの SSL 証明書に 1 つ以上の中間署名機関を使用している場合は、証明書チェーン全体を含めます。

  PingFederate SSL 証明書をエクスポートするには、PingFederate の管理コンソールで [セキュリティ] - [SSL サーバ証明書] の順に移動し、デフォルトの証明書を選択して、[アクションの選択] ドロップダウンから [エクスポート] を選択します。

  ID プロバイダの構成ワークフローの一環として、[OpenID Connect] パネルの vSphere Client を使用して PingFederate SSL 証明書をインポートします。

- OIDC ログインを実行し、ユーザーとグループの権限を管理するには、次の PingFederate アプリケーションを作成する必要があります。
  - サインオン方法として OpenID Connect を使用する PingFederate ネイティブ アプリケーション。このネイティブ アプリケーションには、認可コード、リフレッシュ トークン、リソース所有者パスワードの付与タイプが含まれている必要があります。
  - OAuth 2.0 ベアラー トークンを使用して PingFederate サーバと vCenter Server の間のユーザーおよびグループの同期を実行する System for Cross-domain Identity Management (SCIM) 2.0 アプリケーション（PingFederate では SP 接続と呼ばれます）。
- vCenter Server と共有する PingFederate ユーザーおよびグループを特定しておく必要があります。この共有は SCIM の処理です（OIDC の処理ではありません）。

PingFederate の接続要件：

- vCenter Server は、PingFederate 検出エンドポイントに接続可能で、さらに認可、トークン、JWKS、および検出エンドポイント メタデータにアドバタイズされているその他のエンドポイントに接続可能である必要があります。
- PingFederate も、SCIM プロビジョニング用のユーザーとグループのデータを送信するために vCenter Server に接続できる必要があります。

vCenter Server の要件：

- vSphere 8.0 Update 3
- PingFederate ID ソースを作成する vCenter Server で、VMware Identity Services が有効になっていることを確認します。

  注： vSphere 8.0 Update 1 以降をインストールするか、vSphere 8.0 Update 1 以降にアップグレードすると、VMware Identity Services がデフォルトで有効になります。vCenter Server 管理インターフェイスを使用して、VMware Identity Services のステータスを確認できます。VMware Identity Services の停止と起動を参照してください。

vSphere の権限の要件：

- フェデレーションされた認証に必要な vCenter Server ID プロバイダを作成、更新、削除するには、VcIdentityProviders.Manage 権限が必要です。ユーザーが ID プロバイダの設定情報のみを表示するように制限するには、VcIdentityProviders.Read 権限を割り当てます。

拡張リンク モードの要件：

- 拡張リンク モード構成では、PingFederate に対する vCenter Server ID プロバイダ フェデレーションを構成できます。拡張リンク モード構成で PingFederate を構成する場合は、単一の vCenter Server システムで VMware Identity Services を使用するように PingFederate ID プロバイダを構成します。たとえば、拡張リンク モード構成が 2 つの vCenter Server システムで構成されている場合、PingFederate サーバとの通信には 1 台の vCenter Server とその VMware Identity Services のインスタンスが使用されます。この vCenter Server システムが使用できなくなった場合、ELM 構成内の他の vCenter Server 上の VMware Identity Services を PingFederate サーバと連携させるように構成できます。詳細については、拡張リンク モード構成での外部 ID プロバイダのアクティベーション プロセスを参照してください。

- PingFederate を外部 ID プロバイダとして構成する場合、拡張リンク モード構成のすべての vCenter Server システムでは vSphere 8.0 Update 3 以降を実行する必要があります。

次に参照するドキュメント

手順

1 範囲の作成

PingFederate では、アクセス権限を制約および定義するための範囲の使用がサポートされます。

2 PingFederate ワークフローの共通構成の作成

PingFederate の共通構成の作成では、アクセス トークン マネージャ、objectID 属性、OpenID Connect ポリシー、および OAuth クライアント アプリケーションの作成を行います。

3 パスワード付与フロー構成の作成

PingFederate を vCenter Server で認証するには、パスワード付与フローを設定します。

4 認可コード フロー構成の作成

PingFederate で認可コード フローを作成するには、IdP アダプタを作成および構成します。

5 SCIM Provisioner のインストール

トークンを使用して PingFederate ユーザーとグループを VMware Identity Services に同期する、クロスドメイン ID 管理 (SCIM) アプリケーション用のシステムを作成します。

6 PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成

vSphere 8.0 Update 3 をインストールするか、vSphere 8.0 Update 3 にアップグレードした後、PingFederate に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

7 SCIM アプリケーション（SP 接続）の作成

vCenter Server にプッシュする PingFederate ユーザーおよびグループを指定するには、System for Cross-domain Identity Management (SCIM) 2.0 アプリケーションを作成する必要があります。

8 PingFederate 認証用の vCenter Server の構成

PingFederate ユーザーを vCenter Server グループに割り当てるか、インベントリレベルおよびグローバル権限を PingFederate ユーザーに割り当てることができます。

範囲の作成

PingFederate では、アクセス権限を制約および定義するための範囲の使用がサポートされます。

前提条件

「PingFederate 用に vCenter Server ID プロバイダを構成するための前提条件」を確認してください。

PingFederate 管理コンソールに管理者アカウントでログインします。

手順

1 [システム] - [OAuth 設定] - [範囲管理] の順に移動します。

2 [共通範囲] タブで、次の [範囲値] と説明を追加します。それぞれの値と説明を入力したら、[追加] をクリックします。

- [openid]
- [profile]
- [email]

3 [排他的範囲] タブをスキップします。

4 [デフォルト範囲] タブで、[デフォルト範囲] の説明を入力します。

説明は必須です。[デフォルト範囲の説明] が空の場合、PingFederate は次のエラーをログに記録します。

要求された範囲は、無効、不明、不正な形式、クライアントが要求できる範囲外のいずれかです。

5 [保存] をクリックします。

次のステップ

この後は「PingFederate ワークフローの共通構成の作成」に続きます。

PingFederate ワークフローの共通構成の作成

PingFederate の共通構成の作成では、アクセス トークン マネージャ、objectID 属性、OpenID Connect ポリシー、および OAuth クライアント アプリケーションの作成を行います。

前提条件

次のタスクを実行します。

- 範囲の作成

PingFederate 管理コンソールに管理者アカウントでログインします。

手順

1 アクセス トークン マネージャを作成します。

a [アプリケーション] - [OAuth] - [アクセス トークン管理] の順に移動します。

b [新規インスタンスの作成] をクリックします。

c [タイプ] タブで、次の手順を実行します。

- [インスタンス名] : インスタンス名を入力します。たとえば、vIDB Access Token Manager などです。
- [インスタンス ID] : インスタンス ID を入力します。たとえば、vIDB などです。
- [タイプ] : [JSON Web トークン] を選択します。
- [親インスタンス] : デフォルトの [なし] のままにします。

d [インスタンスの構成] タブで、次の手順を実行します。

- [一元化署名キーを使用] : チェックボックスをオンにします。

  このチェックボックスをオフのままにすると、PingFederate では「アクティブな署名証明書キー ID」が構成されることが想定されます。

- [JWS アルゴリズム] : アルゴリズムを選択します。たとえば、[SHA-256 を使用する RSA] とします。
- 画面の下部にある [詳細フィールドを表示] をクリックします。
  - [JWT ID 要求の長さ] : 0 よりも大きい数値を追加します。たとえば、24 と入力します。値を入力しない場合、JTI 要求はアクセス トークンに含まれません。

e [次へ] をクリックします。

f [アクセス トークン属性契約] タブで、次の手順を実行します。

- [契約の拡張] テキスト ボックスに、Ping アクセス トークン内に生成する次の要求を追加します。各要求を入力した後、[追加] をクリックします。
  - [aud]
  - [iss]
  - [exp]
  - [iat]
  - [userName]
- [サブジェクト属性名] : 監査目的で使用する要求を 1 つ選択します。たとえば、[iss] です。

g [次へ] を 2 回クリックして [リソース URI] タブと [アクセス コントロール] タブをスキップします。

h [保存] をクリックします。

2 objectGUID 属性を追加します。

a [システム] - [データ ストア] - [*マイ データ ストア*] - [LDAP 構成] の順に移動します。

b [LDAP 構成] タブで、下部にある [詳細] をクリックします。

c [LDAP バイナリ属性] タブの [バイナリ属性] 名前フィールドで、[objectGUID] を使用して [追加] をクリックします。

d [保存] をクリックします。

3 OpenID Connect ポリシーを作成します。

a [アプリケーション] - [OAuth] - [OpenID Connect ポリシー管理] の順に移動します。

b [ポリシーの追加] をクリックします。

c [ポリシーの管理] タブで、次の手順を実行します。

- [ポリシー ID] : ポリシー ID を入力します。たとえば、OIDC です。
- [名前] : ポリシー名を入力します。たとえば、OIDC ポリシーです。
- [アクセス トークン マネージャ] : 作成済みのアクセス トークン マネージャを選択します。たとえば、vIDB Access Token Manager などです。

d [次へ] をクリックします。

e [属性契約] タブで、次の手順を実行します。

- [削除] をクリックして、[sub] 以外のすべての属性を削除します。削除しない場合は、後から [契約の履行] タブで値に属性をマッピングする必要があります。

f [次へ] をクリックし、もう一度 [次へ] をクリックして [属性の範囲] タブをスキップします。

g [属性ソースとユーザーのルックアップ] タブで、[属性ソースの追加] をクリックします。

次の各タブに情報を入力したら、[次へ] をクリックして続行します。

- [データ ストア] :
  - [属性ソース ID] : 属性ソース ID を入力します。たとえば、vIDBLDAP などです。
  - [属性ソースの説明] : 説明を入力します。たとえば、vIDBLDAP などです。
  - [アクティブなデータ ストア] : ドロップダウンから Active Directory または OpenLDAP のドメイン名を選択します。
- [LDAP ディレクトリ検索] :
  - [ベース DN] : ユーザーとグループを検索する際のベース DN を入力します。
  - [検索範囲] : デフォルトの [サブツリー] のままにします。
  - [検索から返す属性] : [<すべての属性を表示>] を選択し、[objectGUID] を選択します。

    [属性の追加] をクリックします。
- [LDAP バイナリ属性エンコード タイプ] :
  - [ObjectGUID] : [属性エンコード タイプ] として [16 進] を選択します。
- [LDAP フィルタ] :
  - [フィルタ] : フィルタを入力します。たとえば、**`userPrincipalName=${userName}`** とします。

h [サマリ] 画面で、[完了] をクリックします。

i [次へ] をクリックして先に進み、[契約の履行] タブで ID トークンの [属性契約] をマッピングします。

属性契約	ソース	値
[sub]	作成済みの属性ソース ID を選択します。このドキュメントで使用されている例は、vIDBLDAP です。	[objectGUID]

j [次へ] をクリックし、もう一度 [次へ] をクリックして [保護条件] タブをスキップします。

k [保存] をクリックします。

4 OAuth クライアント アプリケーションを作成します。

a [アプリケーション] - [OAuth] - [クライアント] の順に移動します。

b [クライアントの追加] をクリックします。

c [クライアント | クライアント] 画面で、次の手順を実行します。

- [クライアント ID]：クライアント ID を入力します。たとえば、vIDB などです。

  注： クライアント ID をコピーして、後で PingFederate 用の vCenter Server ID プロバイダを作成するときのために保存します。

- [名前]：名前を入力します。たとえば、vIDB などです。
- [クライアント認証]：[クライアント シークレット] を選択します。
  - [クライアント シークレット]：自分のクライアント シークレットを入力するか、シークレットを生成します。この画面から離れると、シークレットを確認することはできません。シークレットを変更する以外の選択肢はありません。

    注： シークレットをコピーして、後で vCenter Server ID プロバイダを作成するときのために保存します。

- [リダイレクト URI]：リダイレクト URI を **`https://vCenter_Server_FQDN:port/federation/t/CUSTOMER/auth/response/oauth2`** の形式で入力します。
  - [追加] をクリックします。
- [許可される付与タイプ]：[認可コード]、[リフレッシュ トークン]、[クライアント認証情報]、[リソース所有者パスワード認証情報] を確認します。
- [デフォルトのアクセス トークン マネージャ]：作成済みのアクセス トークン マネージャを選択します。たとえば、このドキュメントで使用されているのは vIDB Access Token Manager です。
- [OpenID Connect]：[ポリシー] で、作成済みの値を選択します。たとえば、このドキュメントで使用されているのは OIDC です。

d [保存] をクリックします。

次のステップ

この後は「パスワード付与フロー構成の作成」に続きます。

パスワード付与フロー構成の作成

PingFederate を vCenter Server で認証するには、パスワード付与フローを設定します。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成

PingFederate 管理コンソールに管理者アカウントでログインします。

手順

1 パスワード認証情報バリデータを作成します。

   a [システム] - [データと認証情報ストア] - [パスワード認証情報バリデータ] の順に移動します。

   b [新規インスタンスの作成] をクリックします。

   c [パスワード認証情報バリデータ | 新規インスタンスの作成] 画面で、各タブに次のように情報を入力し、[次へ] をクリックして先に進みます。

      - [タイプ] タブで、次の手順を実行します。
         - [インスタンス名] : インスタンス名を入力します。たとえば、vIDB Validator とします。
         - [インスタンス ID] : インスタンス ID を入力します。たとえば、vIDB などです。
         - [タイプ] : [LDAP ユーザー名パスワード認証情報バリデータ] を選択します。
      - [インスタンスの構成] タブで、次の手順を実行します。
         - [LDAP データストア] : 使用しているデータ ストアを選択します。
         - [検索ベース] : ユーザーとグループを検索するベース DN を入力します。
         - [検索フィルタ] : フィルタを入力します。たとえば、**`userPrincipalName=${username}`** とします。
         - [検索範囲] : [サブツリー] を選択します。
      - [拡張された契約] タブで、次の手順を実行します。
         - デフォルトでは、以下が追加されます。
            - [DN]
            - [email]
            - [givenName]
            - [username]

   d [次へ] をクリックし、[保存] をクリックします。

2 認可サーバ設定でバリデータをマッピングします。

a [システム] - [OAuth の設定] - [認可サーバ設定] の順に移動します。

b [パスワード認証情報バリデータ] で、作成済みのバリデータを選択します。たとえば、このドキュメントでは vIDB Validator です。

c [保存] をクリックします。

3 リソース所有者認証情報付与マッピングを作成します。

a [認証] - [OAuth] - [リソース所有者認証情報マッピング] の順に移動します。

b [リソース所有者認証情報付与マッピング] ウィンドウで、次の手順を実行します。

- [ソース パスワード バリデータ インスタンス] : 作成済みのインスタンスを選択し、[マッピングの追加] をクリックします。

c [リソース所有者認証情報付与マッピング | リソース所有者認証情報マッピング] 画面で、[次へ] をクリックして [属性ソースとユーザーのルックアップ] タブをスキップします。

d [契約の履行] タブで、次の手順を実行します。

- [USER_KEY] で [パスワード認証情報バリデータ] を選択し、[値] で [username] を選択します。

e [次へ] をクリックして [保護条件] タブをスキップし、[保存] をクリックします。

4 アクセス トークン マッピングの作成 - パスワード認証情報バリデータをアクセス トークン マネージャにマッピングします。

このマッピングは、パスワード付与ワークフローに必要です。マッピングがないと、PingFederate は次のエラーを記録します。

選択されたクライアントと認証コンテキストで使用可能なアクセス トークン マネージャがありません。

a [アプリケーション] - [アクセス トークン マッピング] の順に移動します。

- [コンテキスト] : 作成済みのコンテキストを選択します。たとえば、このドキュメントでは vIDB Validator です。
- [アクセス トークン マネージャ] : 作成済みのアクセス トークン マネージャを選択します。たとえば、このドキュメントでは vIDB Access Token Manager です。

b [マッピングの追加] をクリックします。

c [次へ] をクリックして [属性ソースとユーザーのルックアップ] タブをスキップします。

d [契約の履行] タブで、次の表を使用します。

契約	ソース	値
[aud]	[コンテキスト]	作成済みのクライアント ID。たとえば、このドキュメントで使用されている ID は vIDB です。
[exp]	[マッピングなし]	-
[iat]	[式]	次のように入力します。 `@org.jose4j.jwt.NumericDate@now().getValue()`
[iss]	[式] (表示されない場合は、https://docs.pingidentity.com/r/en-us/pingfederate-120/pf_enable_disable_express の PingFederate ドキュメントを参照してください。)	次のように入力します。 `#tmp=#this.get("context.HttpRequest").getObjectValue().getRequestURL().toString(), #url=new java.net.URL(#tmp), #protocol=#url.getProtocol(), #host=#url.getHost(),#port=#url.getPort(), #result=(#port != -1) ? @java.lang.String@format("%s://%s:%d", #protocol, #host, #port) : @java.lang.String@format("%s://%s", #protocol, #host, #port)`
[userName]	[マッピングなし]	- この契約は、後で認可コード ワークフロー用の OIDC ポリシーに対する LDAP フィルタで使用されます。PingFederate ワークフローの場合は不要です。

e [次へ] をクリックして [保護条件] タブをスキップし、[保存] をクリックします。

次のステップ

この後は「認可コード フロー構成の作成」に続きます。

認可コード フロー構成の作成

PingFederate で認可コード フローを作成するには、IdP アダプタを作成および構成します。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成
- パスワード付与フロー構成の作成

PingFederate 管理コンソールに管理者アカウントでログインします。

手順

1 IdP アダプタを作成します。

a [認証] - [統合] - [IdP アダプタ] の順に移動します。

b [新規インスタンスの作成] をクリックします。

c [タイプ] タブで、次の手順を実行します。

- [インスタンス名] : HTML フォーム認証アダプタなどの名前を入力します。
- [インスタンス ID] : HTMLFormAuthAdapter などの ID を入力します。
- [タイプ] : HTML フォーム IdP アダプタを選択します。
- [親インスタンス] : [なし] を選択します。

d [次へ] をクリックします。

e [IdP アダプタ] タブで、次の手順を実行します。

[パスワード認証情報バリデータ インスタンス] で、[「認証情報バリデータ」に新しい行を追加] をクリックし、バリデータ（このドキュメントでは vIDB Validator を使用）を選択して、[更新] をクリックします。

f [IdP アダプタ] タブで、次の手順を実行します。

- [レルム] : [USER_KEY] を選択します。

g [次へ] をクリックします。

h [次へ] をクリックして [拡張された契約] タブをスキップします。

i [アダプタの属性] タブで、次の手順を実行します。

- [一意のユーザー キー属性] : [ユーザー名] を選択し、[Pseudonym] をオンにします。

j [次へ] をクリックして [アダプタ契約マッピング] タブをスキップし、[保存] をクリックします。

2 IdP アダプタ付与マッピングを作成します。

a [認証] - [OAuth] - [IdP アダプタ付与マッピング] の順に移動します。

b [ソース アダプタ インスタンス] : 作成したアダプタ インスタンスを選択し、[マッピングの追加] をクリックします。

c [属性ソースとユーザーのルックアップ] 画面で、[属性ソースの追加] をクリックします。

d 各タブで次のように情報を入力し、[次へ] をクリックして続行します。

- [データストア] タブで、次の手順を実行します。
  - [属性ソース ID] : ID を英数字の値で入力します。
  - [属性ソースの説明]。説明を入力します。
  - [アクティブなデータ ストア] : 使用中の Active Directory を選択します。
- [LDAP ディレクトリ検索] タブで、次の手順を実行します。
  - [ベース DN] : ユーザーとグループを検索する際のベース DN を入力します。
  - [検索範囲] : デフォルトの [サブツリー] を使用します。
  - [検索から返す属性] : [<すべての属性を表示>] を選択し、ロードされたら、属性リストから [userPrincipalName] を選択します。

e [属性の追加] をクリックし、[次へ] をクリックします。

f [LDAP フィルタ] タブで、次の手順を実行します。

- [フィルタ] : フィルタを入力します。たとえば、**`userPrincipalName=${username}`** とします。

g [次へ] をクリックし、[保存] をクリックします。

h [IdP アダプタ付与マッピング | IdP アダプタ マッピング] 画面で、IdP 付与マッピングの作成を完了します。

[契約の履行のルックアップ] タブで、次の表を使用します。

契約	ソース	値
[USER_KEY]	作成済みのソースを選択します。	[サブジェクトの識別名 (DN)]
[USER_NAME]	作成済みのソースを選択します。	[userPrincipalName]

i [次へ] をクリックし、[保存] をクリックします。

作成された IdP アダプタ付与マッピングは、[[*アダプタ名*」から永続的な付与契約] と表示されます。

3 IdP アダプタをアクセス トークン マネージャにマッピングします。

a [アプリケーション] - [OAuth] - [アクセス トークン マッピング] の順に移動します。

- [コンテキスト] : [IdP アダプタ: *アダプタ名*] を選択します。
- [アクセス トークン マネージャ] : 作成済みのアクセス トークン マネージャ インスタンスを選択します。たとえば、このドキュメントでは vIDB Access Token Manager です。

b [マッピングの追加] をクリックします。

このマッピングを実行しない場合、PingFederate によって次のログ ファイル メッセージが生成されます。

選択できるマッピング済みの認証ソースがありません。最初に IdP アダプタまたは IdP 接続をマッピングしてください。

c [属性ソースとユーザーのルックアップ] タブをスキップし、[契約の履行] タブで次の表を使用します。

契約	ソース	値
[aud]	[マッピングなし]	-
[exp]	[マッピングなし]	-
[iat]	[マッピングなし]	-
[iss]	[マッピングなし]	-
[userName]	[アダプタ]	[username]

d [次へ] をクリックして [保護条件] タブをスキップし、[保存] をクリックします。

次のステップ

この後は「SCIM Provisioner のインストール」に続きます。

SCIM Provisioner のインストール

トークンを使用して PingFederate ユーザーとグループを VMware Identity Services に同期する、クロスドメイン ID 管理 (SCIM) アプリケーション用のシステムを作成します。

PingFederate サーバで SCIM Provisioner をインストールし、SCIM を使用してユーザーとグループのプロビジョニングを有効にする必要があります。

注： 既存の PingFederate 環境を使用している場合は、SCIM Provisioner がすでにインストールされている可能性があります。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成
- パスワード付与フロー構成の作成
- 認可コード フロー構成の作成

手順

1 https://support.pingidentity.com/s/marketplace-integration/a7i1W0000004IDNQA2/scim-provisioner から SCIM Provisioner をダウンロードします。

PingIdentity ポータルにログインする必要があります。

2 `pf-scim-quickconnection-1.4.jar` ファイルを、PingFederate サーバの `/opt/out` フォルダにマウントされているフォルダにコピーします。

たとえば、ファイルを `/opt/out/instance/server/default/deploy` フォルダに配置します。

3 `/opt/out/instance/bin/run.properties` ファイルを表示して、次の設定が存在することを確認します。`pf.provisioner.mode=STANDALONE`

PingFederate のドキュメントに従って、次の手順を実行します。

STANDALONE - このサーバは、ユーザー インターフェイス コンソールとプロトコル エンジン（デフォルト）の両方を実行するスタンドアローン インスタンスです。

4 PingFederate サーバ インスタンスがコンテナ イメージとして実行されており、`run.properties` ファイルを更新した場合は、サーバの再起動が必要になることがあります。例：

a SSH を使用して PingFederate サーバに接続します。

b `/root/ping` ディレクトリに移動します。

c 次のコマンドを実行します。

```
docker-compose down
docker-compose up
```

結果

SCIM Connector は、「SCIM アプリケーション（SP 接続）の作成」でユーザー プロビジョニングを構成するときにオプションとして表示されます。

次のステップ

この後は「PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成」に続きます。

PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成

vSphere 8.0 Update 3 をインストールするか、vSphere 8.0 Update 3 にアップグレードした後、PingFederate に対して vCenter Server ID プロバイダ フェデレーションを外部 ID プロバイダとして構成できます。

vCenter Server は、1 つの構成されている外部 ID プロバイダ（1 つのソース）と、vsphere.local ID ソース（ローカル ソース）のみをサポートします。複数の外部 ID プロバイダを使用することはできません。vCenter Server ID プロバイダ フェデレーションは、vCenter Server へのユーザー ログインに OpenID Connect (OIDC) を使用します。

vCenter Server のグローバル権限またはオブジェクト権限による PingFederate グループとユーザーを使用して権限を構成できます。権限の追加の詳細については、ドキュメント『vSphere のセキュリティ』を参照してください。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成
- パスワード付与フロー構成の作成
- 認可コード フロー構成の作成

- SCIM Provisioner のインストール

PingFederate OpenID Connect アプリケーションに、次の情報があることを確認します。

- クライアント識別子
- クライアント シークレット（vSphere Client では共有シークレットとして表示）
- Active Directory ドメイン情報または PingFederate ドメイン情報（Active Directory を実行していない場合）

手順

1 vCenter Server で ID プロバイダを作成するには、次の手順を実行します。

a vSphere Client を使用して、vCenter Server に管理者としてログインします。

b [ホーム] - [管理] - [Single Sign-On] - [構成] の順に移動します。

c [プロバイダの変更] をクリックし、[PingFederate] を選択します。

[メイン ID プロバイダの構成] ウィザードが開きます。

d [前提条件] パネルで、PingFederate と vCenter Server、およびその他の要件を確認します。

e [事前チェックを実行] をクリックします。

事前チェックでエラーが検出された場合は、[詳細表示] をクリックしてエラーを解決する手順を実行します。

f 事前チェックが終了したら、確認のチェックボックスをオンにして、[次へ] をクリックします。

g [ディレクトリ情報] パネルで、次の情報を入力します。

- ディレクトリ名：PingFederate からプッシュされたユーザーとグループを格納する vCenter Server に作成するローカル ディレクトリの名前。**`vcenter-PingFederate-directory`** のように入力します。
- ドメイン名：vCenter Server と同期する PingFederate ユーザーおよびグループを含む PingFederate ドメイン名を入力します。

  PingFederate ドメイン名を入力したら、プラス記号アイコン (+) をクリックして追加します。複数のドメイン名を入力する場合は、デフォルトのドメインを指定します。

h [次へ] をクリックします。

i [OpenID Connect] パネルで、次の情報を入力します。

- リダイレクト URI：自動的に入力されます。このリダイレクト URI は、PingFederate で OpenID Connect アプリケーションを作成するときに使用するものと一致する必要があります。
- ID プロバイダ名：「PingFederate」が自動的に入力されます。
- クライアント識別子：OpenID Connect アプリケーションを作成したときに取得されます。（PingFederate では、クライアント識別子がクライアント ID と呼ばれます）。
- 共有シークレット：PingFederate で OpenID Connect アプリケーションを作成したときに取得されます。（PingFederate では、共有シークレットがクライアント シークレットと呼ばれます）。
- OpenID アドレス：https://*PingFederate_domain_space*/idp/.well-known/openid-configuration という形式になります。

  たとえば、PingFederate ドメイン領域が example.PingFederate.com の場合、OpenID アドレスは `https://example.PingFederate.com/idp/.well-known/openid-config` です。
- SSL 証明書：必要に応じて、PingFederate SSL 証明書、または証明書チェーン（その証明書が既知のパブリック認証局によって発行されていなかった場合）を参照して、vCenter Server にアップロードします。PingFederate SSL 証明書をエクスポートするには、管理コンソールで [セキュリティ] - [SSL サーバ証明書] の順に移動し、デフォルトの証明書を選択して、[アクションの選択] ドロップダウンから [エクスポート] を選択します。詳細については、記事「Exporting a certificate」(https://docs.pingidentity.com/r/en-us/pingfederate-111/nfv1585678806463) を参照してください。プライベート キーは vCenter Server 構成には必要ないため、PingFederate SSL 証明書はプライベート キーなしでエクスポートできます。

j [次へ] をクリックします。

k 情報を確認し、[終了] をクリックします。

vCenter Server で PingFederate ID プロバイダが作成されて、構成情報が表示されます。

2 [ユーザー プロビジョニング] で [生成] をクリックしてシークレット トークンを作成し、ドロップダウンからトークンの有効期間を選択してから、[クリップボードにコピー] をクリックします。トークンを安全な場所に保存します。

PingFederate SP 接続（SCIM アプリケーション）を作成するときは、トークンを使用して PingFederate ユーザーとグループを VMware Identity Services に同期します。

次のステップ

この後は SCIM アプリケーション（SP 接続）の作成に続きます。

SCIM アプリケーション（SP 接続）の作成

vCenter Server にプッシュする PingFederate ユーザーおよびグループを指定するには、System for Cross-domain Identity Management (SCIM) 2.0 アプリケーションを作成する必要があります。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成
- パスワード付与フロー構成の作成
- 認可コード フロー構成の作成
- SCIM Provisioner のインストール
- PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成

手順

1 vCenter Server の信頼できるルート証明書を PingFederate サーバに追加します。

最初に、信頼できるルート証明書を vCenter Server からエクスポートします。証明書は、`/var/lib/vmware/vmca/root.cer` にある vCenter Server のファイル システムから取得できます。または、https://kb.vmware.com/s/article/2108294 にあるナレッジベースの記事を参照してください。

a PingFederate 管理コンソールに管理者アカウントでログインします。

b [セキュリティ] - [証明書とキー管理] の順に移動します。

c [信頼できる CA] を選択し、[インポート] をクリックして vCenter Server の SSL 証明書を追加します。

d PingFederate サーバ インスタンスがコンテナ イメージとして実行されている場合は、トラスト ストアに証明書を追加するためにサーバの再起動が必要な場合があります。例：

1 SSH を使用して PingFederate サーバに接続します。

2 `/root/ping` ディレクトリに移動します。

3 次のコマンドを実行します。

```
docker-compose down
docker-compose up
```

2 SP 接続を作成します。

a PingFederate 管理コンソールに管理者アカウントでログインします。

b [アプリケーション] - [統合] - [SP 接続] の順に移動します。

c [接続の作成] をクリックします。

d [この接続にテンプレートを使用する] を選択し、ドロップダウンから [SCIM コネクタ] を選択します。

[SCIM コネクタ] オプションがドロップダウンに表示されない場合は、SCIM コネクタの `.jar` ファイルを正しいフォルダ（PingFederate サーバの `/opt/out` フォルダ）に配置してあるかどうかを確認します。

e [次へ] をクリックします。

f [送信プロビジョニング] のみを選択し、[次へ] をクリックします。

g [全般情報] タブで、次の手順を実行します。

- [パートナーのエンティティ ID（接続 ID）] : [SCIM コネクタ] を任意の名前に更新します。
- [接続名] : 名前を入力します。
- [ベース URL]:PingFederate 外部 ID プロバイダを構成する vCenter Server の HTTPS アドレスを入力します（例：**`https://vcenter1.example.com`**）。

h [次へ] をクリックします。

i [プロビジョニングの構成] をクリックします。

[ターゲット] タブで、次の手順を実行します。

- [SCIM URL] : ユーザーグループのエンドポイントを入力します。

  これは、vCenter Server の [構成] 画面にある [ユーザー プロビジョニング] で取得できるテナント URL です。例：**`https://vcenter1.example.com/usergroup/t/CUSTOMER/scim/v2`**
- [認証方法] : ドロップダウンから [OAuth 2 ベアラー トークン] を選択します。
- [アクセス トークン] : vCenter Server から生成され、保存しておいたシークレット トークンを貼り付けます。「PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成」の手順 2 を参照してください。
- [一意のユーザー ID] : ドロップダウンから [userName] を選択します。
- [フィルタ式] : 次の式をテキスト ボックスにコピーします。**`externalId eq "%s"`**

j デフォルトの構成の他の部分は設定値を受け入れて、[次へ] をクリックします。

- [プロビジョニング オプション] : [ユーザー作成]、[ユーザー更新]、[ユーザー無効化/削除] がオンになっています。
- [ユーザー アクションの削除] : [無効] が選択されています。

  注： [無効] を選択すると、ユーザーが Active Directory から削除されても VMware Identity Services では自動的に「無効」と表示されません。これは、想定どおりの動作です。

  - Active Directory では、次のプロビジョニング サイクルでユーザーが削除されることはなく、ユーザーのプロパティが "active"="false" になります。
  - 次のプロビジョニング サイクルで別のユーザーが Active Directory 内で作成または更新されるまで、このユーザーは VMware Identity Services で「無効」と表示されることはありません。これを回避するには、「https://support.pingidentity.com/s/article/After-deleting-an-AD-user-account-SaaS-provisioner-does-not-remove-the-user-in-the-next-provisioning-cycle-when-Group-DN-is-specified」に従います。
- [グループ名ソース] : [共通名] が選択されています。

k [チャネルの管理] タブで [作成] をクリックします。

- [チャネル情報]タブで、次の手順を実行します。
  - [チャネル名]：名前を入力します。
  - [最大スレッド数] と [タイムアウト（秒）] のデフォルト値を受け入れます。

l [次へ] をクリックします。

- [ソース] タブで、次の手順を実行します。
  - [アクティブなデータ ストア]：Active Directory ドメインを選択します。

m [次へ] をクリックします。

- [ソースの場所] タブで、次の手順を実行します。
  - [ベース DN]：ユーザーとグループを検索する際のベース DN を入力します。
  - [ユーザー]：環境に合わせてカスタマイズします。例：
    - [グループ DN]：使用しません。
    - [フィルタ]：
      (|(objectClass=person)(objectClass=organizationalPerson)(objectClass=user)) と入力します。
  - グループ：環境に合わせてカスタマイズします。例：
    - [グループ DN]：使用しません。
    - [フィルタ]：**(objectClass=group)** と入力します。

n [次へ] をクリックします。

o [属性マッピング] タブで、デフォルトの設定を受け入れます。

p [次へ] をクリックします。

[アクティベーションとサマリ] タブで、次の手順を実行します。

- [チャネル ステータス]：[有効] を選択します。

q [終了] をクリックします。

SP 接続が作成され、[SP 接続] 画面が表示されます。

r [終了] をクリックします。

s [送信プロビジョニング] タブで、[次へ] をクリックします。

t サマリを確認し、[保存] をクリックします。

u 接続を有効にするには、[有効] スライダを切り替えます。

結果

これによって PingFederate は、構成されたデータ ストアからユーザーとグループを vCenter Server にプッシュします。プッシュが実行されるまで待機します。プッシュされたユーザーとグループを vSphere Client で確認できます。[管理] - [Single Sign-On] - [ユーザーおよびグループ] の順に移動し、PingFederate ドメインを選択します。

次のステップ

この後は「PingFederate 認証用の vCenter Server の構成」に続きます。

PingFederate 認証用の vCenter Server の構成

PingFederate ユーザーを vCenter Server グループに割り当てるか、インベントリレベルおよびグローバル権限を PingFederate ユーザーに割り当てることができます。

PingFederate ユーザーがログインするために必要な最小権限は、読み取り専用権限です。

前提条件

次の操作を行います。

- 範囲の作成
- PingFederate ワークフローの共通構成の作成
- パスワード付与フロー構成の作成
- 認可コード フロー構成の作成
- SCIM Provisioner のインストール
- PingFederate に対する vCenter Server ID プロバイダ フェデレーションの構成
- SCIM アプリケーション（SP 接続）の作成

手順

1. PingFederate ユーザーをグループに割り当てるには、「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。
2. インベントリレベルおよびグローバル権限を PingFederate ユーザーに割り当てるには、『vSphere のセキュリティ』ドキュメントで vCenter Server コンポーネントの権限の管理に関するトピックを参照してください。
3. PingFederate ユーザーに権限を割り当てた後、ユーザーがログインできることを確認します。

VMware Single Sign-On の構成

vSphere 8.0 Update 3 をインストール、または vSphere 8.0 Update 3 にアップグレードした後、vCenter Server ホストを VMware Single Sign-On 用に構成できます。VMware Single Sign-On を構成するには、外部 ID プロバイダを使用して vCenter Server ホストにログインします。

VMware Single Sign-On を使用すると、拡張リンク モードが構成されていない vCenter Server ホストに接続できます。つまり、外部 ID プロバイダを構成してあれば、その構成を他の vCenter Server ホストへのシングル サインオンに活用できます。外部 ID プロバイダが構成されている vCenter Server ホストは、他の vCenter Server ホストに対して ID プロバイダとして機能します。

複数の vCenter Server ホストが VMware Single Sign-On を実行するように構成できます。そのためには、外部 ID プロバイダが構成された vCenter Server ホストを参照するように各 vCenter Server ホストを構成する必要があります。

VMware Single Sign-On 構成を実行した後でも、ローカル アカウントを使用して vCenter Server ホストにログインできます。

注： VMware Single Sign-On では、拡張リンク モードと異なり、vCenter Server ホスト間でインベントリが共有されません。

前提条件

VMware Single Sign-On の要件：

- VMware Single Sign-On を構成する vCenter Server で、vSphere 8.0 Update 3 が実行されていること。
- 接続する vCenter Server ホストで vSphere 8.0 Update 1 以降が実行されていること。
- 次のいずれかの外部 ID プロバイダを構成してあること。
  - Microsoft Entra ID
  - Okta
  - PingFederate
- 外部 ID プロバイダが構成されている vCenter Server ホストから、VMware Single Sign-On を構成する vCenter Server ホストに、信頼できるルート証明書を追加する必要があります。

手順

1. 外部 ID プロバイダが構成されている vCenter Server ホストから、信頼できるルート証明書をダウンロードします。例については、https://kb.vmware.com/s/article/2108294 にある VMware ナレッジベースの記事を参照してください。
2. その信頼できるルート証明書を、VMware SSO を構成する vCenter Server ホストにアップロードします。

   vSphere Client を使用した証明書ストアへの信頼できるルート証明書の追加を参照してください。
3. vSphere Client を使用して、VMware SSO を構成する vCenter Server ホストに管理者としてログインします。
4. [ホーム] - [管理] - [Single Sign-On] - [構成] の順に移動します。
5. [プロバイダの変更] をクリックし、[VMware SSO] を選択します。

   [メイン ID プロバイダの構成] ウィザードが開きます。
6. [前提条件] パネルで、vCenter Server の要件を確認します。

7 [事前チェックを実行] をクリックします。

事前チェックでエラーが検出された場合は、[詳細表示] をクリックしてエラーを解決する手順を実行します。

8 事前チェックが終了したら、確認のチェックボックスをオンにして、[次へ] をクリックします。

9 [OpenID Connect] パネルで、次の情報を入力します。

- ID プロバイダ名：「VMware SSO」が入力されます。
- vCenter Server FQDN：外部 ID プロバイダが構成されている vCenter Server ホストの FQDN を入力します。
- ポート番号：デフォルトの 443 をそのまま受け入れるか、使用するポートに変更します。
- ユーザー名とパスワード：外部 ID プロバイダが構成されているこの vCenter Server ホストの管理者アカウントのユーザー名とパスワードを入力します。

10 [次へ] をクリックします。

11 情報を確認し、[終了] をクリックします。

vCenter Server で VMware SSO プロバイダが作成されて、構成情報が表示されます。これで、この vCenter Server ホストには、構成が作成されたホストと同じ外部 ID プロバイダ構成が含まれました。たとえば、2 台のホスト間で OpenID 構成を比較すると、同じになっています。

12 認証に外部 ID プロバイダを使用するように、この vCenter Server を構成します。

外部 ID プロバイダのユーザーを vCenter Server グループに割り当てるか、インベントリレベルおよびグローバル権限をユーザーに割り当てることができます。ログインするために必要な最小権限は、読み取り専用権限です。

外部 ID プロバイダのユーザーをグループに割り当てるには、「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。インベントリレベルおよびグローバル権限をユーザーに割り当てるには、『vSphere のセキュリティ』ドキュメントで vCenter Server コンポーネントの権限の管理に関するトピックを参照してください。

13 外部 ID プロバイダのユーザーで、この vCenter Server ホストへのログインを検証します。

vSphere Client を起動すると、[VMware vSphere へようこそ] 画面に [SSO を使用してログイン] ボタンが表示されます。このボタンをクリックすると、外部 ID プロバイダのログイン画面にリダイレクトされます。

VMware Identity Services の管理

VMware Identity Services の停止および開始、SCIM トークンの再生成、削除された SCIM ユーザーおよびグループのリストアを行うことができます。

タスクに応じて、vSphere Client または外部 ID プロバイダの管理コンソールのいずれかを使用します。

VMware Identity Services の停止と起動

Okta、Microsoft Entra ID（旧称 Azure AD）、PingFederate を外部 ID プロバイダとして構成して実行するには、vCenter Server で VMware Identity Services を起動する必要があります。デフォルトでは、vSphere 8.0 Update 1 以降をインストールするか、このバージョンにアップグレードすると、VMware Identity Services が起動します。vCenter Server 管理インターフェイスを使用して、VMware Identity Services を管理します。

バージョン 8.0 Update 1 以降、vSphere には、Okta に対する認証をサポートする VMware Identity Services が組み込まれています。バージョン 8.0 Update 2 以降、VMware Identity Services では Microsoft Entra ID に対する認証がサポートされます。バージョン 8.0 Update 3 以降、VMware Identity Services では PingFederate に対する認証がサポートされます。

前提条件

vSphere 8.0 Update 1 以降をインストールまたはアップグレードすると、VMware Identity Services が自動的に開始されます。Okta、Microsoft Entra ID、PingFederate を外部 ID プロバイダとして構成する場合、VMware Identity Services はすでに実行されているため、起動する必要はありません。VMware Identity Services を起動または停止するには、root ユーザーである必要があります。

外部 ID プロバイダは、単一の vCenter Server でのみ構成します。この vCenter Server は、VMware Identity Services のインスタンスを介して ID プロバイダと通信します。拡張リンク モード構成の他の vCenter Server システムでも VMware Identity Services は実行されていますが、ID プロバイダと直接通信するわけではありません。

手順

1 Web ブラウザで、vCenter Server 管理インターフェイス (https://*vcenter-IP-address-or-FQDN*:5480) に移動します。

2 root としてログインします。

デフォルトの root パスワードは、vCenter Server のデプロイ時に設定したパスワードです。

3 [[サービス]] を選択します。

4 VMware Identity Services のステータスを確認します。

5 サービスを停止または起動するには、[VMware Identity Services] を選択し、[停止] または [起動] をクリックします。

VMware Identity Services を起動した後、vCenter Server を再起動する必要はありません。

vCenter Server での SCIM トークンの再生成

vCenter Server では、外部 ID プロバイダに対するクロスドメイン ID 管理 (SCIM) のシステムのトークンを再生成できます。

別のトークンを生成すると、すぐにアクティブになり、以前のトークンは失効します。

前提条件

vCenter Server で外部 ID プロバイダを作成しておく必要があります。

手順

1 vSphere Client を使用して管理者として vCenter Server にログインします。

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 [構成] 画面の [ユーザー プロビジョニング]/[シークレット トークン] で、[再生成] をクリックしてシークレット トークンを再生成し、ドロップダウンからトークンの有効期間を選択して、[クリップボードにコピー] をクリックします。トークンを安全な場所に保存します。

4 コピーされたトークンは、外部 ID プロバイダの構成を更新する際に使用できます。

削除された SCIM ユーザーおよびグループのリストア

SCIM によって vCenter Server にプッシュされたユーザーとグループが外部 ID プロバイダと同期しなくなった場合は、問題を修正する手順を実行できます。

SCIM によってプッシュされたユーザーまたはグループを vCenter Server から削除した後にリストアする場合、ID プロバイダからユーザーまたはグループを単にプッシュすることはできません。vCenter Server ではユーザーおよびグループの管理にクロスドメイン ID 管理 (SCIM) のシステムが使用されるため、見つからないユーザーまたはグループを使用して SCIM 2.0 アプリケーション自体を更新する必要があります。

手順

1 外部 IDP 管理コンソールにログインします。

2 SCIM 2.0 アプリケーションに移動します。

3 削除した、あるいは見つからないユーザーまたはグループを割り当てます。

4 プッシュされたグループまたはユーザーを削除するための適切なアクションを選択して、そのグループまたはユーザーのリンクを解除します。

5 グループをプッシュするための適切なアクションを選択します。

6 外部 IDP がグループまたはユーザーを同期したことを vCenter Server で確認します。

vCenter Single Sign-On

外部 ID プロバイダを使用していない場合は、組み込み ID プロバイダの基盤アーキテクチャ、vCenter Single Sign-On、およびそれら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を理解しておく必要があります。

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、VMware Directory Service (vmdir) が含まれます。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、次のコンポーネントは vCenter Server のデプロイの一環として展開されます。

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 Server 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インタラクティブ ユーザー、スクリプト ユーザー、サービス ユーザー（ソリューション ユーザーを含む）は、vCenter Single Sign-On がサポートしている任意の vCenter Server 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 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 ドメインは、vCenter Server をインストールするときに変更できます。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、各 vCenter Server 環境に含まれています。このサービスは、LDAP ディレクトリをポート 389 で使用できるようにするマルチテナントのピアレプリケート ディレクトリ サービスです。また、vCenter Single Sign-On のユーザーアカウントとパスワードの保存と管理も行います。これらは SHA-512 ハッシュ アルゴリズムで保護されます。

使用している環境にリンク モードで設定された vCenter Server 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。

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。

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、vCenter Single Sign-On への認証にこの証明書を使用します。vCenter Single Sign-On からソリューション ユーザーに SAML トークンが提供されるため、ソリューション ユーザーは環境内の他のサービスと対話できるようになります。
- 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 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 への認証を行うことができるすべてのユーザーは、パスワードをリセットできます。vCenter Single Sign-On パスワードの変更 を参照してください。パスワードを忘れたユーザーのパスワードは、vCenter Single Sign-On の管理者のみがリセットできます。

vCenter Single Sign-On 管理者ユーザー

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

vCenter Single Sign-On を構成し、vCenter Single Sign-On ユーザーとグループを管理するには、administrator@vsphere.local ユーザーまたは vCenter Single Sign-On 管理者グループのユーザーが vSphere 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。

vCenter Server のその他のユーザー アカウント

次のユーザー アカウントは、vsphere.local ドメイン（またはインストール時に作成したデフォルト ドメイン）にある vCenter Server 内に自動的に作成されます。これらのユーザー アカウントはシェル アカウントです。これらのアカウントには、vCenter Single Sign-On パスワード ポリシーは適用されません。

表 4-1. vCenter Server のその他のユーザー アカウント

アカウント	説明
K/M	Kerberos キーの管理用。
krbtgt/VSPHERE.LOCAL	統合 Windows 認証との互換性用。
waiter-*random_string*	Auto Deploy 用。

ESXi ユーザー

スタンドアローンの ESXi ホストは vCenter Single Sign-On と統合されていません。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、ESXCLI、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 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に、サポートされる設定とサポートされない設定を確認するには、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/2064250) 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の実行を許可します。

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。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。

注意： 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 4-2. 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	vCenter サービスのソリューション ユーザー グループ。各ソリューション ユーザーは、証明書により vCenter Single Sign-On に対して個別に認証します。デフォルトでは、VMCA が証明書を使用してソリューション ユーザーをプロビジョニングします。このグループには、メンバーを明示的に追加しないでください。
CAAdmins	CAAdmins グループのメンバーには、VMCA の管理権限があります。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	このグループのユーザーには、すべてのアプライアンス管理 API に対するフル アクセス権があります。デフォルトでは、SSH を使用して vCenter Server に接続するユーザーは制約されたシェルのコマンドにのみアクセスできますが、このグループ内のユーザーには SSH 経由の Bash シェル アクセス権があり、root ユーザーと同様の完全な権限が付与されます。
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。
ExternalIDPUsers	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、ポート 5480 で動作している vCenter Server 管理インターフェイス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、サービスの表示、サービスの起動と再起動、サービスのトラブルシューティングを行うことができます。これらのユーザーは、重要なシステム構成を変更する API 以外のアプライアンス管理 API にアクセスすることもできます。
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。

表 4-2. vsphere.local ドメイン内のグループ （続き）

権限	説明
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。
TrustedAdmins	このグループのメンバーは、VMware® vSphere Trust Authority™ の設定および管理タスクを実行できます。デフォルトでは、このグループにはメンバーが含まれていません。このグループにメンバーを追加して、vSphere Trust Authority のタスクを実行できるようにする必要があります。
Autoupdate	このグループは、vCenter Cloud Gateway の内部で使用されます。
SyncUsers	このグループは、vCenter Cloud Gateway の内部で使用されます。
vSphereClientSolutionUsers	このグループは、vSphere Client の内部で使用されます。
ServiceProviderUsers	このグループのメンバーは、vSphere with Tanzu および VMware Cloud on AWS インフラストラクチャを管理できます。
NsxAdministrators	このグループは VMware NSX で使用されます。
WorkloadStorage	ワークロード ストレージ グループ。
RegistryAdministrators	このグループのメンバーはレジストリを管理できます。
NsxAuditors	このグループは VMware NSX で使用されます。
NsxViAdministrators	このグループは VMware NSX で使用されます。
SystemConfiguration.SupportUsers	SystemConfiguration.SupportUsers グループのメンバーは、サポート バンドル API にアクセスできます。
SystemConfiguration.ReadOnly	このグループのメンバーは、アプライアンス管理中に vCenter Server Appliance の読み取り専用操作にアクセスできます。
VCLSAdmin	このグループのメンバーには、vSphere クラスタ サービス (vCLS) に対する管理権限があります。
AnalyticsService.Administrators	このグループは、VMware 分析サービス API に使用されます。
vStatsGroup	このグループは vStats の収集に使用されます。

vCenter Single Sign-On ID 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。

注： vSphere 7.0 Update 2 以降では、vCenter Server で FIPS を有効にできます。『vSphere のセキュリティ』ドキュメントを参照してください。FIPS が有効な場合、LDAP を介した Active Directory はサポートされません。FIPS モードの場合、外部 ID プロバイダ フェデレーションを使用します。vCenter Server ID プロバイダ フェデレーションの設定を参照してください。

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。インストール後、vCenter Single Sign-On のすべてのインスタンスに ID ソース *your_domain_name* があります（たとえば、vsphere.local など）。この ID ソースは、vCenter Single Sign-On の内部のものです。

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を追加する必要があります。ドメイン名の形式は次のとおりです。

```
DOMAIN\user
```

次の ID ソースが使用可能です。

- LDAP 経由の Active DirectoryvCenter Single Sign-On は、LDAP を介した Active Directory の複数の ID ソースをサポートしています。
- Active Directory（統合 Windows 認証）バージョン 2003 以降。vCenter Single Sign-On を使用すると、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 ナレッジベースの記事 KBhttps://kb.vmware.com/s/article/2064250 では、vCenter Single Sign-On でサポートされている Microsoft Active Directory 信頼について解説しています。

- 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ています。

注： Microsoft Windows の更新によって、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した。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。詳細については、https://portal.msrc.microsoft.com/ja-JP/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。

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 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 プロバイダ] タブで [ID ソース] をクリックし、ID ソースを選択して、[デフォルトとして設定] をクリックします。
5. [OK] 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タイプ列に（デフォルト）と表示されます。

vCenter Single Sign-On ID 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、LDAP を介した Active Directory、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。vCenter Single Sign-On による vCenter Server の ID ソースを参照してください。

インストール直後に、vsphere.local ドメイン（またはインストール時に指定したドメイン）が、vCenter Single Sign-On 内部ユーザーとともに使用可能になります。

注： Active Directory SSL 証明書を更新または置換した場合は、vCenter Server の ID ソースを削除して再度追加する必要があります。

前提条件

Active Directory（統合 Windows 認証）ID ソースを追加する場合は、vCenter Server 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 vCenter Server の追加を参照してください。

手順

1. vSphere Client を使用して vCenter Server にログインします。
2. 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 プロバイダ] タブで [ID ソース] をクリックし、[追加] をクリックします。

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	このオプションでは、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。LDAP [Lightweight Directory Access Protocol] を介した Active Directory 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。LDAP [Lightweight Directory Access Protocol] を介した Active Directory および OpenLDAP Server ID ソースの設定を参照してください。

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に失敗します。ユーザー アカウントは、ユーザーとグループの組織単位（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り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権を提供します。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

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』ドキュメントで、ロールを使用した権限の割り当てに関するトピックを参照してください。

LDAP [Lightweight Directory Access Protocol] を介した Active Directory 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 ソースを構成する場合は、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/2064977) で追加要件を確認してください。

重要: LDAP を介した Active Directory ID ソース内のグループで異なるドメインのユーザーを使用することは、ドメインごとに追加の ID ソースを作成した場合でもできません。

LDAP ID ソース内のグループは、指定されたユーザー ベース DN 内のユーザーのみを認識します。そのため、子ドメインを持つ大規模な Active Directory 環境では予期しない問題が発生する可能性があります。例として、次のシナリオについて考えてみます。

1 ChildA と ChildB の 2 つの子ドメインを持つ Active Directory フォレスト。

2 2 つの LDAP を介した Active Directory ソース（1 つは子ドメイン ChildA 用、もう 1 つは子ドメイン ChildB 用）で構成された vCenter Server。

3 ChildA には UserA1 と UserA2 という名前の 2 人のユーザーが含まれています。

4 ChildB には UserB1 と UserB2 という名前の 2 人のユーザーが含まれています。

vCenter Server 管理者が UserA1、UserA2、UserB1、UserB2 を含む TestGroup という名前の ChildA にグループを作成します。vCenter Server 管理者が TestGroup にログイン（または任意の）権限を付与します。しかし、UserB1 と UserB2 はグループと異なるドメインに含まれているため、ログインできません。

回避策としては、以下を実行します。

1 ChildB に SecondTestGroup という名前の別のグループを作成します。

2 UserB1 と UserB2 を TestGroup から削除します。

3 UserB1 と UserB2 を SecondTestGroup に追加します。

4 vCenter Server で、TestGroup に付与したのと同じ権限を SecondTestGroup に割り当てます。

注： Microsoft Windows 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した。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 4-3. LDAP [Lightweight Directory Access Protocol] を介した Active Directory および OpenLDAP Server 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。

表 4-3. LDAP [Lightweight Directory Access Protocol] を介した Active Directory および OpenLDAP Server の設定 （続き）

オプション	説明
[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 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。ホスト名または IP アドレスのいずれかを使用できます。 **`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。

表 4-3. LDAP [Lightweight Directory Access Protocol] を介した Active Directory および OpenLDAP Server の設定 （続き）

オプション	説明
[セカンダリ サーバの URL]	プライマリ ドメイン コントローラが使用できない場合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。ホスト名または IP アドレスのいずれかを使用できます。LDAP を操作するたびに、vCenter Server は必ずプライマリ ドメイン コントローラを試行してから、セカンダリ ドメイン コントローラにフォールバックします。このため、プライマリ ドメイン コントローラが使用できない場合、Active Directory へのログインには時間がかかり、失敗することもあります。 **注：** プライマリ ドメイン コントローラに障害が発生したときに、セカンダリ ドメイン コントローラに自動的に引き継がれない可能性があります。
[証明書 (LDAPS の場合)]	Active Directory LDAP サーバまたは OpenLDAP Server の ID ソースで LDAPS を使用する場合は、**参照** をクリックして、LDAPS URL で指定されたドメイン コントローラからエクスポートされた証明書を選択します。（ここで使用する証明書はルート CA 証明書ではないことに注意してください。）Active Directory から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。 複数の証明書を参照して選択できます。 **ヒント:** 複数の証明書を参照して選択する場合は、それらを同じディレクトリに配置する必要があります。 vCenter Server は、登録および信頼されている認証局によって直接署名された証明書のみを信頼します。vCenter Server は、登録済みの CA 証明書までの経路を追跡せず、証明書が、登録および信頼されている認証局によって署名されているかどうかのみを確認します。証明書が公的に信頼されている認証局によって署名されているか、自己署名されている限り、それ以上のアクションは必要ありません。ただし、独自の内部証明書を作成する（プライベート認証局を使用する）場合は、それらの証明書を含めることが必要になる可能性があります。たとえば、組織が Microsoft Enterprise ルート認証局を使用して LDAPS 証明書を生成している場合は、そのエンタープライズ ルート証明書を選択して vCenter Server に追加することも必要です。また、LDAPS 証明書とエンタープライズ ルート証明書の間で中間認証局を使用する場合は、それらの中間証明書を選択して vCenter Server に追加することも必要です。

Active Directory ID ソースの設定

Active Directory（統合 Windows 認証）ID 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（統合 Windows 認証）ID ソース使用の前提条件

Active Directory（統合 Windows 認証）ID 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。『vCenter Server 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 (https://kb.vmware.com/s/article/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。

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 4-4. 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 の名前解決が可能である必要があります。
[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` コマンドを実行すると、重複が作成されていないことをチェックできます。`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。

CLI を使用した ID ソースの追加または削除

`sso-config` ユーティリティを使用して、ID ソースを追加または削除できます。

ID ソースとして、ネイティブの Active Directory（統合 Windows 認証）ドメイン、LDAP を介した Active Directory、LDAPS (SSL を介した LDAP) を使用する LDAP を介した Active Directory、または OpenLDAP を使用できます。vCenter Single Sign-On による vCenter Server の ID ソースを参照してください。また、`sso-config` ユーティリティを使用して、スマート カードと RSA SecurID 認証を設定します。

前提条件

Active Directory ID ソースを追加する場合は、vCenter Server 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 vCenter Server の追加を参照してください。

SSH ログインを有効にします。vCenter Server シェルを使用した vCenter Server の管理を参照してください。

手順

1 SSH などのリモート コンソール接続を使用して、vCenter Server システムでセッションを開始します。

2 root としてログインします。

3 `sso-config` ユーティリティが配置されているディレクトリに移動します。

```
cd /opt/vmware/bin
```

4 `sso-config.sh -help` を実行して `sso-config` のヘルプを参照するか、VMware ナレッジベースの記事 (https://kb.vmware.com/s/article/67304) で使用例を参照してください。

vCenter Server Security Token Service の管理

vCenter Server 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。

トークンの発行者である Security Token Service (STS) では、プライベート キーを使用してトークンに署名し、サービスのパブリック証明書を公開してトークンの署名を検証します。vCenter Server では、STS 署名証明書が管理され、VMware Directory Service (vmdir) に保存されます。トークンは有効期間が長く、複数のキーのいずれも、これまで署名に使用された可能性があります。

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、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。

表 4-5. STS ユーザーと認証情報

ユーザーのタイプ	プライマリ認証情報
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。

デフォルトでは、VMware Certificate Authority (VMCA) で STS 署名証明書が生成されます。STS 署名証明書を新しい VMCA 証明書で更新できます。デフォルトの STS 署名証明書をインポートして、カスタムまたはサードパーティによって生成された STS 署名証明書と置き換えることもできます。会社のセキュリティ ポリシーですべての証明書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。

vSphere Client を使用して、以下のことを行えます。

- STS 証明書の管理
- カスタムおよびサードパーティによって生成された STS 証明書のインポートと置き換え
- 有効期限などの STS 証明書の詳細を表示

コマンド ラインを使用して、カスタムおよびサードパーティによって生成された STS 証明書を置き換えることもできます。

STS 証明書の期間と有効期限

vSphere 7.0 Update 1 以降の新規インストールでは、10 年の期間を持つ STS 署名証明書が作成されます。STS 署名証明書の有効期限が近づくと、90 日前から 1 週間に 1 回アラームが表示され、7 日前になると毎日表示されます。

注： 特定の状況では、STS 署名証明書を置き換えると、証明書の有効期間が変わることがあります。証明書の置き換えを実行する場合は、発行日と有効期間に注意してください。

STS 証明書の自動更新

vSphere 8.0 以降で vCenter Single Sign-On を使用すると、VMCA によって生成された STS 署名証明書は自動的に更新されます。自動更新は、STS 署名証明書の有効期限が切れる前、かつ 90 日の期限切れアラームがトリガされる前に実行されます。自動更新が失敗した場合、vCenter Single Sign-On はログ ファイルにエラー メッセージを作成します。必要に応じて、STS 署名証明書を手動で更新できます。

注： vCenter Single Sign-On は、カスタム生成された STS 署名証明書やサードパーティの STS 署名証明書を自動更新しません。

STS 証明書の更新、インポート、および置き換え

vSphere 8.0 以降、STS 署名証明書の更新、インポート、または置き換えでは vCenter Server による再起動が必要ないため、ダウンタイムが発生しません。また、リンクされた構成で、単一の vCenter Server の STS 署名証明書を更新、インポート、または置換すると、リンクされたすべての vCenter Server システムの STS 証明書が更新されます。

注： 特定の状況では、STS 署名証明書の更新、インポート、または置換を行った場合に、手動による vCenter Server システムの再起動が必要になることがあります。

vSphere Client を使用した vCenter Server STS 証明書の更新

vSphere Client を使用して、vCenter Server STS 署名証明書を更新できます。VMware Certificate Authority (VMCA) によって新しい証明書が発行され、現在の証明書が置き換えられます。

STS 署名証明書を更新すると、VMware Certificate Authority (VMCA) によって新しい証明書が発行され、VMware Directory Service (vmdir) の現在の証明書が置き換えられます。STS は新しい証明書を使用して新しいトークンを発行します。拡張リンク モード構成で、vmdir は新しい証明書を発行元の vCenter Server システムからリンクされているすべての vCenter Server システムにアップロードします。STS 署名証明書を更新する場合、vCenter Server システムと、拡張リンク モード構成の一部であるその他の vCenter Server システムを再起動する必要はありません。

カスタム生成された、またはサードパーティの STS 署名証明書を使用している場合、更新によってその証明書が VMCA によって発行された証明書で上書きされます。カスタム生成された、またはサードパーティの STS 署名証明書を更新するには、インポートおよび置換オプションを使用します。vSphere Client を使用した vCenter Server STS 証明書のインポートと置き換えを参照してください。

VMCA によって発行された STS 署名証明書は 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、この証明書は置き換えないでください。

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。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 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [STS 署名] タブで目的の証明書を選択し、[vCenter Server 証明書を使用して更新] をクリックします。

カスタム生成された、またはサードパーティの STS 署名証明書を使用している場合、更新操作によってその証明書が VMCA で生成された証明書で上書きされます。

注： コンプライアンス上の理由でサードパーティの証明書を使用していた場合、更新によって vCenter Server システムが非準拠になることがあります。また、カスタム生成された、またはサードパーティの STS 署名証明書を使用している場合、Security Token Service でそのカスタム証明書またはサードパーティ証明書がトークン署名に使用されなくなります。

6 [更新] をクリックします。

VMCA は、この vCenter Server システムおよびリンクされた vCenter Server システムの STS 署名証明書を更新します。

7 （オプション）[強制的に更新] ボタンが表示される場合、vCenter Single Sign-On で問題が検出されたということです。[強制的に更新] をクリックする前に、以下の予想される結果を考慮してください。

- 影響を受けるすべての vCenter Server システムで vSphere 7.0 Update 3 以降が実行されていない場合、証明書の更新はサポートされません。
- [強制的に更新] を選択する場合は、すべての vCenter Server システムを再起動する必要があり、再起動するまでこれらのシステムが動作不能になる可能性があります。

a 影響が不明な場合、[キャンセル] をクリックして、環境を調査してください。

b 影響がわかっている場合、[強制的に更新] をクリックして、更新を続行してから、手動で vCenter Server システムを更新します。

vSphere Client を使用した vCenter Server STS 証明書のインポートと置き換え

vSphere Client を使用して、vCenter Server STS 証明書をインポートし、カスタム生成証明書またはサードパーティ証明書と置き換えることができます。

デフォルトの STS 署名証明書をインポートして置き換えるには、最初に新しい証明書を生成する必要があります。STS 署名証明書をインポートして置き換えると、VMware Directory Service (vmdir) は新しい証明書を発行元の vCenter Server システムからリンクされているすべての vCenter Server システムにアップロードされます。

STS 証明書は、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、この証明書は置き換えないでください。

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 システムの管理者権限を持つユーザーの 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 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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [STS 署名] タブで目的の証明書を選択し、[証明書をインポートして置き換え] をクリックします。

6 PEM ファイルを選択します。

PEM ファイルには、署名証明書チェーンとプライベート キーが含まれます。

7 [置き換え] をクリックします。

STS 署名証明書は、この vCenter Server システムおよびリンクされた vCenter Server システムで置き換えられます。特に指定がない限り、vCenter Server システムを再起動する必要はありません。

コマンド ラインを使用した vCenter Server STS 証明書の置き換え

CLI を使用して、vCenter Server STS 証明書をカスタム生成された証明書またはサードパーティの証明書と置き換えることができます。

既存の STS 署名証明書を置換することで、会社が求める証明書を使用する、または有効期限切れ間近の証明書を更新することができます。デフォルトの STS 署名証明書を置き換えるには、最初に新しい証明書を生成する必要があります。

STS 証明書は、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、この証明書は置き換えないでください。

注意： ここで説明する手順を使用する必要があります。ファイル システム上の証明書を直接置き換えないでください。

前提条件

vCenter Server への SSH ログインを有効にします。vCenter Server シェルを使用した vCenter Server の管理を参照してください。

手順

1 vCenter Server シェルに root としてログインします。

2 証明書を作成します。

a 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/newsts
```

b 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
```

c Vim などのコマンドライン エディタを使用して、`certool.cfg` ファイルのコピーを開き、ローカルの vCenter Server 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
```

d 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
```

e 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
```

f 証明書チェーンとプライベート キーを使用して、PEM ファイルを作成します。

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 STS 署名証明書を更新します。たとえば、次のようにします。

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

VMCA は、この vCenter Server システムおよびリンクされた vCenter Server システムの STS 署名証明書を更新します。

vSphere Client を使用したアクティブな vCenter Server STS 署名証明書チェーンの表示

vSphere Client を使用して、アクティブな vCenter Server STS 署名証明書チェーンと証明書情報（有効期限の日付など）を表示できます。

手順

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

2 少なくとも 読み取り 権限を持つユーザーのユーザー名とパスワードを入力します。

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 の認証情報の入力を求めるメッセージが表示されたら、この情報を入力します。

5 [STS 署名] タブで、証明書を選択して証明書を展開します。

次を含む、証明書と問題の情報が表示されます。

- 有効期限の日付
- 有効な証明書には緑色のチェックと、証明書の有効期限が切れた証明書について警告するオレンジ色のチェック

コマンド ラインを使用した LDAPS SSL 証明書の有効期限の特定

LDAPS を介した Active Directory を使用している場合は、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。`sso-config.sh` コマンドを使用して、証明書の有効期限を表示し、期限が切れる前に証明書を交換するか更新するかを判断できます。

vCenter Server は、アクティブな LDAP SSL 証明書の有効期限が近づくとアラートを表示します。

LDAP を介した Active Directory または OpenLDAP ID ソースを使用し、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。

前提条件

vCenter Server への SSH ログインを有効にします。vCenter Server シェルを使用した vCenter Server の管理を参照してください。

手順

1 vCenter Server に root としてログインします。

2 次のコマンドを実行します。

```
/opt/vmware/bin/sso-config.sh -get_identity_sources
```

SLF4J メッセージは無視します。

3 有効期限を確認するには、SSL 証明書の詳細を表示し、`NotAfter` フィールドを確認します。

vCenter Single Sign-On ポリシーの管理

vCenter Single Sign-On ポリシーは一般的に、ローカル アカウントとトークンのセキュリティ 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) 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 の組み込みユーザー アカウントのパスワードは 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。

注： 管理者アカウント (administrator@vsphere.local) はロックアウトされず、パスワードも有効期限切れになりません。適切なセキュリティ対策は、このアカウントからのログインを監査し、パスワードを定期的に変更することです。

手順

1 vSphere Client を使用して 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 [ローカル アカウント] タブをクリックします。

5 [パスワード ポリシー] 行の [編集] をクリックします。

6 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。

オプション	説明
最小長	パスワードに必要な最小文字数。最小長は、アルファベット、数字、および特殊文字の最小要件を組み合わせた文字数以上であることが必要です。
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 ■ 隣接する同一値：値は 0 より大きくする必要があります。たとえば 1 と入力すると、「p@$$word」というパスワードは許可されません。 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。

注： パスワード ポリシーは、最小長が 20 文字を超える場合にのみ、最大長の値を取得します。最小長の値が 20 文字を超え、最大長が任意の値に設定されている場合、パスワード ポリシーの動作が未定義になるか、サービスの停止が発生する可能性があります。潜在的な問題を回避するには、最小長をデフォルト値の 8 文字または 20 文字以下に設定します。

7 [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 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 [ローカル アカウント] タブをクリックします。

5 [ロックアウト ポリシー] 行の [編集] をクリックします。

[ロックアウト ポリシー] 行が表示されるまでスクロールが必要な場合があります。

6 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。

7 [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 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 [ローカル アカウント] タブをクリックします。

5 [トークンの信頼性] 行の [編集] をクリックします。

[トークンの信頼性] 行が表示されるまでスクロールが必要な場合があります。

6 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。
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。

7 [保存] をクリックします。

Active Directory（統合 Windows 認証）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 ServerSSO 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。vSphere Client は有効期限の通知を制御します。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。

前提条件

- vCenter Server への SSH ログインを有効にします。vCenter Server シェルを使用した vCenter Server の管理を参照してください。

手順

1 vCenter Server シェルに、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 vSphere Client`webclient.properties` ファイルの場所に変更します。

```
cd /etc/vmware/vsphere-ui
```

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 vSphere Client を再起動します。

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

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。

vSphere Client には、vSphere ドメイン（デフォルトでは vsphere.local）内のユーザーとグループのビューが表示されます。このビューから、ユーザーを追加、編集、および非アクティブ化できます。グループを追加したり、グループ メンバーシップを管理したりすることもできます。

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。

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 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 [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。

ユーザー名に使用できる最大文字数は 300 です。

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 ユーザーの無効化と有効化

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 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、[詳細] 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、[詳細] をクリックし、[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 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。

7 [削除] をクリックします。

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] - [ローカル アカウント] - [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 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 ユーザーを選択し、[編集] をクリックします。

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 [保存] 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 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、[グループの作成] 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。

グループ名に使用できる最大文字数は 300 です。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 [メンバーの追加] ドロップダウン メニューで、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。

AD FS などの外部 ID プロバイダを構成してある場合は、その ID プロバイダのドメインを [メンバーの追加] ドロップダウン メニューで選択できます。

7 検索語を入力します。

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 [終了] をクリックします。

次のステップ

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 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 (https://kb.vmware.com/s/article/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 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 [編集] をクリックします。

6 [ドメイン] ドロップダウン メニューで、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。

AD FS などの外部 ID プロバイダを構成してある場合は、その ID プロバイダのドメインを [ドメイン] ドロップダウン メニューで選択できます。

7 検索語を入力します。

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 vSphere+ 環境で [ドメイン] ドロップダウン メニューから [VMware ID] を選択した場合は、[ユーザー名] フィールドに CSP アカウントの名前を入力します。

注： [ユーザー名] フィールドに、CSP アカウントのメール アドレスを入力します。VMwareID ドメインで CSP アカウントを検索できません。

10 [保存] 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 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] をクリックしてグループを選択します。

5 [編集] をクリックします。

6 現在のメンバー リストで、削除するユーザーまたはグループをクリックします。

7 [終了] をクリックします。

結果

ユーザーまたはグループ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 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、vSphere Client 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 のパスワードは 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 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 ペインでユーザー名をクリックしてメニューをプルダウンし、[パスワードの変更] を選択します。

4 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 [確認] をクリックします。

または、[Single Sign-On] - [ユーザーおよびグループ] の順に選択し、ユーザーを選択して、[編集] をクリックします。

その他の vSphere の認証オプション

vSphere 7.0 以降、vCenter Server の認証方法として、外部 ID プロバイダ フェデレーションが推奨されています。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もできます。

2 要素認証方法

政府機関や大企業では、多くの場合、2 要素認証が必要です。vSphere は、次の 2 要素認証方式をサポートしています。

外部 ID プロバイダ フェデレーション

外部 ID プロバイダ フェデレーションにより、外部 ID プロバイダでサポートされている多要素認証などの認証メカニズムを使用できます。

スマート カード認証

スマート カード認証では、ログインしているコンピュータに物理カード リーダー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。vCenter Server 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 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ます。RADIUS 認証はサポートされていません。

vCenter Server でのデフォルト以外の認証方法の指定

デフォルト以外の認証方法を設定するには、vSphere Client から実行するか、`sso-config` スクリプトを使用します。

- vCenter Single Sign-On にスマート カード認証を設定する場合は、vSphere Client から実行するか、`sso-config` を使用します。設定には、スマート カード認証を有効にしたり証明書の失効ポリシーを構成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。

vCenter Server の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。

注： vSphere 7.0 Update 2 以降では、vCenter Server で FIPS を有効にできます。『vSphere のセキュリティ』ドキュメントを参照してください。FIPS が有効になっている場合、RSA SecureID および CAC 認証はサポートされません。多要素認証には外部 ID プロバイダ フェデレーションを使用します。vCenter Server ID プロバイダ フェデレーションの設定を参照してください。

vCenter Server システムにログインする際に、次のようにスマート カードと PIN を組み合わせた認証を求められます。

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、ブラウザはカード上の証明書を読み取ります。

2 ブラウザは、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 vCenter Single Sign-On は、スマート カード上の証明書が既存のものである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についても確認します。

4 証明書が vCenter Single Sign-On にとって既存のものであり、失効していなければ、ユーザーは認証され、権限を与えられたタスクを実行できます。

注： 通常、テスト環境の場合は、ユーザー名とパスワードによる認証を有効にしても問題ありません。テスト終了後、ユーザー名とパスワードによる認証を無効にして、スマート カード認証を有効にします。その後、vSphere Client ではスマート カード ログインのみを許可します。vCenter Server 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 から vCenter Server に接続する場合、スマート カード認証を行うように環境を設定することができます。

スマート カード認証の構成には、次の手順が含まれます。

1 クライアント証明書を要求するように vCenter Server システムを構成します。

2 スマート カード構成を有効にします。

   vSphere Client または `sso-config` ユーティリティのいずれかを使用して、構成を有効にすることができます。

3 証明書の失効チェックをカスタマイズします。

   vSphere Client または `sso-config` ユーティリティのいずれかを使用して、チェックをカスタマイズできます。

クライアント証明書を要求するための vCenter Server の構成

スマート カード認証を有効にするには、クライアント証明書を要求するように vCenter Server を構成する必要があります。

この構成では、vCenter Server で自動的に設定およびオープンされるポート 3128 が使用されます。

前提条件

認証局 (CA) 証明書を vCenter Server システムにコピーして、信頼できるクライアント CA ストアの作成に使用します。このストアには、クライアント証明書のために CA によって発行された、信頼できる証明書が含まれている必要があります。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。

注： vCenter Server 7.0 以降は、HTTP/2 プロトコルをサポートしています。すべての最新のブラウザおよびアプリケーション（vSphere Client など）は、HTTP/2 を使用して vCenter Server に接続します。ただし、スマート カード認証では、HTTP/1.1 プロトコルを使用する必要があります。スマート カード認証を有効にすると、HTTP/2 の Application-Layer Protocol Negotiation (ALPN、https://tools.ietf.org/html/rfc7301) が無効になるため、実質的にブラウザで HTTP/2 が使用されることはありません。ALPN に依存せず、HTTP/2 のみを使用するアプリケーションは引き続き動作します。

スマート カード認証を完了するには、クライアントが該当する vCenter Server でポート 3128/TCP にアクセスすることを許可する必要があります。境界ファイアウォールを確認して、アクセス権が付与されていることを確認します。

接続は、スマート カード ログイン時にポート 3128 にリダイレクトされます。ポート 3128 は、事前構成済みの相互認証接続のみをサポートしており、直接的なブラウザ エンドポイントとしては想定されていません。HSTS ヘッダーは返されません。脆弱性スキャナからこの動作が報告されても、無視して問題ありません。

手順

1 root ユーザーとして vCenter Server シェルにログインします。

2 正確なパスと PEM 名 (`/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`) を使用して、vCenter Server に信頼できるクライアント CA ストアを作成します。

注意: 正確なパスと PEM 名 (`/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`) を使用する必要があります。

a `/usr/lib/vmware-sso/` ディレクトリに移動します。

```
cd /usr/lib/vmware-sso/
```

b 信頼できるクライアント CA ストアを作成するには、`openssl` コマンドを実行し、信頼された署名証明書を入力として取得します。たとえば、次のコマンドを実行すると、信頼された署名証明書 `xyzCompanySmartCardSigningCA.cer` から `clienttrustCA.pem` ファイルが作成されます。

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

信頼できるクライアント CA ストアに証明書を追加するには、「>>」演算子を使用して `openssl` コマンドを実行し、証明書を追加します。たとえば、次のコマンドを実行すると、既存の `clienttrustCA.pem` ファイルに `xyzCompanySmartCardSigningCA2.cer` が追加されます。

```
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA2.cer >> /usr/lib/vmware-sso/
vmware-sts/conf/clienttrustCA.pem
```

3 スマート カード証明書に署名した信頼できる CA が clienttrustCA.pem ファイルの内容に含まれていることを確認するには、keytool コマンドを実行します。

例：

```
keytool -printcert -file /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem | grep -i
"owner\|sha1\|issuer:\|valid"
```

4 CA 名がスマート カード ユーザー証明書チェーンと一致することを確認します。

たとえば、次のコマンドを実行できます。

```
sso-config.sh -get_authn_policy -t vsphere.local | grep trusted
```

ルート証明書と中間証明書には、一致するサムプリント、名前、有効な日付などが含まれている必要があります。

注： vSphere Client（[管理] - [Single Sign-On] - [構成] - [ID プロバイダ] - [スマート カード認証] - [スマート カード認証の設定] - [信頼できる CA 証明書] - [追加]）を使用することもできます。

5 STS サービスを再起動します。

```
service-control --restart sts
```

vSphere Client を使用したスマート カード認証の管理

vSphere Client から、スマート カード認証のアクティベーションとアクティベーション解除の切り替え、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、他の認証方法が無効になっている場合、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 vCenter Server 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。

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

前提条件

- 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。
- 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。
- 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ていることを確認します。

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。

   a 直接または SSH を使用して vCenter Server コンソールにログインします。

   b シェルを次のように有効にします。

```
Command> shell
chsh -s "/bin/bash" root
chsh -s "bin/appliancesh" 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 vCenter Server 上の `/usr/lib/vmware-sso/vmware-sts/conf` ディレクトリにコピーします。

   d 必要に応じて、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 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 [ID プロバイダ] タブで [スマート カード認証] をクリックし、[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。

   Web インターフェイスから、RSA SecurID 認証のアクティベーションとアクティベーション解除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] タブが表示されます。

7 [信頼できる CA 証明書] タブで、以下を実行します。

   a [追加] をクリックし、[参照] をクリックします。

   b 信頼されている CA 証明書を選択し、[追加] をクリックします。

8 信頼されている CA 証明書を追加するには、ステップ 7 を繰り返します。

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、vCenter Server 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。CLI 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。

CLI 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。

```
/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 vCenter Server 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 vCenter Server 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。

```
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）を使用します。

前提条件

- 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。
- 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。
- 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ていることを確認します。

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。

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 vCenter Server 上の `/usr/lib/vmware-sso/vmware-sts/conf` にコピーします。

d 必要に応じて、シェルを次のように無効にします。

```
chsh -s "/bin/appliancesh" root
```

2 スマート カート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 -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
```

例：

```
sso-config.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.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） 証明書ポリシーの許可リストを設定するには、次のコマンドを実行します。

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

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

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.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.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.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.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.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.sh -get_authn_policy -t tenantName
```

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な場合、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

- 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。
- vCenter Server 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。

手順

1. vSphere Client を使用して 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 プロバイダ] タブで、[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

- 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-On ID 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 vCenter Server ホスト名を解決でき、vCenter Server 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。`sdconf.rec` ファイルを見つけるには、取得した `AM_Config.zip` ファイルを解凍します。
- `sdconf.rec` ファイルを vCenter Server 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。

```
/opt/vmware/bin
```

2 RSA SecurID 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 -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 -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 -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 -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。

vSphere Client ログイン画面のログイン メッセージの管理

vSphere Client ログイン画面に表示されるメッセージを作成できます。

メッセージ、免責事項、使用条件などを設定できます。また、ログイン前にメッセージの確認を要求するようにメッセージを構成することもできます。

vSphere Client ログイン画面のログイン メッセージの管理

vSphere Client ログイン画面に、ログイン メッセージを追加できます。また、カスタムのログイン メッセージを設定し、ユーザーの同意を得るチェック ボックスを配置することもできます。

手順

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

2 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。

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、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。

Network Time Protocol の構成

NTP (Network Time Protocol) を使用すると、すべてのシステムで同じ相対時間ソース（関連するローカル時間オフセットを含む）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るようにすることができます。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。

NTP を使用した時刻同期の構成方法については、vSphere のセキュリティのドキュメントを参照してください。

vCenter Server 認証のトラブルシューティング

5

以降のトピックでは、vCenter Server 認証の問題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。

次のトピックを参照してください。

- Lookup Service エラーの原因の特定
- Active Directory ドメイン認証を使用してログインできない
- 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
- 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
- vCenter Server サポート バンドルのエクスポート
- vCenter Server 認証サービス ログのリファレンス

Lookup Service エラーの原因の特定

vCenter Single Sign-On インストールで、vCenter Server または vSphere 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 vmware-sso デーモンのステータスをチェックして、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。 `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 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。

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 (https://kb.vmware.com/s/article/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。

デフォルトの ID 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 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 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 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 の構成』ドキュメントを参照してください。

4 vCenter Server 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 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 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

拡張リンク モードで接続されている複数の vCenter Server インスタンスが環境内に含まれている場合、その vCenter Server インスタンスのいずれかが使用できなくなっても、環境は引き続き機能し続けます。その vCenter Server 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 30 秒以内に、拡張リンク モードを通じて接続されたパートナーとの間でレプリケートされます。しかし、状況によっては、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 vCenter Server インスタンスが含まれていて、1 つの vCenter Server 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 vCenter Server 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。拡張リンク モードのトポロジによっては、レプリケーションに長い時間がかかることがあります。

原因

通常の動作では、ある vCenter Server 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 30 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。

vCenter Server サポート バンドルのエクスポート

vCenter Server サービスのログ ファイルを含むサポート バンドルをエクスポートするには、vSphere Client から行うか、API を使用します。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。

API の詳細については、『vCenter Server Management プログラミング ガイド』を参照してください。

前提条件

vCenter Server 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://*vcenter_server_ip*:5480 の vCenter Server 設定管理インターフェイスに接続します。
2. vCenter Server 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。

vCenter Server 認証サービス ログのリファレンス

vCenter Server 認証サービスは、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。

表 5-1. vCenter Server 認証サービス 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有用なデータが含まれる場合があります。
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。